Structures and First-Order Definable Relations

Angus J. Macintyre

Vietri sul Mare

6-10 June 2016

Structures and First-Order Definable Relations

Start with a nonempty set M, and consider all cartesian powers M^n where n is one of 0,1,....
For each n we have $Powerset(M^n)$, a Boolean algebra in a natural way, and the elements of this powerset are called n-ary relations on M. The only obvious relation defined uniformly for all M is $=$, the equality relation (the diagonal subset of M^2). The powersets have, by Cantor, cardinality bigger than that of M, for $n \neq 0$.

Truth Values

How to interpret M^0? Since M^n can be construed as the set of functions from $[0, n)$ (or the set of length n sequences of elements of M, M^0 must be thought of as the set whose only element is the empty function (or empty sequence), and so has cardinality 1. Its powerset thus has cardinality 2, with elements 1 and 0, which we later identify with truth values.

Functions

We consider also $n - ary$ functions from M to M (e.g, for $n = 2$, a group operation) and occasionally functions from M^n to M^m, though the latter are naturally m-tuples of n-ary functions to M. It is standard how to construe an n-ary function as an $(n+1)$-ary relation, the graph of the function. The only obvious function is the identity map from M to M. It would be more natural to write this as id_M, but we avoid pedantry.

Functoriality

There are basic functorial operations on relations. Suppose f is a function from M_1 to M_2. This in turn induces maps at the level of powersets. One is the inverse image map, written f^* from $Powerset(M_2)$ to $Powerset(M_1)$. The other is the direct image map, written f_* from $Powerset(M_1)$ to $Powerset(M_2)$.

This gives an action on unary relations. There is a natural extension to n-ary relations. Thus if f is as above, there is a product map f^n from $(M_1)^n$ to $(M_2)^n$, and taking inverse and direct image of this induces maps on n-ary relations.

Laws Connecting the Operations

Exercise Write down laws connecting the image operations with the Boolean operations.

Data for Structures

The data for a structure on M is given by

- For each n , a well-ordered series of n-ary relations on M, with the equality relation being the first element in the series for $n = 2$.
- for each n, a well-ordered series, possibly empty, of n-ary functions on M
- a well-ordered series, possibly empty, of elements of M, to be called constants .

The pioneers, like Tarski, would have been much more pedantic. By now, it is an easy exercise to be pedantic when one has to be.

Defining First-Order Definability - Step 1

Now we can give a definition of the class of relations first-order definable in the structure.The definition is inductive. Firstly, all the following are definable:

- all relations in the data
- the graphs of all functions in the data

This gives you most of the atomic relations. Close under the Boolean operations (for each n) to get the constructible relations.

Functorialities, Quantifiers, Operations on Variables

Now come the closure operations which lead sometimes, even in familiar structures, to very complex relations. The most important involve projections, and the functoriality considerations already discussed.

- The elements of M^n can be construed as functions from $[0, n)$ to M. If h is a function from $[0, k)$ to $[0, n)$ then composition with h gives a map, also denoted h , from M^n to M^k, and this in turn induces h_* from $Powerset(M^n)$ to $Powerset(M^k)$. We require that the class of definable relations is closed under all h_*. Check how this connects to existential quantification! But also how it relates to permutation and identification of variables.

Continued

- The final operation concerns substitution of constants. It suffices to require that the relation $x = c$ is definable, for each constant c in the data. It is classified among the atomic relations.

So keep on closing under Boolean operations and the preceding to get the set of definable relations.

Example

Let G be a group with operation $\cdot$. Suppose M is G, and we take $\cdot$ alone as basic data (with $=$). The $Z(G)$, the centre of G is definable. Why? Well, the relation $xy = yx$ is definable. Why? By definition the set of all (x, y, z) with $xy = z$ is definable in G^3. But so is the set of all (x, y, z) with $yx = z$ by using a suitable h_*. The intersection (Boolean!) is the set of (x, y, z) with $xy = yx = z$.

Now take h as the inclusion from [0,1) to [0,1,2), and then apply h_* to get the relation $xy = yx$. Now the complement of this in G^2 is definable. Now project into G^1 to get complement of $Z(G)$ definable, and then take complement again.

In same vein you can show the graph of the commutator map is definable. But you will not be able to show that the commutator subgroup is in general definable, for it is not! But this is rather difficult to prove from first principles.

