Modules in model theory

Alessandro Achille, Luca Ghidelli

July 27, 2014

1 pp-definable groups

We study the left modules over a given associative ring R with identity (we do not require commutativity). From our point of view an R-module will be a structure over the language $L_R = \{0, +, -, r\}_{r \in R}$, so that a module is effectively an abelian group endowed with a family of endomorphism for every element of R.

Notation In the following text x, y, z will denote single variables, $\boldsymbol{x}$ will denote a tuple of variables $x_1, \ldots, x_n$ and in this case we define $|\boldsymbol{x}| := n$ to be the length of the tuple. $r, r_1, \ldots$ will denote elements of R.

Definition We call *equation* an atomic formula:

$$r_1 x_1 + r_2 x_2 + \cdots + r_n x_n = 0$$

and *positive primitive formula* (ppf) a formula of type:

$$\exists \boldsymbol{z}\ \gamma_1(\boldsymbol{x}, \boldsymbol{z}) \wedge \cdots \wedge \gamma_n(\boldsymbol{x}, \boldsymbol{z})$$

where the γ_i are equations.

The concept of pp-formula is most important, so we would like to give an alternative interpretation. Suppose we have the pp-formula:

$$\varphi(\boldsymbol{x}) \equiv \exists \boldsymbol{z}\ \gamma_1 \wedge \cdots \wedge \gamma_n,$$

given $\boldsymbol{x}$ we can look at it as a proposition about the existence of a solution $\boldsymbol{z}$ to a system of equations, or, alternatively, we ask if for a given vector $\boldsymbol{x}$ is there a solution $\boldsymbol{z}$ to the equation:

$$A\boldsymbol{z} = B\boldsymbol{x}$$

where A e B are matrices with coefficients in R.

Before moving on with the theory, let's look at some of examples and some properties of pp-formula:

Example Suppose $R = k$ is a field and $M = {}_k k$. We want to study the set defined by the formula $\varphi(\boldsymbol{x})$ with $\boldsymbol{x} = (x_1, \ldots, x_n)$. As we said this is the set of vectors $\boldsymbol{x}$ for which the system $A\boldsymbol{z} = B\boldsymbol{x}$ has a solution $\boldsymbol{z}$. By a change of basis (Gauss) we can rewrite it as:

$$\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} \boldsymbol{z}_1 \\ \boldsymbol{z}_2 \end{pmatrix} = \begin{pmatrix} B'_{11} & B'_{12} \\ B'_{21} & B'_{22} \end{pmatrix} \begin{pmatrix} \boldsymbol{x}_1 \\ \boldsymbol{x}_2 \end{pmatrix}$$

We now see that the set defined by the equation is:

$$\varphi(k^n) = \ker \begin{pmatrix} B'_{21} & B'_{22} \end{pmatrix}$$

Note that this is not the same as considering $M = k^n$, in fact in this case the only pp-definable set turns out to be M and 0.

Example Let $\varphi(x)$ be as in the previous example, but suppose now that R is a PID. This time we can't use Gauss reduction, but we can still use Smith normal form to rewrite the equation as:

$$D\boldsymbol{z} = B'\boldsymbol{x},$$

where D is a diagonal matrix. This means that the formula $\varphi(\boldsymbol{x})$ is equivalent to $\varphi'(\boldsymbol{x}) \equiv \exists \boldsymbol{z}\ \gamma'_1 \wedge \cdots \wedge \gamma'_n$ where each $\gamma'_i(\boldsymbol{x}, \boldsymbol{z})$ is of type:

$$d_i z_i = b'_{i1} x_1 + \cdots + b'_{in} x_n$$

We can also take Smith normal form of B and rewrite the equation as

$$A'\boldsymbol{z} = \tilde{D}\boldsymbol{x},$$

where $\tilde{D}$ is a diagonal matrix. In this case each $\gamma'_i(\boldsymbol{x}, \boldsymbol{z})$ is of type:

$$a'_{i1} z_1 + \cdots + a'_{in} z_n = \tilde{d}_i x_i$$

In general we can't give a more explicit description of a pp-definable set. Still we can prove some important properties.

