GALOIS AND HOPF GALOIS

F. FERRI AND L. STEFANELLO

Abstract. These are provisional and expository notes for the workshop in Galois module theory and Hopf–Galois theory held in 2021. Every section corresponds to a lecture, but also with slight revisitation, in order to add details not seen during the talks and to pursue uniformity and smoothness. Every mistake is ours.

We wish to thank all the speakers: Ilaria Del Corso (section 1), Alessandro Cobbe (sections 2 and 8), Fabio Ferri (sections 3 and 5), Henri Johnston (section 4), Francesco Campagna (section 6), Davide Lombardo (section 7), Lorenzo Stefanello (sections 9 and 10), Elena Campedel (section 11), Cornelius Greither (section 12), Anna Rio (section 13), Daniel Gil-Muñoz (section 14), Nigel Byott (section 15), and Paul Truman (section 16).

Contents

Part 1. Galois module theory 2
1. An introduction to Galois module structure. The case of tamely ramified extensions 2
2. More tamely ramified Galois module structure and an introduction to wild Galois module structure 11
3. Results on Galois module structure of wildly ramified extensions and local freeness over the associated order 18
4. Explicit Galois module structure of weakly ramified extensions of p-adic fields 26
5. Almost maximal ramification, dihedral extensions, A_4-, S_4-, A_5-extensions 30
6. Galois module structure of absolutely abelian extensions of p-adic fields 36
7. Cyclic extensions of degree p 41
8. On K-theory, realisable classes, and Hilbert–Speiser fields 48

Part 2. Hopf–Galois theory 53
9. An introduction to Hopf algebras 53
10. Hopf–Galois extensions 64
11. Greither–Pareigis theorem and Byott's translation 74
12. On the algebra structure of Hopf algebras occurring in Hopf–Galois theory 82
13. Induced Hopf–Galois extensions 86
14. Hopf–Galois module theory 89
15. Hopf orders as associated orders 96
16. An assortment of associated orders in Hopf–Galois extensions 103

Date: Version of 30th November 2021.

References 108

Part 1. Galois module theory

In this paper, we consider modules over rings not necessarily commutative. These rings are always algebras over commutative rings; therefore the notion of rank of a free module is well defined. If nothing is said, the modules we consider are left.

1. An introduction to Galois module structure. The case of tamely ramified extensions

In this section, we mainly follow [FT93, Joh11].

Let G be a finite group.

Definition 1.1. Let R be a ring. The *group algebra* of G over R is

$$R[G] = \left\{ \sum_{\sigma \in G} a_\sigma \sigma \mid a_\sigma \in R \right\}.$$

It is an R-algebra, free as R-module with basis G.

Let M be an abelian group. We say that M is a *G-module* if G acts on M via endomorphism, that is, if there exists a group homomorphism $\varphi\colon G \to \mathrm{End}(M)$. Equivalently, a G-module is just a $\mathbb{Z}[G]$-module.

We say that M is a *Galois module* if M is a G-module with $G = \mathrm{Gal}(L/K)$ for an extension L/K and the action of G on M is the Galois action.

Notation 1.2. If K is a number field, that is, a finite extension of $\mathbb{Q}$, then we write $\mathcal{O}_K$ for the ring of integers. If K is a p-adic field, so a finite extension of $\mathbb{Q}_p$ for a prime number p, then we write $\mathcal{O}_K$ for the valuation ring.

We call *primes* of $\mathcal{O}_K$ the nonzero prime ideals, that is, the maximal ideals, of $\mathcal{O}_K$.

Example 1.3. Let L/K be a finite Galois extension with Galois group G.

- L is a $K[G]$-module.

Suppose that L and K are number fields or p-adic fields.

- $\mathcal{O}_L$ is an $\mathcal{O}_K[G]$-module.
- The ideal class group $\mathrm{Cl}(K)$ of K is an $\mathcal{O}_K[G]$-module.
- $\mathcal{O}_L^\times$ is a $\mathbb{Z}[G]$-module.

Definition 1.4. Let L/K be a finite Galois extension with Galois group G. We say that L/K admits a *normal basis* if there exists an element $\alpha \in L$, called a *generator* of the normal basis, such that one of the following equivalent conditions holds:

- $L = K[G] \cdot \alpha$.
- L is a free $K[G]$-module of rank one, with basis $\{\alpha\}$.
- $\{\sigma(\alpha) \mid \sigma \in G\}$ is a K-basis of L.

Every finite Galois extension admits a normal integral basis, as stated by the following deep result. For a proof, see [Ble07].

Theorem 1.5 (Normal basis theorem)**.** *Let L/K be a finite Galois extension. Then L/K admits a normal basis.*

If L/K is a (finite) Galois extension of number fields or p-adic fields with Galois group G, then $\mathcal{O}_L$ is a $\mathcal{O}_K[G]$-module. Is $\mathcal{O}_L$ free over $\mathcal{O}_K[G]$?

Definition 1.6. Let L/K be a finite Galois extension of number fields or p-adic fields with Galois group G. We say that L/K admits a *normal integral basis* if there exists an element $\alpha \in L$, called a *generator* of the normal integral basis, such that one of the following equivalent conditions holds:

- $\mathcal{O}_L = \mathcal{O}_K[G] \cdot \alpha$.
- $\mathcal{O}_L$ is a free $\mathcal{O}_K[G]$-module of rank one, with basis $\{\alpha\}$.
- $\{\sigma(\alpha) \mid \sigma \in G\}$ is an $\mathcal{O}_K$-basis of $\mathcal{O}_L$.

Remark 1.7. If $\mathcal{O}_L$ free over $\mathcal{O}_K[G]$, then the rank has to be one, since if we tensor with K over $\mathcal{O}_K$, we find that this rank equals the rank of L as $K[G]$-module, which is one by Theorem 1.5.

Remark 1.8. If L/K is a Galois extension of number fields or p-adic fields with Galois group G, then $\mathcal{O}_L$ is the integral closure of $\mathcal{O}_K$. This means that for all $\alpha \in L$, there exists an integer $0 \neq d \in \mathcal{O}_K$ such that $d\alpha = \gamma \in \mathcal{O}_L$. If α is a generator of a normal basis, then we immediately find that also γ generates a normal basis, that is, we can always assume that the generator of a normal basis belongs to $\mathcal{O}_L$.

Clearly this does not mean that γ is in general a generator of a normal integral basis. But the converse is true: if $\alpha \in \mathcal{O}_L$ generates a normal integral basis, then it also generates a normal basis. Indeed, it is immediate to see that $\{\sigma(\alpha) \mid \sigma \in G\}$ is a set of K-generators of L with the right cardinality, so a K-basis.

The same argument shows that the apparently weaker condition $\mathcal{O}_L = \mathcal{O}_K[G] \cdot \alpha$ is enough to have that $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$ with basis $\{\alpha\}$.

Not every finite Galois extension L/K of number fields or p-adic fields admits a normal integral basis: since $\mathcal{O}_K[G]$ is free over $\mathcal{O}_K$, if $\mathcal{O}_L$ were free over $\mathcal{O}_K[G]$, then $\mathcal{O}_L$ would also be free over $\mathcal{O}_K$, but we know that if $\mathcal{O}_K$ is not a principal ideal domain, then this may not be the case. Also if $\mathcal{O}_K$ is a principal ideal domain, this may be false.

Example 1.9. Suppose $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$, so $\mathcal{O}_L = \mathbb{Z}[i]$. We claim that L/K does not admit a normal integral basis. We know that $G = \mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{id}, \sigma\}$, where σ is the complex conjugation. Suppose that an element $\alpha = a + ib$ generates a normal integral basis. Then

$$\mathbb{Z}[G] \cdot \alpha = \{\lambda(a+ib) + \mu(a-ib) \mid \lambda, \mu \in \mathbb{Z}\} = \mathbb{Z}[i].$$

Since $1 \in \mathbb{Z}[i] = \mathbb{Z}[G] \cdot \alpha$, we have either $b = 0$ or $\lambda = \mu$. In the former case, $\mathbb{Z}[G] \cdot \alpha = \mathbb{Z}$. In the latter, we find $2\lambda a = 1$, which has no solutions in $\mathbb{Z}$.

Example 1.10. Suppose $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt{5})$. Then $\mathcal{O}_L = \mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ and $L/\mathbb{Q}$ admits a normal integral, generated by $\frac{1+\sqrt{5}}{2}$.

1.1. **Lattices.** Let R be a Noetherian domain with field of fractions $K \neq R$, and let V be a finite-dimensional K-vector space.

Definition 1.11. An *R-lattice* of V is a finitely generated R-submodule M of V with the property that $KM = \operatorname{span}_K(M) = V$, or equivalently, that M contains a K-basis of V. An R-lattice M is *free* if M is free over R.

Remark 1.12. Some authors use the term *full lattice* to define a lattice in the sense of Definition 1.11.

Example 1.13. If L/K is an extension of number fields, then $\mathcal{O}_L$ is an $\mathcal{O}_K$-lattice, not necessarily free.

More generally, if $\mathcal{O}$ is a Dedekind domain with field of fractions K, L/K is a finite separable extension, and $\mathcal{O}_L$ is the integral closure of $\mathcal{O}$ in L, then all fractional ideals of $\mathcal{O}_L$, and so also $\mathcal{O}_L$, are $\mathcal{O}$-lattices.

Remark 1.14. An R-lattice M is always R-torsion-free, since it is contained in the K-vector space V. If M is also free, then M has rank n, where n is the K-dimension of V. Every R-basis $\{x_1, \dots, x_n\}$ of M is also a K-basis of V, as we may identify $V = KM$ with $K \otimes_R M$. For similar results, see [FT93, Chapter II, section 4].

Lemma 1.15. *Let M be an R-module in V. Then M is an R-lattice if and only if there exist free R-lattices F' and F'' such that $F' \subseteq M \subseteq F''$.*

Proof. See [Joh11, Lemma 3.5]. □

Notation 1.16. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K. If $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$, then we write $K_\mathfrak{p}$ and $\mathcal{O}_\mathfrak{p}$ for the completions of K and $\mathcal{O}$, respectively, with respect to the $\mathfrak{p}$-adic topology. We remark that $\mathcal{O}_\mathfrak{p}$ is a discrete valuation ring; see [FT93, Chapter II, section 3]. If M is an $\mathcal{O}$-module, then we write $M_\mathfrak{p} = \mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} M$. If V is a K-vector space, then we write $V_\mathfrak{p} = K_\mathfrak{p} \otimes_K V$. Note that this is indeed well defined, since if V is a K-vector space, then

$$\mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} V \cong \mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} (K \otimes_K V) \cong (\mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} K) \otimes_K V \cong K_\mathfrak{p} \otimes_K V$$

as $\mathcal{O}_\mathfrak{p}$-modules, where the composition is given by the natural inclusion $\mathcal{O}_\mathfrak{p} \hookrightarrow K_\mathfrak{p}$.

Also, if M is finitely generated as $\mathcal{O}$-module, then $M_\mathfrak{p}$ is exactly the completion $\varprojlim_n M/\mathfrak{p}^n M$ of M with respect to $\mathfrak{p}$; see [FT93, Chapter II, 4.6.a].

Note that if M is an $\mathcal{O}$-lattice in V, then $M_\mathfrak{p}$ is an $\mathcal{O}_\mathfrak{p}$-lattice in $V_\mathfrak{p}$, since if $F' \subseteq M \subseteq F''$ (Lemma 1.15), then $F'_\mathfrak{p} \subseteq M_\mathfrak{p} \subseteq F''_\mathfrak{p}$ by [FT93, Chapter II, 4.7]; moreover, as torsion-free finitely generated modules over principal ideal domains are free, $M_\mathfrak{p}$ is a free $\mathcal{O}_\mathfrak{p}$-lattice in $V_\mathfrak{p}$.

Lemma 1.17. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, let V be a finite-dimensional K-vector space, and let M and N be $\mathcal{O}$-lattices in V. Then $M_\mathfrak{p} = N_\mathfrak{p}$ for almost all maximal ideals $\mathfrak{p}$ of $\mathcal{O}$.*

Proof. See [FT93, Chapter II, 4.12] □

1.2. **Module index and discriminant.**

We fix a Dedekind domain $\mathcal{O}$ with field of fractions K and a finite-dimensional K-vector space V.

Let M and N be free $\mathcal{O}$-lattices of V, and let $\mathfrak{p}$ be a maximal ideal of $\mathcal{O}$, so $M_\mathfrak{p}$ and $N_\mathfrak{p}$ are $\mathcal{O}_\mathfrak{p}$-lattices of $V_\mathfrak{p}$. Let $\{\alpha_1, \dots, \alpha_n\}$ and $\{\beta_1, \dots, \beta_n\}$ be bases for $M_\mathfrak{p}$ and $N_\mathfrak{p}$, respectively, as $\mathcal{O}_\mathfrak{p}$-modules, and so also for $V_\mathfrak{p}$ as $K_\mathfrak{p}$-vector space. Consider the $K_\mathfrak{p}$-linear map

$$\begin{aligned} a\colon V_\mathfrak{p} &\to V_\mathfrak{p} \\ \alpha_i &\mapsto \beta_i. \end{aligned}$$

Define $[M_\mathfrak{p} : N_\mathfrak{p}] = \det(a)\mathcal{O}_\mathfrak{p}$. This is a well-defined fractional ideal of $\mathcal{O}_\mathfrak{p}$, as the map a is uniquely defined modulo $\mathrm{Aut}_{\mathcal{O}_\mathfrak{p}}(N_\mathfrak{p})$.

Let now $b\colon V \times V \to K$ be a symmetric nondegenerate K-bilinear form, and define

$$\delta(M_\mathfrak{p}) = \mathrm{disc}(M_\mathfrak{p}) = \det(\{b_\mathfrak{p}(\alpha_i, \alpha_j)\})\mathcal{O}_\mathfrak{p},$$

where $b_\mathfrak{p}$ is the $K_\mathfrak{p}$-bilinear form on $V_\mathfrak{p}$ induced by b:

$$b_\mathfrak{p}\left(\sum \lambda_i \otimes x_i, \sum \mu_j \otimes y_j\right) = \sum_{i,j} \lambda_i \mu_j b(x_i, y_j).$$

Then $\delta(M_\mathfrak{p})$ fractional ideal of $\mathcal{O}_\mathfrak{p}$.

Finally, since for almost all $\mathfrak{p}$, $M_\mathfrak{p} = N_\mathfrak{p}$ by Lemma 1.17 and $\delta(M_\mathfrak{p}) = \mathcal{O}_\mathfrak{p}$ by Lemma 1.18(1), we can define $\delta(M)$ to be the only fractional ideal of $\mathcal{O}$ such that

$$\delta(M)_\mathfrak{p} = \delta(M_\mathfrak{p}),$$

and $[M : N]$ to be the only fractional ideal of $\mathcal{O}$ such that

$$[M : N]_\mathfrak{p} = [M_\mathfrak{p} : N_\mathfrak{p}].$$

Here we are using the fact that if I is a fractional ideal of $\mathcal{O}$ with factorisation

$$I = \prod_\mathfrak{q} \mathfrak{q}^{v_\mathfrak{q}(I)},$$

then the completion of I with respect to a maximal ideal $\mathfrak{p}$ is

$$I_\mathfrak{p} = \mathfrak{p}^{v_\mathfrak{p}(I)}\mathcal{O}_\mathfrak{p}.$$

We state some important facts.

Lemma 1.18. *In the previous setting, the following hold:*

1. *For almost all $\mathfrak{p}$, $\delta(M_\mathfrak{p}) = \mathcal{O}_\mathfrak{p}$.*
2. *If $N \subseteq M$, then $[M : N]$ is an integral ideal; if also $[M : N] = \mathcal{O}$, then $M = N$.*
3. *$\delta(N) = \delta(M)[M : N]^2$.*
4. *Let L be a finite separable extension of K, let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}$ in L, and let $b_L\colon L \otimes_K V \times L \otimes_K V \to L$ be the form induced by b and defined by $b_L(l \otimes x, l' \otimes x') = ll'b(x, x')$. Then*

$$\delta(\mathcal{O}_L \otimes_\mathcal{O} M) = \delta(M)\mathcal{O}_L.$$

Proof.

1. Let $M \subseteq F$ with F free $\mathcal{O}$-lattice (Lemma 1.15). Then for almost all $\mathfrak{p}$, $M_\mathfrak{p} = F_\mathfrak{p}$ (Lemma 1.17). Note that for all $\mathfrak{p}$, $\delta(F)_\mathfrak{p} = \delta(F_\mathfrak{p})$. In particular, if $\mathfrak{p}$ does not occur in the factorisation of $\delta(F)$, then $\delta(F_\mathfrak{p}) = \mathcal{O}_\mathfrak{p}$, and so the assertion follows.
2. The result is clear after completion, and in the general case it follows from the fact that for every $\mathcal{O}$-lattice A,

$$A = V \cap \left(\bigcap_\mathfrak{p} A_\mathfrak{p}\right),$$

where $\mathfrak{p}$ ranges over all maximal ideals of $\mathcal{O}$; see [Rei03, Theorem 5.3].

3. See [FT93, Chapter III, 2.4].
4. See [FT93, Chapter III, 2.10]. □

We can apply this machinery to the case when $V = L$ is a finite separable extension of K and $b = \mathrm{Tr}$ is given by the trace: for all $x, y \in L$,

$$\mathrm{Tr}(x, y) = \mathrm{Tr}_{L/K}(xy).$$

We define $\delta(L/K) = \delta_{L/K}(\mathcal{O}_L)$ to be the discriminant of the $\mathcal{O}$-lattice $\mathcal{O}_L$ with respect to this form, where $\mathcal{O}_L$ is the integral closure of $\mathcal{O}$ in L. Note that $\delta(L/K)$ is an integral ideal of $\mathcal{O}$ (the trace of an element in $\mathcal{O}_L$ is in $\mathcal{O}$), and the following meaningful result holds.

Theorem 1.19. *Let L/K be an extension of number fields or p-adic fields. Then a prime $\mathfrak{p}$ of $\mathcal{O}_K$ is ramified in L if and only if $\mathfrak{p}$ divides $\delta(L/K)$.*

Proof. See [FT93, Chapter III, Theorem 22]. □

1.3. **Linear and arithmetical disjointness.**

Definition 1.20. Let L and F be finite extensions of a field K contained in a separable closure $\overline{K}$. We say that L and F are *linearly disjoint* if the F-algebra homomorphism

$$\begin{aligned} L \otimes_K F &\to LF \\ x \otimes y &\mapsto xy \end{aligned}$$

is bijective.

If we write $F = K(\alpha) \cong K[x]/(\mu_K(x))$, where $\mu_K(x)$ is the minimal polynomial of α over K, then $LF = L(\alpha) \cong L[x]/(\mu_L(x))$, where $\mu_L(x)$ is the minimal polynomial of α over L, and $\mu_L \mid \mu_K$. Since, by extension of scalars,

$$L \otimes_K F \cong L[x]/(\mu_K(x))$$

as F-algebras, we get that L and F are linearly disjoint over K if and only if $\mu_L = \mu_K$, so μ_K remains irreducible in L, if and only if $[F : K] = [LF : L]$, hence

$$[LF : K] = [L : K][F : K].$$

Remark 1.21. If L and F are linearly disjoint over K, then $L \cap F = K$, but the converse is not true. The standard example is given by $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$, and $F = \mathbb{Q}(\zeta_3 \sqrt[3]{2})$, or more generally every two distinct, but conjugate, extensions of prime degree.

Definition 1.22. Let L and F be finite extensions of a field K contained in a separable closure $\overline{K}$. We say that L and F are *arithmetically disjoint* if L and F are linearly disjoint and the discriminants $\delta(L/K)$ and $\delta(F/K)$ are coprime ideals.

Example 1.23. For all $n \geq 1$, let ζ_n be a primitive n-th root of unity. If $n, m \geq 1$ are coprime, then $\mathbb{Q}(\zeta_n)$ and $\mathbb{Q}(\zeta_m)$ are arithmetically disjoint over $\mathbb{Q}$.

Theorem 1.24. *Let K be a number field or a p-adic field, and let L and F be arithmetically disjoint extensions of F. Write*

$$\mathcal{O}_F \cdot \mathcal{O}_L = \mathrm{span}_{\mathcal{O}_K}(\{xy \mid x \in \mathcal{O}_K, y \in \mathcal{O}_L\}).$$

Then

$$\mathcal{O}_{LF} = \mathcal{O}_L \cdot \mathcal{O}_F.$$

Proof. The inclusion $\mathcal{O}_L \cdot \mathcal{O}_F \subseteq \mathcal{O}_{LF}$ is clear.

For the other, set $N = LF$. Via the identification $L \otimes_K F \leftrightarrow N$, we can identify $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F$ with $\mathcal{O}_L \cdot \mathcal{O}_F$. In the same way, we view $\mathcal{O}_N$ as a $\mathcal{O}_K$-lattice in $L \otimes_K F$ containing $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F$. We need to show that $[\mathcal{O}_N : \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F]_{\mathcal{O}_K} = \mathcal{O}_K$ (Lemma 1.18(2)), or equivalently, that for all prime $\mathfrak{p}$ of $\mathcal{O}_K$,

$$\mathfrak{p} \nmid [\mathcal{O}_N : \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F]_{\mathcal{O}_K}.$$

It is enough to show that $\mathfrak{p}\mathcal{O}_F$ is coprime with $[\mathcal{O}_N : \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F]_{\mathcal{O}_F}$. Suppose, without loss of generality, that $\mathfrak{p}$ is coprime with $\delta(L/K)$, that is, $\mathfrak{p}\mathcal{O}_F$ is coprime with $\delta(L/K)\mathcal{O}_F$. We know that

$$[\mathcal{O}_N : \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F]^2_{\mathcal{O}_F} = \delta_{N/F}(\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F)\delta_{N/F}(\mathcal{O}_N)^{-1},$$

where $\delta_{N/F}$ denotes the discriminant with respect to $\mathrm{Tr}_{N/F}$. The trace $\mathrm{Tr}_{N/F}$, under the identification $N \leftrightarrow L \otimes_K F$, is $\mathrm{Tr}_{L/K} \otimes \mathrm{id}$. This implies (Lemma 1.18(4)) that

$$\delta_{N/F}(\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F) = \delta_{L/K}(\mathcal{O}_L)\mathcal{O}_F,$$

and so $\delta_{N/F}(\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F)$ is coprime with $\mathfrak{p}\mathcal{O}_F$. Therefore, as $[\mathcal{O}_N : \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F]^2_{\mathcal{O}_F}$ is integral, it must be coprime with $\mathfrak{p}\mathcal{O}_F$. □

Remark 1.25. If K is a p-adic field and L and F are finite extensions of K contained in a separable closure $\overline{K}$, then L and F are arithmetically disjoint if and only if L/K is unramified and $[L : K]$ and $[F^{\mathrm{unr}} : K]$ are coprime, where F^{unr} is the maximal unramified subextension of F/K (or the same holds with L and F swapped).

Proposition 1.26. *Let K be a number field or a p-adic field. If L and F are arithmetically disjoint over K, L/K is Galois with Galois group G, and $\mathcal{O}_L = \mathcal{O}_K[G] \cdot \alpha$, then $\mathcal{O}_{LF} = \mathcal{O}_F[G] \cdot \alpha$; moreover, if F/K is Galois with Galois group H and $\mathcal{O}_F = \mathcal{O}_K[H] \cdot \beta$, then $\mathcal{O}_{LF} = \mathcal{O}_K[G \times H] \cdot \alpha\beta$.*

Proof. See [Joh11, Proposition 6.4] □

Proposition 1.27. *Let L/K be a Galois extension of number fields or p-adic fields, and let F be an intermediate field, with F/K Galois. If α generates a normal integral basis for L/K, then $\mathrm{Tr}_{L/F}(\alpha)$ generates a normal integral basis for F/K.*

Proof. Write $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/F)$; then H is normal in G, and we may identify $\mathrm{Gal}(F/K)$ with G/H. Write $\mathcal{O}_L = \mathcal{O}_K[G] \cdot \alpha$. If $x \in \mathcal{O}_L$, then

$$x = \sum_{\sigma \in G} a_\sigma \sigma(\alpha),$$

with $a_\sigma \in \mathcal{O}_K$ for all $\sigma \in G$. Suppose $x \in \mathcal{O}_F$; then $\tau(x) = x$ for all $\tau \in H$. We have

$$\sum_{\sigma \in G} a_\sigma \sigma(\alpha) = x = \tau(x) = \sum_{\sigma \in G} a_\sigma \tau\sigma(\alpha) = \sum_{\sigma \in G} a_{\tau^{-1}\sigma} \sigma(\alpha),$$

from which we deduce that $a_\sigma = a_{\tau^{-1}\sigma}$ for all $\sigma \in G$ and $\tau \in H$. Fix a lift $\widetilde{\sigma} \in G$ for all $\overline{\sigma} \in G/H$. Using that H is normal in G, we find that

$$\begin{aligned} x &= \sum_{\overline{\sigma}\in G/H} \sum_{\tau\in H} a_{\tau\widetilde{\sigma}} \tau\widetilde{\sigma}(\alpha) = \sum_{\overline{\sigma}\in G/H} a_{\widetilde{\sigma}} \sum_{\tau\in H} \tau\widetilde{\sigma}(\alpha) \\ &= \sum_{\overline{\sigma}\in G/H} a_{\widetilde{\sigma}} \sum_{\tau'\in H} \widetilde{\sigma}\tau'(\alpha) = \sum_{\overline{\sigma}\in G/H} a_{\widetilde{\sigma}}\widetilde{\sigma}\left(\mathrm{Tr}_{L/F}(\alpha)\right) \\ &= \sum_{\overline{\sigma}\in G/H} a_{\widetilde{\sigma}}\overline{\sigma}\left(\mathrm{Tr}_{L/F}(\alpha)\right). \end{aligned}$$

□

Corollary 1.28. *Let L/K be a Galois extension of number fields or p-adic fields. If L/K admits a normal integral basis, then for all intermediate fields F, $\mathrm{Tr}_{L/F}(\mathcal{O}_L) = \mathcal{O}_F$. In particular, $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$.*

Proof. The inclusion $\mathrm{Tr}_{L/F}(\mathcal{O}_L) \subseteq \mathcal{O}_F$ is clear.

If $x = \sum_{\sigma\in G} a_\sigma\sigma(\alpha) \in \mathcal{O}_F$, then, as before,

$$\begin{aligned} x &= \sum_{\overline{\sigma}\in G/H} a_{\widetilde{\sigma}} \sum_{\tau\in H} \tau\widetilde{\sigma}(\alpha) = \sum_{\overline{\sigma}\in G/H} a_{\widetilde{\sigma}} \,\mathrm{Tr}_{L/F}(\widetilde{\sigma}(\alpha)) \\ &= \mathrm{Tr}_{L/F}\left(\sum_{\overline{\sigma}\in G/H} a_{\widetilde{\sigma}}\widetilde{\sigma}(\alpha)\right) \in \mathrm{Tr}_{L/F}(\mathcal{O}_L). \end{aligned}$$

□

1.4. **Tamely ramified extensions.** Let L/K be a finite extension of number fields or p-adic fields. If $\mathfrak{p}$ is a prime of $\mathcal{O}_K$, then we can write a factorisation in $\mathcal{O}_L$:

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1}\dots\mathfrak{P}_r^{e_r},$$

where for all $i = 1,\dots,r$, $\mathfrak{P}_i$ is a prime of $\mathcal{O}_L$ and $e_i \geq 0$. For example, if the extension is Galois, then $e_i = e$ for all i. If L and K are p-adic fields, then $r = 1$, since $\mathcal{O}_L$ is a discrete valuation ring in this case. We say that primes $\mathfrak{P}_i$ *lies above* $\mathfrak{p}$ and $\mathfrak{p}$ *lies under* $\mathfrak{P}_i$ for all i.

Definition 1.29. Let L/K be a finite extension of number fields or p-adic fields. We say that a prime $\mathfrak{p}$ of $\mathcal{O}_K$ is *tamely ramified* in L if $p \nmid e_i$ for all $\mathfrak{P}_i$ lying above $\mathfrak{p}$, where if K is a number field, then p is the prime number lying under $\mathfrak{p}$. Otherwise, we say that $\mathfrak{p}$ is *wildly ramified.*

We say that L/K is *tamely ramified* if every prime $\mathfrak{p}$ of $\mathcal{O}_K$ is tamely ramified in L. Otherwise, we say that L/K is *wildly ramified.*

We can characterise the tamely ramified extension as follows.

Theorem 1.30. *Let L/K be a finite Galois extension of number fields or p-adic fields. Then L/K is tamely ramified if and only if $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathcal{O}_K$.*

Proof. One can show that a prime $\mathfrak{p}$ of $\mathcal{O}_K$ divides $\mathrm{Tr}_{L/K}(\mathcal{O}_L)$ if and only if $\mathfrak{p}$ is wildly ramified; from this, the result is clear. For the details, see [Joh11, Proposition 7.2]. □

Corollary 1.31. *Let L/K be a Galois extension of number fields or p-adic fields. If L/K admits a normal integral basis, then L/K is tamely ramified.*

Proof. The assertion follows by Corollary 1.28 and Theorem 1.30. □

1.5. **Hilbert–Speiser theorem.** We briefly discuss here tamely ramified extensions of number fields.

Proposition 1.32. *Let n be a squarefree positive integer, and let $L \subseteq \mathbb{Q}(\zeta_n)$. Then $L/\mathbb{Q}$ admits a normal integral basis generated by $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/L}(\zeta_n)$.*

Proof. By Proposition 1.27, it is enough to show that ζ_n generates a normal integral basis for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. We write $n = p_1 \cdots p_r$ and work by induction on r. If $r = 1$, then $n = p$ is prime. We know that a $\mathbb{Z}$-basis for $\mathbb{Z}[\zeta_p]$ is $\{1, \zeta_p, \dots, \zeta_p^{p-2}\}$. Since ζ_p is a unit, then also $\{\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}\}$ is a $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta_p]$, and this is exactly the set of conjugates of ζ_p; thus the assertion follows.

Now let $n = mp$, with $(m, p) = 1$. By induction on m, ζ_m generates a normal integral basis for $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. By base case, ζ_p generates a normal integral basis for $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, and since $\mathbb{Q}(\zeta_m)$ and $\mathbb{Q}(\zeta_p)$ are arithmetically disjoint, we conclude by Proposition 1.26 that $\zeta_n = \zeta_m\zeta_p$ generates a normal integral basis for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. □

Theorem 1.33 (Hilbert–Speiser theorem)**.** *Let $L/\mathbb{Q}$ be a tamely ramified abelian extension. Then L/K admits a normal integral basis.*

Proof. By Kronecker–Weber theorem, if $L/\mathbb{Q}$ is abelian and tamely ramified, then L is contained in cyclotomic tamely ramified extension $\mathbb{Q}(\zeta_n)$ of $\mathbb{Q}$. Since $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is tamely ramified if and only if n is squarefree, we conclude by Proposition 1.32 that $\mathrm{Tr}_{\mathbb{Q}(\zeta_n)/L}(\zeta_n)$ generates a normal integral basis for $L/\mathbb{Q}$. □

The main result of [GRRS99] tells us that we cannot change the base field or look for weaker hypotheses in Theorem 1.33. We discuss this in section 8

The next examples are discussed in [Mar69] and [Mar71], respectively.

Example 1.34. There exists a finite Galois extension $L/\mathbb{Q}$ with Galois group isomorphic to the dihedral group D_{2q} of order $2q$, with $q \neq 2$ a prime number, such that $L/\mathbb{Q}$ admits a normal integral basis.

Example 1.35. Let $F = \mathbb{Q}(\sqrt{5}, \sqrt{21})$. Consider

$$m = \frac{5 + \sqrt{5}}{2} \cdot \frac{21 + \sqrt{21}}{2}.$$

Define $L_1 = F(\sqrt{m})$ and $L_2 = F(\sqrt{-3m})$. Then $\mathrm{Gal}(L_i/\mathbb{Q}) \cong Q_8$, the quaternion group, for $i = 1, 2$, and $L_1/\mathbb{Q}$ admits a normal integral basis, but $L_2/\mathbb{Q}$ does not.

1.6. **Tamely ramified extensions of p-adic fields.** The goal of this subsection is to study normal integral bases for tamely ramified extensions of p-adic fields. We begin with unramified extensions.

Notation 1.36. If K is a p-adic field, we write k_K for the residue field $\mathcal{O}_K/\mathfrak{p}$, where $\mathfrak{p}$ is the prime of $\mathcal{O}_K$.

Theorem 1.37. *Let L/K be an unramified extension of p-adic fields. Then L/K admits a normal integral basis.*

Proof. Let $\mathfrak{p}$ and $\mathfrak{P}$ be the primes of $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively. Since L/K is unramified,

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}$$

and

$$[L : K] = [k_L : k_K].$$

In particular, L/K is Galois with Galois group

$$G = \mathrm{Gal}(L/K) \cong \mathrm{Gal}(k_L/k_K) = \overline{G}.$$

We identify G with $\overline{G}$. By normal basis theorem (Theorem 1.5), there exists $\overline{\alpha} \in k_L$ such that $k_L = k_K[G] \cdot \overline{\alpha}$. Let α be a lift of $\overline{\alpha}$ in $\mathcal{O}_L$, and define $M = \mathcal{O}_K[G] \cdot \alpha$. We claim that $M = L$. We have

$$M/\mathfrak{P}M = k_k[G] \cdot \overline{\alpha} = k_L = \mathcal{O}_L/\mathfrak{P} = \mathcal{O}_L/\mathfrak{p}\mathcal{O}_L;$$

therefore $\mathcal{O}_L = M + \mathfrak{P}\mathcal{O}_L$, and by Nakayama's lemma (see [CR81, (30.2)]), $\mathcal{O}_L = M$. □

Let us now consider totally and tamely ramified extensions.

Theorem 1.38. *Let L/K be a Galois extension of p-adic fields with degree e, and suppose that L/K is totally and tamely ramified. Then L/K admits a normal integral basis. More precisely, given a uniformiser π_K for K, let π_L be a uniformiser for L such that $\pi_L^e = \pi_K$. Then for all $u_0, \dots, u_{e-1} \in \mathcal{O}_K^\times$,*

$$\alpha = \sum_{i=0}^{e-1} u_i \pi_L^i$$

generates a normal integral basis for L/K.

Proof. This result is proved in [Joh11, Proposition 9.4]. Here we give a sketch of the proof.

Every totally ramified and tamely ramified extension of K with degree e is of the form $L = K(\sqrt[e]{\pi_K})$, for a suitable uniformiser π_K of K. In addition, if L/K is Galois, then $K \ni \zeta_e$ and $\mathrm{Gal}(L/K)$ is cyclic by Kummer theory. In particular, let $\pi_L = \sqrt[e]{\pi_K}$. Then $\pi_L \in L$, $v_L(\pi_L) = 1/e$, and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$, with integral basis $\{1, \pi_L \dots, \pi_L^{e-1}\}$.

To show that $\{\sigma(\alpha)\}_{\sigma \in G}$ is a normal integral basis, it is enough to prove that $\{\sigma(\alpha)\}_{\sigma \in G}$ is a basis. We have

$$\langle \{\sigma(\alpha)\}_{\sigma \in G} \rangle_{\mathcal{O}_K} \subseteq \langle \{\pi_L^i\}_{0 \leq i \leq e-1} \rangle_{\mathcal{O}_K}.$$

Our claim is that

$$[\mathcal{O}_L : \langle \{\sigma(\alpha)\}_{\sigma \in G} \rangle_{\mathcal{O}_K}] = \mathcal{O}_K,$$

that is, the determinant of the map sending $\{\pi_L^i\}_{0 \leq i \leq e-1}$ to $\{\sigma(\alpha)\}_{\sigma \in G}$ is invertible in $\mathcal{O}_K$. This would be enough by Lemma 1.18(2).

The Galois group $\mathrm{Gal}(L/K)$ is cyclic, generated by the element σ that sends π_L to $\zeta_e \pi_L$; therefore

$$\sigma^j(\alpha) = \sum_{i=0}^{e-1} u_i \sigma^j(\pi_L^i) = \sum_{i=0}^{e-1} u_i \zeta^{ij} \pi_L^i,$$

so we need to prove that $A = \{u_i \zeta^{ij}\}$ has invertible determinant in $\mathcal{O}_K$. We have

$$\det(A) = \left(\prod_{k=0}^{e-1} u_k \right) \cdot \det(B),$$

with $B = \{\zeta^{ij}\}$. Using that B is a Vandermonde matrix and L/K is tamely ramified, one can conclude that $\det(B) \in \mathcal{O}_K^\times$, and so we derive our assertion. □

Combining these two cases, with some additional work, one can deduce the result for tamely ramified extensions.

Theorem 1.39 (Noether's theorem)**.** *Let L/K be a Galois extension of p-adic fields. Then L/K admits a normal integral basis if and only if L/K is tamely ramified.*

Proof. One direction is Corollary 1.31. The other is quite technical, and we refer to [ET92, Lemma 3.2], [Kaw86], [Joh11, Theorem 9.5]. □

2. More tamely ramified Galois module structure and an introduction to wild Galois module structure

2.1. **Higher ramification groups.** We begin this section with a brief discussion about higher ramification groups; we refer to [Ser79, Chapter IV, sections 1–2].

Let L/K be a Galois extension of p-adic fields with Galois group G, and let $\mathfrak{P}$ be the prime of $\mathcal{O}_L$.

Definition 2.1. For all $i \geq -1$, the *ith ramification group* is

$$G_i = \{\sigma \in G \mid \sigma(x) \equiv x \pmod{\mathfrak{P}^{i+1}} \text{ for all } x \in \mathcal{O}_L\}.$$

Note that it is enough to check the condition on a generator α for $\mathcal{O}_L$ as $\mathcal{O}_K$-algebra, which exists by Hensel's lemma. This implies that G_i is trivial for i sufficiently large, and since every G_i is the kernel of the natural action of G on $\mathcal{O}_L/\mathfrak{P}^{i+1}$, we conclude that the subgroups G_i form a decreasing filtration of normal subgroup of G:

$$G = G_{-1} \geq G_0 \geq \cdots \geq G_n = 1.$$

For $i = 0$, we find the *inertia subgroup* G_0, which has order e, the ramification index of the extension L/K. In particular, L/K is unramified if and only if G_0 is trivial.

Proposition 2.2. *Let $i \geq 0$, let $\sigma \in G_0$, and let π be an uniformiser of L. Then $\sigma \in G_i$ if and only if $\sigma(\pi)/\pi \equiv 1 \pmod{\mathfrak{P}^i}$.*

Proof. Consider the fixed field $K_0 = L^{G_0}$ of G_0. Since $\sigma \in G_0$, it is enough to show the result for a generator of $\mathcal{O}_L$ over $\mathcal{O}_{K_0}$. As L/K_0 is totally ramified, we can pick π as generator; therefore, just dividing $\sigma(\pi) \equiv \pi \pmod{\mathfrak{P}^{i+1}}$ by π, we derive the assertion. □

Recall that, if we denote by U_L the group of units of $\mathcal{O}_K$, then we have a filtration given by $U_{L,i} = 1 + \mathfrak{P}^i = \{x \in U_L \mid x \equiv 1 \pmod{\mathfrak{P}^i}\}$ for all $i \geq 0$. We call U_L^i the *ith higher unit group.*

Proposition 2.3. *For all i ≥ 0, there exists an injective group homomorphism*

$$\theta_i \colon G_i/G_{i+1} \to U_{L,i}/U_{L,i+1},$$

induced by

$$s \mapsto \frac{s(\pi)}{\pi}.$$

The map θ_i is independent of the choice of the uniformiser π for L.

Proof. By Proposition 2.2, if $s \in G_i$, then $s(\pi)/\pi \in U_L^i$. The map is well defined, since if $\pi' = \pi u$, with $u \in U_L$, is another uniformiser, then

$$\frac{s(\pi')}{\pi'} = \frac{s(\pi)}{\pi} \cdot \frac{s(u)}{u},$$

and $s(u)/u \in U_L^{i+1}$.

The map $G_i \to U_L^i/U_L^{i+1}$ is actually a homomorphism, as

$$\frac{(st)(\pi)}{\pi} = \frac{s(t(\pi))}{t(\pi)} \cdot \frac{t(\pi)}{\pi},$$

and $t(\pi)$ is again an uniformiser.

Finally, note that the kernel of this map is precisely G_{i+1}, by Proposition 2.2 applied to $i+1$. □

Corollary 2.4. *The group G_0/G_1 is cyclic of order coprime with p, and G_1 is a p-group.*

Proof. Recall that there are group isomorphisms $U_L/U_{L,1} \cong k_L^\times$ and $U_{L,i}/U_{L,i+1} \cong k_L$ for all $i \geq 1$, by [Ser79, Chapter IV, Proposition 6]. We derive that G_0/G_1 is isomorphic to a subgroup of k_L, so it is cyclic with order coprime with p, and G_i/G_{i+1} is a p-group; since the filtration eventually stops, we conclude that G_1 is a p-group. □

Corollary 2.5. *The extension L/K is tamely ramified if and only if G_1 is trivial.*

Proof. The extension L/K is tamely ramified if and only if p is coprime with e, the order of G_0. As $G_1 \leq G_0$ is a p-group and G_0/G_1 has order coprime with p, we immediately deduce the result. □

Definition 2.6. The extension L/K is *weakly ramified* if G_2 is trivial.

2.2. Orders.

We refer again to [Joh11].

Let R be a Noetherian domain with field of fractions K. Suppose $R \neq K$. Let A be a finite-dimensional K-algebra.

Definition 2.7. An *R-order* in A is a subring Λ of A, with the same unity, such that Λ is an R-lattice.

In particular, an R-order is also an R-algebra.

Example 2.8.

(1) If $R = \mathcal{O}$ is a Dedekind domain, L/K is a finite separable extension, and $\mathcal{O}_L$ is the integral closure of $\mathcal{O}$ in L, then $\mathcal{O}_L$ is an $\mathcal{O}$-order in L.
(2) For all $n \geq 1$, the R-module of $n \times n$ matrices $\mathrm{Mat}_{n\times n}(R)$ is an R-order in $\mathrm{Mat}_{n\times n}(K)$.
(3) Let G be a finite group. Then group ring $R[G]$ is an R-order in $K[G]$.

Let now L/K be a finite Galois extension of number fields or p-adic fields with Galois group G.

Definition 2.9. The *associated order* of L/K is

$$\mathfrak{A}_{L/K} = \{x \in K[G] \mid x \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

Note that $\mathfrak{A}_{L/K}$ always contains $\mathcal{O}_K[G]$, but they may differ, as we see below.

Proposition 2.10. *$\mathfrak{A}_{L/K}$ is an $\mathcal{O}_K$-order in $K[G]$.*

Proof. It is immediate to see that $\mathfrak{A}_{L/K}$ is an $\mathcal{O}_K$-subalgebra of $K[G]$. As it contains $\mathcal{O}_K[G]$, for which $K \cdot \mathcal{O}_K[G] = K[G]$, we deduce that $K \cdot \mathfrak{A}_{L/K} = K[G]$.

We just need to check that $\mathfrak{A}_{L/K}$ is finitely generated as $\mathcal{O}_K$-module. Let $\alpha \in \mathcal{O}_L$ be a generator of a normal basis for L/K, and write $M = \{x \in K[G] \mid x \cdot \alpha \in \mathcal{O}_L\}$, so $M \cdot \alpha = \mathcal{O}_L$. Note that $M \cong \mathcal{O}_L$ as $\mathcal{O}_K$-modules; therefore M is a finitely generated $\mathcal{O}_K$-module. Since $\mathfrak{A}_{L/K} \subseteq M$ and $\mathcal{O}_K$ is Noetherian, we conclude that also $\mathfrak{A}_{L/K}$ is a finitely generated $\mathcal{O}_K$-module. □

By definition, $\mathcal{O}_L$ is an $\mathfrak{A}_{L/K}$-module. Is $\mathcal{O}_L$ free over $\mathfrak{A}_{L/K}$?

Remark 2.11. If $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$, then it needs to have rank one, since if we tensor with K over $\mathcal{O}_K$, we find that this rank equals the rank of L as $K[G]$-module, which is one by Theorem 1.5. In particular, if $\mathcal{O}_L$ is free with basis $\{\alpha\}$, then $L = K \cdot \mathcal{O}_L = K \cdot (\mathfrak{A}_{L/K} \cdot \alpha) = K[G] \cdot \alpha$, that is, α generates a normal basis. As in Remark 1.8, this shows also that the apparently weaker condition $\mathcal{O}_L = \mathfrak{A}_{L/K} \cdot \alpha$ is enough to obtain that $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$ with basis $\{\alpha\}$.

The following meaningful result explains how the associated order is the right ring to study, in relation with $\mathcal{O}_L$.

Proposition 2.12. *Let L/K be a Galois extension of number fields or p-adic fields with Galois group G. If $\mathcal{O}_L$ is free over an $\mathcal{O}_K$-order Γ in $K[G]$, then $\Gamma = \mathfrak{A}_{L/K}$.*

Proof. Suppose $\mathcal{O}_L = \Gamma \cdot \alpha$. If $x \in \mathfrak{A}_{L/K}$, then $x \cdot \alpha \in \mathcal{O}_L = \Gamma \cdot \alpha$, hence we can find $y \in \Gamma$ with $x \cdot \alpha = y \cdot \alpha$. As α is a generator of a normal basis by (a slight variation of) Remark 2.11, we conclude that $x = y \in \Gamma$.

Conversely, if $\gamma \in \Gamma$, then $\gamma \cdot \mathcal{O}_L = \gamma \cdot (\Gamma \cdot \alpha) = \gamma\Gamma \cdot \alpha \subseteq \Gamma \cdot \alpha = \mathcal{O}_L$; thus $\Gamma \subseteq \mathfrak{A}_{L/K}$. □

Example 2.13. Consider the extension $\mathbb{Q}(i)/\mathbb{Q}$, which is wild at the prime 2, with Galois group $G = \{\mathrm{id}, \sigma\}$, where σ is the complex conjugation. Consider $e_1 = \frac{1+\sigma}{2}$ and $e_{-1} = \frac{1-\sigma}{2}$. It is straightforward to show that e_1 and e_{-1} map the ring of integers $\mathbb{Z}[i]$ to itself, so they belong to $\mathfrak{A}_{\mathbb{Q}(i)/\mathbb{Q}}$, which is then strictly larger than $\mathbb{Z}[i]$. Moreover, if $\alpha = 1 + i \in \mathbb{Z}[i]$, then $\mathbb{Z}[e_1, e_{-1}] \cdot \alpha = \mathbb{Z}[i]$, that is, $\mathfrak{A}_{\mathbb{Q}(i)/\mathbb{Q}} = \mathbb{Z}[e_1, e_{-1}]$ by Proposition 2.12.

Corollary 2.14. *Let L/K be a Galois extension of p-adic fields with Galois group G. Then $\mathfrak{A}_{L/K} = \mathcal{O}_K[G]$ if and only if L/K is tamely ramified.*

Proof. If L/K is tamely ramified, then L/K admits a normal integral basis (Corollary 1.31), hence $\mathfrak{A}_{L/K} = \mathcal{O}_K[G]$ by Proposition 2.12.

Conversely, if L/K is wildly ramified, then, by Theorem 1.30, $\mathrm{Tr}_{L/K}(\mathcal{O}_L) \subseteq \pi_K \mathcal{O}_K$, where π_K is an uniformiser of $\mathcal{O}_K$. In particular,

$$\frac{1}{\pi_K} \mathrm{Tr}_{L/K} = \frac{1}{\pi_K} \sum_{\sigma \in G} \sigma$$

belongs to $\mathfrak{A}_{L/K}$ but not to $\mathcal{O}_K[G]$. □

2.3. **Locally free class group.** Here we follow [Joh11] and [Rei03].

We begin with some useful definitions.

Definition 2.15. Let K be a field, and let A be a K-algebra.

- A is *semisimple* if A is the direct sum of a finite number of minimal left ideals.
- A is *separable* if for all field extensions $K \subseteq L$, $L \otimes_K A$ is a semisimple L-algebra.

Remark 2.16. Note that we do not need the algebra structure in Definition 2.15, just the ring structure.

Remark 2.17. It is clear that a separable algebra is semisimple.

Example 2.18.

(1) If K is a field, then every separable K-algebra is semisimple.
(2) If L/K is a finite field extension, then L is a separable K-algebra if and only if L/K is a separable field extension; see [CR81, Proposition 7.4].
(3) If G is a finite group, then the group algebra $K[G]$ is separable, as immediate consequence of Maschke's theorem; see [CR81, Theorem 3.14].

Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, and let Λ be an $\mathcal{O}$-order in a finite-dimensional separable K-algebra. (For example, we can take $K[G]$).

Definition 2.19. A Λ-*lattice* is a Λ-module which is an $\mathcal{O}$-lattice.

Definition 2.20. Two Λ-lattices M and N are *locally isomorphic* if $M_\mathfrak{p} \cong N_\mathfrak{p}$ as $\Lambda_\mathfrak{p}$-modules for all maximal ideals $\mathfrak{p}$ of $\mathcal{O}$; in this case, we write $M \vee N$. We say that M is *locally free* of rank n over Λ if $M \vee \Lambda^n$.

If M is locally free of rank one, then we say that M is a *locally free ideal*.

Remark 2.21. Note that for a finitely generated $\mathcal{O}$-module M and a maximal ideal $\mathfrak{p}$ of $\mathcal{O}$, also the localisation of M with respect to $\mathfrak{p}$ may be denoted by $M_\mathfrak{p}$. In particular, some authors give Definition 2.20 with localisations instead of completions; this ambiguity is justified by [CR81, Proposition 30.17].

Example 2.22.