Syntax 1

Now we set up the notion of formula corresponding to a choice of primitives defining a structure. This is independent of the M chosen. We defined a structure on M by defining data consisting of

- for each n , a well-ordered series, possibly empty when $n \neq 2$, of n-ary relations on M, with the equality relation being the first element of the series for $n = 2$
- for each n, a well-ordered series, possibly empty, of n-ary functions on M
- a well-ordered series, possibly empty, of elements of M, to be called constants.

Signature

Now we abstract away from any specific M. A signature σ is given by the following data:

- For each $n \geq 1$, a well-ordered series Rel_n , with Rel_2 nonempty, and no entries in common for distinct m and n
- For each $n \geq 1$, a well-ordered series Fun_n , with no entries in common with any Rel_n
- A well-ordered set Const, with no entries in common with any of the other series.

We now define the notion of an interpretation of σ in M. This is simply a map on the set of all entries of one of the above series, sending an entry α to an element α^M, which is an n-ary relation on M if α is in Rel_n, an n-ary function on M if α is in Fun_n, and simply an element of M if α is in $Const$. Obviously any interpretation defines a structure on M, and any structure comes from some interpretation of a signature.

Isomorphism of Structures Given by an Interpretation of a Fixed Signature

Suppose M_1 and M_2 are sets , each given with an interpretation of the same signature σ. An isomorphism of the structures is a bijection f from M_1 to M_2 so that for any element (relation symbol, function symbol, or constant) f_* maps the interpretation of that symbol in M_1 to the interpretation of that symbol in M_2. This obviously generalizes the notion of isomorphism in groups and other algebraic systems.

From a signature to a formal language

Now we make a formal language based on the signature σ . We need Boolean connective symbols $\wedge$, $\vee$, $\neg$ and quantifier symbols $\exists$, $\forall$, and an infinite set V of variables, all mutually distinct and with union disjoint from all entries in the data of the signature. In addition we need brackets (and), and a comma for punctuation. Finally we write $=$ for the first element of the series Rel_2. Now we give an informal inductive definition of first-order formula over the signature. A pedantic definition can be found in any logic textbook.

- Variables are terms, and elements of *Const* are terms
- If f is in Fun_n , and $w_0, ..w_{n-1}$ are terms, then $f(w_0, \ldots, w_{n-1})$ is a term.
- The equations are the $(w_0 = w_1)$, where w_0 and w_1 are terms.
- The atomic formulas are the equations and all $R(w_0, \ldots, w_{n-1})$, where R is an element of Rel_n distinct from $=$
- The quantifier-free formulas are built from the atomic formulas in the obvious way, using the Boolean connectives repeatedly, e.g $(A \wedge B)$ is a quantifier-free formula if A and B are.
- Formulas are got by closing the preceding under repeated Boolean operations and quantification, the main point being that if A is a formula and v is a variable and Q a quantifier then QvA is a formula.

Tedious Things

There are various tedious issues concerning occurrences of variables, and in particular the notions of free and bound occurrences of variables. In quantifier-free formulas all occurrences of variables are free, and an occurrence free in a Boolean combination is free iff it is free in the appropriate subformula. In QvA any bound occurrence of a variable w in A is bound, and any occurrence of v is bound.
A formula without free (occurrences of) variables is a *sentence*.

Satisfaction1

A formula with free occurrences of exactly n variables defines (not quite canonically because one may permute variables) an n-ary relation in any L-structure. We do first the case of terms w. If w has no variables, w is a constant c, and we define w^M as the element c^M, and may construe this as a 0-ary function on M. Otherwise, w has a finite set of variables. Let s be a function from V to m, an assignment of values to the variables.The $s(w)$ may naturally be defined as an element of M, by induction, as follows,

- If w is a variable v, $s(w) = s(v)$
- If w is $f(w_0, \ldots, w_n)$ then $s(w) = f^M(s(w_0), \ldots, s(w_n))$

Satisfaction 2

Now we want to define s on formulas, or rather define the action of formulas on assignments. $A(s)$ will be a truth value, i.e an element of $Powerset(M^0)$.

- If A is an equation $w = u$ then $A(s) = T$ if $w(s) = u(s)$, and $A(w) = False$ otherwise
- Similarly for relational atomic formulas
- $(A \vee B)(s) = A(s) \vee B(s)$ with obvious truth table reading.
- $\exists vA(s) =$ supremum of all $A(s^{''})$, where s" differs from s at most at the variable v
- $\forall ... =$ infimum......

One trivially proves that $A(s)$ depends only on the restriction of v to the variables free in A. In this way one gives an unambiguous meaning to $M \models A(b_0, \ldots, b_{n-1})$, where the variables of A, in increasing order of subscripts, are $w_0, \ldots, w_{n-1}$, as $A(s) = True$, where s maps $w_j \rightarrow b_j$.