Proposition 1.1. *Let $\varphi(x_1, \ldots, x_n)$ be a pp-formula. The set $\varphi(M^n)$ is a subgroup of M^n. If moreover R is commutative then it is a submodule.*

Proof. Let $A\boldsymbol{z} = B\boldsymbol{x}$ be the equation associated with φ. The zero is in $\varphi(M^n)$, because the equation $A\boldsymbol{z} = B\,\boldsymbol{0}$ always has the trivial solution $\boldsymbol{z} = \boldsymbol{0}$. Let now $\boldsymbol{x}_1$ and $\boldsymbol{x}_2$ be in $\varphi(M^n)$. This means that we can find $\boldsymbol{z}_1$ and $\boldsymbol{z}_2$ such that $A\boldsymbol{z}_1 = B\boldsymbol{x}_1$ and $A\boldsymbol{z}_2 = B\boldsymbol{x}_2$. The vector $\boldsymbol{x}_1 - \boldsymbol{x}_2$ is then in $\varphi(M^n)$, because the equation $A\boldsymbol{z} = B(\boldsymbol{x}_1 - \boldsymbol{x}_2)$ has a solution (take $\boldsymbol{z} = \boldsymbol{z}_1 - \boldsymbol{z}_2$). The last point follow immediately from $Ar\boldsymbol{z} = rA\boldsymbol{z} = r\boldsymbol{x}$, for any $r \in R$. ☐

We can easily see that, for a pp-formula $\varphi(\boldsymbol{x}, \boldsymbol{y})$, the formula $\varphi(\boldsymbol{x}, \boldsymbol{0})$ still defines a group. The following proposition gives a characterization of the set defined by $\varphi(\boldsymbol{x}, \boldsymbol{a})$.

Proposition 1.2. *Let $\varphi(\boldsymbol{x}, \boldsymbol{y})$ be a pp-formula and $\boldsymbol{a} = (a_1, \ldots, a_m)$ be a sequence of elements in M. Then the set $\varphi(M^n, \boldsymbol{a})$ is empty or a coset of $\varphi(M^n, \boldsymbol{0})$.*

Proof. If $\varphi(M^n, \boldsymbol{a})$ is not empty, fix $\boldsymbol{x}_0$ in $\varphi(M^n, \boldsymbol{a})$. If $\boldsymbol{x}_1$ is in $\varphi(M^n, \boldsymbol{0})$ then $\boldsymbol{x}_0 + \boldsymbol{x}_1$ is in $\varphi(M^n, \boldsymbol{a})$ because the associated system:

$$A\boldsymbol{z} = B \begin{pmatrix} \boldsymbol{x}_0 + \boldsymbol{x}_1 \\ \boldsymbol{a} \end{pmatrix}$$

is easily seen to have a solution. On the other hand if $\boldsymbol{x}_0$ and $\boldsymbol{x}_1$ are in $\varphi(M^n, \boldsymbol{a})$ then $\boldsymbol{x}_1 - \boldsymbol{x}_0$ is in $\varphi(M^n, \boldsymbol{0})$. ☐

Last we note that pp-definable subgroups are closed under $\cap$ and $+$. In fact we can see any equation $\gamma(\boldsymbol{x}, \boldsymbol{y})$ in some variables as an equation $\tilde{\gamma}(\boldsymbol{x}, \boldsymbol{y}, \boldsymbol{z})$ relating more variables, simply attaching zero coefficients to the new variables. Hence we can combine two pp-formulas without mixing up existentials:

$$\begin{aligned}(\varphi \cap \psi)(\boldsymbol{x}) &= \varphi(\boldsymbol{x}) \wedge \psi(\boldsymbol{x}) \\ (\varphi + \psi)(\boldsymbol{x}) &= \exists \boldsymbol{y}, \boldsymbol{z}\ \varphi(\boldsymbol{y}) \wedge \psi(\boldsymbol{z}) \wedge \boldsymbol{x} = \boldsymbol{y} + \boldsymbol{z}.\end{aligned}$$

Example Let $M = {}_R R$. Is easy to see that every pp-definable subgroup of M is a right ideal.