(1) If M is free of rank n, then M is locally free of rank n.
(2) Let L/K be a Galois extension of number fields with Galois group G. For all primes $\mathfrak{p}$ of $\mathcal{O}_K$, write $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_{K_\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathcal{O}_L$. Then $\mathcal{O}_L$ is locally free of rank one over $\mathcal{O}_K[G]$ if and only if $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{O}_{K_\mathfrak{p}}[G]$-module of rank one for all primes $\mathfrak{p}$ of $\mathcal{O}_K$.

We prove the following result in section 5.

Theorem 2.23. *Let L/K be a Galois extension of number fields with Galois group G. If $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ which is tamely ramified in L/K, then $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathcal{O}_{K_\mathfrak{p}}[G]$-module of rank one. In particular, if L/K is tamely ramified, then $\mathcal{O}_L$ is locally free of rank one over $\mathcal{O}_K[G]$.*

We introduce an equivalence relation on the set of locally free Λ-lattices: we write $M \sim N$ if there exist $r, s \in \mathbb{N}$ such that $M \oplus \Lambda^r \cong N \oplus \Lambda^s$ as Λ-modules. We write the class of M as $[M]$, and lattices in $[\Lambda]$ are called *stably free*.

Theorem 2.24. *Let M and M' be locally free Λ-lattices. Then there exist a locally free ideal M'' and $t \in \mathbb{N}$ such that*

$$M \oplus M' \cong \Lambda^t \oplus M''$$

as Λ-modules.

Proof. See [Rei03, Theorem 26.4]. □

Theorem 2.24 implies that every class is represented by a locally free ideal. In addition, if M, M' are locally free Λ-lattices and M'' is a locally free ideal as in Theorem 2.24, then we set

$$[M] + [M'] = [M''].$$

This defines a group structure on the set of classes with respect to the equivalent relation introduced above, where the identity element is $[\Lambda]$. The group we get is called *locally free class group* and is denoted by $\mathrm{Cl}(\Lambda)$.

Example 2.25. Clearly $\mathcal{O}$ is an $\mathcal{O}$-order in the K-algebra K. In this case, $\mathrm{Cl}(\mathcal{O})$ is just the usual ideal class group, a finite group consisting of $\mathcal{O}$-isomorphism classes of fractional $\mathcal{O}$-ideals in K, where the group operation is determined by multiplication of fractional ideals.

The following result implies that if $\mathcal{O}$ is the ring of integers $\mathcal{O}_K$ of a number field K, then $\mathrm{Cl}(\Lambda)$ is finite.

Theorem 2.26 (Jordan–Zassenhaus theorem)**.** *If K is a number field, then for all $t \in \mathbb{N}$, there are only finitely many isomorphism classes of Λ-lattices of $\mathcal{O}$-rank at most t.*

Proof. See [Rei03, Theorem 26.4]. □

Remark 2.27. Let L/K be a tamely ramified Galois extension of number fields. Then $\mathcal{O}_L$ is locally free of rank one over $\mathcal{O}_K[G]$ (Theorem 2.23). In particular, we can consider the class $[\mathcal{O}_L] \in \mathrm{Cl}(\mathcal{O}_K[G])$. Note that if this class is trivial, then it is not necessarily true that $\mathcal{O}_L$ is free over $\mathcal{O}_K[G]$. Rather, if $\mathcal{O}_L$ is stably free, then there exists $r \in \mathbb{N}$ such that

$$\mathcal{O}_L \oplus (\mathcal{O}_K[G])^r \cong (\mathcal{O}_K[G])^{r+1}$$

as $\mathcal{O}_K[G]$-modules. It can be shown that this holds also for $r = 1$, but in [Cou94] there is an example of a tamely Galois extension $L/\mathbb{Q}$ with Galois group Q_{32}, the generalised quaternion group of order 32, where $\mathcal{O}_L$ is stable free but not free over $\mathbb{Z}[Q_{32}]$.

Let K be a number field, and let Λ be an $\mathcal{O}_K$-order in a finite-dimensional separable K-algebra A. We say that Λ has *locally free cancellation* if for all locally free finitely generated Λ-modules X and Y,

$$X \oplus \Lambda^{(k)} \cong Y \oplus \Lambda^{(k)} \text{ for some } k \in \mathbb{N} \implies X \cong Y,$$

where the isomorphisms are as Λ-modules. In this case, stably free is equivalent to free, that is, $[X]$ trivial in $\mathrm{Cl}(\Lambda)$ implies that X is a free Λ-module.

Example 2.28.

(1) If A is Eichler/$\mathcal{O}_K$, then every $\mathcal{O}$-order in A has locally free cancellation. This is Jacobinski cancellation theorem; see [CR87, Theorem 51.24].
(2) If G is a finite group and $A = K[G]$, then an $\mathcal{O}_K$-order in $K[G]$ has locally free cancellation if K is totally complex or if G is abelian, dihedral, symmetric, alternating, or of odd order.

We conclude with a statement of a special case of Fröhlich's conjecture, proved by Taylor in [Tay81].

Theorem 2.29 (Fröhlich's conjecture, special case)**.** *Let L/K be a tamely ramified Galois extension of number fields with Galois group G. Then $[\mathcal{O}_L]^2$ is trivial in* $\mathrm{Cl}(\mathbb{Z}[G])$*; moreover, if G has no irreducible symplectic characters, then $\mathcal{O}_L$ is free of rank $[K:\mathbb{Q}]$ over $\mathbb{Z}[G]$.*

The condition on G of Theorem 2.29 holds, for example, if G is abelian, dihedral, symmetric, alternating, or of odd order.

2.4. **Structural results for generalised normal integral bases.** We briefly summarise the behaviour of the associated order in towers and compositum of fields, referring to [BL96], [Joh11, section 11].

Lemma 2.30. *Let L and F be arithmetically disjoint Galois extensions of a number field or p-adic field K, and let $N = LF$. Then the following hold:*

(1) $\mathfrak{A}_{N/F} \cong \mathfrak{A}_{L/K} \otimes_{\mathcal{O}_K} \mathcal{O}_F$ *$\mathcal{O}_F$-algebras, and* $\mathfrak{A}_{N/K} \cong \mathfrak{A}_{L/K} \otimes_{\mathcal{O}_K} \mathfrak{A}_{F/K}$ *as $\mathcal{O}_K$-algebras.*

(2) *If there exists $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathfrak{A}_{L/K} \cdot \alpha$, then $\mathcal{O}_N = \mathfrak{A}_{L/F} \cdot \alpha$; moreover, if there exists $\beta \in \mathcal{O}_F$ such that $\mathcal{O}_F = \mathfrak{A}_{F/K} \cdot \beta$, then $\mathcal{O}_N = \mathfrak{A}_{N/K} \cdot \alpha\beta$.*

Proof. This is [BL96, Lemma 5], and it makes use of the isomorphism $\mathcal{O}_L \cong \mathcal{O}_{L_1} \otimes_{\mathcal{O}_K} \mathcal{O}_{L_2}$ given by Theorem 1.24, and [CR81, Section 24, Exercise 2]. □

Lemma 2.31. *Let $K \subseteq L \subseteq N$ be a tower of Galois extensions of number fields, and suppose that N/L is tame. If $\mathcal{O}_N = \mathfrak{A}_{N/K} \cdot \alpha$, then $\mathcal{O}_L = \mathfrak{A}_{L/K} \cdot \mathrm{Tr}_{N/L}(\alpha)$.*

Proof. See [Joh11, Lemma 11.2]. □

2.5. **Leopoldt's theorem.** Following [Joh11, section 12], we explicitly prove a particular case of Leopoldt's theorem. We begin with the cyclotomic case.

For every $k \in \mathbb{N}$, choose a primitive kth root of unity ζ_k in such a way that for all $k, \ell \in \mathbb{N}$ with $k \mid \ell$, we have $\zeta_\ell^{\ell/k} = \zeta_k$.

Lemma 2.32. *Let p be a prime, let $n, m \geq 1$ (with $n \geq 2$ if $p = 2$), and let $0 \leq k \leq n+m$. Then*

$$\mathrm{Tr}_{\mathbb{Q}(\zeta_{p^{n+m}})/\mathbb{Q}(\zeta_{p^n})}(\zeta_{p^k}) = \begin{cases} \zeta_{p^k} p^m & \text{if } k \leq n, \\ 0 & \text{otherwise.} \end{cases}$$

Proof. See [Joh11, Lemma 12.2]. □

Proposition 2.33. *Let p be a prime number, let $n \in \mathbb{N}$ ($n \geq 2$ if $p = 2$), let $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$, and let $\alpha = \sum_{k=1}^{n} \zeta_{p^k}$. For $1 \leq k \leq n$, define $e_k = \frac{1}{p^{n-k}} \mathrm{Tr}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}(\zeta_{p^k})}$. Then*

$$\mathbb{Z}[\zeta_{p^n}] = \mathfrak{A}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} \cdot \alpha,$$

where

$$\mathfrak{A}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}} = \mathbb{Z}[G][\{e_k\}_{k=1}^{n-1}].$$

Proof. We assume that p odd (the case $p = 2$ is done similarly) and define $\mathcal{B} = \mathbb{Z}[G][\{e_k\}_{k=1}^{n-1}]$. We want to show that $\mathcal{B} \cdot \alpha = \mathbb{Z}[\zeta_{p^n}]$. We know that every element in $\mathbb{Z}[\zeta_{p^n}]$ is a combination of p-power roots of unity with coefficients in $\mathbb{Z}$.

By Lemma 2.32,

$$e_k \cdot \zeta_{p^\ell} = \begin{cases} \zeta_{p^\ell} & \text{if } 0 \le \ell \le k, \\ 0 & \text{otherwise,} \end{cases}$$

and since all the primitive p^ℓ-roots of unity are G-conjugate and for all $\sigma \in G$ we have $e_k \cdot (\sigma(\zeta_{p^\ell})) = \sigma e_k \cdot \zeta_{p^\ell}$, we derive that $e_k \in \mathfrak{A}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}$, and so

$$\mathcal{B} := \mathbb{Z}[G][\{e_k\}_{k=1}^{n-1}] \subseteq \mathfrak{A}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}.$$

By definition of associated order, $\mathcal{B} \cdot \alpha \subseteq \mathbb{Z}[\zeta_{p^n}]$.

Conversely, it is immediate to see that $\sigma e_1 \cdot \alpha = \sigma(\zeta_p)$ and $\sigma(e_k - e_{k-1}) \cdot \alpha = \sigma(\zeta_{p^k})$ for all $g \in G$ and $2 \le k \le n$; hence $\mathcal{B} \cdot \alpha \supseteq \mathbb{Z}[\zeta_{p^n}]$.

By Proposition 2.12, we conclude that $\mathcal{B} = \mathfrak{A}_{\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}}$. □

If $n \in \mathbb{N}$, write $r(n)$ for the product of all prime numbers dividing n.

Proposition 2.34. *Let $n \in \mathbb{N}$ with $n \not\equiv 2 \pmod 4$, and let $\alpha = \sum_{r(n)|d|n} \zeta_d$. Then $\mathbb{Z}[\zeta_n] = \mathfrak{A}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \cdot \alpha$.*

Proof. This follows from Proposition 2.33 and Lemma 2.30. □

Remark 2.35. The condition $n \not\equiv 2 \pmod 4$ in Proposition 2.34 is due to the fact that if $n = 2m$ with m odd, then $\mathbb{Q}(\zeta_{p^n}) = \mathbb{Q}(\zeta_{p^m})$.

Definition 2.36. Let L be a finite abelian extension of $\mathbb{Q}$. The *conductor* of L is the smallest natural number n such that $L \subseteq \mathbb{Q}(\zeta_n)$. (The natural number n always exists by Kronecker–Weber theorem.)

Lemma 2.37. *Let L be a finite abelian extension of $\mathbb{Q}$ of conductor n. Then $\mathbb{Q}(\zeta_n)/L$ is tamely ramified at all primes lying above odd prime numbers. In particular, if n is odd or $i \in L$, then $\mathbb{Q}(\zeta_n)/L$ is tamely ramified.*

Proof. See [Joh11, Lemmas 12.6 and 12.7]. □

Theorem 2.38 (Leopoldt's theorem, special case)**.** *Let L be a finite abelian extension of $\mathbb{Q}$ of conductor n. Suppose that n is odd or $i \in L$. Let*

$$\alpha = \operatorname{Tr}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \left(\sum_{r(n)|d|n} \zeta_d \right).$$

Then $\mathcal{O}_L = \mathfrak{A}_{L/\mathbb{Q}} \cdot \alpha$.

Proof. By Proposition 2.34, we have $\mathbb{Z}[\zeta_n] = \mathfrak{A}_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} \cdot \alpha$. By Lemma 2.37, $\mathbb{Q}(\zeta_n)/L$ is tamely ramified. The result now follows from Lemma 2.31. □

Remark 2.39. Leopoldt's original proof is presented in [Leo59]. One can prove Leopoldt's theorem for all finite abelian extensions of $\mathbb{Q}$ in almost the same way as this section, by using the *adjusted trace map*, as defined in [Joh06]. Finally, a different and simplified approach can be found in [Let90].

3. Results on Galois module structure of wildly ramified extensions and local freeness over the associated order

Let L/K be a Galois extension of number fields, let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$, and let $\mathfrak{P}$ be a prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Write $\mathfrak{A}_{L/K,\mathfrak{p}} = \mathcal{O}_{K_\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathfrak{A}_{L/K}$. There are three questions that one can ask.

(1) Is $\mathcal{O}_L$ free over $\mathfrak{A}_{L/K}$?
(2) Is $\mathcal{O}_{L,\mathfrak{p}}$ free over $\mathfrak{A}_{L/K,\mathfrak{p}}$?
(3) Is $\mathcal{O}_{L_\mathfrak{P}}$ free over $\mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}}$?

Clearly, if (1) is satisfied, then also (2) is satisfied. The goal of this section is to summarise the main results known about these problems and to understand the relations between them.

Remark 3.1. In all of the previous cases, if we have freeness, then the rank is necessarily one, as taking the tensor product with K over $\mathcal{O}_K$ immediately shows.

Notation 3.2. For all $n > 1$, write S_n and A_n for the symmetric group and the alternating group, respectively, of degree n.

3.1. Brief recall on the tamely ramified case.

If L/K is a tamely ramified Galois extension of number fields with Galois group G, then $\mathcal{O}_L$ defines a class in $\mathrm{Cl}(\mathcal{O}_K[G])$. In particular, if $\mathrm{Cl}(\mathcal{O}_K[G]) = 0$ and $K[G]$ has locally free cancellation, then L/K automatically admits a normal integral basis. If $K = \mathbb{Q}$, the $\mathrm{Cl}(\mathbb{Z}[G]) = 0$ is only true if G is among certain abelian groups, certain dihedral groups, A_4, S_4, A_5; see [RU74, EH79]. In such cases we automatically have locally free cancellation. However, we have already seen the following consequence of Fröhlich's conjecture, which was proved by Taylor in [Tay81] and tells us much more without assuming that the locally free class group is trivial.

Theorem 3.3. *Let $L/\mathbb{Q}$ be a finite tamely ramified Galois extension of $\mathbb{Q}$ with Galois group G. Suppose that G is abelian, dihedral, of odd order, alternating, or symmetric. Then $L/\mathbb{Q}$ has a normal integral basis.*

Indeed, in the hypotheses of Theorem 3.3, G has no irreducible symplectic character, which means that the class of $\mathcal{O}_L$ in $\mathrm{Cl}(\mathbb{Z}[G])$ is trivial, and that there is locally free cancellation, which implies that $\mathcal{O}_L$ is free over $\mathbb{Z}[G]$. Note that this in particular generalises Hilbert–Speiser theorem, and it permits us to conclude that a sufficiently nice (that is, whose Galois group does not have to do with quaternions) tamely ramified nonabelian extension of $\mathbb{Q}$ admits a normal integral basis.

3.2. Clean orders.

One reference for these kind of orders is [Rog70, Chapter IX, section 1].

Definition 3.4. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, let G be a finite group, and let Λ be a $\mathcal{O}$-order in $K[G]$. We say that the order Λ is *clean* if Λ satisfies the following property: if M is a projective Λ-lattice which spans over K a free $K[G]$-module, then M is a free Λ-lattice.

Example 3.5.

(1) If $\mathcal{O}$ is a discrete valuation ring, then $\mathcal{O}[G]$ is a clean order. This is Swan's theorem; see [CR81, Theorem 32.1].

(2) If G is abelian and $\mathcal{O}$ is a discrete valuation ring with characteristic zero and finite residue field, then every $\mathcal{O}$-order in $K[G]$ is clean. This is due to Hattori [Hat65]; see also [Rog70, Chapter IX, Corollary 1.5].
(3) As we see in section 5, if $\mathcal{O}$ is a discrete valuation ring, then every maximal $\mathcal{O}$-order is clean. More precisely, in Definition 3.4, we do not even need to assume that M is projective.

From Swan's theorem, we deduce in Section 5 an important relation between tameness and projectivity.

3.3. **Freeness results for Galois extensions of p-adic fields.** Let p be a prime number. We begin with a consequence of Leopoldt's theorem.

Theorem 3.6 (Leopoldt)**.** *Let $L/\mathbb{Q}_p$ be a finite abelian extension. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}_p}$.*

Lettl further generalised the result in [Let98].

Theorem 3.7 (Lettl)**.** *Let L/K be an extension of p-adic fields such that $L/\mathbb{Q}_p$ is abelian. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$.*

Now we shall consider the nonabelian setting. In this framework, the first important contributions are due to Bergé [Ber72], Martinet [Mar72], and Jaulent [Jau81].

Theorem 3.8 (Bergé)**.** *Let $L/\mathbb{Q}_p$ be a Galois extension with* $\mathrm{Gal}(K/\mathbb{Q}) \cong D_{2p}$. *Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}_p}$.*

Theorem 3.9 (Martinet)**.** *Let $L/\mathbb{Q}_p$ be a Galois extension with* $\mathrm{Gal}(L/\mathbb{Q}) \cong Q_8$. *Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}_p}$.*

Theorem 3.10 (Jaulent)**.** *Assume that p is odd, and let n and r be positive integers such that n divides $p-1$ and r is a primitive nth root modulo p. Let G be the metacyclic group with the following structure:*

$$G = \langle x, y \mid x^p = 1, y^n = 1, yxy^{-1} = x^r\rangle \cong C_p \rtimes C_n. \tag{3.1}$$

Let $L/\mathbb{Q}_p$ be a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}_p) \cong G$. *Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}_p}$.*

Remark 3.11. In the special case $n = 2$, the group G of Theorem 3.10 is dihedral group of order $2p$.

Notation 3.12. If L/K is a finite Galois extension with Galois group G and H is a subgroup of G, then we write $\mathrm{Tr}_H = \sum_{h\in H} h \in K[G]$ and $e_H = \frac{1}{|H|}\mathrm{Tr}_H \in K[G]$. Note that e_H is an idempotent.

Considering a generic base field, Johnston [Joh15] obtained the following result.

Theorem 3.13 (Johnston)**.** *Let L/K be a weakly ramified Galois extension of p-adic fields with Galois group G. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$; moreover, if L/K is wildly and weakly ramified, then $\mathfrak{A}_{L/K} = \mathcal{O}_K[G][\pi_K^{-1}\mathrm{Tr}_{G_0}]$, where G_0 is the inertia subgroup.*

One may suspect that it is always the case that, in a Galois extension of p-adic fields, the ring of integers is free over the associated order, as happens if we further assume tame ramification. We see below that this is not true.

Definition 3.14. Let L/K be a Galois extension of p-adic fields with Galois group G. We say that L/K is *almost maximally ramified* if $e_H \in \mathfrak{A}_{L/K}$ for all subgroups H of G such that $G_{i+1} \leq H \leq G_i$ for some $i \geq 1$.

Remark 3.15. We can give a version of Definition 3.14 also for Galois extensions of number fields: if L/K is such an extension, $\mathfrak{p}$ is a prime of $\mathcal{O}_K$, and $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$, then $\mathfrak{p}$ is *almost maximally ramified* in L if $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is almost maximally ramified. Note that indeed this property does not depend on the prime $\mathfrak{P}$ lying above $\mathfrak{p}$.

The following result is due to Bergé [Ber79a, Proposition 7].

Theorem 3.16 (Bergé)**.** *Let L/K be a dihedral extension of p-adic fields with Galois group G such that $K/\mathbb{Q}_p$ is unramified. Then $\mathcal{O}_L$ is projective over $\mathfrak{A}_{L/K}$ if and only if $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$, if and only if one of the following conditions holds:*

(1) *L/K is almost maximally ramified; in this case*

$$\mathfrak{A}_{L/K} = \mathcal{O}_K[G][\{e_{G_i}\}_{i\geq 1}].$$

(2) *L/K is not almost maximally ramified, and the inertia subgroup G_0 is dihedral of order $2p$; in this case*

$$\mathfrak{A}_{L/K} = \mathcal{O}_K[G][2e_{G_0}].$$

We discuss further results concerning cyclic extensions of prime orders and extensions with cyclic inertia group in section 5.

3.4. **Freeness results for Galois extensions of number fields.** We begin by recalling Leopoldt's theorem [Leo59], which generalises Hilbert–Speiser theorem to wildly ramified abelian extensions of $\mathbb{Q}$.

Theorem 3.17 (Leopoldt's theorem)**.** *Let $L/\mathbb{Q}$ be a finite abelian extension. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$.*

In section 3 we have seen a partial proof in the case K has odd conductor or is imaginary.

Remark 3.18. Leopoldt also specified a generator and the associated order; Lettl in [Let90] gave a simplified and more explicit proof of the same result.

We also have the following result of Bergé [Ber72].

Theorem 3.19 (Bergé)**.** *Let p be a prime number, and let $L/\mathbb{Q}$ be a dihedral extension of degree $2p$. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$.*

Now let $L/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \cong Q_8$, the quaternion group of order 8. Suppose that $L/\mathbb{Q}$ is tamely ramified. Martinet gave examples of such extensions with and without a normal integral basis (see Examples 1.34 and 1.35); moreover, Fröhlich showed in [Frö72] that both possibilities occur infinitely often. By contrast, in the case that $L/\mathbb{Q}$ is wildly ramified, we have the following result of Martinet [Mar72].

Theorem 3.20 (Martinet)**.** *Let $L/\mathbb{Q}$ be a wildly ramified Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \cong Q_8$. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$.*

For other global freeness results, the first author recently obtained the following results.

Theorem 3.21. *Let n be a positive integer, and let $p \geq 5$ be a regular prime number such that the class number of $\mathbb{Q}(\zeta_{p^n})^+$ is 1. Let $L/\mathbb{Q}$ be a dihedral extension of degree $2p^n$. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$ if and only if the ramification index of p in $L/\mathbb{Q}$ is a power of p.*

Corollary 3.22. *Let $K/\mathbb{Q}$ be a dihedral extension of degree $2p^n$, where (p, n) is $(5, 2)$, $(5, 3)$, $(7, 2)$, or $(11, 2)$. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$ if and only if the ramification index of p in $L/\mathbb{Q}$ is a power of p.*

Similar but more complicated results hold when $p = 2$ or $p = 3$.

Definition 3.23. A prime number p has *full decomposition group* in a finite Galois extension $L/\mathbb{Q}$ if there is just one prime of $\mathcal{O}_L$ lying above p; this means that the decomposition group of p in $L/\mathbb{Q}$ is the whole group.

Theorem 3.24. *Let $L/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \cong A_4$. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$ if and only if 2 is tamely ramified or has full decomposition group.*

Theorem 3.25. *Let $L/\mathbb{Q}$ be a Galois extension with Galois group $G \cong S_4$. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$ if and only if one of the following conditions on $L/\mathbb{Q}$ holds:*

1. *2 is tamely ramified.*
2. *2 is weakly ramified and has full decomposition group.*
3. *2 has decomposition group equal to the unique subgroup of G of order 12.*
4. *2 is weakly ramified, it has decomposition group of order 8 in G, and it has inertia subgroup equal to the unique normal subgroup of order 4 in G.*

Here a prime number p is *weakly ramified* in L if the extension $L_{\mathfrak{P}}/\mathbb{Q}_p$ is weakly ramified, where $\mathfrak{P}$ is a prime of $\mathcal{O}_L$ lying above p.

Theorem 3.26. *Let $L/\mathbb{Q}$ be a Galois extension with $\mathrm{Gal}(L/\mathbb{Q}) \cong A_5$. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$ if and only if all of the following conditions on $L/\mathbb{Q}$ hold:*

1. *2 is tamely ramified.*
2. *3 is tamely ramified or not almost maximally ramified.*
3. *5 is tamely ramified or not almost maximally ramified.*

3.5. Local freeness results for Galois extensions of number fields.

Let L/K be a Galois extension of number fields, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Recall that $\mathcal{O}_L$ is locally free at $\mathfrak{p}$ over $\mathfrak{A}_{L/K}$ if $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{p}}$, and $\mathcal{O}_L$ is locally free over $\mathfrak{A}_{L/K}$ if this holds for all $\mathfrak{p}$.

The following results are taken by [Let98, Jau81, Ber79a], respectively.

Theorem 3.27 (Lettl)**.** *Let L/K be an extension of number fields such that $L/\mathbb{Q}$ is an abelian extension. Then $\mathcal{O}_L$ is locally free over $\mathfrak{A}_{L/K}$.*

Theorem 3.28 (Jaulent)**.** *Let $L/\mathbb{Q}$ be a Galois extension such that $\mathrm{Gal}(L/\mathbb{Q})$ is metacyclic of type (3.1). Then $\mathcal{O}_L$ is locally free over $\mathfrak{A}_{L/\mathbb{Q}}$.*

Theorem 3.29 (Bergé)**.** *Let $L/\mathbb{Q}$ be a dihedral extension with Galois group G, let p be an odd prime number which is wildly ramified in L, and let N be the unique cyclic subgroup of G of index 2. Then $\mathcal{O}_{L,p}$ is projective over $\mathfrak{A}_{L/\mathbb{Q},p}$ if and only if $\mathcal{O}_{L,p}$ is free over $\mathfrak{A}_{L/\mathbb{Q},p}$, if and only if one of the following conditions holds:*

1. *p is almost maximally ramified in $L/\mathbb{Q}$ and $G_1 \leq N$; in this case*

$$\mathfrak{A}_{L/\mathbb{Q},p} = \mathbb{Z}_p[G][\{e_{G_t}\}_{t \geq 1}].$$

(2) *p is not almost maximally ramified, $|G_0| = 2p$, and $[G : G_0]$ divides 2; in this case*

$$\mathfrak{A}_{L/\mathbb{Q},p} = \mathbb{Z}_p[G][e_{G_0}].$$

Remark 3.30. In fact, Theorem 3.29 is [Ber79a, Théorème] specialised to the case where p is odd and the base field is $\mathbb{Q}$; the more general statement is somewhat more complicated.

3.6. **Interlude: modules over noncommutative rings.** Until now, we have only considered tensor products of modules over commutative rings. In this case, there is no difference in right and left modules. However, in what follows, we need to consider tensor products over rings which are not necessarily commutative. We summarise some of the facts that we implicitly use.

Let R be a ring, let M be a right R-module, and let N be a left R-module.

(1) We can define $M \otimes_R N$ is the usual way. It is an abelian group, but not necessarily a module over R.
(2) If M is an R-bimodule, then $M \otimes_R N$ is a left R-module.
(3) If R is a subring of a ring S, then S is an R-bimodule. In particular, $S \otimes_R N$ is a left S-module.

3.7. **More on local freeness.** We begin by mentioning a slightly more general definition of associated order; see [Joh11, section 3].

Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, let G be a finite group, and let M be an $\mathcal{O}$-lattice in $K[G]$. The *associated order* of M in $K[G]$ is

$$\mathfrak{A}(K[G], M) = \{\lambda \in K[G] \mid \lambda \cdot M \subseteq M\}.$$

So, with the previous notation, $\mathfrak{A}_{L/K} = \mathfrak{A}(K[G], \mathcal{O}_L)$ (after the identification $L \leftrightarrow K[G]$ given by Theorem 1.5, under which $\mathcal{O}_L$ is identified with an $\mathcal{O}$-order in $K[G]$), and it is immediate to generalise the properties of $\mathfrak{A}_{L/K}$:

(1) $\mathfrak{A}(K[G], M)$ is an $\mathcal{O}$-order in $K[G]$.
(2) $\mathfrak{A}(K[G], M)$ is the largest order over which M has a structure of module.
(3) $\mathfrak{A}(K[G], M)$ is the only $\mathcal{O}$-order over which M can possibly be free, necessarily of rank one.
(4) If M is also an $\mathcal{O}[G]$-module, that is, an $\mathcal{O}[G]$-lattice, then $\mathfrak{A}(K[G], M)$ contains $\mathcal{O}[G]$, and in particular $\mathfrak{A}(K[G], M)$ is an $\mathcal{O}[G]$-module.

Remark 3.31. In the previous setting, by [CR81, section 24, Exercise 2], if $\mathfrak{p}$ is a maximal ideal of $\mathcal{O}$, then

$$\mathfrak{A}(K[G], M)_\mathfrak{p} = \mathfrak{A}(\mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} K[G], \mathcal{O}_\mathfrak{p} \otimes_\mathcal{O} M) \cong \mathfrak{A}(K_\mathfrak{p}[G], M_\mathfrak{p}).$$

In particular, we may identify $\mathfrak{A}(K[G], M)_\mathfrak{p}$ with $\mathfrak{A}(K_\mathfrak{p}[G], M_\mathfrak{p})$, to easily switch from one to the other.

Also, let L/K be a Galois extension of number fields with Galois group G, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. Since $\mathfrak{A}(K_\mathfrak{p}[G], \mathcal{O}_{L,\mathfrak{p}}) = \mathfrak{A}_{L/K,\mathfrak{p}}$, if $\mathcal{O}_{L,\mathfrak{p}}$ is free over some $\mathcal{O}_{K_\mathfrak{p}}$-order in $K_\mathfrak{p}[G]$, then this order is precisely $\mathfrak{A}_{L/K,\mathfrak{p}}$.

Finally, if Λ is an $\mathcal{O}_K$-order in $K[G]$ such that $\mathcal{O}_L$ is locally free over Λ, then Λ has to be $\mathfrak{A}_{L/K}$; see [Rei03, Theorem 5.3].

Now let L/K be a Galois extension of number fields with Galois group G, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. We have decompositions

$$L_{\mathfrak{p}} = K_{\mathfrak{p}} \otimes_K L \cong \prod_{\mathfrak{P}' \mid \mathfrak{p}} L_{\mathfrak{P}'}$$

and

$$\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_{K_{\mathfrak{p}}} \otimes_{\mathcal{O}_K} \mathcal{O}_L \cong \prod_{\mathfrak{P}' \mid \mathfrak{p}} \mathcal{O}_{L_{\mathfrak{P}'}},$$

where $\{\mathfrak{P}' \mid \mathfrak{p}\}$ consists of the primes of $\mathcal{O}_L$ above $\mathfrak{p}$; see [FT93, page 109]. Fix a prime $\mathfrak{P}$ above $\mathfrak{p}$ and, let D be its decomposition group in G. Then, since G acts transitively on $\{\mathfrak{P}' \mid \mathfrak{p}\}$, we have

$$L_{\mathfrak{p}} \cong \prod_{\sigma \in G/D} \sigma(L_{\mathfrak{P}})$$

and

$$\mathcal{O}_{L,\mathfrak{p}} \cong \prod_{\sigma \in G/D} \sigma(\mathcal{O}_{L_{\mathfrak{P}}}),$$

where the products run over a complete system of representatives of the left cosets G/D. Now define

$$\operatorname{Ind}_D^G \mathcal{O}_{L_{\mathfrak{P}}} = \mathcal{O}_{K_{\mathfrak{p}}}[G] \otimes_{\mathcal{O}_{K_{\mathfrak{p}}}[D]} \mathcal{O}_{L_{\mathfrak{P}}}.$$

We deduce that

$$\mathcal{O}_{L,\mathfrak{p}} \cong \operatorname{Ind}_D^G \mathcal{O}_{L_{\mathfrak{P}}}$$

and

$$\mathfrak{A}_{L/K,\mathfrak{p}} = \mathfrak{A}(K[G], \mathcal{O}_L)_{\mathfrak{p}} \cong \mathfrak{A}(K_{\mathfrak{p}}[G], \operatorname{Ind}_D^G \mathcal{O}_{L_{\mathfrak{P}}}).$$

This means that in the context of number fields, local freeness of $\mathcal{O}_L$ at a prime $\mathfrak{p}$ over $\mathfrak{A}_{L/K}$ is equivalent to saying that the induction from D to G of the ring of integers of any completion above $\mathfrak{p}$ is free over its associated order. This opens interesting questions:

- Since we are interested in finding the conditions under which the implication "if $\mathcal{O}_{L_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$, then $\mathcal{O}_L$ is locally free at $\mathfrak{p}$ over $\mathfrak{A}_{L/K}$" holds, we can just analyse when $\operatorname{Ind}_D^G \mathcal{O}_{L_{\mathfrak{P}}}$ is free over its associated order.
- As $\mathfrak{A}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$ is an $\mathcal{O}_{K_{\mathfrak{p}}}[D]$-module, we can consider $\operatorname{Ind}_D^G \mathfrak{A}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$. When is "$\mathcal{O}_{L_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$" enough to deduce that "$\operatorname{Ind}_D^G \mathcal{O}_{L_{\mathfrak{P}}}$ is free over $\operatorname{Ind}_D^G \mathfrak{A}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}}$", and so also necessarily over its associated order $\mathfrak{A}(K_{\mathfrak{p}}[G], \operatorname{Ind}_D^G \mathcal{O}_{L_{\mathfrak{P}}})$?

We try to deal with these questions in a more general setting.

Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, let G be a finite group, let H be a subgroup of G, and let N be an $\mathcal{O}[H]$-lattice in $K[H]$. We define the *induced module of* N to be

$$\operatorname{Ind}_H^G N = \mathcal{O}[G] \otimes_{\mathcal{O}[H]} N.$$

Lemma 3.32. *$\operatorname{Ind}_H^G N$ is an $\mathcal{O}[G]$-lattice in $K[G]$.*

Proof. Since $\mathcal{O}[H]$ is a subring of $\mathcal{O}[G]$, we get that $\operatorname{Ind}_H^G N$ is a $\mathcal{O}[G]$ module.

Since $\mathcal{O}[G]$ is a free $\mathcal{O}[H]$-module, the inclusion $N \subseteq \mathcal{O}[H]$ yields an embedding $\operatorname{Ind}_H^G N \hookrightarrow \mathcal{O}[G] \otimes_{\mathcal{O}[H]} K[H]$, and we may identify $\mathcal{O}[G] \otimes_{\mathcal{O}[H]} K[H]$ with $K[G]$ to find an embedding $\operatorname{Ind}_H^G N \hookrightarrow K[G]$.

Finally, as N is finitely generated over $\mathcal{O}$ and spans $K[H]$ over K, we immediately derive that It is immediate to see that $\operatorname{Ind}_H^G N$ is finitely generated over $\mathcal{O}$ and spans $K[G]$ over K. □

Remark 3.33. In our previous discussion, we have considered $\mathcal{O} = \mathcal{O}_{\mathfrak{p}}$, $K = K_{\mathfrak{p}}$, $H = D$, and $N = \mathcal{O}_{L_{\mathfrak{P}}}$.

Our goal is to understand when we can deduce, assuming that N is free over $\mathfrak{A}(K[H], N)$, that $\operatorname{Ind}_H^G N$ is free over $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$, and more generally the relation between $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$ and $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$ (the latter expression makes sense since, as before, $\mathfrak{A}(K[H], N)$ is an $\mathcal{O}[H]$-module). First of all, if N is free over $\mathfrak{A}(K[H], N)$, then the rank of course must be one, since this is true after we tensor with K. In particular, N and $\mathfrak{A}(K[H], N)$ are isomorphic as $\mathcal{O}[H]$-modules, and this easily implies that $\operatorname{Ind}_H^G N$ and $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$ are isomorphic as $\mathcal{O}[G]$-modules.

However, $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$ is not a ring in general, and so it does not always make sense to conclude that $\operatorname{Ind}_H^G N$ is free over $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$. We begin by stating the main result of [Ber79a, section 1.3], which gives an explicit description of $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$ in terms of $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$.

Lemma 3.34. *We have*

$$\mathfrak{A}(K[G], \operatorname{Ind}_H^G N) = \bigcap_{g \in G} g \operatorname{Ind}_H^G \mathfrak{A}(K[H], N) g^{-1}. \tag{3.2}$$

In particular, $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$ *is a ring if and only if*

$$\operatorname{Ind}_H^G \mathfrak{A}(K[H], N) = \mathfrak{A}(K[G], \operatorname{Ind}_H^G N).$$

Remark 3.35. Lemma 3.34 implies that $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N) \subseteq \operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$; therefore $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$ has a structure of $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$-module.

We recall the following lemma.

Lemma 3.36. *Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, and let $\Lambda \subseteq \Gamma$ be two $\mathcal{O}$-orders in a K-algebra A. Let M and N be Γ-lattices, and let $f : M \to N$ be a Λ-lattice map. Then f is a Γ-lattice map.*

Proof. We just need to show that $f(a \cdot m) = a \cdot f(m)$ for all $a \in \Gamma$ and $m \in M$. Let $r \in \mathcal{O}$ be such that $r\Gamma \subseteq \Lambda$. Then

$$rf(a \cdot m) = f(r(a \cdot m)) = f((ra) \cdot m) = (ra) \cdot f(m).$$

Being N an $\mathcal{O}$-torsion-free module by definition, we derive our assertion. □

As a consequence of Lemmas 3.34 and 3.36, one can prove what follows.

Proposition 3.37. *Suppose that N is free over $\mathfrak{A}(K[H], N)$. If $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$ is a ring, then $\operatorname{Ind}_H^G N$ is free over $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$.*

Remark 3.38. By (3.2), $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$ is a ring if one of the following holds:

(1) There exists a subgroup $K \leq G$ such that $G \cong H \times K$.
(2) H is contained in the center of G.
(3) $\mathfrak{A}(K[H], N) = \mathcal{O}[H]$.

In particular, in all of these cases, Proposition 3.37 allows us to conclude that $\operatorname{Ind}_H^G N$ is free over $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$ if N is free over $\mathfrak{A}(K[H], N)$.

Remark 3.39. Note that Remark 3.38(3), Proposition 3.37, and Theorem 1.39 give us a proof of Theorem 2.23.

We have already mentioned that we have an isomorphism

$$\operatorname{Ind}_H^G N \cong \operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$$

of $\mathcal{O}[G]$-modules. With Lemma 3.36 we can show the following general result, which also gives a converse to Proposition 3.37.

Proposition 3.40. *Suppose that N is a free $\mathfrak{A}(K[H], N)$-module. Then*

$$\operatorname{Ind}_H^G N \cong \operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$$

as $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$-modules.

Remark 3.41. Proposition 3.40, or more direct considerations, tells us that in fact, just assuming that N is a free $\mathfrak{A}(K[H], N)$-module, we have the compatibility

$$\mathfrak{A}(F[G], \operatorname{Ind}_H^G \mathfrak{A}(K[H], N)) = \mathfrak{A}(K[G], \operatorname{Ind}_H^G N).$$

Corollary 3.42. *Suppose that N is a free $\mathfrak{A}(K[H], N)$-module. Then $\operatorname{Ind}_H^G N$ is free over $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$ if and only if $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$ is free over $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$.*

Remark 3.43. It is not necessarily true that, if N is a free $\mathfrak{A}(K[H], N)$-module and $\operatorname{Ind}_H^G N$ a free $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$-module, then $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$ is a ring, or equivalently, that $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N) = \mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$.

Most of the above results are about deducing that $\operatorname{Ind}_H^G N$ is free over $\mathfrak{A}(F[G], \operatorname{Ind}_H^G N)$ if N is free over $\mathfrak{A}(F[H], N)$. A partial converse is given by [Ber79a, Proposition 2], as follows.

Proposition 3.44. *If $\operatorname{Ind}_H^G N$ is projective over $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$, then N is projective over $\mathfrak{A}(K[H], N)$.*

3.8. **Induction when H is normal in G.** Bergé noted that we can restate some conditions if H is normal in G. In this case we can in fact define the order

$$\mathfrak{A}(N)^* = \bigcap_{g \in G} g\mathfrak{A}(K[H], N)g^{-1} \subseteq K[H].$$

Then, using (3.2), one can verify that $\operatorname{Ind}_H^G \mathfrak{A}(N)^* = \mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$ and the following lemma.

Lemma 3.45. *Suppose H is normal in G. Then $\operatorname{Ind}_H^G \mathfrak{A}(F[H], N)$ is a ring if and only if $\mathfrak{A}(F[H], N) = \mathfrak{A}(N)^*$.*

The following result, which is [Ber79a, Proposition 3], tells us something more specific than Proposition 3.44.

Proposition 3.46. *Suppose that H is normal in G. Then $\operatorname{Ind}_H^G N$ is projective over $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$ if and only if N is projective over $\mathfrak{A}(N)^*$.*

3.9. **Induction when H is abelian and normal in G.** We continue to assume the hypotheses and notation of this section. Recall that, if H is abelian and $\mathcal{O}$ is a discrete valuation ring with characteristic zero and finite residue field, then every $\mathcal{O}$-order Λ in $K[H]$ is clean; this implies that in this setting N is projective over $\mathfrak{A}(N)^*$ if and only if it is free. We obtain [Ber79a, Corollaire to Proposition 3] as a consequence, as follows.

Proposition 3.47. *Suppose that $\mathcal{O}$ is a discrete valuation ring with characteristic zero and finite residue field, H is normal in G, and H is abelian. Then the following are equivalent:*

1. $\operatorname{Ind}_H^G N$ *is projective over* $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$.
2. $\operatorname{Ind}_H^G N$ *is free over* $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$.
3. $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$ *is a ring, and* $\operatorname{Ind}_H^G N$ *is free over* $\operatorname{Ind}_H^G \mathfrak{A}(K[H], N)$.
4. N *is free over* $\mathfrak{A}(K[H], N)$*, and* $\mathfrak{A}^* = \mathfrak{A}(K[H], N)$.

Proof. From Proposition 3.46, if (1) holds, then N is projective over $\mathfrak{A}(N)^*$. But the latter is a clean order and so we have freeness. We conclude that (1) implies (4), since $\mathfrak{A}(N)^*$ now has to be the associated order.

By Lemma 3.45 and Proposition 3.37, (4) implies (3).

We derive that (3) implies (2), for instance, from the last sentence of Lemma 3.34.

Finally, it is clear that (2) implies (1). □

Let us write an application of what we have done above. With the notation and results we have introduced, we are now able to have a quite good understanding of local freeness in weakly ramified extensions.

Proposition 3.48. *Let L/K be a finite Galois extension of number fields with Galois group G, and let $\mathfrak{P}$ and $\mathfrak{p}$ be primes of $\mathcal{O}_L$ and $\mathcal{O}_K$, respectively, such that $\mathfrak{P}$ lies above $\mathfrak{p}$ and $L_\mathfrak{P}/K_\mathfrak{p}$ is wildly and weakly ramified. If the inertia subgroup $G_0 = G_0(\mathfrak{P}|\mathfrak{p})$ is normal in G, then $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{p}}$. If the decomposition subgroup $D = D(\mathfrak{P}|\mathfrak{p})$ is abelian and normal in G, then G_0 is normal in G if and only if $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{p}}$.*

Proof. By Theorem 3.13, we know that

$$\mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}} = \mathcal{O}_{K_\mathfrak{p}}[D]\left[\frac{1}{\pi_{K_\mathfrak{p}}}\operatorname{Tr}_{G_0}\right] = \mathcal{O}_{K_\mathfrak{p}}[D] + \frac{1}{\pi_{K_\mathfrak{p}}}\mathcal{O}_{K_\mathfrak{p}}[D]\cdot\operatorname{Tr}_{G_0};$$

hence we can show that

$$\operatorname{Ind}_D^G \mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}} = \mathcal{O}_{K_\mathfrak{p}}[G] + \frac{1}{\pi_{K_\mathfrak{p}}}\mathcal{O}_{K_\mathfrak{p}}[G]\cdot\operatorname{Tr}_{G_0}.$$

It is not difficult to see that $\operatorname{Ind}_D^G \mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}}$ is a ring if and only if G_0 is normal in G. The first statement now follows from Theorem 3.13 and Proposition 3.37, the second one from Proposition 3.47. □

4. Explicit Galois module structure of weakly ramified extensions of p-adic fields

The main reference for this section is Johnston's paper [Joh15]. We fix a Galois extension L/K of p-adic fields with Galois group G. Denote by $\mathfrak{p}$ and $\mathfrak{P}$ the primes of $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively. Write v_K and v_L for the valuations of $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively.

Remark 4.1. All the results of this section work also when L and K are *local fields*, that is, locally compact topological fields with respect to a nondiscrete topology, with the additional hypothesis that the residue fields are finite.

We are interested in the following objects:

(1) for all $n \in \mathbb{Z}$, $\mathfrak{P}^n$ as $\mathcal{O}_K[G]$-module;
(2) $\mathcal{O}_L$ as $\mathfrak{A}_{L/K}$-module.

Remark 4.2. For all $n \in \mathbb{Z}$, $\mathfrak{P}^n$ is an $\mathcal{O}_K$-lattice in L, and since $\mathcal{O}_K$ is a discrete valuation ring, we deduce that $\mathfrak{P}^n$ is a free $\mathcal{O}_K$-module of rank $[L : K]$. In particular, if $\mathfrak{P}^n$ is a free $\mathcal{O}_K[G]$-module, then it has rank one, and with the usual argument (see Remark 1.8), the condition $\mathfrak{P}^n = \mathcal{O}_K[G] \cdot \alpha$, for some $\alpha \in \mathfrak{P}^n$, is enough to ensure that $\mathfrak{P}^n$ is free over $\mathcal{O}_K[G]$ with generator α.

Recall that, for all $i \geq -1$, we can define the ramification groups as follows:

$$G_i = \{\sigma \in G \mid (\sigma - 1)(\mathcal{O}_L) \subseteq \mathfrak{P}^{i+1}\}.$$

The following holds

(1) L/K is unramified if and only if $G_0 = 1$.
(2) L/K is tamely ramified if and only if $G_1 = 1$ (Corollary 2.5).
(3) L/K is weakly ramified if and only if $G_2 = 1$ (Definition 2.6).

Definition 4.3. The *different* $\mathcal{D}_{L/K}$ of L/K is the integral ideal of $\mathcal{O}_L$ defined as follows:

$$\mathcal{D}_{L/K}^{-1} = \{x \in L \mid \mathrm{Tr}_{L/K}(xy) \in \mathcal{O}_K \text{ for all } y \in \mathcal{O}_L\}.$$

Proposition 4.4 (Hilbert's formula)**.** *The following equality holds:*

$$v_L(\mathcal{D}_{L/K}) = \sum_{i=0}^{\infty}(|G_i| - 1).$$

Proof. See [Ser79, Chapter IV, Proposition 4] □

Remark 4.5. The infinite sum in Proposition 4.4 makes sense, since $|G_i| = 1$ for i sufficiently large.

Theorem 4.6. *Suppose that L/K is tamely ramified. Then for all $n \in \mathbb{Z}$, $\mathfrak{P}^n$ is free over $\mathcal{O}_K[G]$.*

For $n = 0$, Theorem 4.6 coincides with Theorem 1.39, and it is usually attributed to Noether, even if she only stated and proved in [Noe32] the result in the case that the residue characteristic of K does not divide $|G|$, as pointed out in [Cha96, section 1]. The general case is proved in [Ull70].

We briefly review part of the proof for $n = 0$.

Unramified case: if L/K is unramified, then there is a natural identification of G with the Galois group of the residue fields extension $G = \mathrm{Gal}(k_L/k_K)$. By Normal basis Theorem (Theorem 1.5), there exists $\overline{\beta} \in k_L$ such that $k_L = k_K[G] \cdot \overline{\beta}$. Using Nakayama's Lemma, for any lift $\beta \in \mathcal{O}_L$ of $\overline{\beta}$, $\mathcal{O}_L = \mathcal{O}_K[G] \cdot \beta$. (This actually can be made in an if and only if statement.)

Totally and tamely ramified case: if L/K is totally and tamely ramified with $e = [L : K]$, then we can find uniformisers $\pi_L \in \mathcal{O}_L$ and $\pi_K \in \mathcal{O}_K$ such that $\pi_L^e = \pi_K$ and $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$. If $\alpha \in \mathcal{O}_L$, then

$$\alpha = u_0 + u_1\pi_L + \cdots + u_{e-1}\pi_L^{e-1},$$

for some $u_i \in \mathcal{O}_K$. Then $\mathcal{O}_L = \mathcal{O}_K[G] \cdot \alpha$ if and only if $u_i \in \mathcal{O}_K^\times$ for every i. This part uses that π_L is a Kummer generator and some determinant calculations.

Tamely ramified case: if L/K is tamely ramified, then we can "glue" the two previous cases together, with an idea of Kawamoro; see [Kaw86].

4.1. **Weakly ramified extensions.** We consider now the weakly ramified case. Two main results are given by Ullom [Ull70] and Köck [Köc04].

Theorem 4.7 (Ullom)**.**

- *If there exists $n \in \mathbb{Z}$ such that $\mathfrak{P}^n$ is free over $\mathcal{O}_K[G]$, then L/K is weakly ramified.*
- *If L/K is totally and weakly ramified, then $\mathfrak{P}$ is free over $\mathcal{O}_K[G]$.*

Theorem 4.8 (Köck)**.** *The fractional ideal $\mathfrak{P}^n$ is free over $\mathcal{O}_K[G]$ if and only if L/K is weakly ramified and $n \equiv 1 \pmod{|G_1|}$.*

The proof of Theorem 4.8 uses cohomological triviality argument; Erez's work in [Ere91] on square root of inverse different uses similar ideas.