Enough of pedantry! On with the mathematics!

Formulas define first-order definable sets

If $A(v_0, \ldots, v_{n-1})$ has the n free variables listed (and we have a fixed interpretation) A defines an n-ary relation, namely

$\{(b_0, \ldots, b_{n-1}) : M \models A(b_0, \ldots, b_{n-1})\}$.
Now we easily show that the definable relations are exactly those defined by formulas.
This is proved by an easy induction, and allows us to compare definability as the L-structure varies.

Exercise Work with unital rings, take L to have addition, multiplication, 0 and 1. Show that the Jacobson radical is first order L-definable.

Identifying the Definable Relations in Special Cases

Case 1: M is any set, and the signature has only $=$. We want a uniform analysis as M varies.

There are some special sentences and formulas out of which everything definable is built.
Cardinality sentences: one may easily write down, for each non-negative integer n a first-order sentence $Card \geq n$ saying that M has cardinality at least n (it needs n existential quantifiers). Then one can write one saying $Card = n$, saying M has exactly n elements. But you will try in vain to find a sentence saying M is infinite. There is no such sentence, as can be proved directly (and can be found in Ackermann's old book on Solvable Cases of the Decision Problem). In fact, all infinite M satisfy exactly the same sentences, independent of cardinality (an instance of a much more general Theorem of Löwenheim-Skolem).

Relations Definable from Equality

How about definable relations? There are very few. Fix n, and any equivalence relation E on $[0, n-1)$. Define, on any M a relation R_E by

$$R_E(v_0, \dots, v_{n-1}) \text{ iff } (v_i = v_j \text{ iff } E(i,j)).$$

Then the definable relations are exactly the finite unions of such R_E, as E varies.
Note that they do not need quantifiers!!

Ordering

Case 2. M is a set, and $<$ is a dense ordering on M with no first or last element. An example is the open unit interval in $\mathbb{Q}$, and another is the open unit interval in the reals $\mathbb{R}$. No such M can be finite, by density. There is an obvious first-order sentence in the signature with $=$ and $<$ expressing that the relation $<$ is a dense linear order with no end points. The Löwenheim-Skolem Theorem shows that any model of this sentence satisfies exactly the same sentences as a countable model. But Cantor showed, in a very well-known argument, that any two countable models of the sentence are isomorphic. Now there is an easily proved general Theorem saying for arbitrary structures that isomorphism (preserving the basic relations of the signature) preserves definable relations, and in particular sentences. Thus any two dense linear orders without end points satisfy the same sentences.

When two structures for a signature satisfy the same sentences, we say they are elementarily equivalent.

Ordering - continued

What about definable relations? A minor adaptation of what Cantor did shows that there are very few definable relations.There are of course the ones already given for $=$, and each of these can be refined to definable sets as follows,Take an R_E as above, and take $<_E$ on the equivalence classes a linear order on the equivalence classes (there are of course only finitely many). Then define S_E as the subrelation of R_E defined by adding the conditions $v_i < v_j$ iff the E-class of i is less than the E-class of j. It turns out that all definable relations are finite unions of such S_E. Note again the remarkable fact that quantifiers are not needed (at all in this case, though in previous case we needed the cardinality statements, which need quantifiers).

Examples from Groups and Rings

The analysis here is much more difficult. But first note that for finite structures we have nothing interesting to say. When M is finite, isomorphism and elementary equivalence are the same thing. This is because you can write down a sentence which characterizes any given R from signature up to isomorphism by a sentence, and go on to show, easily, that isomorphism and elementary equivalence are the same thing. HOWEVER, not every relation is definable. (One sees this already from the $=$ case).

In any case we look now at infinite structures from algebra. We start with groups G, with the signature consisting only of the multiplication $\cdot$.Then $v = e$ (where e is the neutral element) and $Z(G)$ are definable, and the class of abelian groups G can be axiomatized by a single sentence.

Presburger

Our first example is $\mathbb{Z}$. Here there are excellent positive results, due to Moise Presburger, a student of Tarski, and a victim of the Holocaust. We take the signature to have just $+$ and $=$, and ask what can be defined in $\mathbb{Z}$. We will be very informal about definitions, for the sake of intelligibility. It is convenient to extend the signature by two constant symbols, one (written 0) for the neutral element of the group (the relation $v = 0$ is obviously definable in the original signature).The other is for the element 1 and will be written as 1. Note however that $v = 1$ is not definable in the pure signature, because Z has an automorphism mapping 1 to -1. It is convenient also to add the binary $-$ to the signature. It is obviously definable. We write $-w$ for $0 - w$.

