Geometry and first-order logic in groups

Chloe Perin

September 26, 2016

Minicourse for the Second israeli workshop for women in mathematics, Jerusalem, 25-29 September 2016.

Main results proved in this course:

1. Free groups are linear
2. Prove that an infinite system of equations in the free group is equivalent to a finite subsystem
3. Free groups have the Hopf property
4. Describe fg groups that are universally equivalent to the free groups.

1 Free groups and group presentations

1.1 Words and relations

Let S be a set of symbols. To each $s \in S$, we associate a formal inverse, that is, an extra symbol s^{-1}. The set of inverses is denoted S^{-1}

Definition 1.1: *A word w in S is a finite (possibly empty) sequence of the form $s_1 \dots s_n$ where each s_i is an element of $S \cup S^{-1}$. We say a word is reduced if no subsequence of the form ss^{-1} or $s^{-1}s$ appears. We sometimes write $w(S)$.*

Example 1.2: $S = \{a, b\}$. Then $S^{-1} = \{a^{-1}, b^{-1}\}$. The word $w = w(a, b) = aba^{-1}bb$ is reduced, the word $v = v(a, b) = abb^{-1}aa$ isn't. Their formal inverses are $b^{-1}b^{-1}ab^{-1}a$ and $a^{-1}a^{-1}bb^{-1}a^{-1}$ respectively.

Let now G be a group and S be a subset of G.

Definition 1.3: *Let $w = s_1 \dots s_n$ be a word in S. The element g of G represented by w is the product $s_1 \cdot \dots \cdot s_n$ where $\cdot$ denotes the group operation and s^{-1} is taken to be the group inverse of S. By convention the empty word represents the trivial element. We write $w =_G g$.*

Example 1.4: Let $S = \{a, b\}$, and $w = ab$.

- Let $G = (S_4, \circ)$ be the group of permutations on 4 elements. Let $a = (12)$ and $b = (23)$: then $w =_{S_4} (12)(23) = (132)$. If we take $w = aba^{-1}$, then $w =_{S_4} (12)(23)(12) = (13)$
- Let $G = (\mathbb{Z}^2, +)$. Let $a = (1, 0)$ and $b = (0, 1)$. Then $w =_G (1, 0) + (0, 1) = (1, 1)$. Note that the word $v = ba$ also represents the element $(1, 1)$ - and both w, v are reduced.

Thus several distinct words may represent the same element (for example ss^{-1} and $s^{-1}s$ always both represent the trivial element). It is important to keep in mind the distinction between "words" (abstract sequences of symbols) and "elements" (which belong to the group).

Definition 1.5: *Say S generates G if any element of G is represented by a word in S - i.e., if any element is a product of elements in S and their inverses. Say G is finitely generated if it admits a finite subset S which generates it.*

Example 1.6:

- $\{1\}$ generates $(\mathbb{Z}, +)$, but also $\{2, 3\}$.
- $S = \{$ elementary matrices $\}$ generates $GL_n(\mathbb{R})$ (recall - elementary matrix has either 1's on diagonal, and one non zero entry somewhere, or is diagonal with all entries equal to 1 except one, and multiplying by an elementary matrix on the right corresponds to performing an elementary operation on the columns of the matrix).
- Transpositions generate the symmetric group S_n

1.2 Free groups

Definition 1.7: *A relation between the elements of S is a nonempty **reduced** word which represents the trivial element. If S generates G, and there are no relations between the elements of S, the group G is said to be free on S.*

Lemma 1.8: *If G is free on S, there is exactly one reduced word representing each element.*

Proof. On an example: suppose $w_1 = ab^{-1}aa$ and $w_2 = ba$ are distinct reduced words which represent the same group element, i.e. $ab^{-1}aa =_G ba$, we get $(ab^{-1}aa)(a^{-1}b^{-1}) = ab^{-1}ab^{-1} = 1$. The reduction stops before the word is empty because w_1 and w_2 are distinct - thus we get a nontrivial reduced word representing the identity - a contradiction. □

Thus if G is free on S, we can think of each element as a reduced word in S.

Building free groups. In fact, this gives us a way to build free groups: given a set of symbols S, we define a group $F(S)$ whose elements are reduced words in S, and whose product operation is that of concatenation-reduction (i.e. to compute the product of two reduced words, write the words one after the other, and reduce if needed until you get a reduced word). We call $F(S)$ **the free group on** S. (Warning - there are some things to check to see that this is indeed a group, for example, associativity is not obvious).

Example 1.9: Free group on $\{a, b\}$: reduced words on a, b e.g. $aaba^{-1}, abbbab$, product: $aab^{-1}a^{-1} \cdot abbbab = aabbab$.