Conversely every finitely generated right ideal is pp-definable. In fact let $g_1, \ldots, g_n$ be the generators of the ideal, then the $x \in R$ such that

$$\exists \boldsymbol{z} \in R^n\ (g_1, \ldots, g_n)\boldsymbol{z} = x$$

are precisely the elements of the ideal. It follows that every right ideal of a noetherian ring is pp-definable and these are the only pp-definable subgroups. The converse, that is, if every right ideal is pp-definable then R is noetherian, is also true if we assume R to be weakly saturated (the proof is quite simple).

Example Let M be an R module. A definable subgroup of M is closed under endomorphism of M. In fact if $x \in M$ is such that $\exists z(az = bx)$ then we also have $\exists z'(az' = b\,(x\varphi))$, take $z' = z\varphi$.

Let then $R = \mathbb{Z}$ and $M = \mathbb{Q}$. The $\mathbb{Z}$-endomorphisms of $\mathbb{Q}$ act transitively, so by what we just said the only pp-definable subsets of $\mathbb{Q}$ are 0 and $\mathbb{Q}$.

The same is true if we let $R = k$ be a field (or more generally a division algebra) and M a k-vector space.

2 Quantifier elimination

We want to prove the following weak form of quantifier elimination.

Theorem 2.1. *For every module M, every L_R-formula is equivalent to a boolean combination of positive primitive formulas. That is, given a formula $\psi(\boldsymbol{x})$ we can find $\varphi(\boldsymbol{x})$ a boolean combination of pp-formulas so that:*

$$M \models \psi(\boldsymbol{x}) \leftrightarrow \varphi(\boldsymbol{x})$$

for every $\boldsymbol{x}$ in M^n.

Let's first introduce some convenient terminology. Fix a group G. We say that a subset X of G is *G-big* if a finite number of translations of X cover G, else we say that X is *G-small.* Note that a subgroup H of G is G-big if and only if G/H is finite. We leave to the reader to verify that a finite union of small sets is small.

Lemma 2.2 (B.H. Neumann)**.** *Let H_i be subgroups of an abelian group G. If $H_0 + a_0 \subset \bigcup_{i=1}^n H_i + a_i$ and $H_i \cap H_0$ is small in H_0 for $i > k$, then $H_0 + a_0 \subset \bigcup_{i=1}^k H_i + a_i$*

Proof. Translating everything by $-a_0$ and taking the intersection with H_0, the hypothesis reads $H_0 = \bigcup_{i=1}^n H_i + a_i$ with $H_i \subset H_0$ and H_i is H_0-small for $i > k$. We must prove that we can throw away the small set. Let $C = H_0 \setminus \bigcup_{i=1}^k H_i + a_i$. If C is empty we have finished. If it is not empty then C is necessarily H_0-big. In fact $H_1, \dots, H_k$ are H_0-big (e.g. H_0/H_i is finite) and by basic group theory we deduce that $H_1 \cap \cdots \cap H_k$ too is H_0-big. Let now c be an element in C, then $(H_1 \cap \cdots \cap H_k) + c$ is G-big and is contained in C, because $(\bigcap_{j=1}^k H_j + c) \cap (H_i + a_i) \subset (H_i + c) \cap (H_i + a_i) = \emptyset$ for $i \leq k$. But by hypothesis $C \subset \bigcup_{i=k+1}^n H_i + a_i$ and the latter is a finite union of small set, so it can't contain a big set. $\square$

Lemma 2.3. *Let A_i be sets. If A_0 is finite, then $A_0 \subset \bigcup_{i=1}^k A_i$ iff*

$$\sum_{\Delta \subset \{1,\dots,k\}} (-1)^{|\Delta|} \left| A_0 \cap \bigcap_{i \in \Delta} A_i \right| = 0.$$

Proof. A simple application of the inclusion-exclusion principle. $\square$

We are now ready to prove the theorem.