Theorem 4.9 (Johnston)**.** *Suppose that L/K is weakly ramified. Let $n \in \mathbb{Z}$ such that $n \equiv 1 \pmod{|G_1|}$. Then we can explicitly construct ε such that $\mathfrak{P}^n = \mathcal{O}_K[G] \cdot \varepsilon$.*

Proof. We just give an idea of this proof.

We can explicitly construct generators in the following cases:

(1) unramified (Theorem 1.37);
(2) totally and tamely ramified (Theorem 1.38);
(3) totally and weakly ramified p-extensions.

Then we can use a "splitting lemma" (see [Joh15, Section 3]), and "glue" generators together. Finally, we can take the trace to find the element we are looking for.

This is a generalisation of Kawamoto's approach. □

Theorem 4.10 (Johnston)**.** *Suppose that L/K is wildly and weakly ramified, and let π_K be any uniformiser of K. Then $\mathfrak{A}_{L/K} = \mathcal{O}_K[G][\pi_K^{-1} \operatorname{Tr}_{G_0}]$ and if $\mathfrak{P} = \mathcal{O}_K[G] \cdot \varepsilon$, then $\mathcal{O}_L = \mathfrak{A}_{L/K} \cdot \varepsilon$.*

Proof. Again, we just sketch an idea of the proof.

First, we can show that

$$\mathcal{O}_K[G][\pi_k^{-1} \operatorname{Tr}_{G_0}] \subseteq \mathfrak{A}_{L/K}.$$

Let ε be a free generator of $\mathfrak{P}$ over $\mathcal{O}_K[G]$ (for example, as in Theorem 4.9). Then

$$\mathcal{O}_K[G][\pi_k^{-1} \operatorname{Tr}_{G_0}] \cdot \varepsilon \subseteq \mathfrak{A}_{L/K} \cdot \varepsilon \subseteq \mathcal{O}_L. \tag{4.1}$$

We have $\mathfrak{P} = \mathcal{O}_K[G] \cdot \varepsilon \subseteq \mathcal{O}_K[G][\pi_k^{-1} \operatorname{Tr}_{G_0}]$ and $\mathfrak{P} \subseteq \mathcal{O}_L$. We can prove that the indices $[\mathcal{O}_K[G][\pi_k^{-1} \operatorname{Tr}_{G_0}] : \mathcal{O}_K[G] \cdot \varepsilon]_{\mathcal{O}_K}$ and $[\mathcal{O}_L : \mathfrak{P}]_{\mathcal{O}_K}$ are equal, and this forces equality in (4.1). □

Now we see more in details the proof of Theorem 4.9.

4.2. **Totally and weakly ramified p-extensions.** We begin with [Joh15, Theorem 5.2]

Theorem 4.11. *Suppose that L/K is a totally and weakly ramified p-extension.*

1. *G is an elementary abelian p-group.*
2. *$\mathfrak{P}^n$ is free over $\mathcal{O}_K[G]$ if and only if $n \equiv 1 \pmod{|G|}$.*
3. *Suppose $n \equiv 1 \pmod{|G|}$. Then an element $\delta \in L$ is a free generator of $\mathfrak{P}^n$ over $\mathcal{O}_K[G]$ if and only if $v_L(\delta) = n$.*

Proof.

1. This is a standard fact.
2. It follows immediately from Theorem 4.8.
3. This was already shown by others: Vostokov [Vos81], Vinaties (in [Vin05], as consequence of Byott's paper [Byo99]), and Byott–Elder [BE14]. We give the idea of the proof in [Joh15], which does not use cohomology:
   (a) Use Hilbert's formula to compute the different of L/K.
   (b) Obtain a formula for $\mathrm{Tr}_{L/K}(\mathfrak{P}^n)$.
   (c) "Mod out" by $\mathfrak{p}$, working over $k_K[G]$.
   (d) Use a minor variant of a result of Childs.
   (e) Lift using Nakayama's lemma. □

Example 4.12. Let $K/\mathbb{Q}_p$ be an unramified extension, and consider $K(\zeta_{p^2})/K$. If L is the intermediate field such that L/K has degree p, then L/K is a totally and weakly ramified extension.

4.3. **Totally and tamely ramified extensions of arbitrary degree.** If L/K is totally and tamely ramified, then the Galois group G coincides with the inertia subgroup $G_0 = I$. Write $G_1 = W$, the *wild inertia*, an elementary abelian p-group. By Schur–Zassenhaus theorem, we can write $I = W \rtimes C$, where C is a cyclic group. We have the following situation:

$$\begin{tikzcd}
& L \arrow[dl, dash, "W"'] \arrow[dr, dash, "C"] \arrow[dd, dash, "I"] & \\
E \arrow[dr, dash, "C"'] & & F \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

where L/E and F/K are totally and weakly ramified p-extensions, while L/F and E/K are totally and tamely ramified extensions.

Define r by $|W| = p^r$, and let $c = |C|$. By Bézout's theorem, there exist $a, b \in \mathbb{Z}$ such that $ap^r + bc = 1$. Choose uniformisers π_E and π_K such that $\pi_E^c = \pi_K$, and any uniformiser π_F of F. Finally, let $\alpha = 1 + \pi_E + \pi_E^2 + \cdots + \pi_E^{c-1}$.

Proposition 4.13. *The element $\pi_F^b \pi_E^a \alpha$ is a free generator of $\mathfrak{P}$ over $\mathcal{O}_K[I]$.*

Proof. This is a special case of [Joh15, Proposition 6.1]. We just give a sketch of the proof.

The following facts hold:

1. Since $v_L(\pi_F^b \pi_E^a) = 1$, $\mathfrak{P} = \mathcal{O}_E[W] \cdot (\pi_F^b \pi_E^a)$.
2. $\pi_E^a \mathcal{O}_E = \mathcal{O}_K[C] \cdot (\pi_E^a \alpha)$.

With explicit calculation, using semidirect product and that $\pi_F \in F = L^C$ and $\pi_E, \alpha \in E = L^W$, we can derive our assertion. □

Remark 4.14. If L/K is abelian, totally and wildly ramified, and not a p-extension, then L/K cannot be weakly ramified.

Example 4.15.

(1) Suppose that p is odd. Consider the extension $\mathbb{Q}_p(\zeta_{p^2})/\mathbb{Q}_p$, and let L be an intermediate field such that $\mathbb{Q}_p(\zeta_{p^2})/K$ has degree $p-1$ and $L/\mathbb{Q}_p$ has degree p. Then $L/\mathbb{Q}_p$ is weakly ramified, $\mathbb{Q}_p(\zeta_{p^2})/L$ is tame, but $\mathbb{Q}_p(\zeta_{p^2})/\mathbb{Q}_p$ is not weakly ramified (see [Ser79, Chapter IV, Proposition 18]). This is [Joh15, Remark 6.2], where we remark there is a typo.

(2) The extension $\mathbb{Q}_3(\zeta_3, \sqrt[3]{2})/\mathbb{Q}_3$ has Galois group isomorphic to S_3 and is totally and weakly ramified.

5. Almost maximal ramification, dihedral extensions, A_4-, S_4-, A_5-extensions

In this section, we focus again the problems introduced in Section 3. We begin with some clarifications.

5.1. **Local versions of global results.** We have seen how Leopoldt's, Bergé's, and Martinet's works imply that if $L/\mathbb{Q}$ is abelian or dihedral of degree $2p$ or Q_8-extension (wild in the last case), then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$. Can we immediately derive the corresponding result for local fields, so for an extension $K/\mathbb{Q}_p$ with the same Galois group?

(1) The local result about dihedral extensions of degree $2p$ is already contained in [Ber72].

(2) As concerns abelian and Q_8-extensions of $\mathbb{Q}$, it seems natural (and folklore) that the proofs for the global case work as they are in the local case. For example, this is immediate for Q_8-extensions.

(3) By a (nontrivial) result of G. Henniart [Hen01], if $p \neq 2$, then given a finite Galois extension $K/\mathbb{Q}_p$, there exists a Galois extension $L/\mathbb{Q}$ with the same Galois group, such that $L_{\mathfrak{P}} = K$, where $\mathfrak{P}$ is the unique prime of L above p. In particular, if $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$, then $\mathcal{O}_{L,p} \cong \mathcal{O}_K$ is free over $\mathfrak{A}_{L/\mathbb{Q},p} \cong \mathfrak{A}_{K/\mathbb{Q}_p}$. Note that we know this is false for $p = 2$. In our specific cases, we can verify through databases the global realisability of Q_8-extensions of $\mathbb{Q}_2$, and we can find a cyclotomic extension M (which is easily globally realisable) containing K such that M/K is tamely ramified if $K/\mathbb{Q}_p$ is abelian; compare with [Joh11, subsection 12.3].

(4) In a simpler way, the work in [Let98] immediately implies the p-adic version of Leopoldt's theorem.

5.2. **Back to our scheme.** Let L/K be a Galois extension of number fields with Galois group G. Fix a prime $\mathfrak{p}$ of $\mathcal{O}_K$ and a prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$. If $D = D(\mathfrak{P}|\mathfrak{p})$ is the decomposition group, then $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is a Galois extension with Galois group D. We identify $\mathcal{O}_{L,\mathfrak{p}} = \operatorname{Ind}_D^G \mathcal{O}_{L_{\mathfrak{P}}}$ and $\mathfrak{A}_{L/K,\mathfrak{p}} = \mathfrak{A}(K_{\mathfrak{p}}[G], \operatorname{Ind}_D^G \mathcal{O}_{L_{\mathfrak{P}}})$. We know the following facts.

(1) If $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$, then $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{p}}$.

(2) If $\mathcal{O}_{L,\mathfrak{q}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{q}}$ for all primes $\mathfrak{q}$ of $\mathcal{O}_K$ and $\mathrm{Cl}(\mathfrak{A}_{L/K}) = 0$, then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$.

(3) If $\mathcal{O}_{L,\mathfrak{p}}$ is projective over $\mathfrak{A}_{L/K,\mathfrak{p}}$, then $\mathcal{O}_{L_\mathfrak{P}}$ is projective over $\mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}}$ (Proposition 3.44). In particular, if projective implies free over $\mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}}$, then we deduce that if $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{p}}$, then $\mathcal{O}_{L_\mathfrak{P}}$ is free over $\mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}}$.

(4) If $\mathcal{O}_{L_\mathfrak{P}}$ is free over $\mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}}$ and $\mathrm{Ind}_D^G \mathfrak{A}_{L_\mathfrak{P}/k_\mathfrak{p}}$ is a ring (Proposition 3.37) or more generally $\mathrm{Ind}_D^G \mathfrak{A}_{L_\mathfrak{P}/L_\mathfrak{p}}$ is free over $\mathfrak{A}(K_\mathfrak{p}[G], \mathrm{Ind}_D^G \mathcal{O}_{L_\mathfrak{P}})$ (Corollary 3.42), then $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{p}}$.

We call implication $(*)$ the implication "if $\mathcal{O}_{L_\mathfrak{P}}$ is free over $\mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}}$ then $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{p}}$", and implication $(**)$ the implication "if $\mathcal{O}_{L,\mathfrak{q}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{q}}$ for all primes $\mathfrak{q}$ of $\mathcal{O}_K$, then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$".

We have a more general result. Note that we have a natural inclusion $K_\mathfrak{p}[D] \subseteq K_\mathfrak{p}[G]$.

Proposition 5.1. *Let Λ be an $\mathcal{O}_{K_\mathfrak{p}}$-order in $K_\mathfrak{p}[D]$, let N be a Λ-lattice, and let Γ be an $\mathcal{O}_{K_\mathfrak{p}}$-order in $K_\mathfrak{p}[G]$ such that $\Lambda \subseteq \Gamma \subseteq \bigoplus_{t \in H \diagdown G} \Lambda t$. If $\mathrm{Ind}_D^G N$ is projective over Γ, then N is projective over Λ.*

We can apply immediately Proposition 5.1 with $\Lambda = \mathcal{O}_{K_\mathfrak{p}}[D]$ and $\Gamma = \mathcal{O}_{K_\mathfrak{p}}[G]$, as $\mathrm{Ind}_D^G \mathcal{O}_{K_\mathfrak{p}}[D] = \mathcal{O}_{K_\mathfrak{p}}[G]$.

Theorem 5.2. *Let L/K be a Galois extension of number fields with Galois group G. Then the following are equivalent:*

(1) *L/K is tamely ramified.*
(2) *$\mathcal{O}_L$ is projective over $\mathcal{O}_K[G]$.*
(3) *$\mathcal{O}_L$ is locally free over $\mathcal{O}_K[G]$.*
(4) *$\mathcal{O}_K[G] = \mathfrak{A}_{L/K}$.*

Proof. We already know that (1) implies (3). For a proof, see Remark 3.39.

For (1) implies (4), note that tameness implies that $\mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}} = \mathcal{O}_{K_\mathfrak{p}}[D(\mathfrak{P}|\mathfrak{p})]$ for every primes $\mathfrak{P}|\mathfrak{p}$ in L/K with decomposition group $D(\mathfrak{P}|\mathfrak{p})$; therefore, $\mathfrak{A}_{L/K,\mathfrak{p}} = \mathcal{O}_{K_\mathfrak{p}}[G]$. From the local equality of $\mathcal{O}_K[G]$ and $\mathfrak{A}_{L/K}$ at every prime $\mathfrak{p}$ we deduce global equality; see [Rei03, Theorem 5.3].

Now we show the equivalence between (1) and (2). If L/K is tamely ramified, by Theorem 2.23, $\mathcal{O}_L$ is locally free over $\mathcal{O}_F[G]$, and so $\mathcal{O}_{L,\mathfrak{p}}$ is projective over $\mathcal{O}_{K_\mathfrak{p}}$ for every prime $\mathfrak{p}$ of $\mathcal{O}_K$. Since locally projective for every maximal ideal implies projective (see [CR81, Proposition 8.19]), we conclude that $\mathcal{O}_L$ is projective over $\mathcal{O}_K[G]$. Conversely, if $\mathcal{O}_L$ is projective over $\mathcal{O}_K[G]$, then $\mathcal{O}_{L,\mathfrak{p}}$ is projective over $\mathcal{O}_{K_\mathfrak{p}}[G]$ for every prime $\mathfrak{p}$ of $\mathcal{O}_K$. If $\mathfrak{P}$ is any prime of $\mathcal{O}_L$ above $\mathfrak{p}$, and $D = D(\mathfrak{P}|\mathfrak{p})$ is the decomposition group, then by Proposition 5.1, $\mathcal{O}_{L_\mathfrak{P}}$ is projective over $\mathcal{O}_{K_\mathfrak{p}}[D]$, which is clean, and so $\mathcal{O}_{L_\mathfrak{P}}$ is free over $\mathcal{O}_{K_\mathfrak{p}}[D]$, that is, L/K is tamely ramified at $\mathfrak{p}$ for all primes $\mathfrak{p}$ of $\mathcal{O}_K$.

It is clear that (3) implies (2) from the already used fact that locally projective implies projective.

It is now sufficient to show that (4) implies(3). If we assume (4), in particular for all primes $\mathfrak{p}$ of $\mathcal{O}_K$ we know that $\mathfrak{A}_{L/K,\mathfrak{p}} = \mathcal{O}_{K_\mathfrak{p}}[G]$. Let us fix a prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying above $\mathfrak{p}$ and let D be the corresponding decomposition group. Then by the results in Section 3 we have that $\mathfrak{A}_{L/K,\mathfrak{p}} \cong \mathfrak{A}(K_\mathfrak{p}[G], \mathcal{O}_{L,\mathfrak{p}})$ and

$$\mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}} \subseteq \mathfrak{A}(K_\mathfrak{p}[G], \mathcal{O}_{L,\mathfrak{p}}) \cap K_\mathfrak{p}[D] = \mathcal{O}_{K_\mathfrak{p}}[G] \cap K_\mathfrak{p}[D] = \mathcal{O}_{K_\mathfrak{p}}[D].$$

We deduce that $\mathfrak{A}_{L_{\mathfrak{P}}/K_{\mathfrak{p}}} = \mathcal{O}_{K_{\mathfrak{p}}}[D]$, and hence $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is tamely ramified by Theorem 1.39 and Proposition 2.12.

□

5.3. **More on** $(*)$**.** In the previous setting, take $K = \mathbb{Q}$, and suppose that both $G = \mathrm{Gal}(L/\mathbb{Q})$ and $D = \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_p)$ are dihedral. Suppose also that $L_{\mathfrak{P}}/\mathbb{Q}_p$ is almost maximally ramified. Then, by Theorem 3.16, $\mathcal{O}_{L_{\mathfrak{P}}}$ is free over $\mathfrak{A}_{L_{\mathfrak{P}}/K_p} = \mathcal{O}_K[D][\{e_{D_i}\}_{i\geq 1}]$, where the $\{D_i\}_{i\geq 1}$ are (some of) the higher ramification subgroups of D. If $\mathrm{Ind}_D^G \mathfrak{A}_{L_{\mathfrak{P}}/\mathbb{Q}_p}$ is a ring, then, by Proposition 3.37, $\mathcal{O}_{L,p}$ is free over $\mathfrak{A}_{L/\mathbb{Q},p}$. This is the case, for example, if D_i is normal in G for all i, that is, $G \cong N \rtimes C_2$ with $D_1 \subseteq N$. We deduce the following result.

Theorem 5.3. *If both $G = \mathrm{Gal}(L/\mathbb{Q})$ and $D = \mathrm{Gal}(L_{\mathfrak{P}}/\mathbb{Q}_p)$ are dihedral, $L_{\mathfrak{P}}/\mathbb{Q}_p$ is almost maximally ramified, and $G = N \rtimes C_2$ with $D_1 \subseteq N$, then $\mathcal{O}_L$ is locally free at p over $\mathfrak{A}_{L/\mathbb{Q}}$.*

Recall that the more general Theorem 3.16 yields a complete classification on when we have local freeness in dihedral extensions of $\mathbb{Q}$.

Let now $L/\mathbb{Q}$ be an A_4-extension. Consider prime $\mathfrak{P}$ of $\mathcal{O}_L$ lying above the prime number 2. By Theorem 3.24, $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$ if and only if 2 is tamely ramified or has full decomposition group in L. Let us study what happens in the negative case.

If 2 is not tamely ramified and its decomposition group D is not the whole Galois group G, then either $D = V_4$, the Klein subgroup normal in A_4, or D is isomorphic to C_2. In particular, there are three possibilities for the couple (D, D_0) modulo isomorphism class:

- (V_4, V_4),
- (V_4, C_2),
- (C_2, C_2).

Assume that $(D, D_0) = (V_4, C_2)$. Our claim is that $\mathcal{O}_{L,2}$ is not free over $\mathfrak{A}_{L/\mathbb{Q},2}$, and so $\mathcal{O}_L$ is not free over $\mathfrak{A}_{L/\mathbb{Q}}$. It is not hard to show that

$$\mathfrak{A}_{L_{\mathfrak{P}}/\mathbb{Q}_2} = \mathbb{Z}_2[V_4] + \frac{1}{2}\mathbb{Z}_2[V_4] \cdot \mathrm{Tr}_{D_0},$$

hence

$$\mathrm{Ind}_{V_4}^{A_4} \mathfrak{A}_{L_{\mathfrak{P}}/\mathbb{Q}_2} = \mathbb{Z}_2[A_4] + \frac{1}{2}\mathbb{Z}_2[A_4] \cdot \mathrm{Tr}_{D_0}.$$

Now $D_0 = C_2$ is not normal in A_4, and this implies that $\mathrm{Ind}_{V_4}^{A_4} \mathfrak{A}_{L_{\mathfrak{P}}/\mathbb{Q}_2}$ is not a ring. This in general is not enough to get our claim, but since V_4 is abelian and normal in A_4, we can derive our assertion from the equivalence between (2) and (3) in Proposition 3.47.

Remark 5.4. Let K be a p-adic field, let G be a finite group, let H be a subgroup of G, and let N be an $\mathcal{O}_K[H]$-lattice in $K[H]$. Assume that

$$\mathfrak{A}(K[H], N) = \sum_{i=0}^{r} \frac{1}{\pi^{n_i}} \mathcal{O}_K[H] \cdot \mathrm{Tr}_{T_i},$$

where π is an uniformiser of $\mathcal{O}_K$ and T_i is a subgroup of H for all i, with $1 = T_0 \subsetneq T_1 \subsetneq \cdots \subsetneq T_r$ and $0 = n_0 < n_1 < \cdots < n_r$. Then we have

$$\mathrm{Ind}_H^G \mathfrak{A}(K[H], N) = \sum_{i=0}^{r} \frac{1}{\pi^{n_i}} \mathcal{O}_K[G] \cdot \mathrm{Tr}_{T_i},$$

and this is a ring if and only if T_i is normal in G for every i. (This means that if also N is free over its associated order, then $\operatorname{Ind}_H^G N$ is free over its associated order.)

Also, we have

$$\mathfrak{A}(K[H], \operatorname{Ind}_H^G N) = \sum_{i=0}^{r} \frac{1}{\pi^{n_i}} \mathcal{O}_K[G] \cdot \operatorname{Tr}_{U_i},$$

where, for all i, U_i is the normal closure of T_i. Assume also that H is abelian and normal in G. If $\operatorname{Ind}_H^G N$ is projective over $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$, then B_i is normal in G for all i, N is free over $\mathfrak{A}(K[H], N)$, and $\operatorname{Ind}_H^G N$ is free over $\mathfrak{A}(K[G], \operatorname{Ind}_H^G N)$.

5.4. **More on** $(**)$**.** Recall that if $L/\mathbb{Q}$ is a finite Galois extension with Galois group G and $\operatorname{Cl}(\mathbb{Z}[G]) = 0$, then we automatically have locally free cancellation, and $L/\mathbb{Q}$ admits a normal integral basis.

Theorem 5.5. *Let $L/\mathbb{Q}$ a finite Galois extension with Galois group G such that $\operatorname{Cl}(\mathbb{Z}[G]) = 0$. If $\mathcal{O}_L$ is locally free over $\mathfrak{A}_{L/\mathbb{Q}}$, then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$.*

Proof. Clearly, if $\operatorname{Cl}(\mathfrak{A}_{L/\mathbb{Q}}) = 0$, then we immediately derive our assertion. The result follows from a surjection $\operatorname{Cl}(\mathbb{Z}[G]) \twoheadrightarrow \operatorname{Cl}(\mathfrak{A}_{L/\mathbb{Q}})$ induced by the injection $\mathbb{Z}[G] \hookrightarrow \mathfrak{A}_{L/\mathbb{Q}}$; see [CR87, Theorem 50.29]. □

Corollary 5.6. *Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G isomorphic to D_{2n} (and in this case assume also $\operatorname{Cl}(\mathbb{Z}[D_{2n}]) = 0$), A_4, S_4, or A_5. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$ if and only if $\mathcal{O}_L$ is locally free over $\mathfrak{A}_{L/\mathbb{Q}}$.*

Note that Theorem 3.21 is a corollary of Theorem 5.5.

5.5. **Maximal orders.** Let K be a field with characteristic 0, and let G be a finite group. Since $K[G]$ is separable, by Wedderburn's decomposition theorem, we can write

$$K[G] \cong \prod_i \operatorname{Mat}_{n_i}(D_i),$$

where for all i, D_i is a skew-algebra; see [CR81, section 3B]. If we also assume that G is abelian, we find that

$$K[G] \cong \prod_{\gamma \in \Phi} K(\gamma),$$

where Φ is a certain class of characters $\gamma\colon G \to \overline{K}^{\times}$ from the group G to the nonzero elements of the algebraic closure of K.

If K is a number field or a p-adic field, we would like to have the isomorphism between $\mathcal{O}_K[G]$ and $\prod_{\gamma\in\Phi} \mathcal{O}_{K(\gamma)}$. However, this is false in general: on the right-hand side we have a maximal order, while usually $\mathcal{O}_K[G]$ is not maximal.

Definition 5.7. Let K be a number field or a p-adic field, and G let be a finite group. An $\mathcal{O}_K$-order Γ is *maximal* in $K[G]$ if Γ maximal with respect to the inclusion.

The following meaningful result requires some work to be proved.

Proposition 5.8. *Every $\mathcal{O}_K$-order is contained in a maximal order.*

Proof. See [CR81, section 26] □

Remark 5.9. If G is abelian, then there exists a unique maximal order, which is the integral closure of $\mathcal{O}_K$ in $K[G]$, that is, $\prod_{\gamma\in\Phi}\mathcal{O}_{K(\gamma)}$.

Proposition 5.10. *The $\mathcal{O}_K$-order $\mathcal{O}_K[G]$ is maximal if and only if $|G|$ is invertible in $\mathcal{O}_K$.*

Proof. See [CR81, Proposition 27.1]. □

Corollary 5.11.

- *If K is a number field and $G \neq 1$, then $\mathcal{O}_K[G]$ is not a maximal order.*
- *If K is a p-adic field, then $\mathcal{O}_K[G]$ is a maximal order if and only if $p \nmid |G|$.*

Theorem 5.12. *Let K be a p-adic field, and let G be a finite group. Let $\mathcal{M}$ be a maximal $\mathcal{O}_K$-order, and let M be an $\mathcal{M}$-lattice such that $K \otimes_{\mathcal{O}_K} M$ is free over $K[G]$. Then M is free over $\mathcal{M}$.*

Proof. See [Rei03, Theorem 18.10]. □

Corollary 5.13. *Let K be a p-adic field, and let G be a finite group. Then a maximal $\mathcal{O}_K$-order in $K[G]$ is clean.*

Corollary 5.14. *Let L/K be a Galois extension of p-adic fields. If $\mathfrak{A}_{L/K}$ is maximal, then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$.*

Corollary 5.15. *Let L/K Galois extension of number fields, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$. If $\mathfrak{A}_{L/K,\mathfrak{p}}$ is maximal, then $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{p}}$.*

Combining Corollaries 5.11 and 5.15, we deduce that if L/K is a Galois extension of number fields with Galois group G, and $\mathfrak{p}$ is a prime of $\mathcal{O}_K$ such that the prime number p under $\mathfrak{p}$ does not divide $|G|$, then $\mathcal{O}_{F_\mathfrak{p}}[G]$ is maximal and contained in $\mathfrak{A}_{L/K,\mathfrak{p}} = \mathcal{O}_{F_\mathfrak{p}}[G]$, hence $\mathfrak{A}_{L/K,\mathfrak{p}}$ is maximal and $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{p}}$. Indeed, the extension is tamely ramified at $\mathfrak{p}$.

The following result is given in [Let98].

Proposition 5.16 (Lettl)**.** *Let p be an odd prime number, let $L/\mathbb{Q}_p$ be a finite abelian extension, and let K an intermediate field such that L/K is totally ramified. Then $\mathfrak{A}_{L/K}$ is maximal. In particular, $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$.*

The maximal orders are linked with almost-maximal ramification.

Remark 5.17. Let L/K is a Galois extension of p-adic field with Galois group G, let $\mathfrak{P}$ be the prime of $\mathcal{O}_L$, and let H is a subgroup of G. If M is the fixed field of H, then we have the following equivalences, where we employ [Ser79, Proposition III.7] and Proposition 4.4):

$$\begin{aligned}\frac{1}{|H|}\operatorname{Tr}_H \in \mathfrak{A}_{L/K} &\iff \frac{1}{|H|}\operatorname{Tr}_H(\mathcal{O}_L) \subseteq \mathcal{O}_M\\ &\iff \operatorname{Tr}_H(\mathcal{O}_L) \subseteq |H|\mathcal{O}_M \iff \mathcal{O}_L \subseteq |H|\mathcal{O}_M\mathcal{D}_{L/M}^{-1}\\ &\iff \mathcal{D} \subseteq |H|\mathcal{O}_L \iff v_\mathfrak{P}(\mathcal{D}_{L/M}) \geq e(L/\mathbb{Q}_p)\cdot v_p(|H|)\\ &\iff \sum_{i=1}^{\infty}(|H_i|-1) \geq e(L/\mathbb{Q}_p)\cdot v_p(|H|).\end{aligned}$$

This gives us an explicit way to check if the idempotent corresponding to a subgroup of G is in the associated order.

Following [Ber78], we introduce the ramification jumps and see their relation with maximal orders.

Definition 5.18. Let L/K be a Galois extension of p-adic fields with Galois group G. An integer $t \geq 1$ is a *ramification jump* if $G_t \supsetneq G_{t+1}$. Write

$$1 \leq t_1 < t_2 < \cdots < t_m$$

for the ramification jumps of L/K.

We can find explicit information about the ramification jumps in appropriate settings; for example, the next result is [Ber78, Proposition 3 and Corollaire]

Proposition 5.19 (Bergé)**.** *Let L/K be a Galois extension of p-adic fields with Galois group G, and assume thta G_1 is cyclic of order p^n and $K/\mathbb{Q}_p$ is unramified. Write $r = [G_0 : G_1]$. Then*

$$\frac{r}{p-1} \leq t_1 \leq \frac{rp}{p-1}$$

and for all $i = 2, \dots, n$,

$$t_i = \frac{rp^i}{p-1} - \frac{rp}{p-1} + t_1.$$

In particular, L/K is almost maximally ramified if and only if there exists $G_i \neq 1$ such that $e_{G_i} \in \mathfrak{A}_{L/K}$, if and only if $t_1 \geq \frac{rp}{p-1} - 1$.

One might aim to prove that in an almost maximally ramified extension of p-adic fields, given we have a certain number of idempotents in the associated order by definition, the associated order has to be maximal. We state now [Ber78, Proposition 5], which implies that under some conditions this is the case.

Proposition 5.20. *Let L/K be a Galois extension of p-adic fields with Galois group G. Assume that G is cyclic of order rp^n and $K/\mathbb{Q}_p$ is unramified. Consider, for all i, a subgroup H_i of G such that $|H_i| = p^i$. Then the maximal $\mathcal{O}_K$-order in $K[G]$ is $\mathcal{O}_F[G][\{e_{H_i}\}_{i=0}^n]$.*

Corollary 5.21. *Let L/K be a totally ramified cyclic extension of p-adic fields such that $K/\mathbb{Q}_p$ is unramified. If L/K is almost maximally ramified, then $\mathfrak{A}_{L/K}$ is maximal.*

We complete the subsection giving the main result proved in [Ber78].

Theorem 5.22 (Bergé)**.** *Let L/K be a totally ramified cyclic extension of p-adic fields such that $K/\mathbb{Q}_p$ is unramified. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$ if and only if*

$$t_1 > \frac{rp}{p-1} - \frac{p^n}{p^{n-1} - 1}.$$

Remark 5.23. If the extension is not totally ramified and G_0 is cyclic, there are some sufficient conditions to get the statement of Theorem 5.22; see [Ber78, section 2.3].

5.6. **Return to local freeness: hybrid orders.** Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G, and let p be a prime number. Our goal is to determine criteria so that $\mathcal{O}_{L,p}$ is free over $\mathfrak{A}_{L/\mathbb{Q},p}$ without the latter being a maximal order. The idea is to write $\mathfrak{A}_{L/\mathbb{Q},p}$ in the form $\mathfrak{A}_{M/\mathbb{Q},p} \times \mathcal{M}$, where $M/\mathbb{Q}$ is an intermediate Galois extension and $\mathcal{M}$ is a maximal order.

Let N be a normal subgroup of G such that $p \nmid |N|$. Then e_N is a central idempotent in $\mathbb{Z}_p[G]$ and we have the following decomposition of rings:

$$\mathbb{Z}_p[G] = e_N\mathbb{Z}_p[G] \times (1-e_N)\mathbb{Z}_p[G] \cong \mathbb{Z}_p[G/N] \times (1-e_N)\mathbb{Z}_p[G].$$

The next definition was first introduced in [JN16].

Definition 5.24. Let p be a rational prime, let G be a finite group, and let N be a normal subgroup of G such that $p \nmid |N|$. We say that $\mathbb{Z}_p[G]$ is *N-hybrid* if the component $(1-e_N)\mathbb{Z}_p[G]$ of $\mathbb{Z}_p[G]$ is a maximal $\mathbb{Z}_p$-order in $(1-e_N)\mathbb{Q}_p[G]$.

The following result is easy to prove; the key is Theorem 5.12.

Proposition 5.25. *Let $L/\mathbb{Q}$ be a finite Galois extension with Galois group G, and let p be a prime number. Let N be a normal subgroup of G such that $p \nmid |N|$, and let M the subfield of L fixed by N. Suppose that $\mathbb{Z}_p[G]$ is N-hybrid. Then*

$$\mathfrak{A}_{L/\mathbb{Q},p} \cong \mathfrak{A}_{M/\mathbb{Q},p} \times (1-e_N)\mathbb{Z}_p[G]$$

and $\mathcal{O}_{L,p} \cong \mathcal{O}_{M,p} \oplus (1-e_N)\mathcal{O}_{L,p}$ is free over $\mathfrak{A}_{L/\mathbb{Q},p}$ if and only if $\mathcal{O}_{M,p}$ is free over $\mathfrak{A}_{M/\mathbb{Q},p}$.

Example 5.26. Let G be either A_4 or S_4. Note that we can write G as $V_4 \rtimes H$, where H is C_3 or S_3, respectively, and V_4 is the normal subgroup of order 4, which is isomorphic to the Kein group. By [JN16, section 2], $\mathbb{Z}_3[G]$ is V_4-hybrid in both cases. Now let $L/\mathbb{Q}$ be a Galois extension with Galois group G, and let $M = L^{V_4}$. Since $M/\mathbb{Q}$ is either a C_3-extension or an S_3-extension, we know by Theorem 3.17 or Theorem 3.19 that $\mathcal{O}_M$ is free over $\mathfrak{A}_{M/\mathbb{Q}}$, so that in particular $\mathcal{O}_{M,3}$ is free over $\mathfrak{A}_{M/\mathbb{Q},3}$. By Proposition 5.25, we deduce that $\mathcal{O}_{L,3}$ is free over $\mathfrak{A}_{L/\mathbb{Q},3}$.

From Example 5.26 and Corollary 5.6 we can deduce the following fact.

Corollary 5.27. *Let $L/\mathbb{Q}$ be an A_4- or S_4-extension. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/\mathbb{Q}}$ if and only if $\mathcal{O}_{L,2}$ is free over $\mathfrak{A}_{L/\mathbb{Q},2}$.*

The conclusion of Corollary 5.27 holds if 2 is tamely ramified or for any prime $\mathfrak{P}$ of $\mathcal{O}_L$ above 2 the decomposition group $D(\mathfrak{P}|2)$ is equal to $G = \mathrm{Gal}(L/\mathbb{Q})$ and $L_{\mathfrak{P}}/\mathbb{Q}_2$ is weakly ramified, by Theorem 3.13 and Proposition 3.37 (here we are trivially inducing from G to G). Note also that there is only one A_4-extension of $\mathbb{Q}_2$, which is weakly ramified, so that if G is isomorphic to A_4, then we automatically have weak ramification assuming full decomposition group; see Theorem 3.24. We can deduce (3) and (4) of Theorem 3.25 using Proposition 3.48.

6. Galois module structure of absolutely abelian extensions of p-adic fields

The goal of this section is to discuss the following meaningful result of Lettl [Let98, Theorem 1]. Recall that a finite Galois extension of p-adic fields (resp., number fields) L/K is said *absolutely abelian* if $L/\mathbb{Q}_p$ (resp., $L/\mathbb{Q}$) is abelian. By local Kronecker–Weber theorem, all absolutely abelian extensions of a p-adic field lie in a cyclotomic extensions of $\mathbb{Q}_p$.

Theorem 6.1 (Lettl)**.** *Let L/K be an absolutely abelian extension of p-adic fields with Galois group G. Then the following facts hold:*

- *$\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$.*

- *Suppose $p \geq 3$, and let G_0 be the inertia subgroup. Then*
$$\mathfrak{A}_{L/K} \cong \mathcal{O}_K[G] \otimes_{\mathcal{O}_K[G_0]} M_0 = \operatorname{Ind}_{G_0}^G M_0,$$
where M_0 is the unique maximal $\mathcal{O}_K$-order contained in $K[G_0]$.

We wish to thank F. Campagna, who provided examples and slight generalisations of Lettl's statements and proofs. We begin with some comments.

- In general, the element $\alpha \in \mathcal{O}_L$ such that $\mathcal{O}_L = \mathfrak{A}_{L/K} \cdot \alpha$ is not explicit. However, there are cases in which it can be explicitly computed; for example, when $N \subseteq \mathbb{Q}_p(\zeta_{p^n})$ for some $n \in \mathbb{N}$.
- One can give an explicit description of $\mathfrak{A}_{L/K}$ also in the case $p = 2$, by looking at the proof.
- If L/K is an absolutely abelian extension of number fields, then Theorem 6.1 implies that $\mathcal{O}_L$ is locally free over $\mathfrak{A}_{L/K}$. Indeed, let $\mathfrak{p}$ be a prime of $\mathcal{O}_K$, and let $\mathfrak{P}$ a prime of $\mathcal{O}_L$ lying above $\mathfrak{p}$. Write $D = D(\mathfrak{P}|\mathfrak{p})$ for the decomposition group. Then $\mathcal{O}_{L_\mathfrak{P}}$ is free over $\mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}}$ (Theorem 6.1), $\operatorname{Ind}_D^G \mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}} = \mathcal{O}_K[G] \otimes_{\mathcal{O}_K[D]} \mathfrak{A}_{L_\mathfrak{P}/K_\mathfrak{p}}$ is a ring (it is the tensor product of two algebras over a commutative ring), and so by Proposition 3.37, $\mathcal{O}_{L,\mathfrak{p}}$ is free over $\mathfrak{A}_{L/K,\mathfrak{p}}$.
- The same result does not hold for absolutely abelian extension of number fields, as we should see in a moment.

We state a deep result of Brinkhuis [Bri92]. In the statement, "unramified" means "unramified at all finite primes", so we allow ramification at infinite places.

Theorem 6.2. *Let K be a totally ramified number field such that $K \neq \mathbb{Q}$, and let L/K be a finite unramified abelian extension. If L/K is not multiquadratic, then L/K does not admit a normal integral basis.*

We construct now an absolutely abelian extension of number fields L/K where $\mathcal{O}_L$ is not free over its associated order.

Example 6.3 (Campagna)**.** Let $M = \mathbb{Q}(\zeta_7 + \zeta_7^{-1}) \subseteq \mathbb{Q}(\zeta_7)$ and $N = \mathbb{Q}(\zeta_9 + \zeta_9^{-1}) \subseteq \mathbb{Q}(\zeta_9)$. Then $M/\mathbb{Q}$ and $N/\mathbb{Q}$ are arithmetically disjoint cyclic extensions of degree 3. In particular, $\operatorname{Gal}(MN/\mathbb{Q}) \cong C_3 \times C_3$. If $H \leq \operatorname{Gal}(MN/\mathbb{Q})$ corresponds to the diagonal subgroup of $C_3 \times C_3$, then $K = L^H$ is such that $\operatorname{Gal}(K/\mathbb{Q}) \cong C_3$ and $K \neq M, N$. Clearly K is totally real, as it lies inside the compositum of two totally real fields. The only possible (finite) ramification in K is at 3 and 7, and it is immediate to get that K is totally ramified at both primes. By genus theory (see [Frö83]), the *narrow genus field* $L = K_+$ of K is an absolutely abelian unramified extension of K of degree 3. By Theorem 6.2, L/K does not admit an integral normal basis, and since L/K is tameky ramified, $\mathfrak{A}_{L/K} = \mathcal{O}_K[G]$ by Theorem 5.2. We conclude that $\mathcal{O}_L$ is not free over its associated order.

6.1. **Reduction step.** The first step is to show that it is enough to deduce our main result for an absolutely abelian extension L/K with
$$\mathbb{Q}_p \subseteq K \subseteq L \subseteq \mathbb{Q}_p(\zeta_{p^n}),$$
for some $n \geq 1$. We know that by local class field theory (for example, see [Mil20]), if K is a p-adic field and π is an uniformiser, then the maximal abelian extension of K can be written as
$$K^{\text{ab}} = K^{\text{unr}} \cdot K_\pi,$$

where K^{unr} is the maximal unramified extension of K, and K_π is a totally ramified extension depending on the uniformiser π.

We would like to have a similar decomposition for an abelian extension of a p-adic field K. Unfortunately, this claim is false.

Example 6.4. Consider the following diagram:

$$\begin{tikzcd}
 & MN = \mathbb{Q}_5(\zeta_5, \zeta_{624}) \arrow[dl, dash] \arrow[dr, dash] & \\
M = \mathbb{Q}_5(\zeta_5) \arrow[dr, dash] & & N = \mathbb{Q}_5(\zeta_{624}) \arrow[dl, dash] \\
 & \mathbb{Q}_5 &
\end{tikzcd}$$

The extension $\mathbb{Q}_5(\zeta_5)/\mathbb{Q}_5$ is a totally ramified cyclic extension of order 4, while since $624 = 5^4 - 1$, extension $\mathbb{Q}_5(\zeta_{624})/\mathbb{Q}_5$ is unramified and cyclic of order 4. Let σ be the generator of $\mathrm{Gal}(\mathbb{Q}_5(\zeta_5)/\mathbb{Q}_5)$, and let τ be the generator of $\mathrm{Gal}(\mathbb{Q}_5(\zeta_{624})/\mathbb{Q}_5)$. As M and N are arithmetically disjoint, $\mathrm{Gal}(MN/\mathbb{Q}) = \langle\sigma\rangle \times \langle\tau\rangle$. Let H be the subgroup generated by $\sigma\tau^2$, and L be its fixed field. The maximal unramified subfield L^{unr} of L is $L \cap \mathbb{Q}_5(\zeta_{624})$, and it has degree 2 over $\mathbb{Q}_p$. If there existed a field L_t with $L = L^{\mathrm{unr}} \cdot L_t$, then we we would write $\mathrm{Gal}(L/\mathbb{Q}_5)$ as product of cyclic groups of order 2. This is a contradiction, since $\mathrm{Gal}(L/\mathbb{Q}_5)$ is cyclic of order 4.

However, we can reach the following result, which is [Let98, Lemma 1]

Lemma 6.5. *Let L/K be an abelian extension of p-adic fields with Galois group G and degree d. Let $d' \in \mathbb{N}$ such that $d \mid d'$, and let $\widetilde{K}/K$ be the unique unramified extension of K of degree d'. Then there exists an abelian and totally ramified extension L'/L such that, for $\widetilde{L} = L'\widetilde{K}$, the following properties hold:*

1. *$\widetilde{L}/K$ is abelian.*
2. *$L \subseteq \widetilde{L}$.*
3. *$\widetilde{L}/L$ is unramified.*

Proof. The diagram we want is the following:

$$\begin{tikzcd}
 & \widetilde{L} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash] & L' \arrow[d, dash] & \widetilde{K} \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Recall that $\widetilde{K}/K$ is cyclic, and denote by σ its generator. We set $\widetilde{L} = L\widetilde{K}$. Since L/K and $\widetilde{K}/K$ are abelian, also $\widetilde{L}/K$ is abelian. Clearly $L \subseteq \widetilde{L}$ and $\widetilde{L}/L$ is unramified. We only need to find L' as in the statement.

Consider the exact sequence

$$1 \to \mathrm{Gal}(\widetilde{L}/\widetilde{K}) \to \mathrm{Gal}(\widetilde{L}/K) \xrightarrow{\pi} \mathrm{Gal}(\widetilde{K}/K) \to 1.$$

Let $\tau \in \mathrm{Gal}(\widetilde{L}/K)$ such that $\pi(\tau) = \sigma$. We claim that the order of τ is d. Since $\tau^{d'}$ is the identity on $\widetilde{K}$, we find that d' divides the order of τ. Conversely, as $\mathrm{Gal}(\widetilde{L}/K)$

is embedded into $\mathrm{Gal}(L/K) \times \mathrm{Gal}(\widetilde{K}/K)$, we immediately deduce that the order of τ is precisely d'. Therefore $\varphi\colon \mathrm{Gal}(\widetilde{K}/K) \to \mathrm{Gal}(\widetilde{L}/L)$, defined by $\varphi(\sigma) = \tau$, is a splitting homomorphism for the above sequence. In particular, we can write

$$\mathrm{Gal}(\widetilde{L}/K) = \mathrm{Gal}(\widetilde{L}/\widetilde{K}) \times G',$$

where G' is the subgroup of $\mathrm{Gal}(\widetilde{L}/K)$ generated by τ. Define $L' = \widetilde{L}^{G'}$. Then the other claims immediately follow. □

We prove now [Let98, Proposition 1(b)], a new version of Lemma 2.30.

Proposition 6.6. *Let K be a p-adic field, and suppose that L_1 and F are Galois extensions of K such that L/K is totally ramified and F/K is unramified. Write $N = LF$. Then $\mathcal{O}_N$ is free over $\mathfrak{A}_{N/F}$ if and only if $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$.*

Proof. One implication follows immediately from Lemma 2.30, since in this case L and F are arithmetically disjoint over K.

Conversely, suppose that $\mathcal{O}_N$ is free over $\mathfrak{A}_{N/F}$. We need to use abstract commutative algebra, and this implies that we lose information about the generator. We have an isomorphism $\mathcal{O}_N \cong \mathfrak{A}_{N/F}$ as $\mathfrak{A}_{N/F}$-modules. Recall that $\mathcal{O}_N \cong \mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F$ (Theorem 1.24). We can endow both with a structure of $\mathfrak{A}_{L/K}$-module, identifying $\mathfrak{A}_{L/K}$ in $\mathfrak{A}_{N/F} \cong \mathfrak{A}_{L/K} \otimes_{\mathcal{O}_K} \mathcal{O}_F$. In this way, $\mathcal{O}_N$ and $\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F$ are isomorphic as $\mathfrak{A}_{L/K}$-modules. Similarly, the isomorphism $\mathfrak{A}_{N/F} \cong \mathfrak{A}_{L/K} \otimes_{\mathcal{O}_K} \mathcal{O}_F$ can be seen as $\mathfrak{A}_{L/K}$-module isomorphism. Summarising, we have found an $\mathfrak{A}_{L/K}$-module isomorphism

$$\mathcal{O}_L \otimes_{\mathcal{O}_K} \mathcal{O}_F \cong \mathfrak{A}_{L/K} \otimes_{\mathcal{O}_K} \mathcal{O}_F.$$

Since $\mathcal{O}_F$ is free of rank $d = [F : K]$ over $\mathcal{O}_K$, we derive an $\mathfrak{A}_{L/K}$-module isomorphism

$$\mathcal{O}_L^d \cong \mathfrak{A}_{L/K}^d.$$

As $\mathcal{O}_K$ is a complete commutative local ring, we can apply Krull–Schmidt–Azumaya theorem (see [CR81, Theorem 6.12]) to conclude that $\mathcal{O}_L \cong \mathfrak{A}_{L/K}$ as $\mathfrak{A}_{L/K}$-modules, that is, $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$. □

We may now apply our reduction strategy. Suppose that we know that for all extensions

$$\mathbb{Q}_p \subseteq F \subseteq N \subseteq \mathbb{Q}_p(\zeta_{p^n}),$$

$\mathcal{O}_N$ is free over $\mathfrak{A}_{N/F}$. We want to show that for all absolutely abelian extension L/K of p-adic fields, $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$.