Remark 1.10: *Consider the free goup on $\{a, b\}$: it is free on a, b i.e. there are no relations between a and b, but this does not mean that there are no relations between the elements of the group at all! Ex: set $x = ab$, $y = b^{-1}a^{-1}$, then $xy = 1$.*

The following lemma is key. It says that it is very easy to define group morphisms with source G.

Lemma 1.11: *Given any group H and a choice of images $\{h_s \mid s \in S\}$ for the elements of S, there is a unique group morphism $G \to H$ sending each s to h_s.*

Idea: send the reduced word $s_1^{\epsilon_1} \dots s_k^{\epsilon_k}$ (which is an element in G) on the product $h_{s_1}^{\epsilon_1} \dots h_{s_k}^{\epsilon_k}$ in H.

In fact, this universal property can be used as a definition of what it means for a group G to be free on S:

Proposition 1.12: *G is free on S iff for any group H and any choice $\{h_s \mid s \in S\}$ of images for the elements of H, there exists a unique morphism $h : G \to H$ such that $h(s) = h_s$ for every $s \in S$.*

Proof. If G has the universal property can build a morphism $f : G \to F(S)$ sending s to s. On the other hand $F(S)$ has the universal property as well, so there is a natural morphism $h : F(S) \to G$. The composition $h \circ f$ fixes the elements of S, so it must be the identity. Thus f is an isomorphism, in particular G is free on S. □

Exercise 1: *Show that the free group on $\{a, b\}$ is also free on $\{ab, b\}$.*

Hence a group can be free on several different sets of elements! However, we can show that any two such sets must have the same cardinality.

Exercise 2: *If S and S' have distinct cardinalities (say finite), the free groups on S and S' respectively are not isomorphic.*

Remark 1.13: *In particular, if G is free on S and also on T, we have $|S| = |T|$.*

Definition 1.14: *If G is free on S we call S a **basis** for G, and $|S|$ the rank of G.*

Note that the free group of rank 1 is just $\mathbb{Z}$. It is the only (nontrivial) one which is abelian.

1.3 Group presentations

In general however if we take a generating set for a group G, there will be relations between the elements of S. One can in fact build G by taking the free group on S and "adding" the relations the elements of S satisfy in G. Let us now see how to make this formal.

The following is a corollary of Lemma 1.11:

Corollary 1.15: *Any group is the quotient of a free group.*

Proof. Let G be a group with generating set S. We build an abstract set $\hat{S} = \{\hat{s} \mid s \in S\}$, and the free group $F(\hat{S})$ on $\hat{S}$. We let π be the morphism $F(\hat{S}) \to G$ defined by sending each $\hat{s}$ to the corresponding s. It exists by Lemma above, and is surjective because S generates. □

We will now drop the hat, and think of this morphism as $\pi : F(S) \to G$.

Remark 1.16: *Note that if the reduced word $w(S)$ is a relation between the elements of S (in G), then the element $w(S)$ of $F(S)$ is sent to 1 by the morphism π, i.e. relations are in the kernel. Conversely, it is easy to see that any element of the kernel is a relation.*

In particular G is free on S iff $\mathrm{Ker}\pi$ *is trivial, that is iff π is an isomorphism.*

Example 1.17: Let $G = \mathbb{Z}/3\mathbb{Z}$ be the cyclic group of order 3. Let a be a generator, $S = \{a\}$. We have relations: $aaa = 1$, $a^6 = 1$, etc. Note that the second relation is a consequence of the first one, so really we don't need to specify it. (Do it also in additive notation?)

- Exercise 4.1, 4.2: inverses, products of relations and conjugates of relations are consequences of the relations. Hence also products of conjugates of relations.

Exercise 3: *Let G be a group, S a generating set. Let u, v be relations between the elements of S (they are reduced words, so we think of them as elements of $F(S)$), and let w be a reduced word*

1. *Show that uv (the product of u and v in $F(S)$) is a relation.*
2. *Show that wuw^{-1} is a relation.*
3. *Deduce that if $r_1, \ldots, r_n$ are relations, any element of the form $\Pi_{i=1}^k u_i(S) r_i^{\pm 1} u_i^{-1}(S)$ for some $k \in \mathbb{N}, u_i \in G$ is a relation.*

Exercise 4: *Let G be a group, and let A be a subset of G. Show that the set*

$$\{\Pi_{i=1}^k u_i(S) a_i^{\pm 1} u_i^{-1}(S) \mid k \in \mathbb{N}, a_i \in A, u_i \in G\}$$

is a normal subgroup of G, and that it is in fact the smallest normal subgroup of G which contains A. We denote it $\langle\langle A \rangle\rangle$.

The idea of a presentation of a group G with generating set S is that we want to find a set of relations R such that all the other relations are consequences of the relations in R.

