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, \( x \) will denote a tuple of variables \( x_1, \ldots, x_n \) and in this case we define \( |x| := n \) to be the length of the tuple. \( r, r_1, \ldots \) will denote elements of \( R \).

**Definition** We call equation an atomic formula:

\[
r_1x_1 + r_2x_2 + \cdots + r_nx_n = 0
\]

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

\[
\exists z \gamma_1(x, z) \land \cdots \land \gamma_n(x, z)
\]

where the \( \gamma_i \) 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:

\[
\varphi(x) \equiv \exists z \gamma_1 \land \cdots \land \gamma_n,
\]

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

\[
Az = Bx
\]

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 \( \varphi(x) \) with \( x = (x_1, \ldots, x_n) \). As we said this is the set of vectors \( x \) for which the system \( Ax = Bx \) has a solution \( z \). By a change of basis (Gauss) we can rewrite it as:

\[
\begin{pmatrix}
I & 0 \\
0 & 0
\end{pmatrix}
\begin{pmatrix}
z_1 \\
z_2
\end{pmatrix}
= 
\begin{pmatrix}
B'_{11} & B'_{12} \\
B'_{21} & B'_{22}
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2
\end{pmatrix}
\]
We now see that the set defined by the equation is:

\[ \varphi(k^n) = \ker(B'_{21} B'_{22}) \]

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:

\[ Dz = B'x, \]

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

\[ d_i z_i = b'_i x_1 + \cdots + b'_{in} x_n \]

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

\[ A'z = \tilde{D}x, \]

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

\[ a'_i z_1 + \cdots + a'_n z_n = \tilde{d}_i x_i \]

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 \( Az = Bx \) be the equation associated with \( \varphi \). The zero is in \( \varphi(M^n) \), because the equation \( Az = B0 \) always has the trivial solution \( z = 0 \). Let now \( x_1 \) and \( x_2 \) be in \( \varphi(M^n) \). This means that we can find \( z_1 \) and \( z_2 \) such that \( Az_1 = Bx_1 \) and \( Az_2 = Bx_2 \). The vector \( x_1 - x_2 \) is then in \( \varphi(M^n) \), because the equation \( Az = B(x_1 - x_2) \) has a solution (take \( z = z_1 - z_2 \)). The last point follow immediately from \( Arz = rAz = rx, \) for any \( r \in R \).

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

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

**Proof.** If \( \varphi(M^n, \alpha) \) is not empty, fix \( x_0 \) in \( \varphi(M^n, \alpha) \). If \( x_1 \) is in \( \varphi(M^n, 0) \) then \( x_0 + x_1 \) is in \( \varphi(M^n, \alpha) \) because the associated system:

\[ Az = B \begin{pmatrix} x_0 + x_1 \\ \alpha \end{pmatrix} \]

is easily seen to have a solution. On the other hand if \( x_0 \) and \( x_1 \) are in \( \varphi(M^n, \alpha) \) then \( x_1 - x_0 \) is in \( \varphi(M^n, 0) \).

2
Last we note that pp-definable subgroups are closed under ∩ and +. In fact we can see any equation $\gamma(x, y)$ in some variables as an equation $\tilde{\gamma}(x, y, z)$ relating more variables, simply attaching zero coefficients to the new variables. Hence we can combine two pp-formulas without mixing up existentials:

$$(\varphi \land \psi)(x) = \varphi(x) \land \psi(x)$$
$$(\varphi + \psi)(x) = \exists y, z \varphi(y) \land \psi(z) \land x = y + z.$$  

**Example** Let $M = \mathbb{R}$. It 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 $x \in \mathbb{R}$ such that

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

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 $\mathbb{R}$ is noetherian, is also true if we assume $\mathbb{R}$ to be weakly saturated (the proof is quite simple).

**Example** Let $M$ be an $\mathbb{R}$ module. A definable subgroup of $M$ is closed under endomorphism of $M$. In fact if $x \in M$ is such that $\exists z(ax = bx)$ then we also have $\exists z'(az' = bx\varphi)$, 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 $\psi(x)$ we can find $\varphi(x)$ a boolean combination of pp-formulas so that:

$$M \models \psi(x) \leftrightarrow \varphi(x)$$

for every $x$ 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 $H_0 + a_0 \subset \bigcup_{i=1}^{k} H_i + a_i$ 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 \(H_1, \ldots, H_k\) 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 \((\bigcap_{i=1}^{k} H_i + a_i) \subset (H_i + a_i) \cap (H_i + a_i) = \emptyset\) for \(i \leq k\). But by hypothesis \(C \subset \bigcap_{i=k+1}^{n} H_i + a_i\) and the latter is a finite union of small set, so it can’t contain a big set.

\[\text{Lemma 2.3. Let } A_i \text{ be sets. If } A_0 \text{ is finite, then } A_0 \subset \bigcup_{i=1}^{k} A_i \text{ iff}
\]
\[\sum_{\Delta \subset \{1, \ldots, k\}} (-1)^{|\Delta|} \left| A_0 \cap \bigcap_{i \in \Delta} A_i \right| = 0.
\]

Proof. A simple application of the inclusion-exclusion principle.

We are now ready to prove the theorem.

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

\[\varphi \equiv \neg \varphi_0 \lor \varphi_1 \lor \cdots \lor \varphi_k \equiv \varphi_0 \lor \varphi_1 \lor \cdots \lor \varphi_k\]

where \(\varphi_i\) are pp-formulas. Set-wise this means that \(M \models \psi(y)\) iff \(\varphi_0(M, y) \subset \varphi_1(M, y) \cup \cdots \cup \varphi_k(M, y)\). 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 \(M^0\). 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:

\[H_0/(H_0 \cap \cdots \cap H_k) + a_0 \leq \bigcup_{i=1}^{k} H_i/(H_0 \cap \cdots \cap H_k) + a_i\]  \hspace{1cm} (1)

We can now apply Lemma 2.3 to (1). Let \(N_\Delta\) 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 \(N_\Delta\) elements (Proposition 1.2), so Lemma 2.3 reads:

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

where

\[\mathcal{N} = \left\{ \Delta \subset \{1, \ldots, k\} \mid \exists x \left( \varphi_0(x, y) \land \bigwedge_{i \in \Delta} \varphi_i(x, y) \right) \right\} \]
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) $N$ 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.

\[\text{Corollary 2.4.} \quad \text{Two } R\text{-modules } M_1 \text{ and } M_2 \text{ are elementary equivalent iff for every ppf } \varphi \subseteq \psi \text{ we have} \]

\[
\varphi/\psi(M_1) = \varphi/\psi(M_2),
\]

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

\[\text{References}\]