So let L/K be an absolutely abelian extension of p-adic fields with degree d. Let $f = [L : \mathbb{Q}_p] = e_K f_K d$, where e_K is the absolute ramification index of K and f_K is the absolute inertia degree of K. It is quite simple to show that the unique unramified extension of K of degree $e_K d$ is $\widetilde{K} = K\mathbb{Q}_p(\zeta_{p^f-1})$; therefore, by Lemma 6.5, $\widetilde{L} = L\mathbb{Q}_p(\zeta_{p^f-1})$ is the compositum of $\widetilde{K} = K\mathbb{Q}_p(\zeta_{p^f-1})$, which is unramified over K, and L', which is totally ramified over K. After some degree considerations, and the observation that $K^{\mathrm{unr}} = K \cap \mathbb{Q}_p(\zeta_{p^f-1})$, we find the following diagram:

$$\begin{tikzcd}
& \widetilde{L} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
L \arrow[dr, dash, "d"'] \arrow[dddr, dash, "f"'] & L' \arrow[d, dash] & \widetilde{K} \arrow[dl, dash, "e_K d"] \arrow[d, dash] \\
& K \arrow[d, dash, "e_K"] & \mathbb{Q}_p(\zeta_{p^f-1}) \arrow[dl, dash, "e_K d"] \\
& K^{\mathrm{unr}} \arrow[d, dash, "f_K"] & \\
& \mathbb{Q}_p &
\end{tikzcd}$$

Lemma 6.7. *There exists $n \in \mathbb{N}$ such that $\widetilde{L} \subseteq \mathbb{Q}_p(\zeta_{p^n}, \zeta_{p^f-1})$.*

Proof. By local class field theory, $|\mathbb{Q}_p^\times : N_{L/\mathbb{Q}_p}(L^\times)| = [L : \mathbb{Q}_p] = f$, that is, $(\mathbb{Q}_p^\times)^f \subseteq N_{L/\mathbb{Q}_p}(L^\times)$ (here $N_{L/\mathbb{Q}_p}$ is the norm map). This implies that $p^f \in N_{L/\mathbb{Q}_p}(L^\times)$, and since $N_{L/\mathbb{Q}_p}(L^\times)$ is open, $N_{L/\mathbb{Q}_p}(L^\times)$ contains $1 + p^n\mathbb{Z}_p$ for some $n \in \mathbb{N}$. We deduce that $\langle p^f \rangle \times (1+p^n\mathbb{Z}_p) \subseteq N_{L/\mathbb{Q}_p}(L^\times)$, so, again by local class field theory, $L \subseteq \mathbb{Q}_p(\zeta_{p^n}, \zeta_{p^f-1})$. Since $\widetilde{L} = L\mathbb{Q}_p(\zeta_{p^f-1})$, we derive our assertion. □

Now assume that $n \in \mathbb{N}$ is minimal such that $\widetilde{L} \subseteq \mathbb{Q}_p(\zeta_{p^n}, \zeta_{p^f-1})$. Let $\widetilde{\widetilde{L}} = \widetilde{L} \cap \mathbb{Q}_p(\zeta_{p^n})$, and let $\widetilde{\widetilde{K}} = \widetilde{K} \cap \mathbb{Q}_p(\zeta_{p^n})$. We find the following diagram:

$$\begin{tikzcd}
& \mathbb{Q}_p(\zeta_{p^n}, \zeta_{p^f-1}) \arrow[d, dash] \arrow[drr, dash] & & \\
& \widetilde{L} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \mathbb{Q}_p(\zeta_{p^n}) \arrow[d, dash] \\
L \arrow[dr, dash] \arrow[dddr, dash] & L' \arrow[d, dash] & \widetilde{K} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \widetilde{\widetilde{L}} \arrow[d, dash] \\
& K \arrow[d, dash] & \mathbb{Q}_p(\zeta_{p^f-1}) \arrow[dl, dash] & \widetilde{\widetilde{K}} \arrow[ddll, dash] \\
& K^{\mathrm{unr}} \arrow[d, dash] & & \\
& \mathbb{Q}_p & &
\end{tikzcd}$$

By assumption, $\mathcal{O}_{\widetilde{\widetilde{L}}}$ is free over $\mathfrak{A}_{\widetilde{\widetilde{L}}/\widetilde{\widetilde{K}}}$. Note that $\widetilde{\widetilde{K}}\mathbb{Q}_p(\zeta_{p^f-1}) = \widetilde{K}$, by a simple degree reasoning. Hence $\widetilde{K}/\widetilde{\widetilde{K}}$ is unramified, and since $\widetilde{\widetilde{L}}/\widetilde{\widetilde{K}}$ is totally ramified, we can apply Proposition 6.6 to derive that $\mathcal{O}_{\widetilde{L}}$ is free over $\mathfrak{A}_{\widetilde{L}/\widetilde{K}}$. Since L'/K is totally ramified, again by Proposition 6.6 we find that $\mathcal{O}_{L'}$ is free over $\mathfrak{A}_{L'/K}$ (here we lose sight of the generator). As $\mathcal{O}_{\widetilde{K}}$ is free over $\mathfrak{A}_{\widetilde{K}/K}$ (the extension in unramified), $\mathcal{O}_{\widetilde{L}}$ is free over $\mathfrak{A}_{\widetilde{L}/K}$ by Lemma 2.30(2). Finally, since $\widetilde{L}/L$ is unramified, we can apply Lemma 2.31 to conclude that $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$.

6.2. **The pth power cyclotomic case.** We restrict ourselves to $p \geq 3$. Let L/K be a Galois extension of p-adic fields with Galois group G. Suppose that

$$\mathbb{Q}_p \subseteq K \subseteq L \subseteq \mathbb{Q}_p(\zeta_{p^n}),$$

with $n \in \mathbb{N}$ minimal. Let $1 \leq m \leq n$ be the minimal integer such that $K \subseteq \mathbb{Q}_p(\zeta_{p^m})$. For all $t \in \mathbb{N}$, let

$$\mathcal{R}_t \subseteq \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$$

denote a set of automorphisms representing $\mathrm{Gal}(K_t/\mathbb{Q}_p)$ in the absolute Galois group of $\mathbb{Q}_p$, where for all p-adic fields F, we write $F_t = F \cap \mathbb{Q}_p(\zeta_{p^t})$. The crucial result is [Let98, Proposition 3], as follows..

Proposition 6.8 (Lettl)**.**

- *$\mathfrak{A}_{L/K}$ is the maximal $\mathcal{O}_K$-order in $K[G]$.*
- *We have $\mathcal{O}_L = \mathfrak{A}_{L/K} \cdot \alpha$, with*

$$\alpha = \sum_{j=0}^{n-m} \sum_{\sigma \in \mathcal{R}_{n-m-j}} \mathrm{Tr}_{\mathbb{Q}_p(\zeta_{p^{n-j}})/L_{m-j}} \, \sigma(\zeta_{p^n}^{p^j}).$$

Proof. The proof of this proposition is rather long and technical; we just give a brief hint.

Since n is minimal and $\mathbb{Q}_p(\zeta_{p^n})/L$ is tamely ramified, we can assume $L = \mathbb{Q}_p(\zeta_{p^n})$. Write $G = \mathrm{Gal}(\mathbb{Q}_p(\zeta_{p^n})/K)$. The idea is to directly verify that if $\mathcal{M} \subseteq K[G]$ is the maximal $\mathcal{O}_K$-order, then

$$\mathbb{Z}_p[\zeta_{p^n}] = \mathcal{M} \cdot \alpha.$$

Indeed, if this happens, then $M = \mathfrak{A}_{\mathbb{Q}_p(\zeta_{p^n})/K}$ and α is a generating element. The key observation is that in the abelian case, the structure of M is well understood:

$$\mathcal{M} = \bigoplus \mathcal{M} \cdot e_K(\chi),$$

where all $e_K(\chi)$ are idempotent associated to certain characters χ. $\square$

7. Cyclic extensions of degree p

In this section, we are interested in studying cyclic extensions of p-adic fields of prime degree.

Remark 7.1.

(1) If L/K is a cyclic extension of p-adic fields with prime degree $q \neq p$ and Galois group G, then L/K is tamely ramified, so $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K} = \mathcal{O}_K[G]$ by Theorem 1.39.

(2) If L/K is an unramified cyclic extension of p-adic fields with degree p and Galois group G, then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K} = \mathcal{O}_K[G]$ by Theorem 1.37.

This means that we can focus our attention on (totally) ramified cyclic extensions of p-adic fields of degree p.

7.1. **Notation and statement of the result.** We fix the notation, which works for all this section. Let L/K be a totally and wildly ramified cyclic extension of p-adic fields with Galois $G \cong \mathbb{Z}/p\mathbb{Z}$, generated by an element σ. We fix uniformisers π_K and π_L of K and L respectively, and we normalise the valuations by $v_K(\pi_K) = 1$ and $v_L(\pi_L) = 1$. We also use the following symbols:

(1) $e = e_K = v_K(p)$ denotes the absolute inertia degree of K.

(2) t is the ramification jump of the extension, that is, the unique integer such that
$$G = G_{-1} = G_0 = \cdots = G_t, \qquad G_{t+1} = \cdots = \{1\};$$
note that t is equivalently defined by the condition
$$t = \min_{x \in \mathcal{O}_L} v_L((\sigma - 1)x) - 1,$$
where, by convention, $v_L(0) = +\infty$ can never be the minimum.

(3) For all $i \geq 0$, $U_{K,i} = 1 + \pi_K^i \mathcal{O}_K$ is ith higher unit group.

(4) $t = pt_0 + a$, where $0 \leq a \leq p - 1$.

(5) $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x, where $x \in \mathbb{R}$.

In this section, we describe necessary and sufficient conditions for $\mathcal{O}_L$ to be free over the associated order $\mathfrak{A}_{L/K}$. In particular, we prove part of the following theorem, combining the main results of [Fer74, BBF72, BF72].

Theorem 7.2.

(1) *If $t \equiv 0 \pmod p$, then $\mathfrak{A}_{L/K}$ is the maximal order of $K[G]$. In particular, $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$.*

(2) *If $0 < t < \frac{pe}{p-1} - 1$, then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$ if and only if $a \mid p - 1$.*

(3) *If $\frac{pe}{p-1} - 1 \leq t \leq \frac{pe}{p-1}$, then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$ if and only if the continued fraction expansion of $\frac{a}{p}$ has length at most 4, that is, $\frac{a}{p}$ can be written as*
$$\frac{a}{p} = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2 + \cdots}} = [a_0; a_1, \ldots, a_n]$$
with $a_n > 1$ and $n \leq 4$.

Remark 7.3. The papers [Fer74, BF72] are essentially announcements of results and contain few proofs. A proof of Theorem 7.2(3) can be found in [BBF72]. The proofs of Theorem 7.2(1) and Theorem 7.2(2) given here are obtained by following the breadcrumbs left in [BF72] and filling in the gaps with the help of [DCFL20].

We wish to thank D. Lombardo for the meticulous work.

7.2. **Preliminary remarks.** We begin with some general comments on the ramification jump t.

Proposition 7.4.

(1) $t \leq \frac{ep}{p-1}$.

(2) *If $t' \in \mathbb{Z}$ satisfies $-1 \leq t' \leq \frac{ep}{p-1}$, where $p \nmid t'$, then there exists L'/K cyclic of degree p with ramification jump t'.*

(3) *If $p \mid t$, then $t = \frac{ep}{p-1}$. In this case, K contains ζ_p and there exist uniformisers π_K and π_L such that $\pi_K = \pi_L^p$.*

We sketch a proof of these facts, based on the next fundamental result about the groups of local units (the first part is easy; for the second, see [Ser79, Chapter V, Proposition 4]).

Proposition 7.5.

1. *For $i \geq \frac{ep}{p-1}$, every ith higher unit is the pth power of a $(i-e)$th higher unit. In symbols: $U_{K,i} \subseteq U_{K,i-e}^p$.*
2. *Define*

$$\psi(x) = \begin{cases} x & \text{if } x \leq t, \\ t + p(x-t) & \text{if } x \geq t. \end{cases}$$

Then for all $n \geq 0$, the norm map $N_{L/K}$ sends $U_{L,\psi(n)}$ into $U_{K,n}$ and $U_{L,\psi(n)+1}$ into $U_{K,n+1}$.

Sketch of proof of Proposition 7.4.

1. Assume, by contradiction, $t > \frac{ep}{p-1}$, and take

$$\varepsilon = 1 + \pi_K^t \in U_{K,t} \subseteq (U_{K,t-e})^p.$$

Let $\varepsilon_1 \in U_{K,t-e}$ be a pth root of ε. Then on the one hand $N_{L/K}(\varepsilon_1) = \varepsilon_1^p = \varepsilon = 1 + \pi_K^t$ does not belong to $U_{K,t+1}$; on the other, $N_{L/K}(\varepsilon_1) \in N_{L/K}(U_{L,p(t-e)})$. Now $p(t-e) \geq t+1$, hence

$$N_{L/K}(U_{L,p(t-e)}) \subseteq N_{L/K}(U_{L,t+1}) \subseteq U_{K,t+1}$$

by Proposition 7.5(2). The contradiction proves the result.

2. The case $t = -1$ is trivial. For $t > 0$, one takes L to be the splitting field of $x^p - x - \alpha$, where $v_K(\alpha) = -t$ (see Artin–Schreier theory).
3. One begins by proving (using similar tricks) that $t \geq \frac{ep}{p-1}$; hence $t = \frac{ep}{p-1}$. By assumption, $\sigma(\pi_L) - \pi_L = \vartheta\pi_L^{t+1}$, where ϑ is a unit of $\mathcal{O}_L$. Dividing through by π_L we get

$$u = \frac{\sigma(\pi_L)}{\pi_L} = 1 + \vartheta\pi_L^t.$$

Changing ϑ if necessary, since $t = \frac{ep}{p-1}$, we obtain $u = 1 + \vartheta\pi_K^{e/(p-1)}$. As the extension L/K is totally ramified, we have $\mathcal{O}_L/(\pi_L) \cong \mathcal{O}_K/(\pi_K)$, so $\vartheta \equiv \vartheta_K \pmod{\pi_L}$, where now $\vartheta_K \in \mathcal{O}_K$. Thus

$$u \equiv 1 + \vartheta_K\pi_K^i \pmod{\pi_L^{t+1}},$$

or equivalently, $u = (1 + \vartheta_K\pi_K^i)u'$ with $u' \in U_{L,t+1}$. Taking the norm of this equation we obtain

$$1 = (1 + \vartheta_K\pi_K^{e/(p-1)})^p N_{L/K}(u')$$

(note that $1 + \vartheta_K\pi_K^{e/(p-1)}$ is an element of K), with $N_{L/K}(u') \in U_{K,t+1}$ by Proposition 7.5(2). By Proposition 7.5(1), $N_{L/K}(u')$ is the pth power of unit u_0 in $U_{K,t+1-e} = U_{K,e/(p-1)+1}$. Hence we have obtained

$$1 = (1 + \vartheta_K\pi_K^{e/(p-1)})^p u_0^p,$$

so $\zeta := (1 + \vartheta_K\pi_K^{e/(p-1)})u_0 \equiv 1 + \vartheta_K\pi_K^{e/(p-1)} \pmod{\pi_K^{e/(p-1)+1}}$ satisfies $\zeta^p = 1$. In particular, ζ is a pth root of unity in K that is not 1.

The last statement then follows from Kummer theory. □

7.3. **The case $t \equiv 0 \pmod{p}$.** By Proposition 7.4, $t = \frac{ep}{p-1}$, and we may choose uniformisers π_K and π_L such that $\pi_L^p = \pi_K$. Since L/K is totally ramified, $\mathcal{O}_L = \mathcal{O}_K[\pi_L]$.

Theorem 7.6. *If $t \equiv 0 \pmod{p}$, then the associated order $\mathfrak{A}_{L/K}$ is the maximal order in $K[G]$ and the element $\vartheta = 1 + \pi_L + \cdots + \pi_L^{p-1}$ generates $\mathcal{O}_L$ over $\mathfrak{A}_{L/K}$.*

Proof. The fact that ϑ generates a normal integral basis can be proved as the case of tamely and totally ramified extensions (see Sections 1 and 4). We choose a different route, by first describing the associated order $\mathfrak{A}_{L/K}$. We have

$$K[G] \cong K[t]/(t^p - 1) \cong \prod_{i=0}^{p-1} K,$$

where the isomorphisms are given by $\sigma \mapsto t$ and $f(t) \mapsto (f(\zeta_p^i))_{i=0}^{p-1}$ respectively. The unique maximal order of $\prod_{i=0}^{p-1} K$ is clearly $\prod_{i=0}^{p-1} \mathcal{O}_K$; tracing the isomorphisms backwards, we see that the maximal order of $K[G]$ is given by

$$\mathcal{M} = \left\{ \sum_{j=0}^{p-1} a_j \sigma^j \in K[G] \mid \sum_{j=0}^{p-1} a_j \zeta_p^{ij} \in \mathcal{O}_K \text{ for all } i = 0, \dots, p-1 \right\}.$$

Applying any element of $\mathcal{M}$ to a basis element π_L^i, since $\sigma(\pi_L) = \zeta_p \pi_L$ (by Kummer theory), we obtain

$$\sum_{j=0}^{p-1} a_j \sigma^j(\pi_L^i) = \left(\sum_{j=0}^{p-1} a_j \zeta_p^{ij} \right) \pi_L^i \in \mathcal{O}_L.$$

This shows that $\mathcal{M} \subseteq \mathfrak{A}_{L/K}$; hence, by maximality, the associated order coincides with $\mathcal{M}$. From the above calculation we also see that an element $\lambda = (c_0, \dots, c_{p-1}) \in \mathcal{O}_K^p \cong \mathcal{M}$ acts on ϑ as

$$\lambda \cdot \vartheta = \sum_{i=0}^{p-1} c_i \pi_L^i,$$

which immediately implies

$$\mathfrak{A}_{L/K} \cdot \vartheta = \bigoplus_{i=0}^{p-1} \mathcal{O}_K \pi_L^i = \mathcal{O}_L. \qquad \square$$

7.4. **The fractional ideal $\mathfrak{A}_\vartheta$.** From now on, we focus on the case $t \not\equiv 0 \pmod{p}$. In particular, since $t \geq 0$, we will have $t \geq 1$. The method of Bertrandias and Ferton [BF72] centres around the following object.

Definition 7.7. Let $\vartheta \in \mathcal{O}_L$ be a generator of a normal basis for the L/K. Define

$$\mathfrak{A}_\vartheta = \{\lambda \in K[G] \mid \lambda \cdot \vartheta \in \mathcal{O}_L\}.$$

Remark 7.8. $\mathfrak{A}_\vartheta$ is not necessarily a ring: for example, it can easily happen that $p^{-1} \in \mathfrak{A}_\vartheta$, but $\mathfrak{A}_\vartheta$ can never contain all the powers of p^{-1}.

Some basic properties of $\mathfrak{A}_\vartheta$ are easy to establish; see [BF72, Proposition 1].

Proposition 7.9.

(1) $\mathfrak{A}_{L/K} \subseteq \mathfrak{A}_\vartheta$, *and* $\mathfrak{A}_\vartheta$ *is a fractional ideal of* $\mathfrak{A}_{L/K}$.

(2) *The map*

$$\begin{aligned}\mathfrak{A}_\vartheta &\to \mathcal{O}_L\\ \lambda &\mapsto \lambda\cdot\vartheta\end{aligned}$$

is an $\mathfrak{A}_{L/K}$*-module isomorphism.*

(3) *The following are equivalent:*
   (a) $\mathcal{O}_L$ *is free over* $\mathfrak{A}_{L/K}$.
   (b) *There exists a generator* $\vartheta\in\mathcal{O}_L$ *of a normal basis for* L/K *such that* $\mathfrak{A}_\vartheta=\mathfrak{A}_{L/K}$.
   (c) *For all* $\vartheta\in\mathcal{O}_L$ *that generate a normal basis for* L/K*, the* $\mathfrak{A}_{L/K}$*-ideal* $\mathfrak{A}_\vartheta$ *is principal.*
   (d) *For all* $\vartheta\in\mathcal{O}_L$ *that generate a normal basis for* L/K*,* $\mathfrak{A}_\vartheta$ *is a ring.*

Before discussing the structure of $\mathfrak{A}_\vartheta$ for some interesting choices of ϑ, we identify a useful element of $K[G]$ and describe its action on $\mathcal{O}_L$. Let $f=\sigma-1\in\mathcal{O}_K[G]$.

Lemma 7.10.

(1) $\{1,f,f^2,\dots,f^{p-1}\}$ *is an* $\mathcal{O}_K$*-basis of* $\mathcal{O}_K[G]$.
(2) $f^p=-\sum_{j=1}^{p-1}\binom{p}{j}f^j$.

Suppose in addition $a\neq 0$.

(3) $v_L(f^i\pi_L^a)=a+it$ *for all* $i=0,\dots,p-1$.
(4) π_L^a *generates a normal basis for* L/K*; explicitly,* $\{f^i\cdot\pi_L^a\}_{i=0}^{p-1}$ *is a* K*-basis of* L.
(5) $v_L(f^p\pi_L^a)=ep+t+a$.
(6) *For all* $x\in\mathcal{O}_L$*,* $v_L(f\cdot x)\geq v_L(x)+t$.

Proof. Parts (1), (2), (5), and (6) follow from easy reasonings and computation.

For (3), as in the proof of Subsection 7.2, we have

$$\frac{\sigma(\pi_L)}{\pi_L}=1+\pi_L^t u$$

for some $u\in\mathcal{O}_L^\times$. Raising both sides to the jth power, for any j prime to p, gives

$$\frac{\sigma(\pi_L^j)}{\pi_L^j}=1+\pi_L^t u_j,$$

where $u_j\in\mathcal{O}_L^\times$ since $(j,p)=1$. Rearranging the previous equality gives

$$\sigma(\pi_L^j)-\pi_L^j=\pi_L^{j+t}u_j,$$

so we obtain $v_L(f\cdot\pi_L^j)=j+t$, provided that $(j,p)=1$. The claim then follows by induction.

Finally, for (4), notice that the L-valuations of the elements $\{f^i\cdot\pi_L^a\}_{i=0}^{p-1}$ are all distinct modulo p. □

In particular, we can consider $\mathfrak{A}_\vartheta$ with $\vartheta=\pi_K^a$. This special choice of ϑ allows us to easily describe $\mathfrak{A}_\vartheta$.

Proposition 7.11. $\mathfrak{A}_\vartheta$ *is free over* $\mathcal{O}_K$ *with basis* $\{\pi_K^{-\nu_i}f^i\}_{i=0}^{p-1}$*, where* $\nu_i=\lfloor\frac{a+it}{p}\rfloor$ *for all* i.

Proof. An element $\sum_{i=0}^{p-1} c_i f^i \in K[G]$ is in $\mathfrak{A}_\vartheta$ if and only if $\sum_{i=0}^{p-1} c_i f^i \cdot \pi_L^a$ is integral. Since the valuations of the terms $f^i \cdot \pi_L^a$ are all distinct by Lemma 7.10(3), this happens if and only if $c_i f^i \cdot \pi_L^a$ is integral for all i. Since $v_L(f^i \cdot \pi_L^a) = a + it$, the condition is $v_L(c_i) + a + it \geq 0$, or equivalently, $v_K(c_i) \geq -\frac{a+it}{p}$. □

Remark 7.12. An $\mathcal{O}_K$-basis of $\mathcal{O}_L$ is given by $\{\pi_K^{-\nu_i}(f^i \cdot \pi_L^a)\}_{i=0}^{p-1}$. Indeed, the L-valuations of these elements are all distinct modulo p, and are all between 0 and $p-1$.

The description of $\mathfrak{A}_{L/K}$ is only slightly more complicated.

Proposition 7.13. *$\mathfrak{A}_{L/K}$ is free over $\mathcal{O}_K$ with basis $\{\pi_K^{-n_i} f^i\}_{i=0}^{p-1}$, where*

$$n_i = \min_{0 \leq j \leq p-1-i} (\nu_{i+j} - \nu_j).$$

Proof. We just give a sketch of the proof. Take an arbitrary element $\lambda = \sum_{i=0}^{p-1} c_i f^i \in K[G]$; hence λ is in $\mathfrak{A}_{L/K}$ if and only if $\lambda\left(\pi_K^{-\nu_j}(f^j \cdot \pi_L^a)\right)$ is integral for all $i = 0, \ldots, p-1$. One checks that this happens if and only if

$$\sum_{i=0}^{p-1-j} c_i \pi_K^{-\nu_j}(f^{i+j} \cdot \pi_L^a) \in \mathcal{O}_L$$

(the other summands are automatically integral). Since the valuations of the terms are all distinct, this happens if and only if $v_K(c_i) - \nu_j + \nu_{i+j} \geq 0$ for $j = 0, \ldots, p-1-i$, which easily implies the result. □

7.5. **The case** $t \not\equiv 0 \pmod{p}$**.** In this section, we prove Theorem 7.2(2). Theorem 7.2(3) is conceptually similar, but technically much more involved, and so we do not discussed it here. There are also further extensions to cyclic extensions of degree p^n; see [Ber79b].

Remark 7.14. The condition $t < \frac{ep}{p-1} - 1$ is equivalent to ask that the extension L/K is not almost maximally ramified. The only nontrivial idempotent in $K[G]$ is $e_G = \frac{1}{p}\sum_{i=0}^{p-1} \sigma^i$. An amusing computation involving sums of binomials shows that e_G is in $\mathfrak{A}_{L/K}$ if and only if $n_{p-1} \geq e$, and one sees that this is equivalent to $\frac{pe}{p-1} - 1 \leq t \leq \frac{pe}{p-1}$.

We begin by proving that if $a \mid p-1$, then $\mathfrak{A}_\vartheta = \mathfrak{A}_{L/K}$ (where $\vartheta = \pi_L^a$), so that, by Proposition 7.9, the ring of integers $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$ in this case. We need a simple arithmetical lemma.

Lemma 7.15. *If $a \mid p-1$, then $\nu_i = it_0 + \left\lfloor \frac{i}{k} \right\rfloor$ for all $i = 0, \ldots, p-1$, where $k = \frac{p-1}{a}$.*

Proof. It follows from an easy induction on i. □

Proposition 7.16. *Suppose $a \mid p-1$. Then $\mathfrak{A}_{L/K} = \mathfrak{A}_\vartheta$, where $\vartheta = \pi_L^a$. In particular, $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$.*

Proof. Recall that $\mathfrak{A}_{L/K}$ is $\mathcal{O}_K$-free with basis $\{\pi_K^{-n_i} f^i\}_{i=0}^{p-1}$ and $\mathfrak{A}_\vartheta$ is free with basis $\{\pi_K^{-\nu_i} f^i\}_{i=0}^{p-1}$; thus, equality holds if and only if $\nu_i = n_i$ for all $i = 0, \ldots, p-1$.

By definition, $\nu_i \geq n_i$, so it suffices to show the opposite inequality. Since n_i is defined as a minimum, we need to show

$$\nu_{i+j} - \nu_j \geq \nu_i \quad \text{for all indices } i \text{ and } j \text{ with } i+j \leq p-1.$$

Using Lemma 7.15, we simply need to prove

$$(i+j)t_0 + \left\lfloor \frac{i+j}{k} \right\rfloor \geq it_0 + \left\lfloor \frac{i}{k} \right\rfloor + jt_0 + \left\lfloor \frac{j}{k} \right\rfloor,$$

which is clear. □

It remains to show that, under the assumptions $t < \left\lfloor \frac{ep}{p-1} \right\rfloor - 1$ and $a \neq 0$, if the ring $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$, then $a \mid p-1$. The final conclusion follows from the next lemma, which we do not prove, since even though it is not very hard, it is also not very interesting from the point of view of Galois theory.

Lemma 7.17. *Assume $n_i = \nu_i$ for all $i = 0, \ldots, p-1$. Then $a \mid p-1$.*

So we just need to prove that $n_i = \nu_i$ for all i in this case. To this end, we apply Proposition 7.9(3c). Namely, we assume that for our specific $\vartheta = \pi_L^a \in \mathcal{O}_L$, there is an isomorphism $\mathfrak{A}_\vartheta \cong \mathfrak{A}_{L/K}$ of $\mathfrak{A}_{L/K}$-modules, and deduce from this that $n_i = \nu_i$ needs to hold for all i.

Proof. Suppose that $\mathfrak{A}_\vartheta \cong \mathfrak{A}_{L/K}$ as $\mathfrak{A}_{L/K}$-modules. This means that there exists $\alpha \in \mathfrak{A}_\vartheta$ such that

$$\begin{aligned} \varphi\colon \mathfrak{A}_{L/K} &\to \mathfrak{A}_\vartheta \\ \lambda &\mapsto \lambda\alpha \end{aligned}$$

is an isomorphism. We represent φ as a matrix $M(\alpha)$ in the bases of $\mathfrak{A}_\vartheta$ and $\mathfrak{A}_{L/K}$ described above. If $\alpha = \sum_{i=0}^{p-1} x_i(\pi_K^{-\nu_i} f^i)$ (recall that $\alpha \in \mathfrak{A}_\vartheta$, so every x_i is in $\mathcal{O}_K$), then $M(\alpha) = \sum_{i=0}^{p-1} x_i M(\pi_K^{-\nu_i} f^i)$. Note that $M(\alpha) \in \mathrm{Mat}_{p\times p}(\mathcal{O}_K)$, hence it makes sense to reduce it modulo π_K, and φ is an isomorphism if and only if $M(\alpha)$ is invertible over $\mathcal{O}_K$, if and only if $\det M(\alpha) \in \mathcal{O}_K^\times$, if and only if $\det M(\alpha) \not\equiv 0 \pmod{\pi_K}$.

Next we claim that the matrices $M(\pi_K^{-\nu_i} f^i)$ are all lower-triangular when reduced modulo π_K, and in fact strictly lower-triangular unless $i = 0$. Assuming this fact, the matrix $M(\alpha)$ is congruent modulo π_K to a lower-triangular matrix whose kth diagonal coefficient is $x_0\pi_K^{\nu_k - n_k}$. In particular, $M(\alpha)$ is invertible if and only if $v_K(x_0) = 0$ and $\nu_k = n_k$ for all k, as desired.

It remains to show the claim about the matrices $M(\pi_K^{-\nu_i} f^i)$ being strictly lower-triangular for $i > 0$ (for $i = 0$, the matrix $M(\pi_K^{-\nu_i} f^i)$ is easily seen to be diagonal). Consider an entry of $M(\pi_K^{-\nu_i} f^i)$ strictly above the diagonal, say in position (c, d) with $d > c$. The coefficient of $M(\pi_K^{-\nu_i} f^i)$ in position (c, d) is the coefficient of $\pi_K^{-\nu_c} f^c$ in

$$(\pi_K^{-n_d} f^d)(\pi_K^{-\nu_i} f^i).$$

Since $d > c$, if $i + d \leq p-1$, then the coefficient in question is simply 0. Otherwise, using Lemma 7.10 we may rewrite the above as

$$\pi_K^{-n_d-\nu_i} f^{i+d-p} f^p = -\pi_K^{-n_d-\nu_i} \sum_{j=1}^{p-1} \binom{p}{j} f^{i+d+j-p},$$

which we claim is in $\pi_K\mathfrak{A}_\vartheta$, and therefore has coefficient along $\pi_K^{-\nu_c}f^c$ divisible by π_K. To finish the proof, we only need to show that $\pi_K^{-n_d-\nu_i-1}f^{i+d-p}f^p$ is in $\mathfrak{A}_\vartheta$ (notice the -1 in the exponent of π_K). Replacing $-n_d$ by $-\nu_d$ (which is larger in absolute value), this reduces to proving

$$v_L(f^{i+d-p}f^p\pi_L^a) \geq p(\nu_d+\nu_i+1),$$

which follows in a straightforward manner from Lemma 7.10 if one uses the assumption that t is not too large.

Here are the details. By Lemma 7.10(5), we have $v_L(f^p\pi_L^a) = ep+t+a$. By Lemma 7.10(6), every subsequent application of f increases the valuation by at least t, so $v_L(f^{i+d-p}f^p\pi_L^a) \geq ep+t+a+t(i+d-p)$. On the other hand,

$$p(\nu_d+\nu_i+1) \leq a+dt+a+it+p.$$

So we need to check that

$$ep+t+a+t(i+d-p) \geq a+dt+a+it+p.$$

Simplifying like terms, this is equivalent to

$$ep+t-pt \geq a+p \iff ep \geq p+t(p-1)+a.$$

By assumption, the extension L/K is not almost maximally ramified, so by Remark 7.14 we have $e > n_{p-1} = (p-1)t_0+a$, that is, $e \geq (p-1)t_0+a+1$. Multiplying both sides by p, we get

$$pe \geq p(p-1)t_0+(p-1)a+a+p = (p-1)t+a+p,$$

as desired.

□

Given a Galois extension L/K, the quantity

$$m(L/K) \coloneqq \min_{\alpha\in\mathcal{O}_L}[\mathcal{O}_L : \mathcal{O}_K[G]\cdot\alpha]$$

is studied [DCFL20]. By methods not too different from the above, an explicit formula for $m(L/K)$ when L/K is cyclic of degree p is found, as follows.

Theorem 7.18. *Let L/K be a ramified Galois extension of p-adic fields of degree p, with ramification jump t. Let $a \in \{0,\dots,p-1\}$ be the residue class of t modulo p, and let $\nu_i = \left\lfloor \frac{a+it}{p} \right\rfloor$. If $a \neq 0$, then*

$$v_p(m(L/K)) = f_K\left(\sum_{i=0}^{p-1}\nu_i + \min_{0\leq i\leq p-1}(ie_K-(p-1)\nu_i)\right);$$

if $a = 0$, then

$$v_p(m(L/K)) = \frac{1}{2}[L:\mathbb{Q}_p].$$

8. On K-theory, realisable classes, and Hilbert–Speiser fields

8.1. ***K*-groups.** Here we follow the PhD thesis of Breuning [Bre04]. Let A be a ring, and denote by $\mathcal{P}(A)$ the category of finite A-modules.

Definition 8.1. We denote by $K_0(A)$ the *Groethendieck group* of $\mathcal{P}(A)$, that is, the abelian group generated by the isomorphism classes (P) of P for all $P \in \mathcal{P}(A)$, modulo the relations

$$(P) - (P') - (P'')$$

for all short exact sequences $0 \to P' \to P \to P'' \to 0$. We denote by $[P]$ the class of (P) as an element in $K_0(A)$.

Definition 8.2. Let us consider the category of pairs (P, f), where $P \in \mathcal{P}(A)$ and f is an automorphism of P. A morphism $(P, f) \to (Q, g)$ is given by an A-module homomorphism $P \to Q$ which commutes with f and g. The isomorphism classes are denoted by $((P, f))$. The *Whitehead group* $K_1(A)$ is the abelian group with generators $((P, f))$ and relations

$$((P, f)) - ((P', f')) - ((P'', f''))$$

if $0 \to (P', f') \to (P, f) \to (P'', f'') \to 0$ is exact, and

$$((P, fg)) - ((P, f)) - ((P, g))$$

for all $P \in \mathcal{P}(A)$ and automorphisms f and g of P. We denote by $[P, f]$ the class of $((P, f))$ in $K_1(A)$.

There is an alternative description of $K_1(A)$. For all $n \geq 1$, we can define a map $\mathrm{GL}_n(A) \to \mathrm{GL}_{n+1}(A)$ by

$$M \mapsto \begin{pmatrix} M & 0 \\ 0 & 1 \end{pmatrix}.$$

Let $\mathrm{GL}(A) = \varinjlim \mathrm{GL}_n(A)$, and let $\mathrm{GL}(A)' = [\mathrm{GL}(A), \mathrm{GL}(A)]$ be the commutator subgroup. Then $K_1(A) \cong \mathrm{GL}(A)/\mathrm{GL}(A)'$. The isomorphism is obtained as follows: let $[P, f] \in K_1(A)$. Since P is projective, we can find an A-module Q such that $P \oplus Q$ is free. Then $f \oplus \mathrm{id}$ is represented by a matrix $M \in \mathrm{GL}(A)$. For the proof that this is a well-defined map and an isomorphism, see [CR87, Theorem 40.6].

Definition 8.3. Let $\varphi\colon A \to B$ be a ring homomorphism. We consider the category of triples (P, f, Q), where $P, Q \in \mathcal{P}(A)$ and $f : B \otimes_A P \to B \otimes_A Q$ is a B-module isomorphism. A morphism is a pair of morphisms $u : P \to P'$ and $v : Q \to Q'$ such that $f' \circ (\mathrm{id}_B \otimes u) = (\mathrm{id}_B \otimes v) \circ f$. The *relative K-group* $K_0(A, \varphi)$ is the abelian group with generators $((P, f, Q))$ and relations

$$((P, f, Q)) - ((P', f', Q')) - ((P'', f'', Q''))$$

for all short exact sequences

$$0 \to ((P', f', Q')) \to ((P, f, Q)) \to ((P'', f'', Q'')) \to 0$$

(that is, $0 \to P' \to P \to P'' \to 0$ and $0 \to Q' \to Q \to Q'' \to 0$ are both exact), and

$$((P, gf, R)) - ((P, f, Q)) - ((Q, g, R))$$

with $P, Q, R \in \mathcal{P}(A)$, and $f : B \otimes P \to B \otimes Q$ and $g : B \otimes Q \to B \otimes R$ isomorphisms. We denote classes in $K_0(A, \varphi)$ by $[P, f, Q]$.

Proposition 8.4. *For all ring homomorphisms $\varphi : A \to B$, there exists an exact sequence*

$$K_1(A) \xrightarrow{\varphi_*} K_1(B) \xrightarrow{\partial^1_{A,\varphi}} K_0(A, \varphi) \xrightarrow{\varphi^0_{A,\varphi}} K_0(A) \xrightarrow{\varphi_*} K_0(B).$$

Here $\varphi_*([P, f]) = [B \otimes_A P, \mathrm{id}_B \otimes f]$*,* $\partial^1_{A,\varphi}([M]) = [A^n, M, A^n]$ *for* $M \in \mathrm{GL}(B)$*,* $\partial^0_{A,\varphi}([P, f, Q]) = [P] - [Q]$*, and* $\varphi_*([P]) = [B \otimes_A P]$*.*

8.2. **Realisable classes.** Let K be a number field, and let G be a finite group. Denote by $R(\mathcal{O}_K[G])$ the set of classes in $\mathrm{Cl}(\mathcal{O}_K[G])$ which are realisable as Galois module classes of rings of integers $\mathcal{O}_L$ in tamely ramified Galois extensions L/K with Galois group G.

Conjecture 8.5 (McCulloh)**.** *$R(\mathcal{O}_K[G])$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_K[G])$.*

Let ℓ be a prime number, let G be a direct product of n cyclic groups of order ℓ, and let C be a cyclic group of order $\ell^n - 1$. Then G is isomorphic to the additive group of the finite field $\mathbb{F}_{\ell^n}$, and C to its multiplicative group. Via these isomorphisms, there is an action of C on G via multiplication.

For $\delta \in C$, let $t(\delta)$ denote the least non-negative residue modulo ℓ of $\mathrm{Tr}(\delta)$, where $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_{\ell^n}/\mathbb{F}}$. Let

$$\theta = \sum_{\delta \in C} t(\delta)\delta^{-1} \in \mathbb{Z}[C],$$

and let

$$\mathcal{I} = \mathbb{Z}[C](\theta/\ell) \cap \mathbb{Z}[C]$$

be the *Stickelberger ideal* of $\mathbb{Z}[C]$.

Recall that there is an *augmentation map* $\varepsilon\colon \mathcal{O}_K[G] \to \mathcal{O}_K$; it is the $\mathcal{O}_K$-linear map sending σ to 1 for all $\sigma \in G$.

The following result is stated in [McC83].

Theorem 8.6. *If G is elementary abelian, then*

$$R(\mathcal{O}_K[G]) = \mathrm{Cl}^0(\mathcal{O}_K[G])^{\mathcal{I}},$$

where $\mathrm{Cl}^0(\mathcal{O}_K[G])$ is the kernel of the map $\mathrm{Cl}(\mathcal{O}_K[G]) \to \mathrm{Cl}(\mathcal{O}_K)$ induced by the augmentation map $\mathcal{O}_K[G] \to \mathcal{O}_K$.

In [McC87], McCulloh extended this result to abelian groups G, but we do not give a precise formulation here.

We conclude this subsection with an important result of [AM18].

Theorem 8.7. *Suppose that G is of odd order, $|G|$ is coprime to the class number of K, and K contains no non-trivial $|G|$th roots of unity. Then $R(\mathcal{O}_K[G])$ is a subgroup of $\mathrm{Cl}(\mathcal{O}_K[G])$.*

Note that in [AM18] there is an explicit association of elements of $K_0(\mathcal{O}_K[G], \overline{K})$ to number field extensions, where $\overline{K}$ is the algebraic closure of K.

8.3. **Mayer–Vietoris sequence.** Let A, A_1, A_2, and $\widetilde{A}$ be rings, and let

$$\begin{tikzcd} A \arrow[r, "f_1"] \arrow[d, "f_2"'] & A_1 \arrow[d, "g_1"] \\ A_2 \arrow[r, "g_2"'] & \widetilde{A} \end{tikzcd}$$

be a *fibre product* of ring homomorphisms, meaning that the diagram commutes and

$$A \cong \{(a_1, a_2) \in A_1 \oplus A_2 \mid \ g_1(a_1) = g_2(a_2)\}.$$

Theorem 8.8 (Milnor's theorem)**.** *If g_1 or g_2 is surjective, then there is a* Mayer-Vietoris sequence

$$\begin{aligned} K_1(A) \xrightarrow{(f_1,f_2)} K_1(A_1) \times K_1(A_2) \xrightarrow{g_1 \times (1/g_2)} K_1(\widetilde{A}) \\ \xrightarrow{\partial} K_0(A) \xrightarrow{(f_1,f_2)} K_0(A_1) \times K_0(A_2) \xrightarrow{g_1 - g_2} K_0(\widetilde{A}). \end{aligned}$$

Proof. See [CR87, Theorem 42.13]. □

Let K be a number field, let G be an elementary abelian group of order ℓ^n, and let $\Sigma = \sum_{\delta \in G} \delta$. Write $\Gamma \mathcal{O}_K[G]/\mathcal{O}_K\Sigma$ and $\overline{\mathcal{O}_K} = \mathcal{O}_K/\ell^n\mathcal{O}_K$. Then

$$\begin{tikzcd} \mathcal{O}_K[G] \arrow[r, "\phi"] \arrow[d, "\varepsilon"'] & \Gamma \arrow[d, "\bar{\varepsilon}"] \\ \mathcal{O}_K \arrow[r, "\bar{\phi}"'] & \overline{\mathcal{O}_K} \end{tikzcd}$$

is a fibre product of ring homomorphisms. Let us extract a piece of the Mayer–Vietoris exact sequence:

$$K_1(\Gamma) \times K_1(\mathcal{O}_K) \xrightarrow{\bar{\varepsilon} \times (1/\bar{\phi})} K_1(\overline{\mathcal{O}_K}) \xrightarrow{\partial} K_0(\mathcal{O}_K[G]).$$

It can be shown that $K_1(\Gamma) \cong \Gamma^\times$, $K_1(\mathcal{O}_K) \cong \mathcal{O}_K^\times$, and $K_1(\overline{\mathcal{O}_K}) \cong \overline{\mathcal{O}_K}^\times$ (see [CR87, Theorem 40.31], using Gaussian elimination and the fact that elementary matrices are trivial in the K_1-groups. It can also be shown that $\partial(\bar{s}) = [(s, \Sigma)]$, where $(s, \Sigma) = s\mathcal{O}_K[G] + \Sigma\mathcal{O}_K[G]$ is called a *Swan-module* and is locally free. All their classes generate the Swan-subgroup $T \subseteq \mathrm{Cl}(\mathcal{O}_K[G])$. We get

$$\Gamma^\times \times \mathcal{O}_K^\times \xrightarrow{\bar{\varepsilon} \times (1/\bar{\phi})} \overline{\mathcal{O}_K}^\times \xrightarrow{\partial} T \to 0,$$

that is,

$$T \cong \overline{\mathcal{O}_K}^\times / \mathcal{O}_{\mathrm{K}}^\times \bar{\varepsilon}(\Gamma^\times) \tag{8.1}$$

8.4. **Swan modules and Hilbert–Speiser number fields.** Our main reference is [GRRS99].

Note that T is a $\mathbb{Z}[C]$-submodule of D, the subgroup of the class group consisting of those classes that become trivial under extension of scalars to the maximal order. Actually C acts trivially on T since $\delta \in C$ acts as an automorphism of G, so it maps $s\mathcal{O}_K[G]$ and $\mathcal{O}_K\Sigma$ to itself.

Proposition 8.9. *Assume G is elementary abelian of order $\ell^n > 2$. Then*

$$T^{\ell^{n-1}(\ell-1)/2} \subseteq R \cap D.$$

Proof. We have

$$\varepsilon(\theta) = \sum_{\delta \in C} t(\delta) = \ell^{n-1} \sum_{a=1}^{\ell-1} a = \ell^n(\ell-1)/2$$

and $N_C(\theta/\ell) = \varepsilon(\theta/\ell)N_C = \ell^{n-1}(\ell-1)/2N_C \in \mathcal{I}$. Then

$$\varepsilon(\ell^{n-1}\theta - N_C(\theta/\ell)) = \ell^n\ell^{n-1}(\ell-1)/2 - (\ell^{n-1}(\ell-1)/2)(\ell^n - 1) = \ell^{n-1}(\ell-1)/2.$$

Note that $D \subseteq \mathrm{Cl}^0(\mathcal{O}_K[G])$, because the map induced by augmentation commutes with extension of scalars to the maximal order. Since C acts trivially on T, $T^{\mathcal{I}} = T^{\varepsilon(\mathcal{I})}$ and

$$T^{\ell^{n-1}(\ell-1)/2} \subseteq T^{\mathcal{I}} \subseteq D^{\mathcal{I}} \subseteq \mathrm{Cl}^0(\mathcal{O}_K[G])^{\mathcal{I}} \cap D = R \cap D. \qquad \square$$

Lemma 8.10. *If $\gamma \in \Gamma^\times$, then $\bar{\varepsilon}(\gamma)^{\ell^n-1} \in \mathrm{Im}(\mathcal{O}_K^\times) \subseteq \mathcal{O}_K/\ell^n\mathcal{O}_K$.*

Proof. Let e be the identity of G. Then

$$0 \to (\mathcal{O}_K\Sigma)^C \to (\mathcal{O}_K[G])^C \to \Gamma^C \to H^1(C, \mathcal{O}_K\Sigma)$$

and

$$0 \to \mathcal{O}_K\Sigma \to \mathcal{O}_K e \oplus \mathcal{O}_K\Sigma \to \Gamma^C \to \mathrm{Hom}(C, \mathcal{O}_K\Sigma) = 0$$

Hence $\phi : \mathcal{O}_K e \to \Gamma^C$ is an isomorphism (in the paper, it is claimed that $\bar{\varepsilon}$ induces an isomorphism). Let $N : \Gamma^\times \to (\Gamma^\times)^C$ be the norm $N(\gamma) = \prod_{\delta \in C} \gamma^\delta$. Then

$$\bar{\varepsilon}(\gamma)^{\ell^n-1} = \bar{\varepsilon}(N(\gamma)) \subseteq \mathrm{Im}(\mathcal{O}_K^\times). \qquad \square$$

Theorem 8.11. *There is a natural surjective map*

$$T \to V_{\ell^n}^{\ell^n-1} = ((\mathcal{O}_K/\ell^n\mathcal{O}_K)^\times/\mathrm{Im}(\mathcal{O}_K^\times))^{\ell^n-1}.$$

Proof. By (8.1), $T \cong \overline{\mathcal{O}_K}^\times/\mathcal{O}_{\mathrm{K}}^\times\bar{\varepsilon}(\Gamma^\times) \cong V_{\ell^n}/\left(\bar{\varepsilon}(\Gamma^\times)/\mathrm{Im}(\mathcal{O}_K^\times)\right)$. We conclude by raising to the power $\ell^n - 1$ and using Lemma 8.10. □

Definition 8.12. A number field K is *Hilbert–Speiser* if all finite tamely ramified abelian extension L/K admit a normal integral basis.

We recall that $\mathbb{Q}$ is a Hilbert–Speiser field (Theorem 1.33).

Theorem 8.13 (Greither–Replogle–Rubin–Srivastav)**.** *Let K be a Hilbert–Speiser numer field. Then $K = \mathbb{Q}$.*

Proof. We just outline the strategy. For all $K \neq \mathbb{Q}$, one finds a prime ℓ such that V_ℓ is divisible by some prime q, which does not divide $\ell - 1$. Then $V_\ell^{(\ell-1)^2/2}$ is nontrivial. By Theorem 8.11,

$$T^{(\ell-1)/2} \to V_\ell^{(\ell-1)^2/2}$$

is surjective, so also $T^{(\ell-1)/2}$ must be nontrivial. Since, by Proposition 8.9,

$$T^{(\ell-1)/2} \subseteq R \cap D,$$

we conclude that R is nontrivial. □

Part 2. Hopf–Galois theory

9. An introduction to Hopf algebras

9.1. **Introduction.** Let L/K be a Galois extension of number fields or p-adic fields with Galois group G. If L/K is wildly ramified, then we know that L/K does not admit a normal integral basis, that is, $\mathcal{O}_L$ is not free over $\mathcal{O}_K[G]$. More generally, if for example $K = \mathbb{Q}$ and G is abelian, then $\mathcal{O}_L$ is free over its associated order $\mathfrak{A}_{L/K}$ in $K[G]$ (Leopoldt's theorem), but this may be false if G is not abelian or if $K \neq \mathbb{Q}$. Since $\mathfrak{A}_{L/K}$ is the unique $\mathcal{O}_K$-order over which $\mathcal{O}_L$ may be free, and since if $\mathcal{O}_L$ is free of rank one over an $\mathcal{O}_K$-subalgebra A of $K[G]$, then A is an order (by a straightforward reasoning), we deduce that if $\mathcal{O}_L$ is not free over $\mathfrak{A}_{L/K}$, then $K[G]$ is the wrong place where to look.

The main goal of this part is to introduce a new object, the Hopf algebra, which is a generalisation of $K[G]$, to define an associated order also in this context, and to study the freeness of $\mathcal{O}_L$ over this new order.

In this section, we mainly follow [Chi00]. We also refer to [Swe69] and [Und15], where the results are mostly given over fields instead of commutative rings, but the proofs can easily be adapted to our setting.

9.2. **Hopf algebras.** We fix a commutative ring R for the rest of the section. Recall that for us all rings have unity. Unadorned tensors denote tensors over R. If A and B are R-modules, write $\tau\colon A\otimes B \to B\otimes A$ for the switch map: $\tau(a\otimes b) = b\otimes a$ for all $a \in A$, $b \in B$.

In the first part of these notes, we have widely worked with R-algebras (usually for $R = K$ a field). The standard notion we have had in mind of an R-algebra is a ring A, together with a ring homomorphism $R \to A$ with image in the center of A, or equivalently, a ring A with a structure of R-module, with the following compatibility property: if $r \in R$ and $a, a' \in A$, then

$$r(aa') = (ra)a' = a(ra').$$

However, in this setting, it is convenient to give a third equivalent definition.

Definition 9.1. An *R-algebra* is a tuple (A, μ, ι), where A is an R-module, and $\mu\colon A \otimes A \to A$ and $\iota\colon R \to A$ are R-module homomorphisms, called respectively *multiplication* and *unity*, such that the following properties are satisfied:

- *Associativity:* the diagram

$$\begin{tikzcd}
A \otimes A \otimes A \arrow[r, "\mu\otimes\mathrm{id}"] \arrow[d, "\mathrm{id}\otimes\mu"'] & A \otimes A \arrow[d, "\mu"] \\
A \otimes A \arrow[r, "\mu"'] & A
\end{tikzcd}$$

  commutes.
- *Unitary:* the diagram

$$\begin{tikzcd}
R \otimes A \arrow[d, "\iota\otimes\mathrm{id}"'] \arrow[dr, "\mathfrak{s}"] & \\
A \otimes A \arrow[r, "\mu"] & A \\
A \otimes R \arrow[u, "\mathrm{id}\otimes\iota"] \arrow[ur, "\mathfrak{s}"'] &
\end{tikzcd}$$

commutes, where $\mathfrak{s}$ denotes the scalar multiplication.