Definition 1.18: *(Let S generate G, and $\pi : F(S) \to G$). Let R be a subset of $F(S)$ such that* $\mathrm{Ker}\pi = \langle\langle R \rangle\rangle$*, that is* $\mathrm{Ker}\pi$ *is the smallest normal subgroup of $F(S)$ containing R. Then we say G admits the presentation $\langle S \mid R \rangle$.*

By the first isomorphism theorem, we get that $G \simeq F(S)/\mathrm{Ker}\pi = F(S)/\langle\langle R \rangle\rangle$.

In other words, G admits the presentation $G = \langle S \mid R \rangle$ if

1. the elements in R are relations between the elements of S;
2. any relation between the elements of S is a consequence of the relations in R, i.e., belongs to $\langle\langle R\rangle\rangle$.

Example 1.19:
- $\langle a, b \mid\rangle$ is a presentation of $F(a, b)$;
- $\langle a \mid a^7\rangle$ is a presentation of $\mathbb{Z}/7\mathbb{Z}$
- $\langle a, b \mid aba^{-1}b^{-1}\rangle$ is a presentation of $\mathbb{Z}^2$.

We sometimes write $\langle a, b \mid ab = ba\rangle$ instead, the meaning is the obvious one.

Building a group with presentation $\langle S \mid R\rangle$ We can also choose a set of reduced word R in $F(S)$ and build a group which admits the presentation $G = \langle S \mid R\rangle$ simply by setting $G = F(S)/\langle\langle R\rangle\rangle$.

To build a morphism with source the group $\langle S \mid R\rangle$, it is enough to choose images for the generators which satisfy the relations given by R.

Proposition 1.20: *Let $G = \langle S \mid R\rangle$, and let H be any group. For any choice of elements $\{h_s \mid s \in S\}$, there is a morphism $G \to H$ sending s to h_s for each $s \in S$ iff the elements h_s satisfy the relations in R, that is, for any reduced word $s_1 \dots s_r$ in R we have $h_{s_1} \dots h_{s_r} =_H 1$.*

Example 1.21:
- $G = \langle a \mid a^7\rangle$ - to define a morphism need to find an order 7 element in H.
- $G = \langle a, b \mid aba^{-1}b^{-1}\rangle$ - to define a morphism $G \to H$ need to find two commuting elements in H.

1.4 Subgroups of free groups

Let us now consider subgroups of free groups. First example: the free group on $\{a, b, c\}$ contains the free group on $\{a, b\}$ as a subgroup. This type of examples shows that if $k \leq l$ then $\mathbb{F}_k$ embeds in $\mathbb{F}_l$.

But in fact, free groups of any rank embed in $\mathbb{F}_2$.

Exercise 5: *Consider the subgroup H of $\mathbb{F}(a, b)$ generated by $S = \{h_n = b^n ab^{-n}, n \in \mathbb{N}\}$, and show it is free on S.*

In fact we have

Theorem 1.22: *Any subgroup of a free group is free.*

2 Equations over groups

2.1 Equations over fields

Over a field K we are used to think about polynomial equations, that is, equation of the form $P(X) = 0$ where P is a polynomial with coefficients in K - i.e. an element of $K[X]$. More generally, equation with several variables: $P(X_1, \dots, X_n) = 0$ with $P \in K[X_1, \dots, X_n]$. One can also consider systems of equations, that is, sets of (possibly infinityely many) polynomial equations.

Example 2.1: $X^2 - 2X - 5 = 0$, $X_1^3 + 3X_1X_2 + X_2^2 - 7 = 0$

(we will sometimes abuse notation and identify the polynomial P and the equation $P(X) = 0$)

Definition 2.2: *A tuple $(u_1, \dots, u_n) \in K^n$ is a solution of the equation $P(X_1, \dots, X_n) = 0$ if we have $P(u_1, \dots, u_n) = 0$.*

The set of solutions to a system Σ of equations on n variables is a subset of K^n, we call such subsets "varieties".

Remark 2.3: *Equations have "consequences" - if $(u_1, \dots, u_n)$ is a solution of $P(X_1, \dots, X_n) = 0$, it is a solution of $Q = 0$ for every polynomial Q in the ideal (P) generated by P. Similarly a solution to the system Σ also satisfies $Q = 0$ for every Q in the ideal generated by the polynomials corresponding to the equations in Σ.*

Exercise 6: *Check this.*

Recall: an ideal is a subset $I \subseteq K[X_1, \ldots, X_n]$ which is stable by 1. addition (if $P_1, P_2 \in I$ then $(P_1+P_2) \in I$) and 2. multiplication by any polynomial (if $P \in I$ and $Q \in K[X_1, \ldots, X_n]$ then $PQ \in I$).