Note

We will be very casual about bracketing. Thus we write sums without bracketing ($x + y + z$, for example). We write nw for $w + w + \ldots + w$, n times, if n is a nonnegative integer, as 0 if $n = 0$, and as $-nw$ if n is negative. Note that these are individual definitions, one for each n, making sense in every abelian group.

We are not defining multiplication in $\mathbb{N}$ in a first-order way.

In fact one cannot!!

Some Definable Subgroups

There are various definable groups used in elementary abelian group theory. Examples are:

- nG
- $[n]G$, the group of n-torsion elements

From these one can define various coset relations (such as $H(x-y)$, for a definable group H), and all this can be done in higher dimensions too. One gets various definable group via conditions saying an integer linear combination of the variables is 0. You get more groups by taking intersections. Then you get more coset relations in higher dimensions. All this is quite general in abelian groups. You also get projections (existential conditions) of definable groups, and corresponding coset relations.

Positive Primitive Formulas for Abelian groups

The positive primitive formulas are those which are got from conjunctions of homogeneous linear equations over $\mathbb{Z}$ by prefixing some existential quantifiers. Such pp-formulas always define subgroups in the appropriate power of G. nG is perhaps the most basic example. $[n]G$ is also an example, but does not need quantifiers. Note that $\neg$ and $\vee$ do not naturally occur in definitions of groups. Going a little further we can define, by pp-formulas, the relations of congruence modulo a subgroup (cf. example above). This can also relativize, namely if we have two pp-definable subgroups in same dimension, say H_1 and H_2, with $H_1 \subseteq H_2$ there is, for each k a sentence saying that the index of H_1 in H_2 is at least k. Write this as $Index_k(H_1, H_2)$. Notation is being abused harmlessly (the definition depends on the definitions of the H_j). As with cardinality, we can go on to define when index is exactly k, but we CANNOT express that index is infinite (this needs infinitely many sentences).

The special case of $\mathbb{Z}$

For convenience I add 1 as a constant, but the purist will have no trouble avoiding this. There are two first-order properties of $\mathbb{Z}$ clearly visible.

- $\mathbb{Z}$ is torsion free, i.e for each positive integer n we have $n\mathbb{Z} \neq 0$
- the index of $n\mathbb{Z}$ in $\mathbb{Z}$ is n, with coset representatives $0, 1, \ldots, (n-1)$. There is one axiom of each kind for each n. We are going to sketch a proof, due to Presburger in essence, that in $\mathbb{Z}$ every formula is equivalent to one which is a Boolean combination of pp-tformulas.

Note that a conjunction of pp-formulas is equivalent to a pp-formula (uniformly in all abelian groups), and that the existential quantification of a disjunction is equivalent to the disjunction of existential quantifications. Our argument is greatly simplified by the fact that $\mathbb{Z}$ is a module over a Principal Ideal Domain.

The special case of $\mathbb{Z}$ - continued

We try to eliminate a quantifier v from a formula

- $\exists vA$, where A is a conjunction of formulas of one of the two types $n_j v = w_j$, or $\neg n_l v = w_l$, where the n's are integers, and the w_j are linear functions over the integers with v not occurring in the w.

Now let d be the greatest common divisor of the n_j's (we are not using multiplication in the model!!) and write it as a linear combination over $\mathbb{Z}$ of the n_j's. This yields a condition

- $dv = w$ where w is the induced linear combination of the w_j, and in addition linear conditions on w and the w_j.

The special case of $\mathbb{Z}$ - continued

So far we have a necessary condition for the existence of a solution v. If $d = 1$ the solution if it exists is unique, and we get a nec. and suff. condition on the w_j and w_l. So let us assume d is positive. But now we need to work in $\mathbb{Z}/d\mathbb{Z}$, which is represented by $0, 1, \ldots, d-1$. Now we disjunctify the congruence conditions modulo $d\mathbb{Z}$ for the w_j (e.g. consider all combinations $w_j - r \in d\mathbb{Z}$ for r an element of $0, 1, \ldots, d-1$). This will automatically yield the class modulo d of any linear combination of the w_j's. Now our necessary condition translates to a set of condition on the w_j modulo d. If they are not satisfies then our original problem has no solution v in $\mathbb{Z}$. But if they are satisfied, we know that there is a v satisfying the positive conditions, but we are still left with some negative conditions, namely inequalities relating v to the n_l and w_l.