Remark 9.2. Note that A is a ring with unity $1_A = \iota(1_R)$, not necessarily commutative. If there is no risk of confusion, we just write aa' for the element $\mu(a \otimes a') \in A$, for $a, a' \in A$.

Example 9.3.

- R is the simplest example of R-algebra.
- Let A and B be R-algebras. Then $A \otimes B$ is naturally an R-module, and also an R-algebra, with component-wise multiplication:

$$\mu_{A\otimes B} \colon (A \otimes B) \otimes (A \otimes B) \xrightarrow{\mathrm{id}_A \otimes \tau \otimes \mathrm{id}_B} (A \otimes A) \otimes (B \otimes B) \xrightarrow{\mu_A \otimes \mu_B} A \otimes B$$

and

$$\iota_{A\otimes B} \colon R \xrightarrow{\cong} R \otimes R \xrightarrow{\iota_A \otimes \iota_B} A \otimes B.$$

Explicitly, for $a, a' \in A$ and $b, b' \in B$, $(a \otimes b)(a' \otimes b') = (aa') \otimes (bb')$ and $\iota_{A\otimes B}(1_R) = 1_A \otimes 1_B$.

Definition 9.4. Let A and B be R-algebras. An R-module homomorphism $f \colon A \to B$ is an *R-algebra homomorphism* if f respects μ and ι, that is, the diagrams

$$\begin{tikzcd}
A \arrow[r, "f"] & B \\
A \otimes A \arrow[u, "\mu_A"] \arrow[r, "f \otimes f"'] & B \otimes B \arrow[u, "\mu_B"']
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[rr, "f"] & & B \\
& R \arrow[ul, "\iota_A"] \arrow[ur, "\iota_B"'] &
\end{tikzcd}$$

commute. The R-algebra *endomorphisms*, *isomorphisms*, and *automorphisms* are defined in the natural way.

Definition 9.5. Let A and B be R-algebras. An R-module homomorphism $f \colon A \to B$ is an *R-algebra antihomomorphism* if the diagrams

$$\begin{tikzcd}
A \arrow[rr, "f"] & & B \\
A \otimes A \arrow[u, "\mu_A"] \arrow[r, "\tau"'] & A \otimes A \arrow[r, "f \otimes f"'] & B \otimes B \arrow[u, "\mu_B"']
\end{tikzcd}
\qquad
\begin{tikzcd}
A \arrow[rr, "f"] & & B \\
& R \arrow[ul, "\iota_A"] \arrow[ur, "\iota_B"'] &
\end{tikzcd}$$

commute.

Definition 9.1 is useful in this context since it naturally yields the definition of a coalgebra: we just need to "reverse the arrows".

Definition 9.6. An *R-coalgebra* is a tuple (C, Δ, ε), where C is an R-module, and $\Delta \colon C \to C \otimes C$ and $\iota \colon C \to R$ are R-module homomorphisms, called respectively *comultiplication* and *counity*, such that the following properties are satisfied:

- *Coassociativity:* the diagram

$$\begin{tikzcd}
C \otimes C \otimes C & C \otimes C \arrow[l, "\Delta \otimes \mathrm{id}"'] \\
C \otimes C \arrow[u, "\mathrm{id} \otimes \Delta"] & C \arrow[l, "\Delta"] \arrow[u, "\Delta"']
\end{tikzcd}$$

commutes.

- *Counitary:* the diagram

$$\begin{tikzcd}
R \otimes C & \\
C \otimes C \arrow[u, "\varepsilon\otimes\mathrm{id}"] \arrow[d, "\mathrm{id}\otimes\varepsilon"'] & C \arrow[l, "\Delta"'] \arrow[ul, "\mathfrak{r}"'] \arrow[dl, "\mathfrak{l}"] \\
C \otimes R &
\end{tikzcd}$$

  commutes, where for all $c \in C$, $\mathfrak{r}(c) = 1_R \otimes c$ and $\mathfrak{l}(c) = c \otimes 1_R$.

Notation 9.7. We adopt the mysterious but remarkably efficient *Sweedler's notation.* Let C be an R-coalgebra, and let $c \in C$. We write

$$\Delta(c) = \sum_{(c)} c_{(1)} \otimes c_{(2)}.$$

Coassociativity becomes

$$\sum_{(c)} \left(\sum_{c_{(1)}} c_{(1)(1)} \otimes c_{(1)(2)} \right) \otimes c_{(2)} = \sum_{(c)} c_{(1)} \otimes \left(\sum_{c_{(2)}} c_{(2)(1)} \otimes c_{(2)(2)} \right),$$

and we just write this element as

$$\sum_{(c)} c_{(1)} \otimes c_{(2)} \otimes c_{(3)}.$$

Counitary becomes

$$1_R \otimes c = \sum_{(c)} \varepsilon(c_{(1)}) \otimes c_{(2)}, \quad c \otimes 1_R = \sum_{(c)} c_{(1)} \otimes \varepsilon(c_{(2)}),$$

that is,

$$c = \sum_{(c)} \varepsilon(c_{(1)})c_{(2)} = \sum_{(c)} c_{(1)}\varepsilon(c_{(2)}).$$

Example 9.8.

- R is the simplest example of R-coalgebra.
- Let C and D be R-coalgebras. Then $C \otimes D$ is naturally an R-module, and also an R-coalgebra:

$$\Delta_{C\otimes D} \colon C \otimes D \xrightarrow{\Delta_C \otimes \Delta_D} (C \otimes C) \otimes (D \otimes D) \xrightarrow{\mathrm{id}_C \otimes \tau \otimes \mathrm{id}_D} (C \otimes D) \otimes (C \otimes D)$$

  and

$$\varepsilon_{C\otimes D} \colon C \otimes D \xrightarrow{\varepsilon_C \otimes \varepsilon_D} R \otimes R \xrightarrow{\cong} R.$$

Definition 9.9. Let C and D be R-coalgebras. An R-module homomorphism $f \colon C \to D$ is an *R-coalgebra homomorphism* if f respects Δ and ε. In other words, the diagrams

$$\begin{tikzcd}
C \arrow[r, "f"] \arrow[d, "\Delta_C"'] & D \arrow[d, "\Delta_D"] \\
C \otimes C \arrow[r, "f\otimes f"'] & D \otimes D
\end{tikzcd}
\qquad
\begin{tikzcd}
C \arrow[rr, "f"] \arrow[dr, "\varepsilon_C"'] & & D \arrow[dl, "\varepsilon_D"] \\
& R &
\end{tikzcd}$$

commute. The R-coalgebra *endomorphisms*, *isomorphisms*, and *automorphisms* are defined in the natural way.

Definition 9.10. Let C, D be R-coalgebras. An R-module homomorphism $f\colon C \to D$ is an *R-coalgebra antihomomorphism* if the diagrams

$$\begin{tikzcd}
C \arrow[rr, "f"] \arrow[d, "\Delta_C"'] & & D \arrow[d, "\Delta_D"] \\
C \otimes C \arrow[r, "\tau"'] & C \otimes C \arrow[r, "f \otimes f"'] & D \otimes D
\end{tikzcd}
\qquad
\begin{tikzcd}
C \arrow[rr, "f"] \arrow[dr, "\varepsilon_C"'] & & D \arrow[dl, "\varepsilon_D"] \\
& R &
\end{tikzcd}$$

commute.

We are interested in objects that are simultaneously R-algebras and R-coalgebras.

Lemma 9.11. *Let $(H, \mu, \iota, \Delta, \varepsilon)$ be a tuple where (H, μ, ι) is an R-algebra and (H, Δ, ε) is an R-coalgebra. The following are equivalent:*

(1) *μ and ι are R-coalgebra homomorphisms.*

(2) *Δ and ε are R-algebra homomorphisms.*

Proof. It is immediate to see that both conditions are defined by the commutativity of the same diagrams. □

Definition 9.12. An *R-bialgebra* is a tuple $(H, \mu, \iota, \Delta, \varepsilon)$, where (H, μ, ι) is an R-algebra, (H, Δ, ε) is an R-coalgebra, and Δ and ε are R-algebra homomorphisms.

Definition 9.13. Let H and H' be R-bialgebras. An R-module homomorphism $f\colon H \to H'$ is an *R-bialgebra homomorphism* if f is an R-algebra and R-coalgebra homomorphism. The R-bialgebra *endomorphisms*, *isomorphisms*, and *automorphisms* are defined in the natural way.

We are ready for our main definition.

Definition 9.14. An *R-Hopf algebra* is a tuple $(H, \mu, \iota, \Delta, \varepsilon, \lambda)$, where $(H, \mu, \iota, \Delta, \varepsilon)$ is an R-bialgebra and $\lambda\colon H \to H$ is an R-module homomorphism, called *antipode*, such that the following property is satisfied:
Antipode property: the diagram

$$\begin{tikzcd}
& H \otimes H \arrow[rr, "\mathrm{id} \otimes \lambda"] & & H \otimes H \arrow[dr, "\mu"] & \\
H \arrow[ur, "\Delta"] \arrow[rr, "\varepsilon"] \arrow[dr, "\Delta"'] & & R \arrow[rr, "\iota"] & & H \\
& H \otimes H \arrow[rr, "\lambda \otimes \mathrm{id}"'] & & H \arrow[ur, "\mu"'] &
\end{tikzcd}$$

commutes, that is,

$$\iota \circ \varepsilon = \mu \circ (\mathrm{id} \otimes \lambda) \circ \Delta = \mu \circ (\lambda \otimes \mathrm{id}) \circ \Delta,$$

or, in Sweedler's notation,

$$\varepsilon(h) 1_H = \sum_{(h)} h_{(1)} \lambda(h_{(2)}) = \sum_{(h)} \lambda(h_{(1)}) h_{(2)}$$

for all $h \in H$.

Remark 9.15. In the definition of Hopf algebras given in [Chi00], it is required that the antipode λ is an algebra and coalgebra antihomomorphism. However, this is implied already by Definition 9.14; see [Swe69, Proposition 4.0.1] or [Und15, Propositions 3.1.8 and 3.1.10].

Definition 9.16. Let H and H' be R-Hopf algebras. An R-module homomorphism $f\colon H \to H'$ is an *R-Hopf algebra homomorphism* if f is an R-bialgebra homomorphism, and f respects λ, that is, the diagram

$$\begin{tikzcd}
H \arrow[r, "f"] \arrow[d, "\lambda_H"'] & H' \arrow[d, "\lambda_{H'}"] \\
H \arrow[r, "f"'] & H'
\end{tikzcd}$$

commutes. The R-Hopf algebra *endomorphisms*, *isomorphisms*, and *automorphisms* are defined in the natural way.

Definition 9.17. An R-Hopf algebra H is

- *commutative* if H is so as R-algebra, that is, for all $h, h' \in H$,
$$hh' = h'h;$$
- *cocommutative* if $\tau \circ \Delta = \Delta$, that is, for all $h \in H$,
$$\sum_{(h)} h_{(1)} \otimes h_{(2)} = \sum_{(h)} h_{(2)} \otimes h_{(1)};$$
- *abelian* if H is both commutative and cocommutative.

Example 9.18.

- R is the simplest example of R-Hopf algebra. Here λ is R-linear and respects $\iota = \mathrm{id}$, so necessarily $\lambda(r) = r$.
- Let S be an R-algebra. Then S is an S-Hopf algebra, and if H is an R-Hopf algebra, then $S \otimes H$ is naturally an $S \otimes R$-Hopf algebra. Identifying S and $S \otimes R$, we find that $S \otimes H$ is an S-Hopf algebra.

We can finally study our main source of Hopf algebras.

Example 9.19. Let G be a finite group, and consider the R-group algebra $R[G]$. We claim that $R[G]$ is also an R-Hopf algebra. Since $R[G]$ is a free R-module of rank $|G|$ with basis $\{\sigma \mid \sigma \in G\}$, and all the maps defining the structure of R-Hopf algebra are R-module homomorphisms, it is enough to define them on the elements of G: for all $\sigma \in G$,

$$\Delta(\sigma) = \sigma \otimes \sigma,$$
$$\varepsilon(\sigma) = 1_R,$$

and

$$\lambda(\sigma) = \sigma^{-1}.$$

It is straightforward to check the axioms; for example,

$$(\mu \circ (\mathrm{id} \otimes \lambda) \circ \Delta)(\sigma) = (\mu \circ (\mathrm{id} \otimes \lambda))(\sigma \otimes \sigma) = \mu(\sigma \otimes \sigma^{-1}) = 1_{R[G]} = (\iota \circ \varepsilon)(\sigma)$$

and

$$(\mu \circ (\lambda \otimes \mathrm{id}) \circ \Delta)(\sigma) = (\mu \circ (\lambda \otimes \mathrm{id}))(\sigma \otimes \sigma) = \mu(\sigma^{-1} \otimes \sigma) = 1_{R[G]} = (\iota \circ \varepsilon)(\sigma),$$

so λ satisfies the antipode property.

The R-Hopf algebra $R[G]$ is always cocommutative, and $R[G]$ is commutative if and only if G is abelian.

9.3. **Interlude: more on commutative module theory.** We collect here some useful facts about modules, which we use in the following sections.

Let H be an R-module. Denote by H^* the linear dual of H:

$$H^* = \mathrm{Hom}_R(H, R).$$

Clearly, H^* is an R-module, and it shares some properties of H.

Definition 9.20. A *finite* R-module is a finitely generated projective module over R.

Remark 9.21. If R is a field, then finite just means finite-dimensional.

Since the projective modules are exactly the direct summand of the free modules, we can immediately derive the next results.

Lemma 9.22. *Let H be a finite R-module. Then the following facts hold:*

(1) *H^* is a finite R-module.*
(2) *$H \cong H^{**}$ as R-modules.*
(3) *H admits a* projective coordinate system*, that is, a set $\{h_i, f_i\}_{i=1}^n$, where $h_i \in H$ and $f_i \in H^*$ for all $1 \le i \le n$, such that for all $h \in H$,*
$$h = \sum_{i=1}^{n} f_i(h)h_i.$$
(4) *If $\gamma\colon H \to H'$ is an R-module homomorphism between finite modules, we can define the* traspose *of γ to be the R-module homomorphism $\gamma^*\colon H'^* \to H^*$, with $\gamma^*(f')(h) = f'(\gamma(h))$. Then γ is bijective if and only if γ^* is bijective.*

Notation 9.23. Since if H is a finite R-module, then we can identify it with the dual of H^*, we avoid to choose a point of view using the map

$$\langle\ ,\ \rangle\colon H^* \otimes H \to R,$$

defined by $\langle f, h\rangle = f(h)$.

Remark 9.24. Note that if $\{h_i, f_i\}_{i=1}^n$ is a projective coordinate system for a finite R-module H, then $\{f_i, h_i\}_{i=1}^n$ is a projective coordinate system for H^*.

Definition 9.25. An R-module H is

- *flat* if for all exact sequences of R-modules
$$0 \to A \xrightarrow{\varphi_1} B \xrightarrow{\varphi_2} C \to 0,$$
the sequence
$$0 \to H \otimes A \xrightarrow{\mathrm{id}_H \otimes \varphi_1} H \otimes B \xrightarrow{\mathrm{id}_H \otimes \varphi_2} H \otimes C \to 0$$
is exact;
- *faithfully flat* if, for all R-modules A, B and C, the sequence
$$0 \to A \xrightarrow{\varphi_1} B \xrightarrow{\varphi_2} C \to 0,$$
is exact if and only if the sequence
$$0 \to H \otimes A \xrightarrow{\mathrm{id}_H \otimes \varphi_1} H \otimes B \xrightarrow{\mathrm{id}_H \otimes \varphi_2} H \otimes C \to 0$$
is exact;

- *finitely presented* if there exist $n \in \mathbb{N}$ and a surjective R-module homomorphism $\varphi\colon R^n \to H$ with finitely generated kernel;
- *faithful* if the only $r \in R$ such that $rh = 0$ for all $h \in H$ is $r = 0$.

Proposition 9.26.

- *Every projective R-module is flat.*
- *A direct sum of R-modules is flat if and only if each module is flat.*

Proof. See [Rot09, Proposition 3.46]. □

Example 9.27. Suppose that R is Noetherian.

- For all maximal ideals $\mathfrak{m}$ of R, the completion $R_{\mathfrak{m}}$ is flat; see [Mat70, Corollary 1 of Theorem 55]. In particular, the direct sum $\bigoplus_{\mathfrak{m}} R_{\mathfrak{m}}$ over all maximal ideals of R is flat.
- The direct sum $\bigoplus_{\mathfrak{m}} R_{\mathfrak{m}}$ over all maximal ideals of R is also faithfully flat. This follows from [Mat89, Theorem 7.2], flatness of $R_{\mathfrak{m}}$, and the fact that if M is an R-module and $M_{\mathfrak{m}} = 0$ for every $\mathfrak{m}$, then also $M = 0$.

Proposition 9.28. *An R-module H is finite if and only if H is finitely presented and flat.*

Proof. Combine [Rot09, Proposition 3.11], Proposition 9.26, and [Rot09, Theorem 3.56]. □

The following fact is really useful in the sequel.

Theorem 9.29. *Let S be an R-algebra, and let M and N be R-modules. If M is finite, then the natural S-module homomorphism*

$$\theta\colon S \otimes \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(S \otimes M, S \otimes N)$$

is bijective.

Proof. This result is proved in [Rei03, section 2e] for finitely presented flat modules. By Proposition 9.28, we derive our assertion. □

9.4. **Dual algebra.** Let H be a finite R-Hopf algebra. We claim that also H^* is an R-Hopf algebra. As one can expect, we use the R-algebra structure of H to define the structure or R-coalgebra of H^*, and viceversa. If $f, f' \in H^*$ and $r \in R$, then

$$\begin{aligned} \Delta_{H^*}(f) &= f \circ \mu_H, \\ \varepsilon_{H^*}(f) &= f(1_H), \\ \mu_{H^*}(f \otimes f') &= (f \otimes f') \circ \Delta_H \quad \text{(here we are identifying } R \otimes R \text{ with } R), \\ \iota_{H^*}(r) &= r\varepsilon_H \quad \text{(note that } \varepsilon_H \in H^*), \end{aligned}$$

and

$$\lambda_{H^*}(f) = f \circ \lambda_H.$$

Proposition 9.30. *Let H be a finite R-Hopf algebra. Then H^*, with the structure defined above, is a finite R-Hopf algebra.*

Proof. See [Und15, Proposition 3.1.12]. □

Remark 9.31. By the definition, it immediately follows that H is commutative if and only if H^* is cocommutative, and H is cocommutative if and only if H^* is commutative.

Also by definition, it is really straightforward to check the following fact.

Lemma 9.32. *Let H be a finite R-Hopf algebra. Then $H \cong H^{**}$ as R-Hopf algebras.*

From now on, we identify H^{**} with H, when H is a finite R-Hopf algebra.

Example 9.33. Let G be a finite group. Then $H = R[G]$ is a finite R-Hopf algebra, and we can study the dual $H^* = R[G]^*$. Consider the dual basis $\{e_\sigma \mid \sigma \in G\}$, where $e_\sigma(\tau) = \delta_{\sigma,\tau}$ is given by the Kronecker's delta. For all $\sigma, \tau, \rho \in G$ and $r \in R$,

$$\Delta_{H^*}(e_\sigma)(\tau \otimes \rho) = e_\sigma(\tau\rho) = \delta_{\sigma,\tau\rho} \implies \Delta_{H^*}(e_\sigma) = \sum_{\tau\rho=\sigma} e_\tau \otimes e_\rho,$$
$$\varepsilon_{H^*}(e_\sigma) = e_\sigma(1_{R[G]}) = \delta_{\sigma,1_G},$$
$$\mu_{H^*}(e_\sigma \otimes e_\tau)(\rho) = (e_\sigma \otimes e_\tau)(\rho \otimes \rho) = \delta_{\sigma,\rho}\delta_{\tau,\rho} \implies \mu_{H^*}(e_\sigma \otimes e_\tau) = \delta_{\sigma\tau} e_\sigma,$$
$$\iota_{H^*}(r) = r\varepsilon_H = r \sum_{\sigma' \in G} e_{\sigma'},$$

and

$$\lambda_{H^*}(e_\sigma)(\tau) = e_\sigma(\tau^{-1}) = \delta_{\sigma,\tau^{-1}} \implies \lambda_{H^*}(e_\sigma) = e_{\sigma^{-1}}.$$

Note that the elements of the dual basis are pairwise orthogonal idempotents, by definition of μ_{H^*}.

9.5. **Grouplike elements.** If G is a finite group, then $R[G]$ is an R-Hopf algebra, and if $\sigma \in G$, then $\Delta(\sigma) = \sigma \otimes \sigma$. Motivated by this fact, we can give the following definition.

Definition 9.34. Let H be an R-Hopf algebra. A nonzero element $h \in H$ is *grouplike* if $\Delta(h) = h \otimes h$. We write $G(H)$ for the set of grouplike elements.

Proposition 9.35. *Let H be an R-Hopf algebra. Suppose that R has no idempotents different from 0 and 1_R. Then every grouplike element $h \in H$ satisfies $\varepsilon(h) = 1_R$ and $G(H)$ is a subgroup of the multiplicative group of units of H.*

Proof. The first claim follows from counitary: if $h \in G(R)$, then

$$h = (\mathfrak{s} \circ (\varepsilon \otimes \mathrm{id}) \circ \Delta)(h) = \varepsilon(h)h,$$

hence

$$\varepsilon(h) = \varepsilon(\varepsilon(h)h) = \varepsilon(h)\varepsilon(h).$$

Since R has no idempotent different from 0 and 1_R, and $h \neq 0$, we conclude that $\varepsilon(h) = 1_R$.

We claim that $\lambda(h) \in G(H)$ and $\lambda(h)$ is the inverse of h. For the first step, we need to use that λ is an R-coalgebra antihomomorphism:

$$\Delta(\lambda(h)) = ((\lambda \otimes \lambda) \circ \tau \circ \Delta)(h) = \lambda(h) \otimes \lambda(h).$$

Then, by the antipode property,

$$1_H = \iota(\varepsilon(h)) = (\mu \circ (\mathrm{id} \otimes \lambda) \circ \Delta)(h) = h\lambda(h)$$

and

$$1_H = \iota(\varepsilon(h)) = (\mu \circ (\lambda \otimes \mathrm{id}) \circ \Delta)(h) = \lambda(h)h.$$

This also shows that $\lambda(h) \neq 0$. Finally, we see that $G(R)$ is closed under multiplication. Let $h, h' \in G(H)$. As h is invertible, $h \cdot h' \neq 0$. Since Δ is an R-algebra homomorphism, we find

$$\Delta(hh') = \Delta(h)\Delta(h') = (hh') \otimes (hh'),$$

that is, $hh' \in G(H)$. □

Remark 9.36. Let H be a finite R-Hopf algebra, and consider $f \in H^*$ different from the zero map. Recall that, if $h, h' \in H$, then

$$\Delta_{H^*}(f)(h \otimes h') = (f \circ \mu_H)(h \otimes h') = f(hh').$$

If $f\colon H \to R$ is an R-algebra homomorphism, then $f(hh') = f(h)f(h')$, so f is grouplike. Also the converse is true if R has no idempotent different from 0 and 1_R.

Proposition 9.37. *Suppose that R is a field, and let H be an R-Hopf algebra. Then distinct grouplike elements of H are linearly independent over R.*

Proof. Suppose $h, h_1, \ldots, h_n$ are grouplike elements such that $h_1, \ldots, h_n$ are linearly independent and

$$h = \sum_{i=1}^{n} r_i h_i.$$

We claim that $h = h_i$ for some i. Note that

$$\sum_{i,j} r_i r_j (h_i \otimes h_j) = h \otimes h = \Delta(h) = \Delta\left(\sum_{i=1}^{n} r_i h_i\right) = \sum_{i=1}^{n} r_i \Delta(h_i) = \sum_{i=1}^{n} r_i (h_i \otimes h_i).$$

Since $\{h_i \otimes h_j\}_{i,j}$ are linearly independent over R, we deduce that

$$\begin{cases} r_i r_j = 0 & \text{if } i \neq j, \\ r_i^2 = r_i & \text{for all } i. \end{cases}$$

As R is a field and $h \neq 0$, we conclude that there exists exactly one i such that $h = h_i$, as claimed. □

Corollary 9.38. *Suppose that R is a field, and let H be a finite R-Hopf algebra. If there is an R-basis $N = \{h_i\}$ of H consisting of grouplike elements, then $N = G(H)$ is a group, and H is the group ring $R[N]$.*

9.6. **Modules and comodules.** We fix an R-Hopf algebra H for this subsection. We need to work with R-modules which also admit an action of H. We give the following definition, since we require compatibility between the two structures.

Definition 9.39. An R-module S is a *left H-module* if there is an R-module homomorphism $\alpha\colon H \otimes S \to S$ such that the following properties are satisfied:

- *Associativity:* the diagram

$$\begin{tikzcd} H \otimes H \otimes S \arrow[r, "\mu_H \otimes \mathrm{id}"] \arrow[d, "\mathrm{id} \otimes \alpha"'] & H \otimes S \arrow[d, "\alpha"] \\ H \otimes S \arrow[r, "\alpha"'] & S \end{tikzcd}$$

  commutes.

- *Unitary:* the diagram

$$\begin{tikzcd}
R \otimes S \arrow[d, "\iota_H \otimes \mathrm{id}"'] \arrow[dr, "\mathfrak{s}"] & \\
H \otimes S \arrow[r, "\alpha"'] & S
\end{tikzcd}$$

  commutes.

Notation 9.40. If there is no risk of confusion, we just write $h \cdot s$ for the element $\alpha(h \otimes s) \in S$, for $h \in H$, $s \in S$.

Example 9.41.

- R is a left H-module via ε: for all $h \in H$ and $r \in R$,

$$h \cdot r = \varepsilon(h)r.$$

- Let S be a left H-module. Then $S \otimes S$ is a left H-module via Δ: for all $h \in H$ and $s, t \in S$,

$$h \cdot (s \otimes t) = \sum_{(h)} (h_{(1)} \cdot s) \otimes (h_{(2)} \cdot t).$$

Definition 9.42. Let S and S' be left H-modules. An R-module homomorphism $f\colon S \to S'$ is an *H-module homomorphism* if f respects α, that is, the diagram

$$\begin{tikzcd}
S \arrow[r, "f"] & S' \\
H \otimes S \arrow[u, "\alpha_S"] \arrow[r, "\mathrm{id} \otimes f"'] & H \otimes S' \arrow[u, "\alpha_{S'}"']
\end{tikzcd}$$

commutes.

As usual, we can give the "dual" definition.

Definition 9.43. An R-module S is a *right H-comodule* if there is an R-module homomorphism $\beta\colon S \to S \otimes H$ such that the following properties are satisfied:

- *Coassociativity:* the diagram

$$\begin{tikzcd}
S \otimes H \otimes H & S \otimes H \arrow[l, "\beta \otimes \mathrm{id}"'] \\
S \otimes H \arrow[u, "\mathrm{id} \otimes \Delta_H"] & S \arrow[l, "\beta"] \arrow[u, "\beta"']
\end{tikzcd}$$

  commutes.
- *Counitary:* the diagram

$$\begin{tikzcd}
S \otimes H \arrow[d, "\mathrm{id} \otimes \varepsilon_H"'] & S \arrow[l, "\beta"'] \arrow[dl, "\mathfrak{i}"] \\
S \otimes R &
\end{tikzcd}$$

  commutes.

Notation 9.44. If S is a right H-module and $s \in S$, then we can adapt Sweedler's notation as follows:

$$\beta(s) = \sum_{(s)} s_{(0)} \otimes s_{(1)}, \quad \text{for } s_{(0)} \in S \text{ and } \ s_{(1)} \in H.$$

For example, coassociativity becomes

$$(\beta \otimes \mathrm{id})(\beta(s)) = (\mathrm{id} \otimes \Delta_H)(\beta(s)) = \sum_{(s)} s_{(0)} \otimes s_{(1)} \otimes s_{(2)}.$$

Example 9.45.

- R is a right H-comodule via ι: for all $r \in R$,
$$\beta(r) = r \otimes \iota(1_R) = r \otimes 1_H.$$
- Let S be a right H-comodule. Then $S \otimes S$ is a right H-comodule via μ: for all $s, t \in S$,
$$\beta(s \otimes t) = \sum_{(s),(t)} s_{(0)} \otimes t_{(0)} \otimes \mu(s_{(1)} \otimes t_{(1)}).$$

Definition 9.46. Let S and S' be right H-comodules. An R-module homomorphism $f \colon S \to S'$ is an *H-comodule homomorphism* if f respects β, that is, the diagram

$$\begin{tikzcd}
S \arrow[r, "f"] \arrow[d, "\beta_S"'] & S' \arrow[d, "\beta_{S'}"] \\
S \otimes H \arrow[r, "f \otimes \mathrm{id}"'] & S \otimes H
\end{tikzcd}$$

commutes.

Now suppose that H is finite, with projective coordinate system $\{h_i, f_i\}_{i=1}^n$. If S is a right H-comodule, then S becomes a left H^*-module, via

$$f \cdot s = \sum_{(s)} s_{(0)} \langle f, s_{(1)} \rangle.$$

Since we have identified H^{**} with H, this also means that if S is a right H^*-comodule, then S is a left H-module.

Conversely, if S is a left H-module, then S becomes a right H^*-comodule, via

$$\beta(s) = \sum_{i=1}^n (h_i \cdot s) \otimes f_i.$$

Clearly, there are some properties to be carefully checked; see [Chi00, section 2]. Still, we may deduce the next important result.

Proposition 9.47. *Let H be a finite R-Hopf algebra, and let S be an R-module. Then S is a left H-module if and only if S is a right H^*-comodule. In addition, the processes of going from the H-module action to the H^*-comodule action and the opposite are inverse operations.*

Proof. We just prove the final claim. Let $\{h_i, f_i\}_{i=1}^n$ be a projective coordinate system for H. Suppose S is a left H-module. Then S is a right H^*-comodule, where, for all $s \in S$,

$$\beta(s) = \sum_{i=1}^n (h_i \cdot s) \otimes f_i.$$

This H^*-comodule action induces a $H^{**} = H$-module action, as follows:

$$\alpha(h \otimes s) = \sum_{i=1}^n (h_i \cdot s)\langle h, f_i \rangle = \left(\sum_{i=1}^n \langle h, f_i \rangle h_i \right) \cdot s = h \cdot s,$$

that is, we recover the original H-module action on S.

Conversely, suppose S is a right H^*-comodule, via

$$s \mapsto \sum_{(s)} s_{(0)} \otimes s_{(1)} \in S \otimes H^*.$$

Then S is also a left $H^{**} = H$-module, via

$$h \cdot s = \sum_{(s)} s_{(0)} \langle h, s_{(1)} \rangle.$$

This H-module action induces a H^*-comodule action, as follows:

$$\begin{aligned} \beta(s) &= \sum_{i=1}^{n} (h_i \cdot s) \otimes f_i = \sum_{i=1}^{n} \left(\sum_{(s)} s_{(0)} \langle h_i, s_{(1)} \rangle \right) \otimes f_i \\ &= \sum_{i=1}^{n} \sum_{(s)} s_{(0)} \langle h_i, s_{(1)} \rangle \otimes f_i \\ &= \sum_{i=1}^{n} \sum_{(s)} s_{(0)} \otimes \langle h_i, s_{(1)} \rangle f_i \\ &= \sum_{(s)} s_{(0)} \otimes \sum_{i=1}^{n} \langle h_i, s_{(1)} \rangle f_i = \sum_{(s)} s_{(0)} \otimes s_{(1)}, \end{aligned}$$

that is, we recover the original H^*-comodule action on S. □

10. Hopf–Galois extensions

The goal of this section is to introduce Hopf–Galois extensions, fundamental structures in this theory. We follow again [Chi00], and we keep the notation of Section 9.

10.1. Module and comodule algebras.

Let us fix an R-Hopf algebra H.

Definition 10.1. Let S be a left H-module and an R-algebra. We say that S is a *left H-module algebra* if, for all $h \in H$ and $s, t \in S$,

$$\begin{aligned} h \cdot (st) &= \sum_{(h)} (h_{(1)} \cdot s)(h_{(2)} \cdot t), \\ h \cdot 1_S &= \varepsilon(h) 1_S. \end{aligned}$$

Lemma 10.2. *Let S be a left H-module and an R-algebra. Then S is a left H-module algebra if and only if μ_S and ι_S are H-module homomorphisms.*

Proof. This is straightforward, since the two properties defining a left H-module algebra are precisely describing the commutativity of the diagrams

$$\begin{tikzcd} S \otimes S \arrow[r, "\mu_S"] & S & R \arrow[r, "\iota_S"] & S \\ H \otimes S \otimes S \arrow[u, "\alpha_{S \otimes S}"] \arrow[r, "\mathrm{id} \otimes \mu_S"'] & H \otimes S \arrow[u, "\alpha_S"'] & H \otimes R \arrow[u, "\alpha_R"] \arrow[r, "\mathrm{id} \otimes \iota_S"'] & H \otimes S \arrow[u, "\alpha_S"'] \end{tikzcd}$$

which imply that μ_S and ι_S are H-module homomorphisms. □

This equivalent way to see left H-module algebras immediately implies the following definition.

Definition 10.3. Let S be a right H-comodule and an R-algebra. We say that S is a *right H-comodule algebra* if μ_S and ι_S are H-comodule homomorphisms.

Remark 10.4. Recall that μ_S is an H-comodule homomorphism if and only if the diagram

$$\begin{tikzcd} S \otimes S \arrow[r, "\mu_S"] \arrow[d, "\beta_{S\otimes S}"'] & S \arrow[d, "\beta_S"] \\ S \otimes S \otimes H \arrow[r, "\mu_S \otimes \mathrm{id}"'] & S \otimes H \end{tikzcd}$$

commutes. Explicitly, if $s, t \in S$, then

$$\begin{aligned} \beta_S(st) &= \sum_{(s),(t)} s_{(0)}t_{(0)} \otimes s_{(1)}t_{(1)} = \left(\sum_{(s)} s_{(0)} \otimes s_{(1)} \right) \left(\sum_{(t)} t_{(0)} \otimes t_{(1)} \right) \\ &= \beta_S(s)\beta_S(t). \end{aligned}$$

Since ι_S is an H-comodule homomorphism if and only if $\beta_S(1_S) = 1_S \otimes 1_H$, we deduce that S is a right H-comodule algebra if and only if β_S is an R-algebra homomorphism.

Now suppose H is finite. In Proposition 9.47, we have seen how to move between left H-modules and right H-modules. The same results also holds for module and comodule algebras.

Proposition 10.5. *Let S be an R-algebra. Then S is a left H-module algebra if and only if S is a right H^*-comodule algebra.*

Example 10.6. Let H be a finite R-Hopf algebra. Then H^* is a right H^*-comodule via comultiplication map

$$\Delta_{H^*} \colon H^* \to H^* \otimes H^*.$$

This means that H^* is a left H-module: for all $h \in H$ and $f \in H^*$,

$$h \cdot f = \sum_{(f)} f_{(1)} \langle h, f_{(2)} \rangle \in H^*.$$

Since, by definition, Δ_{H^*} is an R-algebra homomorphism, μ_S is an H^*-comodule homomorphism. An easy verification implies that this is true also for ι_S, and so H^* is a right H^*-comodule algebra, or equivalently, a left H-module algebra.

We can think to module and comodule algebras as generalisations of the concepts of actions and gradings of algebras by groups.

If S is a finite commutative R-algebra and G is a finite group of R-algebra automorphisms of S, then for all $\sigma \in G$ and $s, s' \in S$, $\sigma(ss') = \sigma(s)\sigma(s')$. Clearly S is a left $H = R[G]$-module via

$$\left(\sum_{\sigma \in G} r_\sigma \sigma \right) \cdot s = \sum_{\sigma \in G} r_\sigma \sigma(s).$$

We claim that S is also a left $R[G]$-module algebra. Since $\Delta_H(\sigma) = \sigma \otimes \sigma$,

$$\begin{aligned}\left(\sum_{\sigma \in G} r_\sigma \sigma\right) \cdot (st) = \sum_{\sigma \in G} r_\sigma \sigma(st) &= \sum_{\sigma \in G} r_\sigma \sigma(s)\sigma(t) \\ &= \mu_S\left(\sum_{\sigma \in G} r_\sigma (\sigma \otimes \sigma)(s \otimes t)\right) \\ &= \mu_S\left(\left(\sum_{\sigma \in G} r_\sigma \sigma\right) \cdot (s \otimes t)\right).\end{aligned}$$

Since $\varepsilon_H(\sigma) = 1_R$,

$$\left(\sum_{\sigma \in G} r_\sigma \sigma\right) \cdot 1_S = \sum_{\sigma \in G} r_\sigma \sigma(1_S) = \sum_{\sigma \in G} r_\sigma 1_S = \varepsilon_H\left(\sum_{\sigma \in G} r_\sigma \sigma\right) 1_S.$$

Definition 10.7. If G is also abelian, we say that S is a *G-graded R-algebra* if we can write S as direct sum of R-modules

$$S = \bigoplus_{\sigma \in G} S_\sigma,$$

where $\iota_S(R) \subseteq S_1$ and for all $\sigma, \tau \in G$,

$$S_\sigma S_\tau \subseteq S_{\sigma\tau}.$$

If we consider the R-module homomorphism

$$\begin{aligned}\beta \colon S &\to S \otimes R[G] \\ s &\mapsto s \otimes \sigma,\end{aligned}$$

where $s \in S_\sigma$, then it is immediate to see that β is an R-algebra homomorphism and to get that S is a right $R[G]$-comodule algebra.

10.2. **(Hopf–)Galois extensions.** In order to define Hopf–Galois extensions, we need to give a more general definition of Galois extensions.

Theorem 10.8. *Let S be a finite commutative R-algebra, and let G be a finite group of R-algebra automorphisms of S. The following are equivalent:*

(1) *The R-module homomorphism*

$$\begin{aligned}j \colon S \otimes R[G] \cong S[G] &\to \operatorname{End}_R(S) \\ \sum_{\sigma \in G} s_\sigma \sigma &\mapsto \left(t \mapsto \sum_{\sigma \in G} s_\sigma \sigma(t)\right)\end{aligned}$$

is bijective.

(2) *The R-module homomorphism*

$$\begin{aligned}h \colon S \otimes S \to S \otimes \operatorname{Hom}_R(R[G], R) &\cong \operatorname{Hom}_S(S[G], S) \\ s \otimes t &\mapsto \left(\sum_{\sigma \in G} s_\sigma \sigma \mapsto s \sum_{\sigma \in G} s_\sigma \sigma(t)\right)\end{aligned}$$

is bijective.

(3) *For all maximal ideals $\mathfrak{m}$ of S and $\sigma \neq 1$ in G, there exists $s \in S$ such that $\sigma(s) - s \notin \mathfrak{m}$.*

Proof. See [CHR65, Theorem 1.3]. In (2), the isomorphism is given by Theorem 9.29. □

Definition 10.9. Let S be a finite commutative R-algebra, and let G be a finite group of R-algebra automorphisms of S. Then S is a *Galois extension of R with group G* if one condition in Theorem 10.8 holds.

Example 10.10. Let L/K be a finite Galois extension of fields of degree n, and G be a finite group of K-algebra automorphisms of L. If L/K is Galois with Galois group G in the usual sense, then L is a Galois extension of K with group G, in the sense of definition 10.9. Indeed, the injectivity of the map j follows immediately from linear independence of characters, and since

$$\dim_K(L[G]) = \dim_K(L)|G| = \dim_K(L)^2 = \dim_K(\mathrm{End}_K(L)),$$

we derive our assertion.

Conversely, if L is a Galois extension of K with group G in the sense of definition 10.9, then by the isomorphism j we deduce that $|\operatorname{Aut}_K(L)| \geq |G| = n$, and so by Artin's characterisation of Galois extensions, L/K is Galois with Galois group $G = \operatorname{Aut}_K(L)$ is the usual sense.

Example 10.11. Let L/K be a Galois extension of number fields or p-adic fields with Galois group G. Consider $\mathcal{O}_L$ as a finite $\mathcal{O}_K$-algebra (which is projective as an $\mathcal{O}_K$-module, since it is locally projective at every prime). The condition in Theorem 10.8(3) says that for all primes $\mathfrak{P}$ of $\mathcal{O}_L$, the inertia subgroup

$$G_0 = \{\sigma \in G \mid \sigma(x) \equiv x \pmod{\mathfrak{P}} \text{ for all } x \in \mathcal{O}_L\}$$

is trivial, that is, $\mathfrak{P}$ is unramified over $\mathcal{O}_K$. We deduce that $\mathcal{O}_L$ is a Galois extension of $\mathcal{O}_K$ with group G if and only if L/K is unramified.

With Definition 10.9 in mind, we can define Hopf–Galois extensions.

Definition 10.12. Let H be a finite cocommutative R-Hopf algebra. A finite commutative R-algebra S is an *H-Galois extension*, or *H-Galois*, if the following hold:

(1) S is a left H-module algebra.
(2) The R-module homomorphism
$$\begin{aligned} j\colon S \otimes H &\to \mathrm{End}_R(S) \\ s \otimes h &\mapsto (t \mapsto s(h \cdot t)) \end{aligned}$$
is bijective.

Note that this implies that if S and H are free, then their ranks as R-modules coincide.

If we define a suitable multiplication on $S \otimes H$, we get that j is also an R-algebra isomorphism, where that the multiplication in $\mathrm{End}_R(S)$ is given by composition.

Definition 10.13. Let S be a left H-module algebra. We denote by $S\#H$ the *smash product* of S and H: as R-module, $S\#H$ is just $S \otimes H$, and it is endowed with multiplication given by

$$(s\#x)(t\#y) = \sum_{(x)} s(x_{(1)} \cdot t)\#x_{(2)}y,$$

for $s, t \in S$ and $x, y \in H$.

A long but straightforward computation shows that indeed $S\#H$ is an R-algebra, and we have the following fact.

Proposition 10.14. *Let H be a finite cocommutative R-Hopf algebra, and let S be H-Galois. Then the map*

$$\begin{aligned} j\colon S\otimes H &\to \operatorname{End}_R(S)\\ s\otimes h &\mapsto (t\mapsto s(h\cdot t)) \end{aligned}$$

is an R-algebra isomorphism.

Definition 10.15. Let H be a finite cocommutative R-Hopf algebra, and let S be a left H-module, finite as R-module. The *fixed ring of S by H* is

$$S^H = \{s\in S \mid h\cdot s = \varepsilon(h)s, \text{ for all } h\in H\}.$$

Remark 10.16. Note that the elements of S are just fixed up to a scalar, depending on the counity of H. But if $H = R[G]$ for a finite group G, then $\varepsilon(\sigma) = 1$ for every $\sigma\in G$, so we find the usual fixed ring.

Proposition 10.17. *Let H be a finite cocommutative R-Hopf algebra, and let S be H-Galois. Then $S^H = \iota_S(R)$. In particular, if $R\subseteq S$ and ι_S is the inclusion, then $S^H = R$.*

Proof. Ler $r\in R$ and $h\in H$. Then

$$h\cdot\iota_S(r) = h\cdot(r1_S) = r(h\cdot 1_S) = r\varepsilon(h)1_S = \varepsilon(h)\iota_S(r),$$

that is, $\iota_S(R)\subseteq S^H$.

Conversely, suppose $s\in S^H$. We claim that $s\#1_H$ commutes with $t\#h$ in $S\#H$, for all $t\in S$, $h\in H$.

$$\begin{aligned} (t\#h)(s\#1_H) &= \sum_{(h)} t(h_{(1)}\cdot s)\#h_{(2)} = \sum_{(h)} t(\varepsilon(h_{(1)})s)\#h_{(2)}\\ &= \sum_{(h)} \varepsilon(h_{(1)})ts\#h_{(2)} = ts\#\sum_{(h)}\varepsilon(h_{(1)})h_{(2)} = st\#h\\ &= (s\#1_H)(t\#h). \end{aligned}$$

This means that $j(s\#1_H)$, the multiplication-by-s, is in the center of $\operatorname{End}_R(S)$. We claim that every element of the center of $\operatorname{End}_R(S)$ is a multiplication by an element of $\iota_S(R)$ (or equivalently, the scalar multiplication by an element of R). This is clearly true if S is free. In general, consider the ring homomorphism from R to the center of $\operatorname{End}_R(S)$. This map is surjective if and only the localised map at every maximal ideal $\mathfrak{m}$ is surjective, and this is true (after a bit of work) since localising we find local rings, and so freeness.

We conclude that there exists $r\in R$ such that, for all $t\in S$,

$$j(s\#1_H)(t) = st = rt = \iota(r)t,$$

and so, for $t = 1_S$, we find $s = \iota(r)$, as desired. □

Now let H be a finite cocommutative R-Hopf algebra, thus H^* is a finite commutative R-Hopf algebra.

Definition 10.18. A finite commutative R-algebra is S an *H^*-Galois object*, or *H^*-principal homogeneous space*, if the following hold:

- S is a right H^*-comodule algebra, with comodule action given by β.

- The R-module homomorphism
$$\begin{aligned}\gamma\colon S\otimes S &\to S\otimes H^*\\ s\otimes t &\mapsto (s\otimes 1_{H^*})\beta(t)\end{aligned}$$
is bijective.

Remark 10.19. Notice that both $S\otimes S$ and $S\otimes H^*$ are finite S-modules (S acts on the first factor of the pure tensors), and by Remark 10.4 and the commutativity of S and H^*, γ is also an S-algebra homomorphism.

The concepts of H-Galois extensions and H^*-Galois object coincide, as we now shall see.

Proposition 10.20. *Let H be a finite R-Hopf algebra, and let S be a left H-module algebra, finite as R-module. The following are equivalent:*

(1) *The R-module homomorphism*
$$\begin{aligned}j\colon S\otimes H &\to \mathrm{End}_R(S)\\ s\otimes h &\mapsto (t\mapsto s(h\cdot t))\end{aligned}$$
is bijective.

(2) *The R-module homomorphism*
$$\begin{aligned}\gamma\colon S\otimes S &\to S\otimes H^*\\ s\otimes t &\mapsto (s\otimes 1_{H^*})\beta(t)\end{aligned}$$
is bijective.

In particular, S is H-Galois if and only if S is an H^*-principal homogeneous space.

Proof. First of all, S is also a right H^*-comodule algebra, where, for all $s\in S$ and $h\in H$, $\beta(s)=\sum_{(s)} s_{(0)}\otimes s_{(1)}$ and $h\cdot s=\sum_{(s)} s_{(0)}\langle h, s_{(1)}\rangle$.

Since γ is S-linear, γ is a bijective if and only if its transpose
$$\begin{aligned}\gamma^*\colon \mathrm{Hom}_S(S\otimes H^*,S) &\to \mathrm{Hom}_S(S\otimes S,S)\\ f &\mapsto \left(s\otimes t\mapsto f(\gamma(s\otimes t))=f\left(\sum_{(t)} st_{(0)}\otimes t_{(1)}\right)\right)\end{aligned}$$
is bijective. We also have the following isomorphisms as R-modules:
$$\begin{aligned}\omega\colon S\otimes H &\to \mathrm{Hom}_S(S\otimes H^*,S)\\ (s\otimes h) &\mapsto (t\otimes f\mapsto st\langle h,f\rangle),\end{aligned}$$
$$\begin{aligned}\eta\colon \mathrm{Hom}_R(S,S) &\to \mathrm{Hom}_S(S\otimes S,S)\\ f &\mapsto (s\otimes t\mapsto sf(t)).\end{aligned}$$
The map ω follows from the isomorphism $H\cong \mathrm{Hom}_R(H^*,R)$ and Theorem 9.29, while η from the tensor-hom adjunction (see [Rot09, Theorem 2.76]). In particular, we find the diagram
$$\begin{tikzcd}S\otimes H \arrow[r, "j"] \arrow[d, "\omega"'] & \mathrm{Hom}_R(S,S) \arrow[d, "\eta"] \\ \mathrm{Hom}_S(S\otimes H^*,S) \arrow[r, "\gamma^*"'] & \mathrm{Hom}_S(S\otimes S,S),\end{tikzcd}$$

and we claim it is commutative. If so, then we would find that j is bijective if and only if γ^* is bijective, if and only if γ is bijective. So let $s \in S$ and $h \in H$. Then

$$\eta(j(s \otimes h))(t \otimes u) = t(j(s \otimes h)(u)) = ts(h \cdot u).$$

On the other hand,

$$\begin{aligned}\gamma^*(\omega(s \otimes h))(t \otimes u) &= \omega(s \otimes h)(\gamma(t \otimes u)) \\ &= \omega(s \otimes h)\left(\sum_{(u)} tu_{(0)} \otimes u_{(1)}\right) \\ &= \sum_{(u)} stu_{(0)}\langle h, u_{(1)}\rangle \\ &= st\sum_{(u)} u_{(0)}\langle h, u_{(1)}\rangle = st(h \cdot u),\end{aligned}$$

and so the assertion follows. □

Example 10.21. Let H be a finite cocommutative R-Hopf algebra. We have already seen that H^* is a finite commutative right H^*-comodule algebra (Example 10.6). We claim that H^* is an H^*-principal homogeneous space. This holds since the R-module homomorphism

$$\begin{aligned}\gamma\colon H^* \otimes H^* &\mapsto H^* \otimes H^* \\ f \otimes g &\mapsto \sum_{(g)} fg_{(1)} \otimes g_{(2)}\end{aligned}$$

admits an R-linear inverse:

$$\begin{aligned}\delta\colon H^* \otimes H^* &\mapsto H^* \otimes H^* \\ f \otimes g &\mapsto \sum_{(g)} f\lambda_{H^*}(g_{(1)}) \otimes g_{(2)}.\end{aligned}$$

We conclude that H^* is an H-Galois extension, called the *trivial H-Galois extension.*

10.3. **Base change.** Let B be a finite commutative R-algebra, let H be a finite cocommutative R-Hopf algebra, and let S be an H-Galois extension. Consider $B \otimes S$ as B-algebra. It is clearly a left $B \otimes H$-module, and a verification shows that it is also a left $B \otimes H$-module algebra. We claim that $B \otimes S$ is $B \otimes H$-Galois. Consider the following commutative diagram:

$$\begin{tikzcd} B \otimes S \otimes H \arrow[r, "\mathrm{id}_B \otimes j"] \arrow[d, "\psi"'] & B \otimes \mathrm{Hom}_R(S, S) \arrow[d, "\omega"] \\ (B \otimes S) \otimes_B (B \otimes H) \arrow[r, "j_B"'] & \mathrm{Hom}_B(B \otimes S, B \otimes S) \end{tikzcd}$$

Since j is an R-module isomorphism, $\mathrm{id}_B \otimes j$ is an B-module isomorphism. Both the vertical arrows are B-module isomorphisms: ψ because of the associativity and the simmetry of the tensor product, and ω by Theorem 9.29. We conclude that also j_B is an isomorphism, that is, $B \otimes S$ is $B \otimes H$-Galois.