The ideal generated by a set $A \subseteq K[X_1, \ldots, X_n]$ is the smallest ideal containing A, it can be shown to be exactly the set

$$\{Q_1P_1 + \ldots + Q_rP_r \mid r \in \mathbb{N}, P_i \in A \text{ and } Q_i \in K[X_1, \ldots, X_n] \text{ for } i = 1, \ldots, r\}$$

2.2 Equations over groups

Let G be a group.

Definition 2.4: *An equation over G is an expression of the form $w(x_1, \ldots, x_n) = 1$, where w is a word in the variables $x_1, \ldots, x_n$ and their inverses. We can also allow the use of constants from G, to get equations with constants $w(x_1, \ldots, x_n, a_1, \ldots, a_k) = 1$. Can also define systems of equations.*

A tuple $(u_1, \ldots, u_n)$ of G^n is a solution to the equation $w(x_1, \ldots, x_n, a_1, \ldots, a_k) = 1$ if the element represented by the word $w(u_1, \ldots, u_n, a_1, \ldots, a_k)$ is trivial in G.

Example 2.5: $x^7 = 1$, $x^2 = a$, $xax^{-1}a^{-1} = 1$, $xay^2b = 1$, ...

An alternative point of view: let Σ be a system of equations in n variables over the group G (suppose at first without constants): that is,

$$\Sigma = \{w_1(x_1, \ldots, x_n) = 1, w_2(x_1, \ldots, x_n) = 1, \ldots\}$$

We build a group G_Σ defined by the presentation:

$$G_\Sigma = \langle x_1, \ldots, x_n \mid w_1(x_1, \ldots, x_n), w_2(x_1, \ldots, x_n), \ldots \rangle$$

Proposition 2.6: *There is a one to one correspondence between: solutions to the system Σ in G on the one hand and homomorphisms $G_\Sigma \to G$ on the other hand*

Proof. Given a solution $(u_1, \ldots, u_n)$ to Σ, there is a unique morphism $G_\Sigma \to G$ which sends x_i to u_i. Conversely, if $\theta : G_\Sigma \to G$ is a morphism, then the tuple $(\theta(x_1), \ldots, \theta(x_n))$ is a solution for Σ (see paragraph on group presentations). □

Remark 2.7: *Like for equations over fields, equations over groups have "consequences": if u is a solution to the equation $x^2 = 1$, it will also be a solution to $x^4 = 1$, if u is a solution to the equation $xax^{-1}a^{-1} = 1$, it will also be a solution to $xa^2x^{-1}a^{-2} = 1$.*

Exercise 7: *How could we characterize all the consequences of a set of equations - what is the analogue of the ideal I_Σ of $K[X_1, \ldots, X_n]$ in the field case? ANSWER (case where Σ is without constants) first need to think what the analogue of $K[X_1, \ldots, X_n]$ is: it's the free group on $x_1, \ldots, x_n$, and the set of consequences is the subgroup normally generated by the words corresponding to equations of Σ*

3 Equational noetherianity of the free group

Our aim now is to prove

Theorem 3.1: *If G is a free group, and Σ is a system of equations over G, there exists a finite subset Σ_0 of Σ such that Σ and Σ_0 are equivalent.*

(that is, any tuple $(u_1, \ldots, u_n) \in \mathbb{F}^n$ which is a solution to Σ_0 in fact satisfies all the equations of Σ)

Remark 3.2: *This is true of equations over fields: Recall that the ring of polynomials $K[X_1, \dots, X_n]$ is Noetherian, that is, there are no infinite ascending chains of ideals. In particular if Σ is an infinite set of polynomials $P_1(X_1, \dots, X_n), P_2(X_1, \dots, X_n), \dots$, if we define $I_j = (P_1, \dots, P_j)$ we have that for some m, the ideal I_m contains all of Σ. In particular all of the equations $P_j = 0$ for $j > m$ are "consequences" of the first m equations.*

This means precisely that the system of equations Σ is equivalent to the finite subsystem $P_1 = 0, \dots, P_m = 0$.

In fact, the proof in the free group cases precisely rests on the fact that this is true in $\mathbb{R}$. The other ingredient is linearity of the free group:

Proposition 3.3: *Let $\mathbb{F}$ be a finitely generated free group. Then $\mathbb{F}$ embeds in the group $\mathrm{SL}_2(\mathbb{R})$.*

Let us prove Theorem 3.1 using this

Proof. We think of $\mathbb{F}$ as a subgroup of $\mathrm{SL}_2(\mathbb{R})$, in particular, we think of its elements as 2-by-2 matrices - that is, as elements of $\mathbb{R}^4$. Each equation $w(x_1, \dots, x_k) = 1$ in Σ translates as 4 polynomial equations in the coefficients of the x_i's viewed as elements of $\mathbb{R}^4$. Denote by $\hat{\Sigma}$ the set of polynomial equations on the coefficients of the x_i's obtained in this way: by the previous remark, it is equivalent to a finite subsystem $\hat{\Sigma}_0$. This finite subsystem is induced by a finite subsystem Σ_0 of Σ, such that that any element of $\mathbb{R}^{4k}$ which satisfies Σ_0 also satisfies Σ. This is in particular true of elements of $\mathbb{F}$, which proves the claim. $\square$

We must now prove Proposition 3.3.