The special case of $\mathbb{Z}$ - continued

However, note that v if it exists is unique, since $\mathbb{Z}$ is torsion-free. It can be written as $d^{-1}w$, and then we just check, by clearing denominators, if v satisfies each negative condition. So v gets eliminated in favour of a conjunction of positive congruence conditions on the w, linear equations between the w and linear inequations between the w. The argument is constructive and and shows that every set is defined by a positive Boolean combination of congruence conditions, linear equations and linear inequations. Thus they are nearly Boolean combinations of cosets.

Three ways to improve this

One way is to add expressive power to the group $\mathbb{Z}$, say by adding a symbol for the usual order relation. Another is to try to extend the above procedure to all abelian groups, uniformly. Yet another is to consider modules over more complicated rings (now the formalism to use is not so clear). All three have resulted in success, respectively due to

- Presburger
- Wanda Szmielew in the 1950's
- Walter Baur and Leonard Monk in the 1970's

We discuss each briefly.

The case of adding the order to the group $\mathbb{Z}$ is hardly more difficult than what we have just sketched. The ordered group $\mathbb{Z}$ has 1 as its least positive element, and of course as far as the group analysis is concerned we already understand definable sets. The reader will hardly be surprised to learn that adding $<$ does not greatly extend the stock of definable sets. All we need add to the above mix, are conditions saying that some linear polynomial is greater than 0. We still have a quantifier elimination, constructively. Note that $<$ is not definable in the group formalism, since there is an automorphism of order 2 of the group $\mathbb{Z}$.

Exercise. Show that multiplication is not definable from $+$ and $<$, assuming the result just stated.
(Hint: Consider rate of growth of definable functions. In this case the formalism is not important).

What Wanda Szmielew did for general Abelian Groups

She worked with abelian groups G with $+$ and $-$ and 0 in signature, and (essentially) looked for uniformity in definability as G varied. Actually her primary purpose was to show that the first-order theory of abelian groups is decidable, that is that there is an algorithm for deciding, given a sentence ϕ whether it holds in <u>all</u> abelian groups. In succeeding, she obtained one of the most comprehensive decidability results ever. The proof uses heavily that we are dealing with modules over a PID, which allows us, by nontrivial modifications of Presburger's method, to get quantifier-elimination down to Boolean combinations of rather simple positive primitive formulas. The crucial groups are

- nG
- $[n]G$, the group of n-torsion elements

Wanda Szmielew - continued

The crucial pp-formulas correspond to coset conditions on these. Note that unlike the case of $\mathbb{Z}$ one does not have explicit coset representatives defined from the constant 1. There are no extra constants in Szmielew's formalism. Instead there are various auxiliary sentences involved, of the following type. You have your basic subgroups listed above,and you may form finite intersections of them to get more definable groups. The sentences have to say that the index of one such group in another is at least k for various k, and from those, Booleanly, you can say that index is exactly k. For example, you can say that the index of $6G$ in $3G$ is 1, or 2, or 4, etc. (Exercise give examples). Then Szmielew proved, effectively, that each definable relation is a Boolean combination of such sentences and formulas built from linear functions and formulas defining the basic groups.

Wanda Szmielew - continued

This enables her to give the fundamental Szmielew invariants for elementary equivalence of abelian groups. Basically, these invariants capture

- The index of $(p^{n+1}G)[p]$ in $(p^nG)[p]$, as being at least m for varying p, n, m. Since the groups here are vector spaces over $\mathbb{F}_p$, we write this in terms of dimension.
- The p-dimension of $(p^nG)[p]$ as being at least k
- Similar things for $p^{n+1}G$ in p^nG
- The cardinal of p^nG is at least k.

For more detail see Hodges-Model Theory, or Prest-Model Theory of Modules.

The case of modules

This was completed by Baur and Monk in the early 1970's, and is much more complicated. Once again one works with abelian groups G , but fixes a ring R (not necessarliy commutative) acting unitally to make G an R-module. We have no quantification over R. What we have is the language of abelian groups, enriched by constants r for each r in R.These are to be interpreted as operators on G, and we write rg for the action of r on g. There are natural axioms for R-modules, giving the composition rules for the various operators. This does not involve any quantification over the ring R. For each R we have the class of R-modules. Overcoming major difficulties, Baur and Monk gave a natural generalization of Szmielew's work, in terms of a pp-elimination, for arbitrary R. Thus one has strong limitations on the definable sets, for fixed R. But one has no decidability result, as Baur showed that the theory of R modules can be undefinable even for certain finite commutative rings (by coding the word problem for groups therein).