Suppose now that B is a faithfully flat R-algebra, H is a finite cocommutative R-Hopf algebra, S is a left H-module algebra, and $B \otimes S$ is $B \otimes H$-Galois, with the action given by the H-action on S. Using the previous diagram, we find that $\mathrm{id}_B \otimes j\colon B \otimes S \otimes H \to B \otimes \mathrm{End}_R(S)$ is a B-module isomorphism, and by faithfully flatness of B, $j\colon S \otimes H \to \mathrm{End}_R(S)$ is an R-module isomorphism, so S is H-Galois.

Example 10.22. Let H be a finite cocommutative R-Hopf algebra, and let S be a commutative left H-module algebra, finite as R-module. Suppose that R is Noetherian.

(1) The completion $R_{\mathfrak{m}}$ at a maximal ideal $\mathfrak{m}$ is flat, so if S is H-Galois, then $S_{\mathfrak{m}}$ is $H_{\mathfrak{m}}$-Galois.

(2) The direct sum $\bigoplus_{\mathfrak{m}} R_{\mathfrak{m}}$ over all the maximal ideals of R is faithfully flat. If, for every $\mathfrak{m}$, $S_{\mathfrak{m}}$ is $H_{\mathfrak{m}}$-Galois, then it is immediate to see that $\bigoplus_{\mathfrak{m}} R_{\mathfrak{m}} \otimes S$ is $\bigoplus_{\mathfrak{m}} R_{\mathfrak{m}} \otimes H$-Galois, and so that S is H-Galois.

Summarising, S is H-Galois if and only if $S_{\mathfrak{m}}$ is $H_{\mathfrak{m}}$-Galois for all maximal ideals $\mathfrak{m}$ of R.

With base change, we may prove a specific version of Noether's theorem. First, a fundamental fact.

Theorem 10.23. *Suppose that R is a complete local ring. Let H be a finite cocommutative R-Hopf algebra, and let S be an H-Galois extension. Then S is a free H-module (of rank one).*

Proof. Since R is local and S is projective, S is also free. Let n be its rank. Both $S \otimes S$ and $S \otimes H^*$ have the structure of H-modules, where H acts on the second factors. We claim that $\gamma\colon S \otimes S \to S \otimes H^*$ is also an H-module homomorphism. To show this, we recall the coassociativity property of the right H^*-comodules: if $t \in S$, then

$$(\beta \otimes \mathrm{id}_{H^*})(\beta(t)) = (\mathrm{id} \otimes \Delta_{H^*})(\beta(t)) = \sum_{(t)} t_{(0)} \otimes t_{(1)} \otimes t_{(2)}.$$

Therefore for all $s, t \in S$ and $h \in H$,

$$\begin{aligned}\gamma(h \cdot (s \otimes t)) = \gamma(s \otimes (h \cdot t)) &= \gamma\left((s \otimes \sum_{(t)} t_{(0)} \langle h, t_{(1)} \rangle\right) \\ &= \sum_{(t)} st_{(0)} \otimes t_{(1)} \langle h, t_{(2)} \rangle \\ &= \sum_{(t)} st_{(0)} \otimes (h \cdot t_{(1)}) = h \cdot \gamma(s \otimes t).\end{aligned}$$

We deduce that $S^n \cong (H^*)^n$ are H-modules, and as H is a finite algebra over a complete local ring, by Krull–Schmidt–Azumaya theorem (see [CR81, Theorem 6.12]), $S \cong H^*$ as H-modules. Since $H^* \cong H$ as H-modules by Theorem 14.6, the assertion follows. □

Corollary 10.24. *Let L/K be an unramified Galois extension of number fields with Galois group G. Then $\mathcal{O}_L$ is locally free over $\mathcal{O}_K[G]$.*

Proof. If L/K is unramified, then $\mathcal{O}_L$ is an $\mathcal{O}_K[G]$-Galois extension of $\mathcal{O}_K$ (Theorem 10.8). Since $\mathcal{O}_K$ is Noetherian, by Example 10.22 if $\mathfrak{p}$ is a prime of $\mathcal{O}_K$, then $\mathcal{O}_{L,\mathfrak{p}}$ is an $\mathcal{O}_{K_{\mathfrak{p}}}[G]$-Galois extension of $\mathcal{O}_{K_{\mathfrak{p}}}$. By Theorem 10.23, since $\mathcal{O}_{K_{\mathfrak{p}}}$ is local and complete, we conclude that $\mathcal{O}_{L,\mathfrak{p}}$ is free $\mathcal{O}_{K_{\mathfrak{p}}}[G]$ of rank one. □

We have also found a different proof of the normal basis Theorem.

Corollary 10.25. *Let L/K be an finite Galois extension with Galois group G. Then L is a free $K[G]$-module (of rank one).*

Proof. This is immediate from Theorem 10.23, since every field is a complete local ring. □

10.4. **Galois descent.** Fix a Galois extension S of R with Galois group G, and assume that S is a faithful R-module. If A is an S-module (or more generally a left module over an R-algebra), then A is also an R-module: if $r \in R$ and $a \in A$, then $ra = \iota_R(r)a$. Note that naturally $S \hookrightarrow \operatorname{End}_R(S)$, hence a left $\operatorname{End}_R(S)$-module is also an S-module.

Remark 10.26.

1. If M is an R-module, then $S \otimes M$ is an S-module.
2. If M is an R-algebra, then $S \otimes M$ is an S-algebra.
3. If M is an R-Hopf algebra, then $S \otimes M$ is an S-Hopf algebra.
4. If $f \colon M \to N$ is an R-module homomorphism, then $\mathrm{id}_S \otimes f \colon S \otimes M \to S \otimes N$ is an S-module homomorphism.

We wish to find information about the opposite situation. When is an S-module A isomorphic to $S \otimes M$, for an R-module M? (In this situation, we say that A *descends*.) Morita theory gives answers to this kind of questions.

Lemma 10.27. *Let S be H-Galois, faithful as R-module. Let A be an $E = \operatorname{End}_R(S)$-module. Then the map*

$$\begin{aligned} S \otimes A^H &\to A \\ s \otimes a &\mapsto sa \end{aligned}$$

is an E-module isomorphism.

Proof. See [Chi00, Lemma 2.13]. The result follows from the isomorphism

$$A \cong S \otimes_R \operatorname{Hom}_E(S, E) \otimes_E A,$$

which is implied by Morita theory; see [CR81, section 3D].

In the statement, if A is a left E-module, then A is also a left H-module, and so writing A^H makes sense. Indeed, a left E-module is also a left $S\#H$-module, and since S is faithful and H is flat, we deduce that the R-module map

$$\begin{aligned} H &\to S\#H \\ h &\mapsto 1\#h \end{aligned}$$

is injective. Also, a simple verification shows that this map is a ring homomorphism, and so we conclude that we can see H as a subring of $S\#H$, and so A is also an H-module. □

Consider now $R = K$ a field, and let L/K be a finite Galois extension of fields with Galois group G. Let us write $D(L, G)$ for $L\#K[G]$. This is just $L[G]$ as L-module, with multiplication given by

$$(x_\sigma \sigma)(x_\tau \tau) = x_\sigma \sigma(x_\tau) \sigma\tau.$$

Since $D(L, G) \cong \operatorname{End}_K(L)$ as rings, we want to analyse the category of left $D(L, G)$-modules. It turns out that there is an easy description.

Proposition 10.28. *Let A be an S-module, and let G act on A.*

(1) *A is a $D(S,G)$-module if and only if the S-scalar multiplication on A is G-equivariant, where G acts on $S \otimes_S A$ diagonally.*
(2) *If $f\colon B \to C$ is S-linear and B and C are left $D(S,G)$-modules, then f is a $D(S,G)$-module homomorphism if and only if f is G-equivariant.*

Proof. This follows from long but straightforward observations. □

In particular, applying Lemma 10.27, we find what follows.

Corollary 10.29. *Let L/K be a finite Galois extension of fields with Galois group G. Then the category ${}_K\mathcal{M}$ of the K-vector spaces and the category ${}_E\mathcal{M}$ of left $E = \mathrm{End}_K(L)$-modules are equivalent: the* base change functor *$L\otimes -$ sends $M \in {}_K\mathcal{M}$ to $L \otimes M$, and $f\colon M \to N$ to $\mathrm{id} \otimes f\colon L \otimes M \to L \otimes M$; the* fixed module functor *$(-)^G$ sends $A \in {}_E\mathcal{M}$ to A^G, and $f\colon A \to B$ to $f_{|A^G}\colon A^G \to B^G$. Finally, if $M \in {}_K\mathcal{M}$, then there is a K-linear bijection*

$$\begin{aligned} M &\to (L \otimes M)^G \\ m &\mapsto 1 \otimes m, \end{aligned}$$

where G acts on the first factor of $L \otimes M$. Conversely, if $A \in {}_E\mathcal{M}$, then there is a left E-module isomorphism

$$\begin{aligned} L \otimes A^G &\to A \\ l \otimes a &\mapsto la. \end{aligned}$$

In particular, we find that if A is an L-vector space with an action of G such that the scalar multiplication is G-equivariant (we say that the G-action is *compatible*), then A is a $D(L,G)$-module, so an $\mathrm{End}_K(L)$-module, and by Corollary 10.29, $A \cong L \otimes A^G$ as $\mathrm{End}_K(L)$-modules, for the K-vector space A^G: this means that A descends.

We can also do something more.

Lemma 10.30. *Let A and B be a left E-modules. Then the K-module homomorphism*

$$\begin{aligned} A^G \otimes B^G &\to (A \otimes_L B)^G \\ a \otimes a' &\mapsto a \otimes a' \end{aligned}$$

is a bijection.

Proof. It is clear that the image of this map is in $(A \otimes_L B)^G$. Now note that

$$L \otimes (A^G \otimes B^G) \cong (L \otimes A^G) \otimes_L (L \otimes B^G) \cong A \otimes_L B \cong L \otimes (A \otimes_L B)^G,$$

via

$$x \otimes (a \otimes b) \mapsto (x \otimes a) \otimes (1 \otimes b) \mapsto (xa \otimes b) \mapsto x \otimes (a \otimes b).$$

We may conclude since L is faithfully flat as K-module. □

This implies that if a property of an L-module A with compatible action of G is defined by a commutative diagram where the arrows are $D(L,G)$-module homomorphisms (that is, G-equivariant L-module homomorphisms), then A^G presents the same property as K-module. For example, if A is an L-algebra, there is a commutative diagram

$$\begin{tikzcd}
A \otimes_L A \otimes_L A \arrow[r, "\mu\otimes\mathrm{id}"] \arrow[d, "\mathrm{id}\otimes\mu"'] & A \otimes_L A \arrow[d, "\mu"] \\
A \otimes_L A \arrow[r, "\mu"'] & A
\end{tikzcd}$$

and if the arrows are G-equivariant, then this yields the commutative diagram

$$\begin{tikzcd}
(A \otimes_L A \otimes_L A)^G \arrow[r] \arrow[d] & (A \otimes_L A)^G \arrow[d] \\
(A \otimes_L A)^G \arrow[r] & A^G
\end{tikzcd}$$

which by Lemma 10.30 implies the desired diagram for A^G. In this way, we derive the following fundamental fact.

Proposition 10.31. *Let L/K be a finite Galois extension of fields with Galois group G. Let A, H be L-vector spaces with compatible actions of G.*

(1) *If A is an L-algebra and the maps defining the structure of L as algebra are G-equivariant, then A^G is a K-algebra.*
(2) *If H is an L-Hopf algebra and the maps defining the structure of H as Hopf algebra are G-equivariant, then H^G is a K-Hopf algebra.*
(3) *If H is an L-Hopf algebra, A is a left H-module algebra, the maps defining the structures of H and A are G-equivariant, and the action of H on A is G-equivariant, then A^G is a left H^G-module algebra.*

Remark 10.32. Note that the isomorphisms given in Corollary 10.29 and in Lemma 10.30 respect also additional structures. For example, if H is an L-Hopf algebra and a G-module with suitable action, then L^G is a K-Hopf algebra, and $L \otimes H^G \cong H$ as L-Hopf algebras.

We can summarise the previous discussion as follows, combining it with base change.

Proposition 10.33. *Let L/K be a finite Galois extension with Galois group G.*

(1) *If a finite commutative K-algebra M is H-Galois, for a finite cocommutative R-Hopf algebra H, then $L \otimes M$ is $L \otimes H$-Galois.*
(2) *Suppose A is a finite commutative L-algebra and H is a finite cocommutative L-Hopf algebra such that A is H-Galois. Suppose that G acts on A and H such that all the structures are given by G-equivariant maps. Then A^G is H^G-Galois.*

11. Greither–Pareigis theorem and Byott's translation

In this section, we study Hopf–Galois extensions of fields. We fix a field K. As usual, unadorned tensors denote tensor over K.

Recall that if L/K is a finite extension of fields and H is a finite cocommutative K-Hopf algebra, then L is an H-Galois extension of K (or simply, L/K is H-Galois) if L is an H-module algebra and the K-linear map

$$\begin{aligned} j\colon L\otimes H &\to \operatorname{End}_K(L)\\ x\otimes h &\mapsto (y\mapsto x(h\cdot y)) \end{aligned}$$

is an isomorphism.

Definition 11.1. Let L/K be a finite extension of fields. A *Hopf–Galois structure* on L/K consists on a finite cocommutative K-Hopf algebra H, together with an action of H on L, such that L/K is H-Galois.

A groundbreaking result by Greither and Pareigis (see [GP87, Theorem 3.1]) allows us to find all the Hopf–Galois structures on separable finite field extensions using group theory. Our main goal is to state and prove this theorem.

11.1. Greither–Pareigis theorem.

For a finite set X, write $\operatorname{Perm}(X)$ for the group of bijective maps on X.

Definition 11.2. A subgroup $N\leq \operatorname{Perm}(X)$ is *regular* if two, and hence all of the following three conditions hold:

(1) $|N|=|X|$.
(2) N acts on X transitively.
(3) For all $x\in X$, the stabiliser of x in N is trivial.

The next result is almost immediate from the definition.

Lemma 11.3. *A subgroup $N\leq \operatorname{Perm}(x)$ is regular if and only if for some $x\in X$, and so for all $x\in X$, the map from N to G sending η to $\eta(x)$ is bijective.*

Let L/K be a separable finite field extension with normal closure E, and consider $G=\operatorname{Gal}(E/K)$, $G'=\operatorname{Gal}(E/L)$, and $X=G/G'$. Write $\overline{\Lambda}$ for the left translation map:

$$\begin{aligned} \overline{\Lambda}\colon G &\to \operatorname{Perm}(X)\\ \tau &\mapsto (\overline{\sigma}\mapsto \overline{\tau\sigma}). \end{aligned}$$

This is an injective map; see [Chi00, Lemma 6.6].

Theorem 11.4 (Greither–Pareigis)**.** *There is a bijection between Hopf–Galois structures on L/K and regular subgroups of* $\operatorname{Perm}(X)$ *normalised by* $\overline{\Lambda}(G)$.

We follow the discussion in [Chi00, section 6] for the proof. Since we are interested in Galois module theory, we will specialise the proof in the Galois case.

11.1.1. *The space GL.*

Let G be a finite group, and let L be a field. Consider the L-vector space GL of the maps from G to L. The space GL is also an L-algebra, with point-wise multiplication and identity sending all the elements of the group to 1_L. An L-basis for GL is given by $\{u_\sigma \mid \sigma\in G\}$, where for all $\sigma,\tau\in G$,

$$u_\sigma(\tau)=\delta_{\sigma,\tau}.$$

Note that this is a basis of pairwise orthogonal idempotents, so $1_{GL}=\sum_{\sigma\in G}u_\sigma$. Moreover, every idempotentof GL has the form $\sum_{\sigma\in\widetilde{G}}u_\sigma$, for a subset $\widetilde{G}$ of G. This immediately implies that the u_σ are *primitive*: they cannot be written as sums of nonzero orthogonal idempotents.

Remark 11.5. Since the operation is point-wise, the natural E-linear bijection $L^n \cong GL$, with $n = |G|$, is actually an L-algebra isomorphism.

Lemma 11.6. *There is an L-linear bijection*

$$GL \cong \mathrm{Hom}_L(L[G], L).$$

Proof. This is immediate, since every L-linear map from $L[G]$ to L is uniquely determined by its values on the elements of G. □

In particular, GL is also a G-module: if $\sigma, \tau \in G$ and $f \in GL$, then

$$(\sigma \cdot f)(\tau) = \sigma(f(\sigma^{-1}\tau)).$$

The space GL is important since the we may nicely describe the L-Hopf algebras H such that GL is H-Galois.

Theorem 11.7. *If H is a finite cocommutative L-Hopf algebra such that GL is H-Galois, then $H = L[N]$, where N is (identified with) a regular subgroup of* $\mathrm{Perm}(G)$.

Conversely, if N is a regular subgroup of $\mathrm{Perm}(G)$*, then GL is $L[N]$-Galois.*

Proof. Suppose GL is H-Galois over L. Let $n = |G|$. We have the following chain of L-algebra isomorphisms:

$$L^{n^2} \overset{(1)}{\cong} GL \otimes_L GL \overset{(2)}{\cong} GL \otimes_L H^* \overset{(3)}{\cong} (H^*)^n.$$

Here

(1) follows by Remark 11.5:

$$L^{n^2} \cong L^n \otimes_L L^n \cong GL \otimes_L GL;$$

(2) holds since GL is H-Galois;

(3) follows again by Remark 11.5: $GL \cong L^n$ as L-algebras.

In particular,

$$L^{n^2} \cong (H^*)^n$$

as L-algebras. We claim that H^* is semisimple.

(1) $L^{n^2} \cong (H^*)^n$ is a semisimple artinian ring, so its radical $\mathrm{Rad}((H^*)^n)$ is zero; see [CR81, Theorem 5.18].

(2) Since the ideals of $(H^*)^n$ are direct products of ideals of H^*, $\mathrm{Rad}((H^*)^n) = \mathrm{Rad}(H^*)^n$, so also $\mathrm{Rad}(H^*) = 0$.

(3) H^* is artinian: every ideal is also an L-vector space, so a descending chain of ideals eventually stops.

(4) Again by [CR81, Theorem 5.18], H^* is semisimple.

In particular, from Wedderburn–Artin theorem (see, for example, [CR81, Theorem 3.22]), we deduce that

$$H^* \cong L^n$$

as L-algebras. Since a basis of the dual of L^n is given by the projections p_i on the ith coordinate, we find that a basis of $H = H^{**}$ is $\{\eta_i\}_{i=1}^n$, where $\eta_i \colon H \to L$ is given by

$$H = H^{**} \cong L^n \xrightarrow{p_i} L.$$

As every η_i is an L-algebra homomorphism, by Remark 9.36, η_i is grouplike. Let $N = \{\eta_i\}_{i=1}^n$. Since N is a basis consisting of grouplike elements, by Corollary 9.38, $H = L[N]$ is a group ring.

Now we need to identify N with a subgroup of $\mathrm{Perm}(G)$. The idea is the following: if we show that for all $\eta \in N$ and $\tau \in G$, there exists a unique $\sigma \in G$ such that $\eta \cdot u_\tau = u_\sigma$, then we can set $\eta(\tau) = \sigma$.

An immediate computation shows that the $\eta \cdot u_\tau$, for $\tau \in G$, are pairwise orthogonal idempotents of GL. We claim that these are also primitive. First of all we show that they are non-zero: suppose that $\eta \cdot u_\tau = 0$; then

$$u_\tau = 1_N \cdot u_\tau = (\eta^{-1}\eta) \cdot u_\tau = \eta^{-1} \cdot (\eta \cdot u_\tau) = \eta^{-1} \cdot 0 = 0,$$

contradiction. Hence $\eta \cdot u_\tau \neq 0$. Moreover, since GL is an H-module algebra and η is grouplike, $\eta \cdot 1_{GL} = \varepsilon(\eta) \cdot 1_{GL} = 1_{GL}$, and so

$$1_{GL} = \eta \cdot 1_{GL} = \eta \cdot \left(\sum_{\tau \in G} u_\tau \right) = \sum_{\tau \in G} \eta \cdot u_\tau.$$

Every $\eta \cdot u_\tau$ is idempotent, so it is a sum of primitive idempotents of GL, and by $1_{GL} = \sum_{\tau \in G} \eta \cdot u_\tau$, we deduce that each primitive idempotent may appear as a summand of $\eta \cdot u_\tau$ for exactly one τ. Finally, since $\sum_{\tau \in G} \eta \cdot u_\tau$ is a sum of $|G|$ nonzero terms, and it is also equal to $\sum_{\tau \in G} u_\tau$, a sum of primitive idempotents, we conclude that for every $\tau \in G$, there exists a unique $\sigma \in G$ such that $\eta \cdot u_\tau = u_\sigma$. This implies that we can see N as subgroup of $\mathrm{Perm}(G)$, via $\eta(\tau) = \sigma$.

We need to show that N is regular. Note that $|N| = |G|$, since $L[N] = H$ and GL is H-Galois. Now suppose that the action of N on G is not transitive: we may find $\tau \in G$ with $N \cdot u_\tau = \{u_\sigma \mid \sigma \in \widetilde{G}\}$, with $\widetilde{G}$ proper subset of G. If $\pi \in G$ is not in $\widetilde{G}$, then define $e_{\tau,\pi} \in \mathrm{End}_L(GL)$ by $e_{\tau,\pi}(u_\sigma) = \delta_{\tau,\sigma} u_\pi$. Since

$$j \colon GL \otimes_L L[N] \to \mathrm{End}_L(GL)$$

is an isomorphism, $e_{\tau,\pi}$ should be in the image under j; but

$$\sum_{\xi \in G, \eta \in N} a_{\xi,\eta} u_\xi (\eta \cdot u_\tau) \in \sum_{\sigma \in \widetilde{G}} L u_\sigma,$$

and $u_\pi \notin \sum_{\sigma \in G} L u_\sigma$, contradiction

Conversely, suppose N is a regular subgroup of $\mathrm{Perm}(G)$, and define $e_{\tau,\pi}$ as before. Then $\{e_{\tau,\pi} \mid \tau, \pi \in G\}$ is an L-basis of $\mathrm{End}_L(GL)$. Since N is regular, for all $\tau, \pi \in G$, there exists η such that $\eta(\tau) = \pi$; define the $H = L[N]$-module algebra action on GL via

$$\eta \cdot u_\tau = u_\pi.$$

Then the map $j \colon GL \otimes_L L[N] \to \mathrm{End}_L(GL)$ is surjective:

$$j(u_\pi \otimes \eta) = e_{\tau,\pi}.$$

Since $|G| = |N|$, j is a bijection, and so the assertion follows. □

11.1.2. *The main result.* We are almost in the right position to prove Greither–Pareigis theorem for Galois extensions.

Let L/K is a finite Galois extension of fields with Galois group G. Then there is an L-linear isomorphism

$$\gamma \colon L \otimes L \to \mathrm{Hom}_L(L[G], L) \cong GL.$$

Also $L \otimes L$ is a G-module, with action on the first factor. In particular, with a straightforward verification, we have the following result.

Proposition 11.8. *The map*

$$\begin{aligned} L \otimes L &\to GL \\ x \otimes y &\mapsto (\sigma \mapsto x\sigma(y)) \end{aligned}$$

is an L-algebra G-equivariant isomorphism.

Write

$$\begin{aligned} \Lambda \colon G &\to \mathrm{Perm}(G) \\ \tau &\mapsto (\sigma \mapsto \tau\sigma) \end{aligned}$$

for the left regular representation.

Remark 11.9. In the literature, the left regular representation is denoted by λ, which here is already taken by the antipode of a Hopf algebra.

Theorem 11.10 (Greither–Pareigis, special case)**.** *There is a bijection between Hopf–Galois structures on L/K and regular subgroups of* $\mathrm{Perm}(G)$ *normalised by* $\Lambda(G)$*.*

Proof. Suppose that L/K is H-Galois. Since L is a free (and so flat) K-vector space, by base change $L \otimes L$ is $L \otimes H$-Galois. The action

$$(L \otimes H) \otimes_L (L \otimes L) \to L \otimes L \tag{11.1}$$

can easily be shown to be G-equivariant (G acts on the first factors on $L \otimes H$ and $L \otimes L$, and diagonally on $(L \otimes H) \otimes_L (L \otimes L)$). By Proposition 11.8, $L \otimes L \cong GL$. This means that GL is $L \otimes H$-Galois, and so, by Theorem 11.7, $L \otimes H$ is a group ring $L[N]$, where N is the group of grouplike elements of $L \otimes H$, and N is identified with a regular subgroup of $\mathrm{Perm}(G)$. In particular, we find an action

$$L[N] \otimes_L GL \to GL. \tag{11.2}$$

Since (11.1) is G-equivariant, G acts on $L[N] = L \otimes H$ such that (11.2) is G-equivariant. We want now to explicitly describe the action of G on N, to deduce that N is normalised by $\Lambda(G)$.

Write the usual basis $\{u_\tau \mid \tau \in G\}$ of GL. Recall that G acts of GL ad follows: if $\pi, \sigma, \tau \in G$, then

$$(\sigma \cdot u_\tau)(\pi) = \sigma(u_\tau(\sigma^{-1}\pi)) = u_{\sigma\tau}(\pi) = u_{\Lambda(\sigma)(\tau)}(\pi),$$

that is,

$$\sigma \cdot u_\tau = u_{\Lambda(\sigma)(\tau)}.$$

Since the G-action on $L \otimes H$ respects the Hopf algebra structure, in particular, it respects the comultiplication, so G sends grouplike elements in grouplike elements: G acts on N. As (11.2) is G-equivariant, we find that, for all $\eta \in N$ and $\sigma, \tau \in G$,

$$\sigma \cdot (\eta \cdot u_\tau) = (\sigma \cdot \eta) \cdot (\sigma \cdot u_\tau).$$

(Note that here we are using $\cdot$ for the G-action on $L[N]$ and GL, and also for the $L[N]$-action on GL.) Now

$$\sigma \cdot (\eta \cdot u_\tau) = \sigma \cdot u_{\eta(\tau)} = u_{\Lambda(\sigma)(\eta(\tau))}$$

and

$$(\sigma \cdot \eta) \cdot (\sigma \cdot u_\tau) = u_{(\sigma \cdot \eta)(\Lambda(\sigma)(\tau))},$$

hence

$$u_{\Lambda(\sigma)(\eta(\tau))} = u_{(\sigma \cdot \eta)(\Lambda(\sigma)(\tau))},$$

that is,

$$\Lambda(\sigma)(\eta(\tau)) = (\sigma \cdot \eta)(\Lambda(\sigma)(\tau)),$$

or

$$\sigma \cdot \eta = \Lambda(\sigma)\eta\Lambda(\sigma^{-1}) :$$

G acts on N via conjugation in $\mathrm{Perm}(G)$, after the identification $G \leftrightarrow \Lambda(G)$, and so N is normalised by $\Lambda(G)$. In particular, if $x \in L$, $\eta \in N$, and $\sigma \in G$, then G acts on $L[N]$ by

$$\sigma \cdot (x\eta) = \sigma(x)(\Lambda(\sigma)\eta\Lambda(\sigma^{-1})).$$

Conversely, let N be a regular subgroup of $\mathrm{Perm}(G)$ normalised by $\Lambda(G)$. By Theorem 11.7, GL is $L[N]$-Galois, and the action

$$\alpha\colon L[N] \otimes_L GL \to GL$$

is L-linear. We wish to apply Morita theory. We collect a few facts here, skipping the details (see [Chi00, Theorem 6.8]), where we use Proposition 10.28.

(1) Both G-actions on $L[N]$ and GL are compatible, hence both $L[N]$ and GL are left $D(L, G)$-modules.
(2) α is G-equivariant, hence α is a left $D(L, G)$-module homomorphism.
(3) The G-action on $L[N]$ respects the Hopf algebra structure.
(4) The G-action on GL respects the algebra structure, and also the $L[N]$-module algebra structure.

This means that we may apply Morita theory: by Proposition 10.33, $(GL)^G$ is $L[N]^G$-Galois. Finally, as the map

$$\begin{aligned} L &\to (GL)^G \\ x &\mapsto \sum_{\tau \in G} \tau(x)u_\tau \end{aligned}$$

is a K-algebra isomorphism, we may conclude that L/K is $L[N]^G$-Galois over K, where the $L[N]^G$-action on L is induced by the $L[N]^G$-action on $(GL)^L$.

We still need to check that in this way we obtain a bijective correspondence. Suppose N is a regular subgroup of $\mathrm{Perm}(G)$ normalised by $\Lambda(G)$. Then GL is $L[N]$-Galois over L. This implies that L is $L[N]^G$-Galois, with the action induced by the isomorphism $L \cong (GL)^G$. Thus $GL \cong L \otimes (GL)^G \cong L \otimes L$ is $L \otimes L[N]^G \cong L[N]$-Galois, and it is immediate to see that this action is the one we have started with.

Conversely, if L/K is H-Galois, then GL is $L \otimes H$-Galois over L, where the action is induced by $GL \cong L \otimes L$. In particular, $L \otimes H \cong L[N]$ for some regular subgroups of $\mathrm{Perm}(G)$ normalised by $\Lambda(G)$. This implies that L/K is $L[N]^G$-Galois. By Morita theory, there is an isomorphism of K-Hopf algebras $H \cong (L \otimes H)^G$, so we derive that L is $L[N]^G \cong (L \otimes H)^G \cong H$-Galois, and as before, carefully checking, step by step, we could see that this action is the one we have started with (for more details, see [GP87, Lemma 3.3]). This concludes the proof. □

Remark 11.11. Let L/K be a finite Galois extension of fields with Galois group G. If N is a regular subgroup of $\mathrm{Perm}(G)$ normalised by $\Lambda(G)$, then L/K is $L[N]^G$-Galois. We may describe very explicitly the $L[N]^G$-action on L. As shown in the proof, this action follows from the isomorphism $L \cong (GL)^G$. If $\sum_{\eta \in N} a_\eta \eta \in L[N]^G$

and $\sum_{\sigma \in G} b_\sigma u_\sigma \in (GL)^G$, then

$$\left(\sum_{\eta \in N} a_\eta \eta\right) \cdot \left(\sum_{\sigma \in G} b_\sigma u_\sigma\right) = \sum_{\eta \in N} \sum_{\sigma \in G} a_\eta b_\sigma u_{\eta(\sigma)}.$$

Let $x \in L$, and write $1 = 1_G$. We claim that the $L[N]^G$-action we obtain on L is given by

$$\left(\sum_{\eta \in N} a_\eta \eta\right) \cdot x = \sum_{\eta \in N} a_\eta (\eta^{-1}(1))(x).$$

Since the isomorphism $L \cong (GL)^G$ is given by $x \mapsto \sum_{\sigma \in G} \sigma(x) u_\sigma$, we need to show that

$$\sum_{\eta \in N} \sum_{\sigma \in G} a_\eta \sigma(x) u_{\eta(\sigma)} = \sum_{\sigma \in G} \sigma \left(\sum_{\eta \in N} a_\eta (\eta^{-1}(1))(x)\right) u_\sigma. \tag{11.3}$$

Fix $\sigma \in G$. Since $\sum_{\eta \in N} a_\eta \eta \in L[N]^G$, then

$$\sum_{\eta \in N} \sigma(a_\eta) \Lambda(\sigma) \eta \Lambda(\sigma^{-1}) = \sigma \cdot \left(\sum_{\eta \in N} a_\eta \eta\right) = \sum_{\eta \in N} a_\eta \eta;$$

thus for all $\eta \in N$, there exists a unique η_σ, such that $\Lambda(\sigma)\eta_\sigma\Lambda(\sigma^{-1}) = \eta$ and $\sigma(a_{\eta_\sigma}) = a_\eta$. In particular,

$$\eta^{-1}\Lambda(\sigma) = \Lambda(\sigma)\eta_\sigma^{-1} \in N.$$

After computing on 1 and then on x, we find

$$a_\eta \eta^{-1}(\sigma)(x) = \sigma(a_{\eta_\sigma})\sigma(\eta_\sigma^{-1}(1)(x)).$$

This works for all $\eta \in N$ and $\sigma \in G$, so

$$\sum_{\sigma \in G} \left(\sum_{\eta \in N} a_\eta \eta^{-1}(\sigma)(x)\right) u_\sigma = \sum_{\sigma \in G} \left(\sum_{\eta \in N} \sigma(a_{\eta_\sigma})\sigma(\eta_\sigma^{-1}(1)(x))\right) u_\sigma.$$

Consider the left-hand side. Since, for all $\eta \in N$, η^{-1} is a bijection, we find that

$$\begin{aligned}\sum_{\sigma \in G} \left(\sum_{\eta \in N} a_\eta \eta^{-1}(\sigma)(x)\right) u_\sigma &= \sum_{\eta \in N} a_\eta \left(\sum_{\sigma \in G} \eta^{-1}(\sigma)(x) u_\sigma\right) \\ &= \sum_{\eta \in N} a_\eta \left(\sum_{\sigma \in G} \sigma(x) u_{\eta(\sigma)}\right).\end{aligned}$$

As the right-hand side is

$$\begin{aligned}\sum_{\sigma \in G} \left(\sum_{\eta \in N} \sigma(a_{\eta_\sigma})\sigma(\eta_\sigma^{-1}(1)(x))\right) u_\sigma &= \sum_{\sigma \in G} \left(\sum_{\eta \in N} \sigma(a_\eta)\sigma(\eta^{-1}(1)(x))\right) u_\sigma \\ &= \sum_{\sigma \in G} \sigma \left(\sum_{\eta \in N} a_\eta (\eta^{-1}(1))(x)\right) u_\sigma,\end{aligned}$$

we find that (11.3) holds.

11.1.3. *Examples: Galois extensions.* Let L/K be a finite Galois extension of fields with Galois group G. Two standard regular subgroups of $\mathrm{Perm}(G)$ normalised by $\Lambda(G)$ are $\Lambda(G)$ itself and $P(G)$, where P is the right regular representation:

$$\begin{aligned} P\colon G &\mapsto \mathrm{Perm}(G) \\ \tau &\mapsto (\sigma \mapsto \sigma\tau^{-1}). \end{aligned}$$

Note that the action of $\Lambda(G)$ on $P(G)$ via conjugation is trivial, as the two subgroups commute.

Lemma 11.12. *For all finite groups G, $\Lambda(G) = P(G)$ if and only if G is abelian.*

Proof. If G is abelian, the result is clear.

Conversely, suppose $\sigma\tau \neq \tau\sigma$. Note that if $P(\sigma) = \Lambda(\pi)$ for $\pi \in G$, then computing in 1 we find $\pi = \sigma^{-1}$. This implies that $P(\sigma) \notin \Lambda(G)$, because $P(\sigma) \neq \Lambda(\sigma^{-1})$:

$$P(\sigma)(\tau) = \tau\sigma^{-1} \neq \sigma^{-1}\tau = \Lambda(\sigma^{-1})\tau. \qquad \square$$

Corollary 11.13. *Let L/K be a finite Galois extension of fields with nonabelian Galois group G. Then L/K admits at least two different Hopf–Galois structures.*

The structure corresponding to $\Lambda(G)$ is the *standard nonclassical structure.*

Proposition 11.14. *Let L/K be a finite Galois extension of fields with Galois group G. Then $P(G) \leq \mathrm{Perm}(G)$ corresponds to the classical action of G on L.*

Proof. Since $\Lambda(G)$ and $P(G)$ commute, $L[P(G)]^G = K[P(G)]$. If

$$\sum_{\sigma\in G} k_\sigma P(\sigma) \in K[P(G)]$$

and $x \in L$, then

$$\left(\sum_{\sigma\in G} k_\sigma P(\sigma)\right)\cdot x = \sum_{\sigma\in G} k_\sigma (P(\sigma^{-1})(1))(x) = \sum_{\sigma\in G} k_\sigma \sigma(x). \qquad \square$$

11.1.4. *Examples: separable extensions.* Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. This is a separable extension which is not Galois, and the normal closure is $E = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. It is well known that $G = \mathrm{Gal}(E/K) = S_3$ and $G' = \mathrm{Gal}(E/L) = C_2$. In particular, $|X| = 3$, where $X = G/G'$. Consider the map

$$\Lambda\colon S_3 \to \mathrm{Perm}(X) = \mathrm{Perm}(G/G') \cong S_3.$$

Then the subgroups of $\mathrm{Perm}(G)$ normalised by $\Lambda(G)$ are the precisely the normal subgroups of S_3. The only normal subgroup of S_3 with the same order of X is A_3. Since we can show that A_3 is regular, it yields a Hopf–Galois structure on L/K. This structure is described in details in [GP87].

Suppose now that L/K is separable extension of degree 5 such that, if E is the normal closure, then $\mathrm{Gal}(E/K) = S_5$. Since no normal subgroups of S_5 have order 5, we deduce that L/K does not admit Hopf–Galois structures.

11.2. **Byott's translation.** While useful is plenty of situations, the result by Greither and Pareigis presents a difficulty: the order of S_n grows really fast with n. To deal with this issue, it is effective to reverse the relationship between G and N, as explicitly described in [Byo96]. We just give a hint about this construction.

Suppose that L/K is Galois with Group G. If $N \leq \mathrm{Perm}(G)$ is a regular subgroup normalised by $\Lambda(G)$, then the map

$$\begin{aligned} b\colon N &\mapsto G \\ \eta &\mapsto \eta(1) \end{aligned}$$

is bijective and yields a group isomorphism

$$\begin{aligned} \varphi\colon\ \mathrm{Perm}(G) &\mapsto \mathrm{Perm}(N) \\ \pi &\mapsto b^{-1} \circ \pi \circ b. \end{aligned}$$

Now $N \leq \mathrm{Perm}(G)$ is mapped to $\Lambda(N)$ in $\mathrm{Perm}(N)$ under φ, and G is mapped to some $G_0 \leq \mathrm{Perm}(N)$ isomorphic to G. Since $\Lambda(G)$ normalised N in $\mathrm{Perm}(G)$, G_0 normalises $\Lambda(N)$ in $\mathrm{Perm}(G)$, that is, G_0 is contained in the holomorph of N.

Definition 11.15. Let N be a finite group. The *holomorph* of N, $\mathrm{Hol}(N)$, is the normaliser of $\Lambda(N)$ in $\mathrm{Perm}(N)$.

The following description of the holomorph is well known.

Proposition 11.16. *Let N be a finite group. Then*

$$\mathrm{Hol}(N) = P(N) \rtimes \mathrm{Aut}(N).$$

Proof. See [Chi00, Proposition 7.2]. □

We only state the Byott's translation [Byo96], a proof of which may be found in [Chi00, section 7]. It is really a useful result, since $\mathrm{Hol}(G)$ is smaller than $\mathrm{Perm}(G)$ and easier to describe.

Theorem 11.17 (Byott)**.** *Let G and N be finite groups of the same order. Then there is a bijection between*

$$\mathcal{N} = \{\alpha\colon N \to \mathrm{Perm}(G) \mid \alpha \textit{ is injective and } \alpha(N) \textit{ is regular}\}$$

and

$$\mathcal{G} = \{\beta\colon G \to \mathrm{Perm}(N) \mid \beta \textit{ is injective and } \beta(G) \textit{ is regular}\}.$$

Under this bijection, if $\alpha, \alpha' \in \mathcal{N}$ correspond to $\beta, \beta' \in \mathcal{G}$, then

1. *$\alpha(N) = \alpha'(N)$ if and only if $\beta(G)$ and $\beta'(G)$ are conjugate by an element of* $\mathrm{Aut}(G)$*;*
2. *$\alpha(N)$ is normalised by $\Lambda(G)$ if and only if $\beta(G)$ is contained in* $\mathrm{Hol}(N)$.

12. On the algebra structure of Hopf algebras occurring in Hopf–Galois theory

In this section, we follow [Gre21], where all the details we will skip are given (see also [KO74]).

Let us fix a field K with characteristic zero. As usual, unadorned tensors are over K. In the sequel, we refer to *structures* over K. These are K-algebras, K-Hopf algebras, or just K-vector spaces. In particular, morphisms are tacitly assumed to be in the appropriate category: for example, in this section, if A is a K-Hopf algebra, then $\mathrm{Aut}_K(A)$ denotes the K-Hopf algebra automorphisms of A.

Consider a finite Galois extension of fields L/K with Galois group G.

Definition 12.1. Let A be a structure over K. A second structure B is an *L-form* of A if

$$L \otimes A \cong L \otimes B.$$

We are interested in forms up to K-isomorphism.

Example 12.2.

(1) If A is an n-dimensional K-vector space, then every L-form of A is again an n-dimensional K-vector space: the dimension is invariant under base change. In particular, finite-dimensional vector spaces do not have nontrivial forms.

(2) If H is a K-Hopf algebra and M/K is H-Galois, then

$$M \otimes M \cong M \otimes H^*$$

as M-algebras. This means that M is an M-form of H^*.

We wish to describe a general machinery to determine the set of all L-forms of a structure A, modulo K-isomorphism. We denote this set by $\mathrm{Forms}_{L/K}(A)$.

Definition 12.3. Let G act on a group X. The *first cohomology set* is the set $H^1(G, X)$ of 1-cocycles $G \to X$, modulo an appropriate equivalent relation.

Remark 12.4. Unless X is abelian, $H^1(G, X)$ is just a pointed set, not necessarily a group.

Theorem 12.5. *Let A be a structure over K. Then there is a bijection*

$$\mathrm{Forms}_{L/K}(A) \to H^1(G, \mathrm{Aut}_L(L \otimes A)),$$

where the trivial form A corresponds to the distinguished element.

Proof. See [Gre21, Proposition 1.9]. We just explain how the forms arise from a given cocycle. Suppose $\vartheta = (\vartheta_g)_{g\in G}$ is a 1-cocycle of automorphisms of $L \otimes A$. Consider

$$\beta_g = \vartheta_g \circ (g \otimes \mathrm{id}_A) \in \mathrm{Aut}_L(L \otimes A).$$

It can be shown that the cocycle condition on ϑ implies that, for all $g, h \in G$, $\beta_{gh} = \beta_g \beta_h$, so G acts semilinearly on $L \otimes A$. Then the form B is the common fixed set of all β_g. □

Example 12.6.

(1) Let V an n-dimensional K-vector space, so we may assume $V = K^n$. Therefore

$$\mathrm{Aut}_L(L \otimes_K V) = \mathrm{GL}_n(L)$$

Since, by a generalisation of Hilbert's theorem 90, $H^1(G, \mathrm{GL}_n(L))$ is trivial, we deduce that all the forms in the category of finite-dimensional vector spaces are trivial, as observed before.

(2) Suppose $L = K(i)$, with $i \notin K$. Write $G = \{1, \tau\}$. Let $A = K[N]$, where $N = \{1, \eta, \eta^2, \eta^3\}$ is the cyclic group of order 4. Define a 1-cocycle of L-automorphisms of $L[N]$ as follows: $\vartheta_1 = \mathrm{id}$, $\vartheta_\tau \colon \eta \to \eta^{-1} = \eta^3$. To find the associated form, we need to look for elements $x \in L \oplus L\eta \oplus L\eta^2 \oplus L\eta^3$ such

that if we apply ϑ_τ and then τ on the coefficients we find again x. On can check that $B = K[c, s]$, where

$$c = \frac{\eta + \eta^3}{2}; \quad s = \frac{\eta - \eta^3}{2i}.$$

This Hopf algebra B shows up in Hopf–Galois situation: let $M = K(w)$, where $w^4 = u \in K^\times$ and $[M : K] = 4$. There is an action making M into a B-Hopf–Galois extension. For example, $c \cdot w = 0$, $s \cdot w = w$, $c \cdot w^2 = -w^2$, and $s \cdot w^2 = 0$.

(3) Let $A = K[N]$, with $N = G$. Note that G acts on $L[N]$ by inner automorphisms: $\vartheta_g(\eta) = g\eta g^{-1}$. This 1-cocycle describes a form B. We will see that as soon as N is not abelian, B is not isomorphic to $K[N]$ as K-Hopf algebra. It is called the *anticlassical Hopf form*.

As R. Underwood observed, if $K = \mathbb{Q}$ and $M/\mathbb{Q}$ is a Galois extension of fields with Galois group $N = S_3$, then, as in the previous example, the anticlassical M-form B of the group ring $\mathbb{Q}[S_3]$ is not trivial as $\mathbb{Q}$-Hopf algebra, but it is trivial in the category of $\mathbb{Q}$-algebras. We try to see why this happens and if this situation can be generalised.

Fix a field L and a finite group N. Clearly, every automorphism ν of N induces an L-Hopf algebra automorphism of $A_L = L[N]$, and it can be easily shown that also the converse is true: every L-Hopf algebra automorphism of $A_L = L[N]$ arises in this way.

Consider the 1-cocycles $G \to \mathrm{Aut}_L(A_L) = \mathrm{Aut}(N)$. We say that the 1-cocycles $(\vartheta_g)_{g\in G}$ and $(\vartheta'_g)_{g\in G}$ are *cohomologous* if there exists $\nu \in \mathrm{Aut}(N)$ such that for all $g \in G$,

$$\vartheta'_g = \nu \vartheta_g \nu^{-1}.$$

By this definition, it follows that the trivial cocycle $\vartheta_g = \mathrm{id}_N$ is only cohomologous to itself. Since this precisely the relation which yields the definition of $H^1(G, \mathrm{Aut}_L(L[N]))$, we deduce that every nontrivial cocycle defines a nontrivial Hopf form. If N is not abelian, this applies to the anticlassical Hopf form of $K[N]$, which then is not isomorphic to $K[N]$ as K-Hopf algebras. But we shall show that it is isomorphic to $K[N]$ as K-algebras. We need the following ingredients.

Recall that an automorphism of a group N is *inner* if it is given as conjugation $C(\eta)$ for some $\eta \in N$. Write $\mathrm{Inn}(N)$ for the group of the inner automorphisms. There is an injective map

$$C \colon N \to \mathrm{Inn}(N),$$

whose kernel is the center of N. For example, for all $n \neq 6$, S_n has only inner automorphisms. Clearly if N is abelian, then $\mathrm{Inn}(N) = 1$.

Consider again a finite Galois extension of fields L/K with Galois group G.

Definition 12.7. A cocycle $\vartheta \colon G \to \mathrm{Aut}(N) = \mathrm{Aut}_L(L[N])$ is

(1) *inner* if every ϑ_g is in $\mathrm{Inn}(N)$, that is, $\theta \colon G \to \mathrm{Inn}(N)$;

(2) *liftable* if there exists a homomorphism $\Theta \colon G \to N$ such that for all $g \in G$, $\vartheta_g = C(\Theta(g))$.

Clearly liftable cocycle are inner. Since it can be shown that these notions also make sense for cohomology classes, we can talk about *inner forms* and *liftable forms*.

Remark 12.8. If the group N has trivial center, then C identifies N with $\operatorname{Inn}(N)$, so inner and liftable are the same.

Theorem 12.9. *Every liftable form of the K-Hopf algebra $K[N]$ is isomorphic to $K[N]$ as K-algebras.*

Note that this applies to the anticlassical form, which is liftable: just take $\Theta = \mathrm{id}$, which makes sense since $G = N$ in that case. Before the proof, we need an important result. It is another generalisation of Hilbert's theorem 90.

Proposition 12.10. *If A is a simple finite-dimensional K-algebra, then*

$$H^1(G, (L \otimes A)^\times)$$

is trivial.

Proof. See [Gre21, Lemma 2.5]. □

Proof of Theorem 12.9. Write $A = K[N]$ and $A_L = L[N]$. Assume that we have a liftable 1-cocycle $\vartheta = C \circ \Theta$. Since A is semisimple (Example 2.18), it decomposes, via Wedderburn's theorem, as finite product of simple algebras (these are matrix rings over skew fields, finite-dimensional over K). We can show that every automorphism ϑ_g respects this decomposition, so we assume, for simplicity, that A is a simple algebra. (Note that this is never true, as A has always the augmentation ideal given by the counity ε.)