Proof of Theorem 2.1. The only thing we have to prove is that if $\varphi(x, \boldsymbol{y})$ is equivalent to a boolean combination of pp-formulas, so is $\psi(\boldsymbol{y}) \equiv \forall x \varphi(x, \boldsymbol{y})$. Note that pp-formulas are closed under conjunction, so we can write:

$$\varphi \equiv \neg\varphi_0 \vee \varphi_1 \vee \cdots \vee \varphi_k \equiv \varphi_0 \to \varphi_1 \vee \cdots \vee \varphi_k$$

where φ_i are pp-formulas. Set-wise this means that $M \models \psi(\boldsymbol{y})$ iff $\varphi_0(M, \boldsymbol{y}) \subset \varphi_1(M, \boldsymbol{y}) \cup \cdots \cup \varphi_k(M, \boldsymbol{y})$. Setting $H_i = \varphi_i(M, 0)$, by Proposition 1.2 we can rewrite this as $H_0 + a_0 \subset \bigcup_{i=1}^n H_i + a_i$ for some a_i in M^n. By Lemma 2.2 we can assume $H_0 + a_0 \subset \bigcup_{i=1}^k H_i + a_i$ and $H_0/H_i \cap H_0$ finite. We now have to find a boolean combination of pp-formulas that express this inclusion, but being H_0 infinite this isn't a simple task (if it were finite we could simply impose the inclusion element by element). However if we take the quotient by $H_0 \cap \cdots \cap H_k$ (a H_0-big set) we are left with the inclusion of a finite set:

$$H_0/(H_0 \cap \cdots \cap H_k) + a_0 \subseteq \bigcup_{i=1}^k H_i/(H_0 \cap \cdots \cap H_k) + a_i \tag{1}$$

We can now apply Lemma 2.3 to (1). Let N_Δ be

$$N_\Delta = \left| \left(H_0 \cap \bigcap_{i \in \Delta} H_i \right) / (H_0 \cap \cdots \cap H_k) \right|.$$

The set $((H_0 + a_0) \cap \bigcap_{i \in \Delta} (H_i + a_i))/(H_0 \cap \cdots \cap H_k)$ is empty or it has N_Δ elements (Proposition 1.2), so Lemma 2.3 reads:

$$M \models \forall x\ \varphi \iff \sum_{\Delta \in \mathcal{N}} (-1)^{|\Delta|} N_\Delta = 0, \tag{2}$$

where

$$\mathcal{N} = \left\{ \Delta \subset \{1, \dots, k\} \mid \exists x \left(\varphi_0(x, \boldsymbol{y}) \wedge \bigwedge_{i \in \Delta} \varphi_i(x, \boldsymbol{y}) \right) \right\}$$

We have to prove that the sum in (2) can be written as a boolean combination of pp-formulas. To do this, list all the (finite) $\mathcal{N}$ for which the sum is zero and write a formula that says that we are in one of those cases. It is easily seen that this can be done with boolean combination of pp-formulas. $\square$

Corollary 2.4. *Two R-modules M_1 and M_2 are elementary equivalent iff for every ppf $\varphi \subseteq \psi$ we have*

$$\varphi/\psi(M_1) = \varphi/\psi(M_2),$$

where by $\varphi/\psi(M)$ we mean $[\varphi(M) : \psi(M)]$ if it is finite, or else ∞.

References

[1] Mike Prest. *Model Theory and Modules.* London Mathematical Society Lecture Note Series. Cambridge University Press, 1988.