Proof. We will show that $\mathrm{SL}_2(\mathbb{Z})$ contains a free group of rank 2. Since the free group of rank 2 contains subgroups of arbitrarily large rank, any fg free group embeds in $\mathrm{SL}_2(\mathbb{Z})$.

Consider the subgroup F of $SL_2(\mathbb{Z})$ generated by the two matrices $\alpha = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ and $\beta = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$.

We will show it is free on $\{\alpha, \beta\}$. Note that for any $n \in \mathbb{Z}$ we have $\alpha^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}$ and $\beta^n = \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix}$

Consider the linear action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathbb{R}^2$. Let $U = \{(x, y) \mid |y| > |x|\}$, and $V = \{(x, y) \mid |y| < |x|\}$. Note that $\alpha^n(U) \subseteq V$ and $\beta^n(V) \subseteq U$ for any $n \in \mathbb{Z}$ with $n \neq 0$.

Let w be a non empty reduced word in α, β: assume first that w starts and ends by a power of α. Take $x \in U$: then $w \cdot x$ is in V, so it cannot be equal to x. Thus the element represented by w is not trivial.

Reduce to this case by conjugating w by an appropriate power of α. Show that the conjugate w' of w is non trivial, thus w itself is non-trivial. $\square$

4 Hopf property for the free group

From the linearity of the free group we will now deduce another property - the fact that it is Hopf.

We start by a very general remark: if A is a set, we can look at maps $A \to A$. If A is finite, a surjective map is necessarily also injective. In fact, this can be seen as a characterization of finiteness for sets (A is finite iff any surjective map $A \to A$ is also injective). Counterexample for infinite sets: e.g. $A = \mathbb{N}$, $f(0) = 0$ and $f(n) = n - 1$ for $n > 1$.

(Think: what is the analogue for vector spaces? finite dimension!)

For a group G, the natural analogue is to look at morphisms $f : G \to G$.

Definition 4.1: *We say G has the Hopf property if any surjective morphism $G \to G$ is also injective.*

Example: finite groups are Hopf (just look at f as a map between sets!). The group $(\mathbb{Z}/2\mathbb{Z})^{\mathbb{N}}$ is not Hopf - take f to be a left shift (forget the first coordinate).

Proposition 4.2: *Free groups are Hopfian.*

In fact, to prove this we will show first

Proposition 4.3: *Free groups are residually finite.*

Definition 4.4: *We say a group G is* ***residually finite*** *if for any non trivial element $g \in G$, there exists a morphism $h : G \to A$ where A is a finite group, such that $h(g) \neq 1$.*

Note that a subgroup of a residually finite group is residually finite.

Proof. We show $\mathrm{SL}_2(\mathbb{Z})$ is residually finite: let M be a matrix which is not the identity. Let n be larger than the absolute value of all the entries of the matrix. Consider the map $\pi_n : \mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$ which consists in taking the entries of a matrix modulo n: this is a group morphism to a finite group (check this!), and $\pi_n(M)$ is non trivial.

Since $\mathbb{F}$ can be thought of as a subgroup of $\mathrm{SL}_2(\mathbb{Z})$, it is itself residually finite. □

We now prove

Proposition 4.5: *Residually finite groups are Hopfian.*

Proof. Let G be a residually finite group. Suppose $f : G \to G$ is surjective but not injective. Let $g \in \mathrm{Ker} f$ with $g \neq 1$. By residual finiteness there is a morphism $h : G \to A$ with $h(g) \neq 1$. Consider the morphisms $h \circ f^k$, show they are all different (each one kills some element that the ones of lower power do not kill). This gives an infinite number of morphisms from a fg group to a finite group, a contradiction. □

We deduce from the Hopf property the following corollary

Corollary 4.6: *Suppose G is a free group of rank n. Any generating set S of G has size at least n. If S it consists of exactly n elements, then it is a basis of G.*

Proof. Suppose G is free on $a_1, \ldots, a_n$, and let $\{u_1, \ldots, u_m\}$ be another generating set for G. Let $\mathbb{F} = \mathbb{F}(s_1, \ldots, s_m)$ be the free group on $s_1, \ldots, s_m$.