Ordered Abelian Groups

Here the definitive result is due to Yuri Gurevich, in 1964. The objective is to generalize Presburger. He proves the decidability of the class, and gives a kind of elimination. But this is not very explicit. However, it provides a nice family of examples in more advanced definability theory.

Groups nilpotent of class 2

Now we work with groups G with the group operation in multiplicative version. We can add a constant 1 for the unit element. There are some possibilities for confusion, since we may occasionally write infinite cyclic subgroups additively. We now study definability (for the signature just mentioned) in groups nilpotent of class 2. These are the groups G with $G/Z(G)$ abelian and the class is easily axiomatized in a first-order way by saying that all commutators are in the centre. It turns out that from a logical point of view these nilpotent groups are much more complex than abelian groups (or modules). The fundamental work was done by Anatoli Malcev in the 1950's. Nowadays we know a metatheorem saying that any model-theoretic pathology can be manifested in the class of nilpotent groups of class 2. Though Malcev, and Yuri Ersov, laid the foundations, a definitive treatment was spelled out by Alan Mekler

Two noncommutative examples, one nilpotent, the other not, one well-behaved, the other not

I will discuss in some detail two examples, the infinite dihedral group and the Heisenberg group. The first is well-behaved in terms of definability, the second is not.The second is nilpotent of class 2, the first is solvable, but not nilpotent.

The infinite dihedral group

This group G can be presented on two generators r and s, with the relations

- $s^2 = 1$
- $s^{-1}rs = r^{-1}$.

Clearly r generates a normal cyclic subgroup of infinite order, and s acts on this as the inverse map. Every element of G has a unique representation as a product ab, where a is in the cyclic group $< r >$ and b is in the cyclic group $< s >$. G is solvable, but not nilpotent, as it has trivial centre. It looks as if G can be "interpreted " in the Presburger group already analyzed. Let us work in the Presburger model M with the signature used earlier, but now replacing the confusing use of 1 by use of another constant, c still to be interpreted as the integer 1. An isomorphic copy of G can be defined in M^2, on the Presburger-definable set of pairs (x, y) such that either $y = 0$ or $y = c$.

We define a multiplication on this set by mimicking the action of s on the normal subgroup $< r >$

- $(x, y) \circ (u, v) = (x + u, 0)$ if $y = v = 0$
- $(x, y) \circ (u, v) = (x - u, c)$ if $y = c$ *and* $v = 0$
- $(x, y) \circ (u, v) = (x - u, 0)$ if $y = v = c$
- $(x, y) \circ (u, v) = (x + u, c)$ if $y = 0$ *and* $v = c$

Obviously this group is isomorphic to G. Thus one easily shows that any definable relation in G are replicated in the abelian group $\mathbb{Z}$ and thus is not complicated. I do not attempt to make this more explicit. I suggest that the interested reader makes a direct attack on quantifier elimination in G using the fact that G has a single element of order 2 which acts on the centre by inverse. In this way you get a more internal grasp on definability.

Further Exercise Show that no nontrivial ring structure can be defined on the centre of G, using its multiplication as addition.

A related well-behaved example

This time modify the presentation by not requiring s to have order 2. Now we have a semidirect product, and the group is torsion free. Now the group generated by the two elements r and s^2 is normal, and abelian, and is no longer elementarily equivalent to Presburger (exercise), but very well understood by Szmielew. Moreover, $< r, s^2 >$ is of index 2 in the group G.

Exercise Repeat the analysis from the last subsection.

The Heisenberg Group (s)

We now consider the group H of strictly upper triangular 3x3 matrices over the ring $\mathbb{Z}$. The elements are the matrices of the form

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$$

with the usual matrix multiplication. I follow a concise lucid account of the logic from Borovik-Nesin ”Groups of Finite Morley Rank” (page 37 ff). Thus one defines three maps α, β and γ from $\mathbb{Z}$ to H.

- $$\alpha(n) = \begin{pmatrix} 1 & n & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

- $$\beta(n) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & n \\ 0 & 0 & 1 \end{pmatrix}$$

- $$\gamma(n) = \begin{pmatrix} 1 & 0 & n \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Let A, B, C be respectively the images of α, β, γ

- A, B, C are subgroups of H respectively isomorphic to the additive group $\mathbb{Z}$ under α, β, γ.
- $H = ABC$
- $[\alpha(m), \beta(n)] = \gamma(mn)$, where mn is the product of m and n in the ring $\mathbb{Z}$
- $C = Z(G) =$ the derived group G''
- AC and BC are normal abelian subgroups of G
- Let a, b, c be respectively $\alpha(1), \beta(1), \gamma(1)$. Then AC is the centralizer of a and BC is the centralizer of b

Let us extend the group signature by two constants to stand for a and b respectively. We just write the constants as a and b.
Exercise. There is an automorphism of H sending the group element a to the group element b, so neither a nor b is definable in the group signature.