The goal is to show that the liftable 1-cocycle ϑ is trivial if considered as cocycle $G \to \operatorname{Aut}_L(A_L)$, where we forget the Hopf algebra structure of A_L.

So consider the L-algebra homomorphism $c\colon A_L^\times \to \operatorname{Aut}_L(A_L)$, which sends x to conjugation by x. Then for all $g \in G$, $\vartheta_g = c(\Theta(g))$. Since $\Theta\colon G \to N \subseteq A_L^\times$ is again a 1-cocycle, by Proposition 12.10, Θ is equivalent to the trivial cocycle $G \to A_L^\times$; therefore if we apply c we find that ϑ is equivalent to the trivial cocycle $G \to \operatorname{Aut}_L(A_L)$. □

We conclude this section analysing situations in which Theorem 12.9 does not hold: if a form is not inner or is inner but not liftable.

If N is abelian, then every nontrivial 1-cocycle is not inner.

Example 12.11. In Example 12.6(2), we have considered N cyclic of order 4 and $G = \operatorname{Gal}(K(i)/K)$ of order 2. The nontrivial element $\sigma \in G$ gives the automorphism ϑ_σ, which coincides to the inversion on N. One can show that $K[N] \cong K \times K \times K[i]$, while the form B is a product of four copies of K: the main theorem does not hold.

We shall now find an example of inner form which is not liftable. Consider the dihedral group of order 8 and $N = D_4$, which has center of order 2. Write s and t for the generators: s has order 4, t has order 2, and $tst = s^3 = s^{-1}$. As well know by representation theory, we can decompose $K[D_4]$ as

$$K \times K \times K \times K \times \operatorname{Mat}_2(K),$$

where $K \times K \times K \times K$ can be identified with $K[D_4^{\mathrm{ab}}] = K[C_2 \times C_2]$. One can also show that every inner cocycle leads to a form B whose "abelian part" is again K^4. So what really matters is what happens to the nonabelian part. The corresponding factor B' of B will be also a central simple K-algebra of dimension 4, and the question is whether it is a matrix algebra or a skew field. Let now $G = Q_8$, with presentation

$$\langle \sigma, \tau \mid \sigma^4 = 1, \tau^2 = \sigma^2, \tau\sigma\tau = \sigma^3 \rangle.$$

Define $\vartheta\colon Q_8 \to \mathrm{Inn}(D_4)$ by $\vartheta_\sigma = C(s)$ and $\vartheta_\tau = C(t)$. Then, intuitively, Q_8 and D_4 are in a way similar enough for ϑ to be a group homomorphism, but not similar enough for ϑ to be liftable through $C\colon N \to \mathrm{Inn}(N)$. To be more precise, denote respectively by $K(\sqrt{a})$ and $K(\sqrt{b})$ fixed fields of σ and τ, which are quadratic over K.

Theorem 12.12. *The L-form B' of $\mathrm{Mat}_2(K)$ given by the cocycle ϑ is the quaternion algebra*

$$B' = (-a, b)_K.$$

Proof. See [Gre21, Theorem 2.6]. □

In this way, with appropriate choices of K, a, and b, one can produce examples of B' being a matrix algebra (and so B is a trivial form in the category of K-algebras) and examples of B' being a skew-field (and so B is not trivial even as a K-algebra). For example, one can check that the latter situation happens when $K = \mathbb{Q}$, $a = 3$, and $b = 2$.

13. Induced Hopf–Galois extensions

The main references for this section are [CRV16a] and [GMR20]. We begin with a group-theoretical formulation of Hopf–Galois extensions.

Let G be a group, and let G' be a core-free subgroup, that is, a subgroup for which

$$\bigcap_{g\in G} gG'g^{-1} = 1.$$

In particular, G' is not normal (except for the trivial case $G' = 1$). Write $\Lambda_{G,G'}\colon G \to \mathrm{Perm}(G/G')$ for the left regular representation on left cosets.

Definition 13.1. A *Hopf–Galois structure* for (G, G') is a regular subgroup N of $\mathrm{Perm}(G/G')$ normalised by $\Lambda_{G,G'}$.

Note the analogy with Theorem 11.4, where L/K is a finite separable field extension, E/K is the normal closure, $G = \mathrm{Gal}(E/K)$, and $G' = \mathrm{Gal}(E/L)$.

Definition 13.2. A Hopf–Galois structure N for (G, G') is *almost classically Galois* if $N \subseteq \Lambda_{G,G'}(G)$.

This is equivalent to ask that G' has a normal complement J; see [GP87, Proposition 4.1]. Explicitly, if J is a normal complement of G', then $N = \Lambda_{G,G'}(J) \subseteq \Lambda_{G,G'}(G)$ is almost classically Galois.

Remark 13.3. Note that a normal complement is not necessarily unique: in the dihedral group $G = D_{16} = \langle r, s \mid r^8 = s^2 = 1, sts = r^{-1}\rangle$, both $J_1 = \langle r\rangle \cong \mathbb{Z}_8$ and $J_2 = \langle r^2, rs\rangle \cong D_8$ are normal complement of $G' = \langle s\rangle$.

Almost classically Galois extensions for fields (defined compatibly with Definition 13.2) are interesting to study for the Hopf–Galois correspondence, given by [CS69, Theorem 7.6] and here reported in the formulation of [GP87, Theorem 5.1]. Let L/K be a finite separable H-Galois extension, and for a K-sub Hopf algebra W of H, write $L^W = \{x \in L \mid w \cdot x = \varepsilon(w)x,\ \text{for all } w \in W\}$, the *fixed field* of W.

Theorem 13.4. *The map*

$$\{K\text{-sub-Hopf algebras of } H\} \to \{\text{Intermediate fields of } L/K\}$$
$$W \mapsto L^W$$

is injective and inclusion-reversing.

Indeed, in [GP87, Theorem 5.2] it is proved that if L/K is almost classically Galois, then there exists a Hopf–Galois structure such that the correspondence in Theorem 13.4 is surjective; namely, it is the one yield by the centraliser N' of N in $\mathrm{Perm}(G/G')$.

Remark 13.5. Note that Theorem 13.4 can be restated using more explicitly group theory: see [CRV16b, Theorem 2.3]. We also refer to this paper for some results concerning almost classically Galois structures.

Now consider the following situation: E/K is a finite separable field extension with normal closure L/K, $G = \mathrm{Gal}(L/K)$, and $G' = \mathrm{Gal}(E/K)$. Then G' is core-free, and we may consider Hopf–Galois structures for (G, G') (or for E/K), for $(G, 1)$ (or for L/K), and for $(G', 1)$ (or for L/E). Are these structures related?

Suppose that G' has a normal complement J, so $G = J \rtimes G'$. Then one can show that the map

$$l\colon \mathrm{Perm}(G/G') \times \mathrm{Perm}(G') = \mathrm{Perm}(J) \times \mathrm{Perm}(G') \to \mathrm{Perm}(G),$$

defined by $l(\sigma, \tau)(g) = \sigma(x)\tau(y)$, where $g = xy$ is the factorisation of $g \in G = J \rtimes G'$, in an injective homomorphism, and one can see that the following result holds; see [CRV16a, Theorem 3].

Theorem 13.6. *If N_1 is a Hopf–Galois structure for (G, G') and N_2 is a Hopf–Galois structure for $(G', 1)$, then $N = l(N_1 \times N_2)$ is a Hopf Galois structure for $(G, 1)$.*

This Hopf–Galois structure is called *induced*.

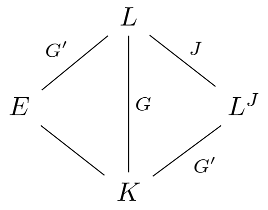
Corollary 13.7. *If $G = J \rtimes G'$ is a finite group, with G' a core-free subgroup, then $(G, 1)$ has a Hopf–Galois structure of type $J \times G'$.*

Proof. Just apply Theorem 13.6 the almost classically Galois structure for (G, G'), given by J and the classical for $(G', 1)$. □

Example 13.8. Combining Remark 13.3 and Corollary 13.7, we find that D_{16} has Hopf–Galois structures of type $\mathbb{Z}_8 \times \mathbb{Z}_2$ and $D_8 \times \mathbb{Z}_2$.

More examples can be found in [CRV16a, section 3].

Note that it is more natural to consider Hopf–Galois structures for L^J/K instead of L/E:



If N_1 is a regular subgroup of $\mathrm{Perm}(J)$ normalised by $\Lambda_{G,G'}$ (so $H_1 = L[N_1]^G$ gives a Hopf–Galois structure on E/K) and N_2 is a regular subgroup of $\mathrm{Perm}(G/J)$ normalised by $\Lambda_{G'}(G')$ (so $H_2 = L^J[N_2]^{G'}$ gives a Hopf–Galois structure on E/K), then the induced Hopf–Galois structure for L/K is given by $H = H_1 \otimes_K H_2$; see [GMR20, Propositions 5.3 and 5.5].

Moreover, if we write $\rho_{H_1} \colon H_1 \to \mathrm{End}_K(E)$ for the representation given by the action of H_1 on E, and $\rho_{H_2} \colon H_2 \to \mathrm{End}_K(L^J)$ for the representation given by the action of H_2 on L^J, then $\rho_H \colon H \to \mathrm{End}_K(L)$ is precisely $\rho_H = \rho_{H_1} \otimes \rho_{H_2}$; see [GMR20, Proposition 5.8]. In particular for a suitable choice of basis, matrices of ρ_H are Kronecker products of matrices of ρ_{H_1} and ρ_{H_2}.

We summarise all of this in the following result, which is [GMR20, Theorem 1.3] and makes use, in his statement, of [GMR20, Proposition 5.3].

Theorem 13.9. *Let L/K be a finite Galois extension with Galois group $G = J \rtimes G'$, let $E = L^{G'}$, and let $F = L^J$. Then the following facts hold:*

1. *E/K and F/K are Hopf–Galois extensions.*
2. *$L = EF$ and $E \cap F = K$.*
3. *E/K and F/K are linearly disjoint.*

Let E/K be H_1-Galois, and let L/E be H_2-Galois. We consider the corresponding induced Hopf–Galois structure of L/K. Let H be its associated Hopf algebra.

4. *$H = H_1 \otimes_K \overline{H}$, where $\overline{H}$ is the Hopf Galois structure of F/K such that $H \otimes_K E = H_2$.*
5. *The Hopf-action of H on L is the Kronecker product of the Hopf-actions of H_1 and E and of $\overline{H}$ on F.*

Remark 13.10. A comparison with [GMR20, Proposition 1.2] shows that induced structures mimic the classical direct products.

We conclude this section with a result regarding the arithmetic of Dedekind domains. Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, let L/K be a finite separable extension of fields, and let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}$ in L. If L/K is H-Galois, then we may define the *associated order* of $\mathcal{O}_L$ in H:

$$\mathfrak{A}_H = \{h \in G \mid h \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

It is not difficult to see that $\mathfrak{A}_H$ shares the nice properties of the classical associated order defined in the classical Galois setting. We discuss more about the associated order in the section 14.

We can conclude this section with [GMR20, Theorem 1.5].

Theorem 13.11. *Let $\mathcal{O}$ be a principal ideal domain with field of fractions K, let L/K be a finite separable Hopf–Galois extension, and let $\mathcal{O}_L$ be the integral closure of $\mathcal{O}$ in L. Assume that the structure is induced and its Hopf algebra is $H = H_1 \otimes_K \overline{H}$. If E/K and F/K are arithmetically disjoint, then the following statements hold:*

1. *$\mathfrak{A}_H = \mathfrak{A}_{H_1} \otimes_{\mathcal{O}_K} \mathfrak{A}_{\overline{H}}$.*
2. *If $\mathcal{O}_E$ is $\mathfrak{A}_{H_1}$-free and $\mathcal{O}_F$ is $\mathfrak{A}_{\overline{H}}$-free, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-free. Moreover, an $\mathfrak{A}_H$-generator of $\mathcal{O}_L$ is the product of an $\mathfrak{A}_{H_1}$-generator of $\mathcal{O}_E$ and an $\mathfrak{A}_{\overline{H}}$-generator of $\mathcal{O}_F$.*

Remark 13.12. Theorem 13.11 is a generalisation of Lemma 2.30 in the Hopf–Galois setting, when the structure is induced.

14. Hopf–Galois module theory

Here we mainly follow [Chi00, Chapters 1 and 3].

14.1. First notions.

14.1.1. *Integrals.* Fix a commutative ring R and an R-Hopf algebra H.

Definition 14.1. An element $\theta \in H$ is

(1) a *left integral* if for all $h \in H$, $h\theta = \varepsilon(h)\theta$;
(2) a *right integral* if for all $h \in H$, $\theta h = \theta\varepsilon(h)$.

If M is a left H-module, then we consider

$$M^H = \{m \in M \mid h \cdot m = \varepsilon(h)m, \quad \text{for all } h \in H\},$$

again a left H-module. Clearly we may see H as left H-module via multiplication. In this case, H^H coincides with the set of left integrals, which we denote by $\int_H^l$.

Lemma 14.2. *$\int_H^l$ is a two-sided ideal of H.*

Proof. If $\theta \in \int_H^l$ and $x, y \in H$, then

$$y(x\theta) = (yx)\theta = \varepsilon(yx)\theta = \varepsilon(y)(\varepsilon(x)\theta) = \varepsilon(y)(x\theta)$$

and

$$y(\theta x) = (y\theta)x = (\varepsilon(y)\theta)x = \varepsilon(y)(\theta x). \qquad \square$$

Example 14.3. Let G be a finite group.

(1) If $H = R[G]$, then
$$\theta = \sum_{\sigma \in G} \sigma$$
is a left and right integral and every other left or right integral is an R-multiple of θ (for the easy verification, see [Und15, Proposition 3.2.4]).
(2) If $H = R[G]^*$ with basis $\{e_\sigma \mid \sigma \in G\}$ as in Example 9.33, then e_1 is a left and right integral. It is enough to check the defining property on a basis, so let $\sigma \in G$. Then $e_\sigma e_1 = \delta_{\sigma,1}e_1 = \varepsilon(e_\sigma)e_1$ and $e_1 e_\sigma = e_1\delta_{\sigma,1} = e_1\varepsilon(e_\sigma)$.

Definition 14.4. We say that H is *unimodular* if the module of left integrals coincide with the module of right integrals.

Example 14.5.

(1) If H is commutative, then H is unimodular.
(2) If $H = R[G]$ for a finite group G, then H is unimodular.

We shall use the integrals to better understand the action of a finite Hopf algebra over its dual. Recall that if H is finite, then H^* is a left H-module algebra:

$$h \cdot f = \sum_{(f)} f_{(1)}\langle h, f_{(2)}\rangle,$$

for $h \in H$ and $f \in H^*$. For example, if $H = R[G]$ for a finite group G and $\sigma, \tau \in G$, then

$$\sigma \cdot e_\tau = \sum_{\rho \in G} e_\rho \langle \sigma, e_{\rho^{-1}\tau}\rangle = e_{\tau\sigma^{-1}}.$$

In particular, for all $\sigma \in G$, we have $e_\sigma = \sigma^{-1} \cdot e_1$, and we find that

$$R[G]^* = R[G] \cdot e_1,$$

with e_1 left integral.

Conversely, $R[G]$ is a left $R[G]^*$-module algebra:

$$e_\sigma \cdot \tau = \delta_{\sigma,\tau}\tau.$$

In a similar way, we find that

$$R[G] = R[G]^* \cdot \sum_{\sigma \in G} \sigma,$$

with $\sum_{\sigma \in G} \sigma$ left integral.

We can generalise this fact as follows.

Theorem 14.6 (Larson–Sweedler)**.** *If H is finite, then there exixts an H-module isomorphism*

$$H \otimes_R \int_{H^*}^l \cong H^*.$$

Proof. See [Swe69, Theorem 5.1.3]. Explicitly, the isomorphism associates the element $h \cdot \theta$ to a pure tensor $h \otimes \theta$. □

Corollary 14.7. *If H is finite, then $\int_{H^*}^l$ is a projective R-module. If in addition R is a principal ideal domain or a local ring, then $\int_{H^*}^l$ is a free R-module of rank one.*

Proof. Consider the counity $\varepsilon_H \colon H \to R$. If $r \in R$, then

$$\varepsilon_H(\iota_H(r)) = r\varepsilon_H(1_H) = r.$$

This implies that $\varepsilon_H \circ \iota_H = \mathrm{id}_R$, so the sequence of R-modules

$$0 \to \ker(\varepsilon_H) \to H \xrightarrow{\varepsilon_H} R \to 0.$$

is exact and split. We find that R is a direct summand of H, and by Theorem 14.6, $\int_{H^*}^l \cong R \otimes_R \int_{H^*}^l$ is a direct summand of H^*. Since H^* is projective, we conclude that also $\int_{H^*}^l$ is projective.

If in addition R is a principal ideal domain or a local ring, then every projective R-module is free. Since the R-ranks of H and H^* coincide, we conclude that $\int_{H^*}^l$ is a free R-module of rank one. □

Note that if $\int_{H^*}^l$ is free and θ is a generator, then, by Theorem 14.6, H^* is a free left H-module of rank one, with generator θ, the isomorphism given by the H-module map

$$\begin{aligned} H &\mapsto H^* \\ h &\mapsto h \cdot \theta. \end{aligned}$$

We conclude with a standard application of Sweedler notation.

Lemma 14.8. *Let θ be a left integral of H. Then for all $h \in H$,*

$$(h \otimes 1)((\mathrm{id} \otimes \lambda)\Delta(\theta)) = ((\mathrm{id} \otimes \lambda)\Delta(\theta))(1 \otimes h).$$

Proof. For all $h \in H$,

$$\begin{aligned}
(h \otimes 1)((\mathrm{id} \otimes \lambda)\Delta(\theta)) &= \sum_{(\theta)} h\theta_{(1)} \otimes \lambda(\theta_{(2)}) \\
\text{(by counitary)} \quad &= \sum_{(\theta),(h)} h_{(1)}\varepsilon(h_{(2)})\theta_{(1)} \otimes \lambda(\theta_{(2)}) \\
\text{(by linearity)} \quad &= \sum_{(\theta),(h)} h_{(1)}\theta_{(1)} \otimes \lambda(\theta_{(2)})\varepsilon(h_{(2)}) \\
\text{(by antipode property)} \quad &= \sum_{(\theta),(h)} h_{(1)}\theta_{(1)} \otimes \lambda(\theta_{(2)})\lambda(h_{(2)})h_{(3)} \\
(\lambda \text{ is antihomomorphism}) \quad &= \sum_{(\theta),(h)} h_{(1)}\theta_{(1)} \otimes \lambda(h_{(2)}\theta_{(2)})h_{(3)} \\
(\Delta \text{ is a homomorphism and by coassociativity}) \quad &= \sum_{(h)} ((\mathrm{id} \otimes \lambda)\Delta(h_{(1)}\theta))(1 \otimes h_{(2)}) \\
(\theta \text{ is a left integral}) \quad &= \sum_{(h)} ((\mathrm{id} \otimes \lambda)\Delta(\varepsilon(h_{(1)})\theta))(1 \otimes h_{(2)}) \\
\text{(by linearity)} \quad &= \sum_{(h)} ((\mathrm{id} \otimes \lambda)\Delta(\theta))(1 \otimes \varepsilon(h_{(1)})h_{(2)}) \\
\text{(by counitary)} \quad &= ((\mathrm{id} \otimes \lambda)\Delta(\theta))(1 \otimes h).
\end{aligned}$$

□

Corollary 14.9. *Let $H = R[G]$, where G is a finite group. Then for all $\sigma \in G$,*

$$\sum_{\tau} \sigma\tau \otimes \tau^{-1} = \sum_{\tau} \tau \otimes \tau^{-1}\sigma.$$

Proof. Just apply Lemma 14.8 with the left integral $\theta = \sum_{\tau} \tau$. □

14.1.2. *Hopf orders.* Let $\mathcal{O}$ be a Dedekind domain with field of fractions K, and suppose that the characteristic of K is zero. Let A be a finite K-Hopf algebra, and let H be a finite $\mathcal{O}$-submodule of A for which $KH = A$.

Lemma 14.10. *The $\mathcal{O}$-linear map*

$$\begin{aligned}
\varphi \colon H \otimes_{\mathcal{O}} H &\to A \otimes_K A \\
a \otimes b &\mapsto a \otimes b
\end{aligned}$$

is injective.

Proof. Suppose first that H is free as $\mathcal{O}$-module. Since $KH = A$, an $\mathcal{O}$-basis of H is also a K-basis of A, and so the result immediately follows.

In general, we can tensor with the direct sum $\bigoplus_{\mathfrak{m}} \mathcal{O}_{\mathfrak{m}}$ over all maximal ideals of R, a faithfully flat $\mathcal{O}$-module, and work again in a setting where we have free modules. □

If we identify $H \otimes_{\mathcal{O}} H$ with a subset of $A \otimes_K A$, it makes sense to ask if H is an $\mathcal{O}$-Hopf algebra with the structure induced by A, that is, if the following hold:

- $\mu \colon A \otimes_K A \to A$ restricts to $\mu \colon H \otimes_{\mathcal{O}} H \to H$.
- $\iota \colon K \to A$ restricts to $\iota \colon \mathcal{O} \to H$.
- $\Delta \colon A \to A \otimes_K A$ restricts to $\Delta \colon H \to H \otimes_{\mathcal{O}} H$.
- $\varepsilon \colon A \to K$ restricts to $\varepsilon \colon H \to \mathcal{O}$.

- $\lambda\colon A \to A$ restricts to $\lambda\colon H \to H$.

Definition 14.11. An *$\mathcal{O}$-Hopf order* in A is an $\mathcal{O}$-order H in A which is an $\mathcal{O}$-Hopf algebra with the operations induced by A.

Example 14.12. If G is a finite group and $A = K[G]$, then $H = \mathcal{O}[G]$ is an $\mathcal{O}$-Hopf order in A. In fact, H is the minimal $\mathcal{O}$-Hopf order in A, as we now shall see.

Proposition 14.13. *Let H be an $\mathcal{O}$-Hopf order in $K[G]$. Then $\mathcal{O}[G] \subseteq H$.*

Proof. Since H is an $\mathcal{O}$-Hopf order in $K[G]$, the dual H^* is an $\mathcal{O}$-Hopf order in $K[G]^* = \sum_{\sigma \in G} Ke_\sigma$, a commutative $\mathcal{O}$-algebra with unique maximal order $\sum_{\sigma \in G} \mathcal{O}e_\sigma$. We deduce that $H^* \subseteq \sum_{\sigma \in G} \mathcal{O}e_\sigma$, so $\mathcal{O}[G] \subseteq H$. □

When $A = K[G]$, in order to show that an $\mathcal{O}$-order is an $\mathcal{O}$-Hopf order is enough to show that the comultiplication restricts correctly.

Proposition 14.14. *If G is a finite group, H is an $\mathcal{O}$-order in $K[G]$, and $\Delta(H) \subseteq H \otimes_{\mathcal{O}} H$, then H is an $\mathcal{O}$-Hopf order in $K[G]$.*

Proof. See [Tru09, Proposition 2.3.12]. □

14.1.3. *Associated orders in Hopf algebras.* Let L/K be an extension of number fields or p-adic fields, and let A be a finite K-Hopf algebra such that L/K is A-Galois. We may define an associated order in this setting.

Definition 14.15. The *associated order* of $\mathcal{O}_L$ in A is

$$\mathfrak{A}_A = \{\alpha \in A \mid \alpha \cdot \mathcal{O}_L \subseteq \mathcal{O}_L\}.$$

As in the classical case, $\mathfrak{A}_A$ is an $\mathcal{O}_K$-order in A, but $\mathfrak{A}_A$ is not necessarily an $\mathcal{O}_K$-Hopf order (see [Chi87, section 5]). Moreover, if $\mathcal{O}_L$ is free over $\mathfrak{A}$, then it is free of rank one, and the following result holds.

Proposition 14.16. *Suppose that $\mathcal{O}_L$ is free over an $\mathcal{O}_K$-order Γ in A. Then $\Gamma = \mathfrak{A}_A$.*

Proof. This works exactly as Proposition 2.12, since also in this case L is free of rank one over H (Theorem 10.23). □

14.1.4. *H-tame extensions.* Here we generalise the notion of tamely ramified extension for H-Galois extensions.

If L/K is an extension of p-adic fields, then L/K is tamely ramified if and only if the trace map $\mathrm{Tr}\colon \mathcal{O}_L \to \mathcal{O}_K$ is surjective (Theorem 1.30). Since $\mathrm{Tr}(a) = \theta \cdot a$, where $\theta = \sum_{\sigma \in G} \sigma$ is a generator of the two-sided ideal $\int_{K[G]}^{l}$, we deduce that L/K is tamely ramified if and only if $\int_{K[G]}^{l} \cdot \mathcal{O}_L = \mathcal{O}_K$. With this is mind, we can give the following definition. Fix a commutative local ring R and a finite cocommutative R-Hopf algebra H. The following discussion can also be generalise to rings which are not necessarily local.

Definition 14.17. Let S be a finite R-algebra which is a left H-module algebra. Suppose $S^H = \iota_S(R)$. We say that S is *H-tame* if the following hold:

1. $\mathrm{rank}_R(S) = \mathrm{rank}_R(H)$.
2. S is a faithful H-module.
3. $\int_H^l \cdot S = S^H = \iota_S(R)$.

Condition (3) means that $\int_H^l \cdot S$ is as large as possibile, because of the next result.

Proposition 14.18. *Let S be a left H-module algebra. Then $\int_H^l \cdot S \subseteq S^H$.*

Proof. Let $\xi = \sum_{i=1}^n \theta_i \cdot s_i \in \int_H^l \cdot S$, where for all i, $\theta_i \in \int_H^l$ and $s_i \in S$. Then, for all $h \in H$,

$$h \cdot \xi = h \cdot \left(\sum_i \theta_i \cdot s_i \right) = \sum_i (h\theta_i) \cdot s_i = \sum_i (\varepsilon(h)\theta_i) \cdot s_i = \varepsilon(h)\xi. \qquad \square$$

14.2. **Linking notions.** We study the relation between the notions of H-free, H-tame, and H-Galois.

14.2.1. *Maximal order implies freeness.*

Proposition 14.19. *Let K be a p-adic field, and let A be a commutative separable K-algebra. Let $\mathfrak{M}$ be the maximal $\mathcal{O}_K$-order in A, and let S be a finite $\mathcal{O}_K$-module which is also an $\mathfrak{M}$-module. If $S \otimes_{\mathcal{O}_K} K$ is A-free of rank one, then S is $\mathfrak{M}$-free of rank one.*

Proof. See [Tru09, Proposition 2.55]. □

In particular, if L/K is an A-Galois extension of p-adic fields, where A is a commutative (and so necessarily separable, by [Tru09, Proposition 2.3.9]) K-Hopf algebra and $\mathfrak{A}_A$ is the maximal order in A, then L is A-free of rank one (Theorem 10.23), and so $\mathcal{O}_L$ is $\mathfrak{A}_A$-free.

14.2.2. *Tameness implies freeness.*

Theorem 14.20. *Let R be a commutative local ring, let H be a finite cocommutative R-Hopf algebra, and let S be a finite R-algebra which is a left H-module algebra. If S is H-tame, then S is H-projective.*

Proof. Since R is local, by 14.7, $\int_H^l$ is R-free of rank one. Let θ be a generator. Since S is H-tame, $\theta \cdot S = \iota_S(R)$, so we can find $z \in S$ such that $\theta \cdot z = 1_S$. Since S is R-projective, $H \otimes_R S$ is H-projective, where the action is given on the first factor. Therefore, in order to conclude, it is enough to show that S is isomorphic to a direct summand of $H \otimes_R S$.

Consider the H-multiplication $\alpha\colon H \otimes_R S \to S$, clearly a left H-module homomorphism. Since this map is surjective, we have an exact sequence

$$0 \to \ker(\alpha) \to H \otimes_R S \xrightarrow{\alpha} S \to 0,$$

and if the sequence splits, then $H \otimes_R S \cong \ker(\alpha) \oplus S$ as left H-modules (see [Rot09, Proposition 2.28]); this isomorphism would imply the assertion. Define $\beta\colon S \to H \otimes_R S$ by

$$\beta(s) = \sum_{(\theta)} \theta_{(1)} \otimes z(\lambda(\theta_{(2)}) \cdot s).$$

The map β is an H-module homomorphism: if $h \in H$ and $s \in S$, then

$$\begin{aligned}
h \cdot (\beta(s)) &= h \cdot \left(\sum_{(\theta)} \theta_{(1)} \otimes z(\lambda(\theta_{(2)}) \cdot s) \right) \\
&= \sum_{(\theta)} h\theta_{(1)} \otimes z(\lambda(\theta_{(2)}) \cdot s) \\
&= (1_H \otimes z) \left(\sum_{(\theta)} h\theta_{(1)} \otimes \lambda(\theta_{(2)}) \right) \cdot (1_H \otimes s) \\
\text{(by Proposition 14.8)} \quad &= (1_H \otimes z) \left(\sum_{(\theta)} \theta_{(1)} \otimes \lambda(\theta_{(2)})h \right) \cdot (1_H \otimes s) \\
&= \sum_{(\theta)} \theta_{(1)} \otimes z(\lambda(\theta_{(2)}) \cdot (h \cdot s)) = \beta(h \cdot s).
\end{aligned}$$

The only thing left to show is that for all $s \in S$, $\alpha(\beta(s)) = s$:

$$\begin{aligned}
\alpha(\beta(s)) &= \sum_{(\theta)} \theta_{(1)} \cdot (z(\lambda(\theta_{(2)}) \cdot s)) \\
\text{(S is a left H-module algebra)} \quad &= \sum_{(\theta)} (\theta_{(1)} \cdot z)((\theta_{(2)}\lambda(\theta_{(3)})) \cdot s) \\
\text{(by antipode property)} \quad &= \sum_{(\theta)} (\theta_{(1)} \cdot z)(\varepsilon(\theta_{(2)})s) \\
\text{(by linearity)} \quad &= \sum_{(\theta)} ((\theta_{(1)}\varepsilon(\theta_{(2)})) \cdot z)(s) \\
\text{(by counitary)} \quad &= (\theta \cdot z)s = s.
\end{aligned}$$

□

We need now an intermediate result, which can be found in [Sch77].

Theorem 14.21 (Schneider)**.** *Let R be a local domain with field of fractions K of characteristic zero. Let H be a finite cocommutative R-Hopf algebra, and let P and Q be finitely generated projective left H-modules. If $K \otimes_R P \cong K \otimes_R Q$ as left $K \otimes_R H$-modules, then $P \cong Q$ as left H-modules.*

Proposition 14.22. *Let K be a p-adic field, and let A be a finite cocommutative K-Hopf algebra. Let S be an $\mathcal{O}_K$-order in an A-Galois extension L of K. If H is an $\mathcal{O}_K$-Hopf order in A and S is H-projective, then S is H-free of rank one.*

Proof. This is an immediate application of Theorems 14.21 and 10.23. □

Putting all together, we find the desired result.

Corollary 14.23. *Let L/K be an A-Galois extension of p-adic fields. Let H be an $\mathcal{O}_K$-Hopf order in A such that S is H-tame. Then S is H-free. In particular, $H = \mathfrak{A}_A$.*

14.2.3. *Hopf order implies freeness.*

Theorem 14.24. *Let L/K be an A-Galois extension of p-adic fields. If $\mathfrak{A}_A$ is an $\mathcal{O}_K$-Hopf order in A, then $\mathcal{O}_L$ is $\mathfrak{A}_A$-tame and so $\mathfrak{A}_A$-free.*

Proof. The only condition in Definition 14.17 we need to check is (3).

Since $\mathcal{O}_K$ is local, $\int_{\mathfrak{A}_A}^l$ is $\mathcal{O}_K$-free of rank one by Corollary 14.7. Let θ be a generator. As L is A-Galois, $L^A = K$ by Proposition 10.17, and this easily implies that $\mathcal{O}_L^{\mathfrak{A}_A} = \mathcal{O}_K$. By Proposition 14.18, we find $\theta \cdot \mathcal{O}_L \subseteq \mathcal{O}_L^{\mathfrak{A}_A} = \mathcal{O}_K$.

For the other inclusion, let π be an uniformiser of $\mathcal{O}_K$. Since $\theta \cdot \mathcal{O}_L$ is an ideal of $\mathcal{O}_K$, there exists $i \geq 0$ such that $\theta \cdot \mathcal{O}_L = \pi^i \mathcal{O}_K$. Therefore $(\theta/\pi^i) \cdot \mathcal{O}_L = \mathcal{O}_K$, and so $\theta/\pi^i \in \mathfrak{A}_A$. Finally, since θ/π^i is an integral and θ is a generator of $\int_{\mathfrak{A}_A}^l$ as R-module, we find that $i = 0$, that is, $\theta \cdot \mathcal{O}_L = \mathcal{O}_K$. □

14.2.4. *Galois implies tameness.* Let R be a commutative local ring, and let H be a finite cocommutative R-Hopf algebra. Let S be an H-Galois extension, and let $E = \mathrm{End}_R(S)$.

Proposition 14.25. *If M is a left E-module, then*

$$M^H \cong \int_H^l \cdot M$$

as R-modules. In particular, $M \cong S \otimes_R \int_H^l \cdot M$ as left E-modules.

Proof. See [Chi00, Proposition 14.3]. This is an application of Morita theory, discussed also in Lemma 10.27. □

Proposition 14.26. *Let S be an H-Galois extension of R. Then S is H-tame.*

Proof. Conditions (1) and (2) of Definition 14.17 follow from the isomorphisms in Proposition 10.20.

If we apply Proposition 14.25 for $M = S$, we immediately deduce condition (3). □

14.2.5. *Freeness implies tameness.* Let R be a commutative local ring, and let H be a finite cocommutative R-Hopf algebra.

Corollary 14.27. *Let S be an H-module algebra with $S^H = \iota_S(R)$. If $S \cong H^*$ as H-modules, then S is H-tame.*

Proof. Since H^* is a faithful H-module, so it is S, and $\mathrm{rank}_R(H) = \mathrm{rank}_R(H^*) = \mathrm{rank}_R(S)$.

We need to check that $\int_H^l \cdot S = R$. Since H^* is H-Galois, $\int_H^l \cdot H^* = R$ (Proposition 14.26), and since $\int_H^l \cdot S$ is mapped to $\int_H^l \cdot H^*$ under the isomorphism $S \cong H^*$, we derive our assertion. □

Since R is local, $H \cong H^*$ as H-modules, and so we derive the next result.

Corollary 14.28. *Suppose that R is local, and let S be an H-module algebra with $S^H = \iota_S(R)$. If S is H-free, then S is H-tame.*

14.2.6. *Equivalence between notions.* If also the Hopf algebra is local, then all the notions are equivalent.

Theorem 14.29. *Let R be a commutative local ring, let H be a local cocommutative R-Hopf algebra, and let S be a finite R-algebra which is also a faithful R-module algebra. Then the following are equivalent:*

- *S is H-tame.*

- *S is H-free.*
- *S is H-Galois.*

Proof. See [Chi00, Theorem 14.7]. Explicitly, if $\int_H^l = R\theta$ and $t \in S$ is an element such that $\theta \cdot t = 1$, then t is an H-generator of S. □

15. Hopf orders as associated orders

In this section, we mainly follow [Byo95], [Byo97], and [Chi00, Chapters 8, 11, and 12].

15.1. **The set-up.** We recall the main result of Section 14.

Theorem 15.1. *Let L/K be an H-Galois extension of p-adic fields, where H is a cocommutative K-Hopf algebra. If the associated order $\mathfrak{A}_H$ of $\mathcal{O}_L$ in H is an $\mathcal{O}_K$-Hopf order, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-tame and so $\mathfrak{A}_H$-free. If in addition $\mathfrak{A}_H$ is a local ring, then $\mathcal{O}_L$ is $\mathfrak{A}_H$-Galois.*

15.2. **Hopf orders in $K[C_p]$.** Let K be a p-adic field with normalised valuation v_K, and let $\mathfrak{p}_K$ be the maximal ideal of $\mathcal{O}_K$. Let π_K be an uniformiser of K, so $v_K(\pi_K) = 1$, and write $e = e_{K/\mathbb{Q}_p}$ for the ramification index: $p\mathcal{O}_K = \pi_K^e \mathcal{O}_K$. Let $G = C_p$ be a cyclic group of order p with generator σ, and write $X = \sigma - 1 \in \mathcal{O}_K[G]$.

As $\mathcal{O}_K[X] = \mathcal{O}_K[G]$ (Lemma 7.10), we get that $\mathcal{O}_K[X]$ is an $\mathcal{O}_K$-Hopf order in $K[G]$. This can be also shown directly: since $(X+1)^p = \sigma^p = 1$, we find that

$$X^p + pX^{p-1} + \binom{p}{2} X^{p-2} + \cdots + pX = 0;$$

thus $\mathcal{O}_K[X]$ is finitely generated over $\mathcal{O}_K$. Clearly, $K\mathcal{O}_K[X] = K[G]$. Moreover,

$$\begin{aligned}\Delta(X) &= \Delta(\sigma - 1) = \Delta(\sigma) - \Delta(1) = \sigma \otimes \sigma - 1 \otimes 1 \\ &= X \otimes 1 + 1 \otimes X + X \otimes X \in \mathcal{O}_K[X] \otimes_{\mathcal{O}_K} \mathcal{O}_K[X]\end{aligned}$$

and so by Proposition 14.14 we conclude that $\mathcal{O}_K[X]$ is an $\mathcal{O}_K$-Hopf order in $K[G]$.

Now we generalise this construction. For $i \in \mathbb{Z}$, write $X_i = \pi^{-i} X$ and $H_i = \mathcal{O}_K[X_i]$. For which i is H_i a Hopf order? For H_i to be a finitely generated $\mathcal{O}_K$-module, we need X_i to satisfy a monic equation over $\mathcal{O}_K$. Since $K\mathcal{O}_K[X_i] = K[G]$ and, as before,

$$X_i^p + p\pi^{-i} X_i^{p-1} + \binom{p}{2} \pi^{-2i} X_i^{p-2} + \cdots + p\pi^{-(p-1)i} X_i = 0,$$

we deduce that if $p\pi^{-(p-1)i} \in \mathcal{O}_K$, that is, if $i \le e/(p-1)$, then H_i is an $\mathcal{O}_K$-order in $K[G]$ with basis $\{X_i^j\}_{j=1}^p$.

For H_i to be an $\mathcal{O}_K$-Hopf order we also need $\Delta(X_i) \in H_i \otimes_{\mathcal{O}_K} H_i$. Since

$$\Delta(X_i) = X_i \otimes 1 + 1 \otimes X_i + \pi^i X_i \otimes X_i,$$

we find that $\Delta(X_i) \in H_i \otimes_{\mathcal{O}_K} H_i$ if and only if $i \ge 0$, and so we get a family of Hopf orders $H_i \subseteq K[G]$ for $0 \le i \le \lfloor e/(p-1) \rfloor$. One can show that H_i is a local ring unless $i = e/(p-1)$ and these are the only Hopf orders in $K[C_p]$; see [Und11, Chapter 7].

Now we study when these Hopf orders occur as associated orders.

Let L/K be a Galois extension of degree p with Galois group G and ramification jump t: if $\mathfrak{p}_L$ is the prime of $\mathcal{O}_L$, then

$$t = \max\{j \mid (\sigma - 1) \cdot \mathcal{O}_L \subseteq \mathfrak{p}_L^{j+1}\}.$$

Recall Proposition 7.4: $1 \leq t \leq ep/(p-1)$, and $p \nmid t$ unless $(p-1) \mid e$ and $t = ep/(p-1)$. If $t = -1$, then L/K is unramified. If $t > 0$, then L/K is totally (and wildly) ramified. Note that $t \neq 0$, as $G_0 = G_1$ (Corollary 2.4). By [Byo97, Proposition 3.1], if $t > 0$, then for all $\rho \in L^\times$,

$$v_L((\sigma - 1) \cdot \rho) \begin{cases} = v_L(\rho) + t & \text{if } p \nmid v_L(\rho), \\ > v_L(\rho) + t & \text{if } p \mid v_L(\rho). \end{cases}$$

Combining [Byo95, section 7] and [BF72], we find that there are four cases to consider:

- Suppose $t > 0$ and $t \equiv -1 \pmod p$, say $t = pi - 1$ with $1 \leq i \leq e/p - 1$. Pick $\rho \in L$ such that $v_L(\rho) = p - 1$. If $0 \leq s \leq p-1$, then, by an easy computation,
$$v_L(X_i^s \cdot \rho) = p - 1 - s$$
and
$$v_L(X_i^p \cdot \rho) \geq 0.$$
Since L/K is totally ramified, we deduce that the elements $X_i^s \cdot \rho$ for $0 \leq s \leq p-1$ form an $\mathcal{O}_K$-basis of $\mathcal{O}_L$, that is, $\mathcal{O}_L$ is a free H_i-module with generator ρ. Also, $\mathcal{O}_L$ is H_i-Galois.
- Suppose $t = -1$. Then L/K is unramified, and $\mathcal{O}_L$ is free over $H_0 = \mathcal{O}_K[G]$ and H_0-Galois.
- Suppose $t = pi - a$ with $2 \leq a \leq p - 1$. Then
$$H_{i-1} \subsetneq \mathfrak{A}_{L/K} \subsetneq H_i,$$
and so $\mathfrak{A}_{L/K}$ is not an $\mathcal{O}_K$-Hopf order in $K[G]$. Moreover, $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$ if and only if $p - a$ divides $p - 1$, unless $t + 1 \geq ep/(p-1)$.
- Suppose $t = pe/(p-1)$. Then we can apply Theorem 7.6: $\zeta_p \in K$ and $L = K(\alpha)$ with $\alpha = \sqrt[p]{\pi}$, for some choice of an uniformiser π. Then $\mathcal{O}_L$ is free over H_i for $i = e/(p-1)$, with generator
$$1 + \alpha + \alpha^2 + \cdots + \alpha^{p-1}.$$
In this case H_i is the maximal order, and it is not a local ring. In particular, $\mathcal{O}_L$ is H_i-tame, and so H_i-free, but not H_i-Galois.

Summarising, $\mathcal{O}_L$ is H-Galois for some Hopf order H if and only if $t \equiv -1 \pmod p$. The only other case where the associated order is a Hopf order is when $t = ep/(p-1)$; see [Byo95, Lemma 7.1].

15.3. **A weak congruence for the ramification jumps.** Let us now consider a totally ramified Galois extension L/K of degree p^n with Galois group G. We list the ramification jumps "with multiplicity": $t_1 \leq t_2 \leq \cdots \leq t_n$, where

$$t_i = \max\{j \mid |G_j| > p^{n-i}\}.$$

In particular, by Hilbert's formula (Proposition 4.4), the inverse different

$$\mathcal{D}_{L/K}^{-1} = \{x \in L \mid \mathrm{Tr}_{L/K}(x\mathcal{O}_L) \subseteq \mathcal{O}_K\}$$

equals $\mathfrak{p}_L^{-w}$, where

$$w = (p^n - 1)(t_1 + 1) + \sum_{i=1}^{n-1} (t_{i+1} - t_i)(p^{n-i} - 1) \equiv -(t_n + 1) \pmod p.$$

Theorem 15.2. *Suppose $\mathfrak{A}_{L/K}$ is a local $\mathcal{O}_K$-Hopf order in $K[G]$. Then for all $1 \leq i \leq n$,*

$$t_i \equiv -1 \pmod{p^i}.$$

Proof. We proceed by induction on n, where the base case $n = 1$ has been already performed.

Let N be a normal subgroup of G of order p contained in G_{t_n}, and let $F = L^N$. With this choice of N, L/F has ramification jump t_n and F/K has ramification jumps $t_1, \dots, t_{n-1}$. Attached to the exact sequence of groups

$$1 \to N \to G \to G/N \to 1$$

we have an exact sequence of $\mathcal{O}_K$-Hopf orders, in the sense of [Chi00, sections 4 and 5]:

$$\mathcal{O}_K \to H_1 \to H \to \overline{H} \to \mathcal{O}_K,$$

where $H_1 = H \cap K[N]$ and $\overline{H}$ is the image of H in $K[G/N]$ (in particular, see [Chi00, Propositions 4.14 and 5.3]). Then H_1 and $\overline{H}$ are still local by [Chi00, Proposition 29.1], and $\mathcal{O}_L$ and $\mathcal{O}_F$ are tame for the Hopf orders $\mathcal{O}_F \otimes_{\mathcal{O}_K} H_1 = \mathfrak{A}_{L/F}$ and $\overline{H} = \mathfrak{A}_{F/K}$, respectively; see [Chi00, Theorem 28.1].

Applying the induction hypothesis to F/K, we get $t_i \equiv -1 \pmod{p^i}$ for all $1 \leq i \leq n-1$.

Applying the induction hypothesis to L/F, we get $t_n \equiv -1 \pmod{p}$, say $t_n = pm - 1$. We need to strengthen this congruence.

By [Byo95, Corollary 1.5],

$$\int_{H_1}^{l} = \mathfrak{a}^{-1} \sum_{\sigma \in N} \sigma,$$

where $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$. We deduce that

$$\int_{\mathfrak{A}_{L/F}}^{l} = \mathfrak{a}^{-1}\mathcal{O}_F \sum_{\sigma \in N} \sigma,$$

and by [Byo95, Proposition 3.2], $\mathrm{Tr}_{L/K}(\mathcal{O}_L) = \mathfrak{a}\mathcal{O}_K$. On the other side, since $\mathcal{D}_{L/F}^{-1} = \mathfrak{p}_L^{-w}$ with $w = (p-1)(t_n+1) = (p-1)pm$, we get

$$\mathfrak{p}_F^{(p-1)m} = \mathrm{Tr}_{L/K}(\mathcal{O}_F) = \mathfrak{a}\mathcal{O}_F.$$

As F/K is totally ramified of degree p^{n-1}, we deduce that

$$(p-1)m \equiv 0 \pmod{p^{n-1}},$$

that is, $p^{n-1} \mid m$, so

$$t_n = pm - 1 \equiv -1 \pmod{p^n}. \qquad \square$$

Corollary 15.3. *Suppose that $\mathfrak{A}_{L/K}$ is a local $\mathcal{O}_K$-Hopf order in $K[G]$. Then $\mathcal{D}_{L/K}^{-1} = \mathfrak{a}^{-1}\mathcal{O}_L$ for an $\mathcal{O}_K$-ideal $\mathfrak{a}$.*

Proof. We have $\mathcal{D}_{L/K}^{-1} = \mathfrak{p}_L^{-w}$, where

$$w = (p^n - 1)(t_1 + 1) + \sum_{i=1}^{n-1} (t_{i+1} - t_i)(p^{n-i} - 1) \equiv -(t_n + 1) \equiv 0 \pmod{p},$$

since $t_i \equiv -1 \pmod{p^i}$, for every i. In particular,

$$\mathcal{D}_{L/K}^{-1} = \mathfrak{p}_K^{-w/p^n}. \qquad \square$$

Remark 15.4. Corollary 15.3 implies that if $\mathfrak{A}_{L/K}$ is a local $\mathcal{O}_K$-Hopf order in $K[G]$, then $\mathcal{D}_{L/K}^{-1}$ and $\mathcal{O}_L$ have the same associated order $\mathfrak{A}_{L/K}$, and both are free over it.

15.4. **A strong congruence for the ramification breaks.**

Theorem 15.5. *Let L/K be a totally ramified abelian extension of degree p^n with $\mathcal{D}_{L/K}^{-1} = \mathfrak{a}^{-1}\mathcal{O}_L$, where $\mathfrak{a}$ is an $\mathcal{O}_K$-ideal. Suppose that $\mathcal{D}_{L/K}^{-1}$ is free over its associated order $\mathfrak{A} = \mathfrak{A}_{L/K}$ in $K[G]$ and $\mathfrak{A}$ is a local ring. Then for all $1 \le i \le n$, the ramification jumps t_i of L/K satisfy*

$$t_i \equiv -1 \pmod{p^n}.$$

Proof. Write $\mathcal{M}$ for the unique maximal ideal of $\mathfrak{A}$, and let $\mathcal{D}^{-1} = \mathcal{D}_{L/K}^{-1}$ be free over $\mathfrak{A}$ with generator y. For all $\alpha \in \mathfrak{A}$,

$$\mathfrak{A} \cdot (\alpha \cdot y) = \mathcal{D}^{-1} \iff \alpha \notin \mathcal{M}.$$

Write $\{y_j\}_{j=1}^{p^n}$ for an $\mathcal{O}_K$-basis of $\mathcal{D}^{-1}$, so for all $1 \le j \le p^n$, we have that $y_j = \alpha_j \cdot y$ and $\{\alpha_j\}_{j=1}^{p^n}$ is an $\mathcal{O}_K$-basis of $\mathfrak{A}$. Since $\mathcal{M}$ is strictly contained in $\mathfrak{A}$, there is j with $\alpha_j \notin \mathcal{M}$; thus $\mathfrak{A} \cdot y_j = \mathcal{D}^{-1}$.

Assume, by contradiction, $t_i \not\equiv -1 \pmod{p^n}$ for some i. We construct a basis $\{y_j\}_{j=1}^{p^n}$ for $\mathcal{D}^{-1}$ over $\mathcal{O}_K$ so that none of the y_j satisfy $\mathfrak{A} \cdot y_j = \mathcal{D}^{-1}$.

To show that $\mathfrak{A} \cdot y_j \neq \mathcal{D}^{-1}$, it is enough to find $\beta_j \in \mathfrak{A}$ such that $\beta_j \cdot y_j \in \pi_K \mathcal{D}^{-1}$, but $\beta_j \notin \pi_K \mathfrak{A}$; see [Byo97, Lemma 2.2].