We build a morphism $\tau \circ \sigma : \mathbb{F}(S) \to \mathbb{F}(S)$ as follows: first, let $\sigma : F(S) \to G$ send s_i to u_i, then let $\tau : \mathbb{F}(S) \to G$ send a_i to s_i for $i \leq m, n$ and a_i to 1 for $m < i \leq n$ (if such i's exist).

If $m \leq n$ then $\tau \circ \sigma$ is surjective, it is in fact an isomorphism by Hopf property. In particular we must have in fact $m = n$. Since there are no relations between the a_i's, there are no relations between the s_i's and G is free on S. □

We further deduce

Proposition 4.7: *Two elements g, h which do not commute in a free group do not satisfy any other non trivial relation.*

Proof. The subgroup H generated by g, h is free, since every subgroup of a free group is free. Now H has rank at most 2, since it is generated by 2 elements. If it were of rank 0 or 1 it would be abelian, but it contains noncommuting elements so it has rank 2. By the corollaery above, $\{g, h\}$ is a basis for H - thus there are no relations between h and g. □

5 First-order logic

The simplest example of a first order formula on groups is an equation. But we also allow:

- inequations;
- conjunction and disjunction of equations and inequations;
- using quantifiers on the variables.

Example 5.1: $\forall y \ \ xy = yx$ and $x \neq 1$

$\exists z \ \ z^2y^{-1} \neq 1$ or $z^3 = 1$

Important: the variables $x, y, \ldots$ always represent **elements of the group**. They cannot represent integers, or subsets of the group.

Example 5.2: The following are NOT first-order formulas:

- $\forall x \ \exists n \ x^n = 1$;
- $\exists n \ \exists x_1 \exists y_1 \ldots \exists x_n \exists y_n \ \ z = [x_1, y_1] \ldots [x_n, y_n]$;
- $\forall H \leq G \ (\forall x \ xHx^{-1} = H) \Rightarrow (H = 1$ or $H = G)$.

Remark 5.3: *It is not hard to see that every first-order formula is equivalent to a formula where all the quantifiers are at the beginning, that is, something of the form*

$$\Delta_1 x_1 \ \Delta_2 x_2 \ \ldots \Delta_r x_r \ AND_{i=1}^{m} \ OR_{j=1}^{n_i} \ w_{ij}(x_1, \ldots, x_r) \ = (\neq) \ 1 \ \ (*)$$

where for each k, $\Delta_k \in \{\forall, \exists\}$

Definition 5.4: *A first-order formula is said to be **universal** if it is equivalent to a formula of the form $(*)$ in which only $\forall$ quantifiers appears at the beginning.*

Consider the formula $\exists x \exists y \ z = [x, y]$. Its "truth value" on a group G depends on the value we assign to the variable z.

Definition 5.5: *A variable z that appears in a formula ϕ is said to be free in ϕ if neither $\forall z$ nor $\exists z$ appear before it. If a first-order formula ϕ has free variables $x_1, \ldots, x_n$, we will denote it $\phi(x_1, \ldots, x_n)$.*

A first order formula without free variables is also called a **sentence**.

Definition 5.6: *Given a group G and a sentence ϕ, we say G satisfies ϕ if ϕ is true on G. We then write $G \models \phi$.*

Example 5.7: $\phi: \ \forall x \ \forall y \ xyx^{-1}y^{-1} = 1$.
A group G satisfies ϕ iff it is abelian.

Let G be group. Some properties of G can be expressed by first-order sentences (e.g. abelianity), some others cannot.

Question: How much can we say about a group just with first-order sentences?

Definition 5.8: *The **first-order theory** of a group G is the set $\mathrm{Th}(G)$ of sentences satisfied by G.*

If $G_1 \simeq G_2$, then $\mathrm{Th}(G_1) = \mathrm{Th}(G_2)$. Conversely?

Exercise 8:

1. *If G_1 is finite, and $\mathrm{Th}(G_1) = \mathrm{Th}(G_2)$, show that $G_1 \simeq G_2$.*
2. *Show that $\mathrm{Th}(\mathbb{Z}) \neq \mathrm{Th}(\mathbb{Z}^2)$.*
3. *If G_1 finitely generated abelian and G_2 finitely generated, and $\mathrm{Th}(G_1) = \mathrm{Th}(G_2)$, show that $G_1 \simeq G_2$.*

6 The space of marked groups

The following is a way to "draw" groups:

Definition 6.1: *Let G be a group, let S be a finite generating set for G - we assume that $1 \notin S$. The Cayley graph $X(G, S)$ is the labelled graph given by*

- *vertex set G;*
- *edge set $\{\{g, gs\} \mid g \in G, s \in S\}$;*
- *label s on the edge $\{g, gs\}$.*

Example 6.2: Draw $X(\mathbb{Z}, \{1\})$, $\mathbb{Z}^2$, ...