This is why we extend the signature. Note that by the centralizer result above AC and BC are now definable. C is of course definable in the original signature, as the centre. Now one can define a map from the cartesian product $AC \times BC$ to $Z(H)$ by sending a pair (x, y) to the commutator $[x, y]$. It is easy to show that $\gamma(n)$ is the commutator of $\alpha(n)$ and b, and also the commutator of a and $\beta(n)$, so the map is surjective to C. But now we can put a ring structure on C by taking as $+$ the multiplication on C, and then defining a multiplication on C as follows. Pick elements u and v in C. Select g in AC so that $u = [g, b]$ and pick h in BC so that $v = [a, h]$. Then it turns out that $[g, h]$ is independent of choices of g and h, and we define this to be the product of u and v. I remind you of $[\alpha(m), \beta(n)] = \gamma(mn)$, where mn is the product of m and n in the ring $\mathbb{Z}$.

Definitions in Arithmetic

In contrast to the case of $+$ on $\mathbb{Z}$ (and also the case of multiplication on $\mathbb{Z}$, done by Skolem) the integers as a ring, with signature $+, \cdot$ has an essentially unintelligible theory of first-order definitions. This is a result of Kleene, in the wake of the work of Gödel, Church and Turing. Not only can one define sets which code the action of universal Turing machines, but one gets more and more definable sets by increasing alternations of $\exists$ and $\forall$ in definitions (arithmetical hierarchy). By the preceding, all this complexity can be simulated in the Heisenberg group using only the group operation! Ershov showed that a similar situation holds in other finitely generated nilpotent group of class 2 not finitely generated over its centre.

Other Natural Rings and their Definable Relations

There are however important rings with an intelligible definability theory (and some kind of quantifier elimination). The most fundamental examples are the field of complex numbers (or, more, generally, algebraically closed fields), the real field (or, more generally, real closed fields) and finite extensions of p-adic fields (and, more generally, various Henselian fields). The basic results are due to Tarski, Ax-Kochen-Ershov, and, for the finer detail of the p-adics, A.J.Macintyre. The latter was brilliantly exploited by Jan Denef in the theory of p-adic Poincare series, and, ultimately by him and Francois Loeser in motivic integration. Numerous applications of logic to geometry depend on the definability theory for the above fields. However, some basic fields have unintelligible definabilty theory. The most basic is the field of rationals, where, rather startlingly, one can define the ring of integers (Julia Robinson, with much later refinements by Poonen and Koenigsmann).

Heisenberg groups over fields

One may simply replace $\mathbb{Z}$ in the definition of the Heisenberg group by another ring, and in particular by a field K. How do the groups behave, vis-a-vis definability, as K varies? Let us stick to K of characteristic 0. One may readily check that most of the analysis taken from Borovik-Nesin goes through. We write H for the Heisenberg group over K, bearing in mind that K is hidden in it. Firstly, the maps α, β, γ still make sense, and we define a, b, c as before, as do A, B, C. B is the centre of H, but no longer cyclic. Rather it is a K-vector space of dimension 1. Similarly AC and BC are the centralizers of a and b respectively, C is the set of commutators, and H/C is abelian, no longer a product of two cyclic groups, but rather a K-space of dimension 2.

Heisenberg groups over fields - continued

It turns out (please check as an **Exercise**) that the definition given for $\mathbb{Z}$ works in the present case also, giving C a ring structure with addition its old multiplication, and the multiplication as defined via commutators.
Moreover, the ring is isomorphic to K, via the map γ. Thus any definition in the field K can be simulated in H, so the definability theory is at least as complicated as that of K. But conversely, H is obviously definable in K. So, bearing in mind the results of Tarski et al., the definability theory of H is very well-understood for the classical cases.

Heisenberg groups over fields - continued

It is possible to get by without using constants for a, b, c, but at the cost of defining a family of multiplications. (Exercise)

For other matrix groups, not necessarily nilpotent, there are analogous complexity results, to be found in Malcev's Collected Papers. However, some major problems remain. If $G = SL_2(\mathbb{Z})$ then it is widely believed that there is an almost intelligible definability theory, based on exceedingly deep ideas of Zlil Sela. He has told me that he expects it all to work out, along the lines of his famous work on free groups, but as far as I know no details have yet appeared.