Write $\mathcal{D}^{-1} = \mathfrak{p}_L^{-w}$, with $w \equiv 0 \pmod{p^n}$. Then

$$\mathrm{Tr}_{L/K}(\mathcal{D}^{-1}) = \mathcal{O}_K, \qquad \mathrm{Tr}_{L/K}(\mathfrak{p}_L^{-1}\mathcal{D}^{-1}) = \mathfrak{p}_K^{-1},$$

so

$$\mathrm{Tr}_{L/K}(\pi_K \mathcal{D}^{-1}) = \mathfrak{p}_K, \qquad \mathrm{Tr}_{L/K}(\pi_K \mathfrak{p}_L^{-1}\mathcal{D}^{-1}) = \mathcal{O}_K.$$

This means that if we choose $z \in \pi_K \mathfrak{p}_L \mathcal{D}^{-1}$ with $\mathrm{Tr}_{L/K}(z) = 1$, then $v_L(z) = p^n - w - 1$. Now choose $z_1 = z, z_2, \ldots, z_{p^n}$ with $v_L(z_j) = p^n - w - j$. Then the z_j form an $\mathcal{O}_K$-basis of $\mathcal{D}^{-1}$. We adjust this to get a nicer basis: $y_1 = z$ and for $2 \le j \le p^n$,

$$y_j = z_j - \mathrm{Tr}_{L/K}(z_j) z_1.$$

Then $\mathrm{Tr}_{L/K}(y_j) = 0$ for $2 \le j \le p^n$, and still $v_L(y_j) = p^n - w - j$.

Recall that we need to find, for all $2 \le j \le p^n$, $\beta_j \in \mathfrak{A} \backslash \pi_K \mathfrak{A}$ with $\beta_j \cdot y_j \in \pi_K \mathcal{D}^{-1}$. For $2 \le j \le p^n$, we take

$$\beta_j = \beta = \pi_K^{-w/p^n} \sum_{\sigma \in G} \sigma.$$

Then

$$\beta \cdot y_j = \pi_K^{-w/p^n} \mathrm{Tr}_{L/K}(y_j) = 0 \in \pi_K \mathcal{D}^{-1},$$

and since $\mathcal{D}^{-1} = \pi_K^{-w/p^n} \mathcal{O}_L$, we deduce that $\beta \in \mathfrak{A}$ but $\beta \notin \pi_K \mathfrak{A}$.

It remains to find β_1. Recall that $t_i \not\equiv -1 \pmod{p^n}$. Write $t_i = p^n m + a$, with $1 \le a \le p^n - 2$. (Note that $t_i \not\equiv 0 \pmod{p^n}$, as $t_i \equiv -1 \pmod{p^i}$.) Take

$\beta_1 = \pi_K^{-m}(\sigma - 1)$, with $\sigma \in G_{t_i} \setminus G_{t_i+1}$. By Proposition [Byo97, Proposition 3.1], for all $y \in L^\times$,

$$v_L(\beta_1 \cdot y) \begin{cases} = v_L(y) + a & \text{if } p \nmid v_L(y), \\ > v_L(y) + a & \text{if } p \mid v_L(y), \end{cases}$$

and so $\beta_1 \in \mathfrak{A}$. Since

$$v_L(\beta_1 \cdot y_1) \geq v_L(y_1) + a = p^n - w - 1 + a \geq p^n - w,$$

we derive $\beta_1 \cdot y_1 \in \pi\mathcal{D}^{-1}$. On the other hand,

$$v_L(\beta_1 \cdot y_{p^n-1}) = (p^n - w - (p^n - 1)) + a \leq p^n - w - 1,$$

so $\beta_1 \cdot y_{p^n-1} \notin \pi_K \mathcal{D}^{-1}$, and $\beta_1 \notin \pi_K \mathfrak{A}_{L/K}$. □

We summarise what we have done so far. Let L/K be a totally ramified Galois extension of p-adic fields of degree p^n with Galois group G such that $\mathfrak{A}_{L/K}$ is an $\mathcal{O}_K$-Hopf order in $K[G]$. Then $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$. If in addition $\mathfrak{A}_{L/K}$ is a local ring, then $\mathcal{O}_L$ is $\mathfrak{A}_{L/K}$-Galois, $\mathcal{D}^{-1} = \mathfrak{a}^{-1}\mathcal{O}_L$ for an $\mathcal{O}_K$-ideal $\mathfrak{a}$, and the ramification jumps of L/K satisfy

$$t_i \equiv -1 \pmod{p^n}.$$

15.5. **Formal groups and Hopf orders.** We deal now with a way of creating Hopf orders. Let K be a p-adic field.

Definition 15.6. A *(one-dimensional) formal group* over $\mathcal{O}_K$ is a power series $F(X,Y) \in \mathcal{O}_K[[X,Y]]$ such that the following hold:

(1) $F(X,Y) \equiv X + Y \pmod{\deg \geq 2}$.
(2) $F(F(X,Y),Z) = F(X,F(Y,Z))$.
(3) $F(X,0) = X$, $F(0,Y) = Y$.
(4) $F(X,Y) = F(Y,X)$.
(5) There exists a series $i(X) \in \mathcal{O}_K[[X]]$ with $i(0) = 0$ such that

$$F(X, i(X)) = 0.$$

Remark 15.7. We may write $F(F(X,Y),Z)$ in Definition 15.6(2) because $F(X,Y)$ has no constant term.

If E is an algebraic extension of K (not necessarily finite) and $\mathfrak{p}_E$ is the maximal ideal of the valuation ring of E, then $(\mathfrak{p}_E, +_F)$ is an abelian group, where, for all $x, y \in \mathfrak{p}_E$,

$$x +_F y = F(x,y).$$

This makes sense as $K(x,y)$ is again a p-adic field, so it is complete and the series defining $x +_F y$ converges. The identity is 0 and the inverse of x is $i(x)$.

Example 15.8. Let E be an algebraic extension of K.

- The *additive formal group*

$$F(X,Y) = X + Y$$

gives the usual addition on $\mathfrak{p}_E$.

- The *multiplicative formal group* is

$$F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1.$$

The group $(\mathfrak{p}_E, +_F)$ is isomorphic to $1 + \mathfrak{p}_E \subseteq \mathcal{O}_E^\times$ with the usual operation, via the map $x \mapsto 1 + x$.

Definition 15.9. Let F and F' be formal groups over $\mathcal{O}_K$. A *homomorphism* $f\colon F \to F'$ is a power series $f(X) \in \mathcal{O}_K[[X]]$ without constant term such that

$$f(F(X,Y)) = F'(f(X), f(Y)).$$

If $F = F'$, then f is an *endomorphism.*

Note that a homomorphism $f\colon F \to F'$ yields a group homomorphism

$$f\colon (\mathfrak{p}_E, +_F) \to (\mathfrak{p}_E, +_{F'})$$

for all algebraic extensions E of K, and we can talk about the kernel $\ker(f)$ of f.

The connection between formal groups and Hopf algebras is given by the following result.

Proposition 15.10. *Let $F(X,Y)$ be a formal group over $\mathcal{O}_K$. Then F induces a "formal" $\mathcal{O}_K$-Hopf algebra structure on $\mathcal{O}_K[[T]]$.*

Proof. See [Chi00, Proposition 34.1]. We just give some details. Let $U = T \otimes 1$ and $V = 1 \otimes T$. Write $\mathcal{O}_K[[U]]\hat{\otimes}_{\mathcal{O}_K}\mathcal{O}_K[[V]]$ for the completed tensor product: it is the completion of $\mathcal{O}_K[[U]]\otimes_{\mathcal{O}_K}\mathcal{O}_K[[V]]$ with respect to the I-adic topology, where

$$I = \langle U \rangle \otimes_{\mathcal{O}_K} \mathcal{O}_K[[V]] + \mathcal{O}_K[[U]] \otimes_{\mathcal{O}_K} \langle V \rangle.$$

Now define the following continuous algebra maps:

$$\begin{aligned} \Delta\colon \mathcal{O}_K[[T]] &\to \mathcal{O}_K[[U,V]] = \mathcal{O}_K[[U]]\hat{\otimes}_{\mathcal{O}_K}\mathcal{O}_K[[V]] \\ T &\mapsto F(U,V), \end{aligned}$$

$$\begin{aligned} \varepsilon\colon \mathcal{O}_K[[T]] &\to \mathcal{O}_K \\ T &\mapsto 0, \end{aligned}$$

and

$$\begin{aligned} \lambda\colon \mathcal{O}_K[[T]] &\to \mathcal{O}_K[[T]] \\ T &\mapsto i(T). \end{aligned}$$

Then these maps satisfy the usual Hopf algebra axioms. □

Definition 15.11. Let $f\colon F \to F'$ be a homomorphism of formal groups, and let $H_f = \mathcal{O}_K[[X]]/(f)$. Then f is an *isogeny* if H_f is a finite $\mathcal{O}_K$-module.

Proposition 15.12. *If $f\colon F \to F'$ is an isogeny, then H_f is an $\mathcal{O}_K$-Hopf algebra with operations induced from those on $\mathcal{O}_K[[X]]$ by F.*

Proof. See [Chi00, Proposition 34.3]. □

In particular, let $f(X) = a_1X + a_2X^2 + \cdots : F \to F'$ be a homomorphism of formal groups such that there exists $d \geq 2$ with $a_j \in \mathfrak{p}_K$ for all $1 \leq j \leq d-1$, and $a_d \notin \mathfrak{p}_K$. By Weierstrass preparation theorem (see [Lan02, Chapter IV, Theorem 9.2]), $f(X) = f_0(X)u(X)$, where $f_0(X)$ is a monic polynomial of degree d with $f_0(X) \equiv X^d \pmod{\mathfrak{p}_K}$, and $u(X) \in \mathcal{O}_K[[X]]^\times$. This implies that f is an isogeny (see [Chi00, Proposition 35.6]), and $H_f = \mathcal{O}_K[[X]]/(f)$ is an $\mathcal{O}_K$-Hopf algebra of rank d.

Now let $c \in \mathfrak{p}_K$, and write $S = \mathcal{O}_K[[T]]/(f(T) - c)$. There is a well defined map

$$\begin{aligned} S &\to S \otimes_{\mathcal{O}_K} H \\ T &\mapsto F(T \otimes 1, 1 \otimes X). \end{aligned}$$

This makes S into a Galois H-object (see [Chi00, proposition 39.1]) and so into a Galois H^*-extension, where H^* is the dual of H. If $v_K(c) = 1$, then we can use again Weierstrass preparation theorem to find that $f(T) - c = f_0(T)u(T)$, where $f_0(T)$ is an Eisenstein polynomial of degree d and $S = \mathcal{O}_L$ for some totally ramified extension L/K of degree d. Summarising, we have created an extension L/K for which $\mathcal{O}_L$ is free over H^*, a commutative and cocommutative $\mathcal{O}_K$-Hopf order in $K \otimes_{\mathcal{O}_K} H^*$, and the key point one can note is that $K \otimes_{\mathcal{O}_K} H^*$ is a group algebra (and so we are in the classical case) if and only if $\ker(f) \subseteq K$.

Consider, for example, $F(X, Y) = X + Y + XY$, and the (shifted) p^n-power endomorphism $f \colon F \to F$ defined by

$$f(X) = (1 + X)^{p^n} - 1 = p^n X + \cdots + X^{p^n}.$$

Then $H^* \subseteq K[C_p]$ if and only if $\zeta_{p^n} \in K$. If $v_K(c) = 1$, then $S = \mathcal{O}_K[\sqrt[p^n]{c}]$, which is the valuation ring of $L = \mathbb{Q}_p(\sqrt[p^n]{c})$, and is free over the Hopf order H^*.

If we start with $K = \mathbb{Q}_p(\zeta_p)$ and we take $c = \zeta_p - 1$, we find $L = \mathbb{Q}_p(\zeta_{p^{n+1}})$, which is a Galois extension of K in the classical sense, but if $n > 1$, then H^* gives a nonclassical structure.

15.6. **Lubin–Tate formal groups.** For this final part, we change the notation: let k be a p-adic field with residue field of order $q = p^f$, and let $\pi = \pi_k$ be a uniformiser of k. Write $\overline{\mathfrak{p}}$ for the maximal ideal in the valuation ring of the algebraic closure of k. We follow the discussion of [Byo97, sections 5 and 6]; see also [Chi00, Section 40], where more details are given.

Let $f(X) \in \mathcal{O}_K[[X]]$ such that

$$f(X) \equiv \pi X \pmod{\deg \geq 2}$$

and

$$f(X) \equiv X^q \pmod{\pi}.$$

For example, if $k = \mathbb{Q}_p$ and $\pi = p$, we may take

$$f(X) = (1 + X)^p - 1 = pX + \cdots + X^p.$$

Then there is a unique formal group $F(X, Y)$ over $\mathcal{O}_k$ such that $f(X)$ is an endomorphism of F; see [Chi00, Theorem 36.2]. In fact, the ring of endomorphisms of F (with operations defined in the natural way) is canonically isomorphic to $\mathcal{O}_k$. If we write $[a]$ for the image of $a \in \mathcal{O}_k$ under this isomorphism, then $[\pi] = f(X)$.

For all $n \geq 1$, consider the torsion points

$$F_n = \ker[\pi^n] = \{x \in \overline{\mathfrak{p}} \mid [\pi^n](x) = 0\}.$$

Then F_n is an $\mathcal{O}_k$-module, where addition is via F, and where $a \in \mathcal{O}_k$ acts via $[a]$. For all $n \geq 1$, let $k_n = k(F_n)$, with valuation ring $\mathcal{O}_{k_n}$. Then k_n/k is a totally ramified Galois extension of degree $q^{n-1}(q-1)$, with Galois group

$$\operatorname{Gal}(k_n/k) \cong \frac{\mathcal{O}_k^\times}{1 + \mathfrak{p}_k^n}.$$

Moreover, if $\omega_n \in F_n \setminus F_{n-1}$, then w_n is a uniformiser for k_n.

Now let $K = k_m$ and $L = k_{m+n}$, for $n, m \geq 1$. Then L/K is a totally ramified abelian extension of degree q^n with Galois group $G \cong (1 + \mathfrak{p}_k^m)/(1 + \mathfrak{p}_k^{m+n})$.

Theorem 15.13. *If $n > m$ and $k \neq \mathbb{Q}_p$, then $\mathcal{O}_L$ is not free over $\mathfrak{A}_{L/K}$.*

Proof. This is [Byo97, Theorem 5.1]. We just sketch the proof.

The ramification jumps (with multiplicity) can be computed as follows:

$$\begin{gathered}t_1 = \cdots = t_f = q^m - 1, \\ t_{f+1} = \cdots = t_{2f} = q^{m+1} - 1, \\ \vdots \\ t_{(n-1)f+1} = \cdots = t_{nf} = q^{m+n-1} - 1.\end{gathered}$$

In particular, $t_1 = q^m - 1 \not\equiv -1 \pmod{q^n}$, and since we can prove that $\mathfrak{A}_{L/K}$ is local if and only if $k \neq \mathbb{Q}_p$, we conclude by Theorem 15.5 that $\mathcal{O}_L$ is not free over its associated order $\mathfrak{A}_{L/K}$ in $K[G]$, provided $k \neq \mathbb{Q}_p$. □

On the other side, since $L = K(\omega_{m+n})$, where ω_{m+n} is a root of

$$[\pi^n](X) - \omega_m = 0$$

with ω_m a uniformiser for $\mathcal{O}_K$, the formal group construction gives an $\mathcal{O}_K$-Hopf order H^* so that $\mathcal{O}_L$ is a free H^*-module of rank one (note that $F_m \not\subseteq K$, so we are in a nonclassical setting).

16. An assortment of associated orders in Hopf–Galois extensions

16.1. **Standing assumptions.** Fix a finite separable extension L/K. For the most part of this section, L/K is a Galois extension of number fields or p-adic fields.

Let E be the Galois closure of L/K, and write $G = \mathrm{Gal}(E/K)$, $G_L = \mathrm{Gal}(E/L)$, and $X = G/G_L$. As in Section 11, if $\Lambda\colon G \to \mathrm{Perm}(G)$ denotes the left translation map, then regular subgroup of $\mathrm{Perm}(X)$ normalised by $\Lambda(G)$ yield Hopf–Galois structures on L/K: the Hopf algebra giving the structure is $E[N]^G$. In what follows, we call *G-stable* the subgroups of $\mathrm{Perm}(X)$ normalised by $\Lambda(G)$.

Denote by $\mathfrak{A} = \mathfrak{A}_N$ the associated order of $\mathcal{O}_L$ in $E[N]^G$.

Remark 16.1. Many of the results in this section remain valid if $\mathcal{O}_L$ is replaced with any fractional ideal of L.

16.2. **Generalised normal basis generator.** Here we mainly follow [Tru18].

Recall that a Hopf–Galois analogue of the normal basis theorem holds: if L is H-Galois, then L is a free H-module of rank one (Theorem 10.23). In particular, [Tru18, Lemma 3.2] gives an explicit way to find a generator, as follows.

Lemma 16.2. *An element $x \in L$ is a free generator of L as an $E[N]^G$-module if and only if the matrix $T_N(x) = (\eta(\overline{g})[x])_{\eta \in N, \overline{g} \in X}$ is nonsingular.*

Corollary 16.3. *If M and N are isomorphic G-stable regular subgroups of* $\mathrm{Perm}(X)$, *then $E[M]^G$ and $E[N]^G$ have the same generalised normal basis generators.*

Proof. By a well-known result in group theory, if two regular G-stable subgroup of $\mathrm{Perm}(X)$ are isomorphic, then the isomorphism is a conjugation. So let $\pi \in \mathrm{Perm}(X)$ such that $M = \pi N \pi^{-1}$. For $x \in L$ we have

$$T_M(x) = (\pi\eta\pi^{-1}(\overline{g})[x]),$$

which differs from $T_N(x)$ by permutations of the rows and columns. □

Example 16.4. Suppose L/K is Galois with nonabelian Galois group G. Consider the regular G-stable subgroups $P(G)$ and $\Lambda(G)$ (recall that $P\colon G \to \mathrm{Perm}(G)$ denotes the right translation map). Clearly, $\rho(G)$ and $\Lambda(G)$ are isomorphic (both are isomorphic to G). Explicitly, an isomorphism is given by conjugation by π, where for all $g \in G$, $\pi(g) = g^{-1}$. Indeed, for all $g, h \in G$,

$$\pi\Lambda(g)\pi^{-1}[h] = \pi[gh^{-1}] = hg^{-1} = \rho(g)[h].$$

We deduce that $K[G]$ and $L[\Lambda(G)]^G$ have the same generalised normal basis generators.

16.3. **Opposite Hopf–Galois structures.** We follow again [Tru18].

Denote by N' the centraliser in $\mathrm{Perm}(G)$ of N. It is again regular G-stable subgroup of $\mathrm{Perm}(G)$, as observed in [GP87]. We always have $N \cong N'$, but the equality holds if and only if N is abelian. Moreover, $(N')' = N$. We call the structure corresponding to N and N' *opposites* of one another, and we write $\mathfrak{A}' = \mathfrak{A}_{N'}$.

Example 16.5. If L/K is Galois with Galois group G, the structures given by $K[G]$ and $L[\Lambda(G)]^G$ are opposites of one another, as $\rho(G)$ is the centraliser in $\mathrm{Perm}(G)$ of $\Lambda(G)$.

The following result is [Tru18, Proposition 2.4].

Proposition 16.6. *If $h \in E[N]^G$ and $h' \in E[N']^G$, then for all $x \in L$,*

$$h \cdot (h' \cdot x) = h' \cdot (h \cdot x)$$

Theorem 16.7 (Truman)**.** *Let L/K be an extension of number fields or p-adic fields. Then $\mathcal{O}_L$ is a free $\mathfrak{A}$-module if and only if $\mathcal{O}_L$ is a free $\mathfrak{A}'$-module.*

Proof. Suppose that $\mathcal{O}_L$ is a free $\mathfrak{A}$-module with generator x. Thus x is a free generator of L as an $E[N]^G$-module, and by Corollary 16.3, as an $E[N']^G$-module. For all $a \in \mathfrak{A}$, define $z_a \in E[N']^G$ by $z_a \cdot x = a \cdot x$. We claim that

$$\mathfrak{A}' = \{z_a \mid a \in \mathfrak{A}\}.$$

If $y = b \cdot x \in \mathcal{O}_L$ with $b \in \mathfrak{A}$, then

$$z_a \cdot y = z_a \cdot (b \cdot x) = b \cdot (z_a \cdot x) \in \mathcal{O}_L,$$

so $z_a \in \mathfrak{A}$.

The other inclusion follows immediately by $E[N]^G$-freeness of L. Since clearly $\mathcal{O}_L = \{z_a \mid a \in \mathfrak{A}\} \cdot x$, we derive our claim. □

Corollary 16.8. *Let L/K be a weakly ramified Galois extension of p-adic fields. Then $\mathcal{O}_L$ is free over its associated order in $L[\Lambda(G)]^G$.*

If the characteristic of K does not divide the degree of the extension, then $\mathfrak{A}$ is a maximal order in $E[N]^G$ if and only if $\mathfrak{A}'$ is a maximal order in $E[N^{\mathrm{opp}}]^G$ ([Tru18, Proposition 4.3]). But as Example 16.15 shows, it is possible for $\mathfrak{A}$ to be a Hopf order in $E[N]^G$ without $\mathfrak{A}'$ being a Hopf order in $E[N']^G$.

16.4. **A subextension technique.** Now suppose that L/K is Galois with Galois group G.

If Q is a G-stable subgroup of N, then $L[Q]^G$ is a K-Hopf-subalgebra of $L[N]^G$; see [CRV16b, Proposition 2.2]. We can form the corresponding "fixed field":

$$L^Q = \{x \in L \mid h \cdot x = \varepsilon(h)x \text{ for all } h \in L[Q]^H\}.$$

It follows that $[L : L^Q] = \dim_K(L[Q]^G) = |Q|$. The details of the next result are described in [KKTU19]; see in particular [KKTU19, Theorem 2.10].

Theorem 16.9. *If Q is normal in N, then $L[N/Q]^G$ gives a Hopf–Galois structure on L^Q/K.*

Example 16.10. Let L be the splitting field of $x^3 - 2$ over $\mathbb{Q}$. It is well known that $L/\mathbb{Q}$ is Galois with $G \cong D_6$, the dihedral group with 6 elements. Let N be a G-stable regular subgroup of $\mathrm{Perm}(G)$ isomorphic to C_6. Then $L/\mathbb{Q}$ is Hopf–Galois for $L[N]^G$. If Q is the unique subgroup of N of order 2, then Q is normal and G-stable; therefore, by Theorem 16.9, $L^Q/\mathbb{Q}$ is $L[N/P]^G$-Galois. Note that $L^Q/\mathbb{Q}$ is not Galois.

In this way, one can obtain a slight generalisation of the results of section 13, as follows.

Lemma 16.11. *Suppose $N = M \times Q$ for G-stable subgroups M and Q of N. Then*

- *L^Q/K is Hopf–Galois for $L[M]^G$;*
- *L^M/K is Hopf–Galois for $L[Q]^G$.*

Suppose in addition that

- *L^Q/K and L^M/K are arithmetically disjoint;*
- *$\mathcal{O}_{L^M}$ is free over its associated order in $L[Q]^G$;*
- *$\mathcal{O}_{L^P}$ is free over its associated order in $L[M]^G$.*

Then $\mathcal{O}_L$ is free over its associated order in $L[N]^G$.

16.5. **Tamely ramified extensions.** Here we follow [Tru11].

If L/K is a tamely ramified extension of p-adic fields, then $\mathfrak{A}_{L/K} = \mathcal{O}_K[G]$ and $\mathcal{O}_L$ is free over $\mathfrak{A}_{L/K}$. But there are interesting questions to deal with, also in this "simplified" setting. For example, is $\mathcal{O}_L$ free over its associated order in all Hopf–Galois structures? What about tamely ramified extensions of number fields? What if L/K is non-normal?

With the previous notation, the order $\mathcal{O}_E[N]^G$ in $E[N]^G$ is a formal analogue of $\mathcal{O}_K[G]$ in $K[G]$. Note that $\mathcal{O}_E[N]^G \subseteq \mathfrak{A}$, as immediately follows by the explicit description of the Hopf-action in Remark 11.11 (generalised to the separable case).

As in the classical setting, if L/K is wildly ramified, then $\mathcal{O}_E[N]^G \subsetneq \mathfrak{A}$. Indeed, we have $\theta = \sum_{\eta \in N} \eta \in \mathcal{O}_E[N]^G$, and $\theta \cdot x = \mathrm{Tr}_{L/K}(x)$ for all $x \in \mathcal{O}_L$, so $\pi_K^{-1}\theta \in \mathfrak{A}$.

However, we ofter have equality in the tamely ramified case.

Theorem 16.12. *Let L/K be a tamely ramified Galois extension of p-adic fields, and let N be an abelian G-stable regular subgroup of* $\mathrm{Perm}(G)$. *Then $\mathfrak{A} = \mathcal{O}_L[N]^G$ and $\mathcal{O}_L$ is a free $\mathfrak{A}$-module.*

Before the proof, we analyse two particular situations.

Theorem 16.13. *Let L/K be an unramified Galois extension of p-adic fields, and let N be an abelian G-stable regular subgroup of* $\mathrm{Perm}(G)$. *Then $\mathfrak{A} = \mathcal{O}_L[N]^G$, $\mathfrak{A}$ is a $\mathcal{O}_K$-Hopf order in $L[N]^G$, and $\mathcal{O}_L$ is a free $\mathfrak{A}$-module.*

Proof. If L/K is unramified, then $\mathcal{O}_L/\mathcal{O}_K$ is a Galois extension of rings with group G. In particular, we can apply Galois descent: since $\mathcal{O}_L[N]$ is an $\mathcal{O}_L$-Hopf order in $L[N]$, we find that $\mathcal{O}_L[N]^G$ is an $\mathcal{O}_K$-Hopf order in $L[N]^G$. Now consider the element $\theta = \sum_{\eta\in N} \eta$, a left integral of $\mathcal{O}_L[N]^G$. For all $x \in \mathcal{O}_L$, $\theta \cdot x = \mathrm{Tr}_{L/K}(x)$, and since L/K is unramified, we can find $x \in \mathcal{O}_L$ such that $\theta \cdot x = 1$. This implies that $\mathcal{O}_L$ is an $\mathcal{O}_L[N]^G$-tame extension of $\mathcal{O}_K$, so the assertion follows. □

Theorem 16.14. *Let L/K be an extension of p-adic fields, and let N be an abelian G-stable regular subgroup of* $\mathrm{Perm}(X)$. *Then $\mathfrak{A} = \mathcal{O}_E[N]^G$, $\mathfrak{A}$ is the maximal $\mathcal{O}_K$-order in $E[N]^G$, and $\mathcal{O}_L$ is a free $\mathfrak{A}$-module.*

Proof. Note that $|N| = |X| = [L : K]$, so $p \nmid |N|$. Since N is abelian, we derive that $\mathcal{O}_E[N]$ is the maximal order in $E[N]$. Let $\mathcal{M}$ be the maximal $\mathcal{O}_K$-order in $E[N]^G$. If $z \in \mathcal{M}$, then z is an element of $E[N]$ which is clearly fixed by G, so $z \in \mathcal{O}_E[N]^G$. We deduce that $\mathcal{O}_E[N]^G = \mathcal{M}$, and since $\mathcal{O}_E[N]^G \subseteq \mathfrak{A}$, we conclude that $\mathcal{O}_E[N]^G = \mathfrak{A}$, and by Theorem 5.12, $\mathcal{O}_L$ is free over $\mathfrak{A}$. □

Now we can prove the main result.

Proof of Theorem 16.12. Write $N = M \times Q$, with $|M| = m$, $|Q| = p^r$, and $p \nmid m$. Then M ans N are normal G-stable subgroups, and so we can apply 16.9 to find that L^Q/K is Hopf–Galois for $L[M]^G$ and that L^M/K is Hopf–Galois for $L[Q]^G$. Since L/K is tamely ramified, L^M/K is unramified. Therefore L^M/K and L^Q/K are arithmetically disjoint. Since L^M/K is unramified, $\mathcal{O}_{L^M}$ is a free $\mathcal{O}_L[Q]^G$-module. Since $p \nmid [L^Q : K]$ and M is abelian, $\mathcal{O}_{L^Q}$ is a free $\mathcal{O}_L[M]^G$-module. We conclude that $\mathcal{O}_L$ is a free $\mathcal{O}_L[N]^G$-module by Lemma 16.11. □

Example 16.15. Let $p \equiv 2 \pmod 3$ be a rational prime, and let L be the splitting field over $\mathbb{Q}_p$. Then $L/\mathbb{Q}_p$ is a tamely ramified Galois extension with Galois group $G \cong D_6$. Let N be a G-stable regular subgroup of $\mathrm{Perm}(G)$ isomorphic to C_6. Then $\mathcal{O}_L$ is free over $\mathfrak{A} = \mathcal{O}_L[N]^G$.

Note that $\mathcal{O}_L$ is also free over its associated order $\mathfrak{A}_{L/\mathbb{Q}_p}$ in $\mathbb{Q}_p[G]$, which is $\mathbb{Z}_p[G]$, and so also over its associated order in $L[\Lambda(G)]^G$. But it can be shown that the associated order $L[\Lambda(G)]^G$ strictly contains $\mathcal{O}_L[\Lambda(G)]^G$; thus we need to assume that the subgroup N is abelian.

Conjecture 16.16 (Truman). *If L/K is a tamely ramified extension of p-adic fields, then $\mathcal{O}_L$ is free over its associated order in all the Hopf–Galois structures.*

16.6. **Extensions of number fields.** Let L/K be a Galois extension of number fields. If K has class number one, then we can study $\mathcal{O}_L$ directly: let $x_1, \dots, x_n$ be an $\mathcal{O}_K$-basis of $\mathcal{O}_L$, and let $h_1, \dots, h_n$ be a K-basis of $L[N]^G$. We can analyse the action of the h_i on the x_j, to try to determine an $\mathcal{O}_K$-basis of the associated order $\mathfrak{A}$. If x is a candidate generator of $\mathcal{O}_L$ as an $\mathfrak{A}$-module, then we can compute the generalised module index $[\mathcal{O}_L : \mathfrak{A} \cdot x]$, to see if x is actually a generator.

For example, with this method, D. Gil-Muñoz studied in this PhD thesis Galois extensions of $\mathbb{Q}$ of degree 4. He obtained criteria for $\mathcal{O}_L$ to be free over various associated orders in terms of solubility of generalised Pell equations, showing in particular that the naive analogue of Leopold's theorem does not hold.

Another approach concerns locally freeness: one can study whether $\mathcal{O}_L$ is locally free over $\mathfrak{A}$, where as usual, if $\mathfrak{p}$ is a prime of $\mathcal{O}_K$, we write $\mathcal{O}_{L,\mathfrak{p}} = \mathcal{O}_{K,\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathcal{O}_L$ and

$\mathfrak{A}_\mathfrak{p} = \mathcal{O}_{K,\mathfrak{p}} \otimes_{\mathcal{O}_K} \mathfrak{A}$, and we ask if $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_\mathfrak{p}$-module. As showed in [Tru11], the result of the previous subsection can be translated in this setting.

Proposition 16.17. *Suppose that $\mathfrak{p}$ is unramified. Then $\mathfrak{A}_\mathfrak{p} = \mathcal{O}_{L,\mathfrak{p}}[N]^G$, $\mathfrak{A}_\mathfrak{p}$ is an $\mathcal{O}_{K_\mathfrak{p}}$-Hopf order in $L_\mathfrak{p}[N]^G$, and $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_\mathfrak{p}$-module.*

Proposition 16.18. *Suppose that $\mathfrak{p}$ does not divide $[L : K]\mathcal{O}_K$, and let N be an abelian G-stable regular subgroup of* $\mathrm{Perm}(G)$*. Then $\mathfrak{A}_\mathfrak{p} = \mathcal{O}_{L,\mathfrak{p}}[N]^G$, $\mathfrak{A}_\mathfrak{p}$ is the maximal $\mathcal{O}_{K_\mathfrak{p}}$ order in $L_\mathfrak{p}[N]^G$, and $\mathcal{O}_{L,\mathfrak{p}}$ is a free $\mathfrak{A}_\mathfrak{p}$-module.*

In particular, the next meaningful result is [Tru11, Theorem 5.9].

Theorem 16.19. *Suppose that no prime ideal of $\mathcal{O}_K$ dividing $[L : K]\mathcal{O}_K$ is ramified in L, and let N be an abelian G-stable regular subgroup of* $\mathrm{Perm}(G)$*. Then $\mathfrak{A} = \mathcal{O}_L[N]^G$ and $\mathcal{O}_L$ is a locally free $\mathfrak{A}$-module.*

16.6.1. *Some local to global machinery.* If $\mathcal{O}_L$ is locally free over $\mathfrak{A}$, then $\mathcal{O}_L$ defines a class in the locally free class group $\mathrm{Cl}(\mathfrak{A})$. There is a description of $\mathrm{Cl}(\mathfrak{A})$ via idèles, which we sketch now. If $H = L[N]^G$, we write

$$\mathbb{J}(H) = \left\{ (h_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} H_\mathfrak{p}^\times \mid h_\mathfrak{p} \in \mathfrak{A}_\mathfrak{p}^\times \text{ for almost all } \mathfrak{p} \right\}.$$

Then $\mathrm{Cl}(\mathfrak{A})$ is isomorphic to a quotient of $\mathbb{J}(H)$ by a certain subgroup arising from $\mathfrak{A}$. In particular, to obtain the class of $\mathcal{O}_L$ in $\mathrm{Cl}(\mathfrak{A})$, one can follow this procedure:

(1) Fix $x \in L$ such that $L = H \cdot x$.
(2) For all $\mathfrak{p}$, let $x_\mathfrak{p}$ be such that $\mathcal{O}_{L,\mathfrak{p}} = \mathfrak{A}_\mathfrak{p} \cdot x_\mathfrak{p}$.
(3) Define $(h_\mathfrak{p})_\mathfrak{p}$ by $h_\mathfrak{p} \cdot x = x_\mathfrak{p}$.
(4) Study the class of $(h_\mathfrak{p})_\mathfrak{p}$ in the quotient.

This approach was employed for

- tamely ramified $C_p \times C_p$-extensions in [Tru12, Tru16];
- tamely ramified Q_8-extensions of $\mathbb{Q}$ in [TT19];
- tamely ramified non-normal extensions of the form $L = K(\sqrt[p]{a})$ with $\zeta_p \notin K$ in [Tru20].
- tamely ramified non-normal extensions of the form $L = K(\sqrt[p]{a_1}, \dots, \sqrt[p]{a_r})$ with $\zeta_p \notin K$ by G. Prestidge.

References

[AM18] Adebisi Agboola and Leon R. McCulloh, *On the relative Galois module structure of rings of integers in tame extensions*, Algebra Number Theory **12** (2018), no. 8, 1823–1886. MR 3892966

[BBF72] Françoise Bertrandias, Jean-Paul Bertrandias, and Marie-Josée Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A1388–A1391. MR 296048

[BE14] Nigel P. Byott and G. Griffith Elder, *Integral Galois module structure for elementary abelian extensions with a Galois scaffold*, Proc. Amer. Math. Soc. **142** (2014), no. 11, 3705–3712. MR 3251712

[Ber72] Anne-Marie Bergé, *Sur l'arithmétique d'une extension diédrale*, Ann. Inst. Fourier (Grenoble) **22** (1972), no. 2, 31–59. MR 371857

[Ber78] ———, *Arithmétique d'une extension galoisienne à groupe d'inertie cyclique*, Ann. Inst. Fourier (Grenoble) **28** (1978), no. 4, 17–44, ix.

[Ber79a] ———, *Projectivite des anneaux d'entiers sur leurs ordres associes.*, Astérisque **61** (1979), 15–28 (French).

[Ber79b] Françoise Bertrandias, *Sur les extensions cycliques de degré p^n d'un corps local*, Acta Arith. **34** (1979), no. 4, 361–377. MR 543208

[BF72] Françoise Bertrandias and Marie-Josée Ferton, *Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local*, C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A1330–A1333. MR 296047

[BL96] Nigel P. Byott and Günter Lettl, *Relative Galois module structure of integers of abelian fields*, J. Théor. Nombres Bordeaux **8** (1996), no. 1, 125–141. MR 1399950

[Ble07] Dieter Blessenohl, *On the normal basis theorem*, Note Mat. **27** (2007), no. 1, 5–10. MR 2367749

[Bre04] Manuel Breuning, *Equivariant epsilon constants for galois extensions of number fields and p-adic fields*, Ph.D. thesis, King's College London (University of London), 2004.

[Bri92] Jan Brinkhuis, *On the Galois module structure over CM-fields*, Manuscripta Math. **75** (1992), no. 4, 333–347. MR 1168172

[Byo95] N. P. Byott, *Tame and Galois extensions with respect to Hopf orders*, Math. Z. **220** (1995), no. 4, 495–522. MR 1363852

[Byo96] Nigel P. Byott, *Uniqueness of Hopf Galois structure for separable field extensions*, Comm. Algebra **24** (1996), no. 10, 3217–3228. MR 1402555

[Byo97] ———, *Galois structure of ideals in wildly ramified abelian p-extensions of a p-adic field, and some applications*, J. Théor. Nombres Bordeaux **9** (1997), no. 1, 201–219. MR 1469668

[Byo99] ———, *Integral Galois module structure of some Lubin-Tate extensions*, J. Number Theory **77** (1999), no. 2, 252–273. MR 1702149

[Cha96] Robin J. Chapman, *A simple proof of Noether's theorem*, Glasgow Math. J. **38** (1996), no. 1, 49–51. MR 1373957

[Chi87] Lindsay N. Childs, *Taming wild extensions with Hopf algebras*, Trans. Amer. Math. Soc. **304** (1987), no. 1, 111–140. MR 906809

[Chi00] ———, *Taming wild extensions: Hopf algebras and local Galois module theory*, Mathematical Surveys and Monographs, vol. 80, American Mathematical Society, Providence, RI, 2000. MR 1767499

[CHR65] S. U. Chase, D. K. Harrison, and Alex Rosenberg, *Galois theory and Galois cohomology of commutative rings*, Mem. Amer. Math. Soc. **52** (1965), 15–33. MR 195922

[Cou94] Jean Cougnard, *Un anneau d'entiers stablement libre et non libre*, Experiment. Math. **3** (1994), no. 2, 129–136. MR 1313877

[CR81] Charles W. Curtis and Irving Reiner, *Methods of representation theory. Vol. I*, John Wiley & Sons, Inc., New York, 1981, With applications to finite groups and orders, Pure and Applied Mathematics, A Wiley-Interscience Publication. MR 632548

[CR87] ———, *Methods of representation theory. Vol. II*, Pure and Applied Mathematics (New York), John Wiley & Sons, Inc., New York, 1987, With applications to finite groups and orders, A Wiley-Interscience Publication. MR 892316

[CRV16a] Teresa Crespo, Anna Rio, and Montserrat Vela, *Induced Hopf Galois structures*, J. Algebra **457** (2016), 312–322. MR 3490084

[CRV16b] ______, *On the Galois correspondence theorem in separable Hopf Galois theory*, Publ. Mat. **60** (2016), no. 1, 221–234. MR 3447739

[CS69] Stephen U. Chase and Moss E. Sweedler, *Hopf algebras and Galois theory*, Lecture Notes in Mathematics, Vol. 97, Springer-Verlag, Berlin-New York, 1969. MR 0260724

[DCFL20] Ilaria Del Corso, Fabio Ferri, and Davide Lombardo, *How far is an extension of p-adic fields from having a normal integral basis?*, arXiv:2005.07932 (2020).

[EH79] Shizuo Endô and Yumiko Hironaka, *Finite groups with trivial class groups*, J. Math. Soc. Japan **31** (1979), no. 1, 161–174. MR 519042

[Ere91] B. Erez, *The Galois structure of the square root of the inverse different*, Math. Z. **208** (1991), no. 2, 239–255. MR 1128708

[ET92] B. Erez and M. J. Taylor, *Hermitian modules in Galois extensions of number fields and Adams operations*, Ann. of Math. (2) **135** (1992), no. 2, 271–296. MR 1154594

[Fer74] Marie-José Ferton, *Sur l'anneau des entiers d'extensions cycliques d'un corps local*, Journées Arithmétiques (Grenoble, 1973), 1974, pp. 69–74. Bull. Soc. Math. France Mém., No. 37. MR 0374104

[Frö72] A. Fröhlich, *Artin root numbers and normal integral bases for quaternion fields*, Invent. Math. **17** (1972), 143–166. MR 323759

[Frö83] Albrecht Fröhlich, *Central extensions, Galois groups, and ideal class groups of number fields*, Contemporary Mathematics, vol. 24, American Mathematical Society, Providence, RI, 1983. MR 720859

[FT93] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, vol. 27, Cambridge University Press, Cambridge, 1993. MR 1215934

[GMR20] Daniel Gil-Muñoz and Anna Rio, *On induced hopf galois structures and their local hopf galois modules*, arXiv:1910.06083 (2020).

[GP87] Cornelius Greither and Bodo Pareigis, *Hopf Galois theory for separable field extensions*, J. Algebra **106** (1987), no. 1, 239–258. MR 878476

[Gre21] Cornelius Greither, *Descent theory and the structure of hopf algebras acting on separable field extensions*, chapter 9 of: Hopf algebras and Galois Module theory (Lindsay N. Childs, Cornelius Greither, Kevin Keating, Alan Koch, Timothy Kohl, Paul J. Truman, and Robert Underwood, eds.), to appear as an AMS monograph, 2021.

[GRRS99] Cornelius Greither, Daniel R. Replogle, Karl Rubin, and Anupam Srivastav, *Swan modules and Hilbert-Speiser number fields*, J. Number Theory **79** (1999), no. 1, 164–173. MR 1718724

[Hat65] Akira Hattori, *Rank element of a projective module*, Nagoya Math. J. **25** (1965), 113–120. MR 175950

[Hen01] Guy Henniart, *Relèvement global d'extensions locales: quelques problèmes de plongement*, Math. Ann. **319** (2001), no. 1, 75–87. MR 1812820

[Jau81] Jean-François Jaulent, *Sur la l-structure galoisienne des idéaux ambiges dans une extension métacyclique de degré nl sur le corps des rationnels*, Number theory, 1979–1980 and 1980–1981, Publ. Math. Fac. Sci. Besançon, Univ. Franche-Comté, Besançon, 1981, pp. Exp. No. 3, 20. MR 748000

[JN16] Henri Johnston and Andreas Nickel, *On the equivariant Tamagawa number conjecture for Tate motives and unconditional annihilation results*, Trans. Amer. Math. Soc. **368** (2016), no. 9, 6539–6574. MR 3461042

[Joh06] Henri Johnston, *On the trace map between absolutely abelian number fields of equal conductor*, Acta Arith. **122** (2006), no. 1, 63–74. MR 2217325

[Joh11] ______, *Notes on galois modules*, Notes accompanying the course 'Galois Modules' given in Cambridge (2011).

[Joh15] ______, *Explicit integral Galois module structure of weakly ramified extensions of local fields*, Proc. Amer. Math. Soc. **143** (2015), no. 12, 5059–5071. MR 3411126

[Kaw86] Fuminori Kawamoto, *On normal integral bases of local fields*, J. Algebra **98** (1986), no. 1, 197–199. MR 825142

[KKTU19] Alan Koch, Timothy Kohl, Paul J. Truman, and Robert Underwood, *Normality and short exact sequences of Hopf-Galois structures*, Comm. Algebra **47** (2019), no. 5, 2086–2101. MR 3977722

[KO74] Max-Albert Knus and Manuel Ojanguren, *Théorie de la descente et algèbres d'Azumaya*, Lecture Notes in Mathematics, Vol. 389, Springer-Verlag, Berlin-New York, 1974. MR 0417149

[Köc04] Bernhard Köck, *Galois structure of Zariski cohomology for weakly ramified covers of curves*, Amer. J. Math. **126** (2004), no. 5, 1085–1107. MR 2089083

[Lan02] Serge Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR 1878556

[Leo59] Heinrich-Wolfgang Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*, J. Reine Angew. Math. **201** (1959), 119–149. MR 108479

[Let90] Günter Lettl, *The ring of integers of an abelian number field*, J. Reine Angew. Math. **404** (1990), 162–170. MR 1037435

[Let98] ———, *Relative Galois module structure of integers of local abelian fields*, Acta Arith. **85** (1998), no. 3, 235–248. MR 1627831

[Mar69] Jacques Martinet, *Sur l'arithmétique des extensions galoisiennes à groupe de Galois diédral d'ordre* $2p$, Ann. Inst. Fourier (Grenoble) **19** (1969), no. fasc. 1, 1–80, ix. MR 262210

[Mar71] ———, *Modules sur l'algèbre du groupe quaternionien*, Ann. Sci. École Norm. Sup. (4) **4** (1971), 399–408. MR 291208

[Mar72] ———, *Sur les extensions à groupe de Galois quaternionien*, C. R. Acad. Sci. Paris Sér. A-B **274** (1972), A933–A935. MR 299593

[Mat70] Hideyuki Matsumura, *Commutative algebra*, W. A. Benjamin, Inc., New York, 1970. MR 0266911

[Mat89] ———, *Commutative ring theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1989, Translated from the Japanese by M. Reid. MR 1011461

[McC83] Leon R. McCulloh, *Galois module structure of elementary abelian extensions*, J. Algebra **82** (1983), no. 1, 102–134. MR 701039

[McC87] ———, *Galois module structure of abelian extensions*, J. Reine Angew. Math. **375**/**376** (1987), 259–306. MR 882300

[Mil20] J.S. Milne, *Class field theory (v4.03)*, 2020, Available at www.jmilne.org/math/, pp. 287+viii.

[Noe32] Emmy Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. **167** (1932), 147–152. MR 1581331

[Rei03] I. Reiner, *Maximal orders*, London Mathematical Society Monographs. New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003, Corrected reprint of the 1975 original, With a foreword by M. J. Taylor. MR 1972204

[Rog70] Klaus W. Roggenkamp, *Lattices over orders. II*, Lecture Notes in Mathematics, Vol. 142, Springer-Verlag, Berlin-New York, 1970. MR 0283014

[Rot09] Joseph J. Rotman, *An introduction to homological algebra*, second ed., Universitext, Springer, New York, 2009. MR 2455920

[RU74] I. Reiner and S. Ullom, *Remarks on class groups of integral group rings*, Symposia Mathematica, Vol. XIII (Convegno di Gruppi e loro Rappresentazioni, INDAM, Rome, 1972), 1974, pp. 501–516. MR 0367043

[Sch77] Hans-Jürgen Schneider, *Cartan matrix of liftable finite group schemes*, Comm. Algebra **5** (1977), no. 8, 795–819. MR 439857

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237

[Swe69] Moss E. Sweedler, *Hopf algebras*, Mathematics Lecture Note Series, W. A. Benjamin, Inc., New York, 1969. MR 0252485

[Tay81] M. J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), no. 1, 41–79. MR 608528

[Tru09] Paul J. Truman, *Hopf-galois Module Structure Of Some Tamely Ramified Extensions*, PhD thesis, The University of Exeter (2009), `https://ore.exeter.ac.uk/repository/handle/10036/71817`.

[Tru11] Paul J. Truman, *Towards a generalisation of Noether's theorem to nonclassical Hopf-Galois structures*, New York J. Math. **17** (2011), 799–810. MR 2862153

[Tru12] ———, *Hopf-Galois module structure of tame biquadratic extensions*, J. Théor. Nombres Bordeaux **24** (2012), no. 1, 173–199. MR 2914905

[Tru16] ———, *Hopf-Galois module structure of tame $C_p \times C_p$ extensions*, J. Théor. Nombres Bordeaux **28** (2016), no. 2, 557–582. MR 3509724

[Tru18] ———, *Commuting Hopf-Galois structures on a separable extension*, Comm. Algebra **46** (2018), no. 4, 1420–1427. MR 3780516

[Tru20] ———, *Hopf-Galois module structure of tamely ramified radical extensions of prime degree*, J. Pure Appl. Algebra **224** (2020), no. 5, 106231, 13. MR 4046237

[TT19] Stuart Taylor and Paul J. Truman, *The structure of Hopf algebras giving Hopf-Galois structures on quaternionic extensions*, New York J. Math. **25** (2019), 219–237. MR 3933762

[Ull70] S. Ullom, *Integral normal bases in Galois extensions of local fields*, Nagoya Math. J. **39** (1970), 141–148. MR 263790

[Und11] Robert G. Underwood, *An introduction to Hopf algebras*, Springer, New York, 2011. MR 2986663

[Und15] ———, *Fundamentals of Hopf algebras*, Universitext, Springer, Cham, 2015. MR 3379140

[Vin05] Stéphane Vinatier, *Galois module structure in weakly ramified 3-extensions*, Acta Arith. **119** (2005), no. 2, 171–186. MR 2167720

[Vos81] S. V. Vostokov, *Normal basis for an ideal in a local ring*, Journal of Soviet Mathematics **17** (1981), no. 2, 1755–1758.

(F. Ferri) Department of Mathematics, University of Exeter, Rennes Dr, Exeter EX4 4RN, United Kingdom

Email address: ff263@exeter.ac.uk

URL: http://emps.exeter.ac.uk/mathematics/staff/ff263

(L. Stefanello) Dipartimento di Matematica, Università di Pisa, Largo Bruno Pontecorvo, 5, 56127 Pisa, Italy

Email address: lorenzo.stefanello@phd.unipi.it

URL: https://people.dm.unipi.it/stefanello