Definition 6.3: *A marked group is a pair (G, S) where G is a group and $S = (s_1, \ldots, s_k)$ is an ordered generating set for G.*

Two marked groups $(G, (s_1, \ldots, s_k))$ and $(G', (s'_1, \ldots, s'_{k'}))$ are identified if $k = k'$ and the bijection $s_i \mapsto s'_i$ extends to an isomorphism.

The set of all (isomorphism classes of) marked groups (G, S) where S is a k-tuple is denoted $\mathcal{G}_k$.

Note that if G is a group and T, S are distinct generating sets, then (G, S) and (G, T) are not in general equal as marked groups.

Exercise 9: *Show that $(\mathbb{Z}, 1)$ ans $(\mathbb{Z}, -1)$ are isomorphic as marked groups (and thus identified in $\mathcal{G}_\infty$). Show that $(\mathbb{Z}, (2, 3))$ and $(\mathbb{Z}, (1, 3))$ are not.*

Here are two other ways to think about marked groups:

Remark 6.4:
- *a marked group is a group G together with an epimorphism $\pi : \mathbb{F}_k \to G$ (if $a_1, \ldots, a_k$ standard basis of $\mathbb{F}_k$, the marking S is given by $s_i = \pi(a_i)$).*
- *choosing a point in $\mathcal{G}_k$ corresponds exactly to choosing a normal subgroup in $\mathbb{F}_k$.*

We want to say that two marked groups are close if their generators satisfy the same relations of a given length:

Definition 6.5: *Let (G, S) and (G', S') be two points in $\mathcal{G}_k$. Let*

$$R((G,S),(G',S')) = \max\{n \mid \forall w \text{ reduced word on } k \text{ letters with } l(w) \leq n,\\ w(S) =_G 1 \iff w(S') =_{G'} 1\}$$

The space of marked groups is the set $\mathcal{G}_k$ endowed with the metric d defined by:

$$d((G,S),(G',S')) = 2^{-R((G,S),(G',S'))}$$

Exercise 10: *Check this is a metric*

So (G, S) and (G', S') are at least 2^{-r}-close, iff they satisfy exactly the same relations of length at most r.

Geometrically:

Exercise 11: *$R((G, S), (G', S')) \geq r$ iff the balls of radius $r/2$ of their Cayley graphs are isomorphic as labeled graphs (that is, there is a graph isomorphism between them which sends edges labeled s_i to edges labeled s'_i)*

Examples of convergent sequences:

Example 6.6:
- the sequence $(\mathbb{Z}/m, (1))$ converges to $(\mathbb{Z}, (1))$ as m tends to ∞.

  Indeed, $R((\mathbb{Z}/m, (1)), (\mathbb{Z}, (1))) \geq m - 1$ since in $(\mathbb{Z}/m, (1))$ there are no relations of length less than m;
- the sequence $(\mathbb{Z}, (1, 2m))$ converges to $\mathbb{Z}^2$ with the standard generating set as m tends to ∞.

  Indeed, $R((\mathbb{Z}, (1, 2m)), (\mathbb{Z}, (1))) \geq 2m$ (in $(\mathbb{Z}, (1, 2m))$ aside from the relations induced by commutation of the form $a^k b^j a^{-k} b^{-j}$, the shortest relation is $a^{2m} b$ which has length $2m + 1$).

By a similar argument it can be shown that $\mathbb{Z}^n$ can be obtained as a limit of some marking of $\mathbb{Z}$.

Proposition 6.7: *The set $\mathcal{A} = \{(G, S) \in \mathcal{G}_k \mid G \text{ is abelian } \}$ is both open and closed.*

Proof. Let $(G, S) \in \mathcal{A}$. Then any group (G', S') at distance less than 2^{-4} is abelian, indeed then for all i, j we have $s'_i s'_j (s'_i)^{-1}(s'_j)^{-1} = 1$.

Suppose that $(G_n, S_n) \to (G, S)$ and G_n abelian for all n. For n large enough $d((G_n, S_n), (G, S)) < 2^{-4}$ so (G, S) satisfies the same relations of length 4 as (G_n, S_n) so (G, S) is abelian. □

In a similar way we can show:

Proposition 6.8: *Let ϕ be a universal formula in the language of groups. The set $\mathcal{U}_\phi = \{(G, S) \in \mathcal{G}_k \mid G \models \phi\}$ is closed.*

Proof. Suppose that $(G_n, S_n) \to (G, S)$. Suppose $G \not\models \phi$: we can find witnesses $g_1, \dots g_p \in G$ such that none of the conjunctions $\bigwedge_{j=1}^{M} w_{i,j}(g_1, \dots, g_p) = (\neq)1$ hold. The g_i can be seen as words $\tilde{g}_i(S)$ in S.