Groups with noninteger exponents

One can readily show that in the original Heisenberg group every element has a unique representation in the form $a^k b^l c^m$, for k, l, m in $\mathbb{Z}$. Show that over a field K as above there is a similar representation where now the exponents come from K.

More on ordering

For G the Heisenberg group over $\mathbb{Z}$, the centre is left orderable, and so is $G/Z(G)$ which is the direct sum of two copies of $\mathbb{Z}$. Both of these are orderable, and a general theorem then tells us that G is left orderable. Now in the ring $\mathbb{Z}$ the natural order is algebraically definable by Lagrange's Theorem (being nonnegative is the same as being a sum of four squares). Can we define in the Heisenberg group a left ordering? Yes, if we allow a and b as constants. Obviously, we can on $Z(G)$ by the preceding analysis, and then it turns out that we can internally define α, β, γ and thereby define a left-order on $G/Z(G)$, and then on G by a standard method.

Automorphisms and Orderings

Let M be some infinite structure, for a countable signature. By Löwenheim Skolem there will be many structures M_1 elementarily equivalent to M but not isomorphic. Is there one with an automorphism? Note that M itself may not have a nontrivial automorphism. For example, with the ring signature the real field has no nontrivial automorphism, because the order is algebraically definable (the nonnegative elements are the squares). However, it is virtually general set-theoretic nonsense that any M as above has an elementarily equivalent M_1 with lots of automorphisms (use the compactness theorem). The proof is however not informative about the nature of $Aut(M_1)$ qua group. For example, for M the real field no $Aut(M_1)$ has an element of order 2, since the order is algebraically definable, and no order has an automorphism of order 2.

Gradually one posed the question:

What are the groups G that act faithfully on some structure elementarily equivalent to M, for an arbitrary infinite structure? Conceivably the answer might have turned out to be that the trivial group was the only possibility. Fantastically, this is not the answer!! The answer came in the mid-fifties from Andrzej Ehrenfeucht and Andrzej Mostowski in a brilliant paper that changed model theory utterly and led to some very deep general theorems about notions of dimension and dependence in model theory. The authors knew, because of the case when M has a definable order, that any solution G must be torsion-free. Moreover, G must act on various infinite linear orders (and then it known, perhaps not to the authors, that G must be left orderable).

Models "generated" by a linearly ordered set

This has no clear meaning, though in group theory one could imagine having a set with a set S with a linear order and generating some group from S in such a way that any order isomorphism of S extends to an automorphism of the group. But in general one needs to get more than just a group, but rather a group elementarily equivalent to some group given in advance. Ehrenfeucht and Mostowski use a classic trick of "Skolemizing" which essentially extends the signature by adding choice functions to instantiate all existential quantifiers. There is no natural way to do this, but it is always possible.

For example, you might add to group theory a square root function that selects a square root if one exists. The basic methodology is to convert a structure axiomatized using quantifiers into another which is more like a classical algebraic system where you get substructures by closing under "algebraic" operations. Now you work in this extended language and look for an M_1 elementarily equivalent to M in the extended language, and on which G acts faithfully. Well, you pick any infinite linear order Λ on which G acts faithfully, and add to your language constants for the elements of the linear order, together with "indiscernibility" statements basically saying that any two tuples of constants corresponding to elements of Λ arranged in the same order satisfy the same formulas. You prove, by Ramsey's Theorem, used then for the first time in model theory, that there is a model M_2 of these axioms in the extended language. Skolemization guarantees that the substructure M_2 generated by the constants is elementarily equivalent to your original M and the action of G on the order extends to a faithful action on M_2. Done!

Universal Groups

Thus a group G acts on some model elementarily equivalent to any given infinite M (no matter the signature!!) if and only if G acts on an infinite linear order.This is in turn equivalent to G being left orderable! In particular, the Heisenberg group acts universally in this way.
For a bit more detail on this, see Rabin's article in Model Theory, Berkeley 1963, North Holland (including reference to the original E-M paper)

Stability and Indiscernibles

An infinite M is called stable, whenever in any M_1 elementarily equivalent to M any set of order-indiscernibles (as in sketch above) is actually a set of indiscernibles, i.e the obvious symmetric group action on the indiscernibles preserves satisfaction.
Separably closed fields are stable, and it is conjectured there are no other stable fields. The reals and the p-adics are unstable.