Let R be larger than the lengths of all the $w_{i,j}(\tilde{g}_1(S), \dots, \tilde{g}_p(S))$ seen as words in S.

For n large enough (G_n, S_n) and (G, S) satisfy exactly the same relations of length R, hence $\tilde{g}_1(S_n), \dots, \tilde{g}_p(S_n)$ in G_n witness the fact that $G_n \not\models \phi$. □

Remark 6.9: *In particular recover that $\mathcal{A}$ is closed since $\mathcal{A} = \mathcal{U}_\phi$ for $\phi : \forall x \forall y \; xy = yx$.*

But cannot extend the openness to the general case: in abelian case, you know that if a group fails to satisfy ϕ, can find "witnesses" of length 1, in general the length of these witnesses is arbitrary.

7 Limit groups

Definition 7.1: *We define $\mathcal{L}_k$ to be the closure in $\mathcal{G}_k$ of the set*

$$\mathcal{F} = \{(G, S) \mid G \text{ is free } \}$$

Caution! do not require of G to be free **on** S.

Definition 7.2: *We say that G is a limit group if there exists an integer k and a marking $S = (s_1, \dots, s_k)$ such that $(G, S) \in \mathcal{L}_k$.*

Exercise 12: *If G is a limit group, then for any marking S of G, there exists a sequence (G_n, S_n) converging to (G, S) with G_n free.*

Exercise 13: *Show that every finitely generated subgroup of a limit group is a limit group.*

Example 7.3:
- Free groups are limit groups;
- Free abelian groups are limit groups (limits of $\mathbb{Z}$).

First properties of limit groups:

Proposition 7.4:
- *Limit groups are torsion free;*
- *Limit groups are commutative transitive;*
- *Any two elements in a limit group which do not commute generate a free group of rank 2.*

Proof. By the proposition above, any universal formula satisfied by free groups is also satisfied by limit groups.

- Fix n. The following formula holds in any free group: $\forall x \; x = 1 \vee x^n \neq 1)$, thus it holds in all limit groups.
- All free groups satisfy $\forall x, y, z \{y \neq 1 \wedge [x, y] = 1 \wedge [y, z] = 1\} \to [x, z] = 1$, hence so does any limit group.

- True in free groups by Remark 4.7. Thus for any non empty reduced word w on two elements the formula $\phi_w : \forall x, y [x, y] \neq 1 \to w(x, y) \neq 1$ holds in $\mathbb{F}$, hence in any limit group. Thus if a, b are elements in a limit group which do not commute, no non trivial word on a, b represents the trivial element, hence a and b generate a free group of rank 2.

$\square$

Example 7.5: The group $\mathbb{F}_2 \times \mathbb{Z}$ is NOT a limit group, since it is not commutative transitive

Proposition 7.6: *Let G be a fg group. Then G is a non abelian limit group iff it has the same universal theory as $\mathbb{F}_2$.*

Remark 7.7: *All non abelian free groups have the same universal theory. Indeed, for any $k > 1$ we have that $\mathbb{F}_2 \leq \mathbb{F}_k$ so $\mathrm{Th}_\forall(F_k) \subseteq \mathrm{Th}_\forall(\mathbb{F}_2)$, and $\mathbb{F}_k$ embeds in $\mathbb{F}_2$ so the other inclusion also holds.*

Proof. Suppose G is a non abelian limit group: it contains two noncommuting elements, hence it contains a copy of $\mathbb{F}_2$, hence $\mathrm{Th}_\forall(G) \subseteq \mathrm{Th}_\forall(\mathbb{F}_2)$. On the other hand, if ϕ is a universal formula satisfied by all free groups, it will be satisfied by G since this is a closed property.

Suppose G is a fg group which has the same universal theory as $\mathbb{F}_2$. Let $S = (s_1, \ldots, s_k)$ be a finite generating set for G. For each N, write the following formula:

$$\phi_N : \exists x_1, \ldots, x_k \bigwedge_{w \in B_N(\mathbb{F}_k)} w(x_1, \ldots, x_k) = (\neq) 1$$

where we put $=$ if $w(s_1, \ldots, s_k) =_G 1$ and $\neq$ otherwise. This holds in G, hence it holds in $\mathbb{F}_2$ (if not, its negation, which is a universal formula, would hold in $\mathbb{F}_2$). Let $S(n) = (s_1(n), \ldots, s_k(n))$ be witnesses that this holds. It is easy to see that $(\mathbb{F}_2, S(n))$ converges to (G, S), so G is a limit group. $\square$