Math 551 – Algebra – Fall 2000

A. Groups

4. Free groups and presentations.

We detour to this important way of describing groups.

4a. Free groups

Definition. *Let S be a set. A word in S is a formal expression*

$$s_1^{\epsilon_1} * s_2^{\epsilon_2} * \cdots * s_n^{\epsilon_n}$$

where $n \geq 0$, $s_1, \ldots, s_n \in S$ and $\epsilon_i \pm 1$ for each i. We may also write $s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n}$, although sometimes this requires care since this "product" expression may simultaneously have a different meaning. The above word is reduced if it does not contain two adjacent terms of the form $s^1 * s^{-1}$ or $s^{-1} * s^1$ for any $s \in S$. In the case $n = 0$ there is one word, the empty word, also written 1. It is customary to write s^3 in place of sss, etc.

If G is a group and $S \subseteq G$ then every word in S represents an element of G. The elements so represented constitute the subgroup $\langle S \rangle$. Moreover, an element represented by a non-reduced word is also represented by a reduced word (obtained by making formal cancellations).

Definition. *If G is a group and $S \subseteq G$ then G is free on S if and only if $G = \langle S \rangle$ and distinct reduced words in S represent distinct elements of G. A group is free if and only if it is free on some subset.*

We can thus think of elements of a free group as reduced words, multiplied formally. For example, an infinite cyclic group $\langle x \rangle$ is free on $\{x\}$.

Theorem. *Let S be a set. Then there exists a free group on S. If G and H are free groups on S then there exists an isomorphism $G \to H$ fixing each element of S.*

One proof is to assert that this is essentially obvious; we let G be the set of reduced words in S, and multiply them formally. This seems a triviality, but it is a little unsettling to realize that there is something to check: associativity, e.g. for $S = \{a, b\}$, what is

$$(baba)(a^{-1}b^{-1}b^{-1})(bbbab)?$$

There really are two somewhat distinct ways of proceeding. What needs to be checked can be checked, but instead we construct a free group on S as follows. Let W be the set of all

reduced words in S. Instead of putting a group structure on W we construct G as a group of permutations of W. Namely for each $s \in S$ we define $\rho_s \in \Sigma_W$ as follows:

$$\rho_s(s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n}) = \begin{cases} s s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n} & \text{if } s_1^{\epsilon_1} \neq s^1 \\ s_2^{\epsilon_2} \cdots s_n^{\epsilon_n} & \text{if } s_1^{\epsilon_1} = s^1 \end{cases}$$

We define $\rho_{s^{-1}}$ similarly. It is easy to check that $\rho_s \rho_{s^{-1}} = \rho_{s^{-1}} \rho_s = id_W$, so each $\rho_s \in \Sigma_W$ and $\rho_{s^{-1}} = \rho_s^{-1}$. We then set

$$G = \langle \rho_s \,|\, s \in S \rangle,$$

identify each $s \in S$ with $\rho_s \in G$, and argue that G is free on S. Namely, for any reduced word $w = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n})$, if we let ρ_w be the corresponding word in the ρ_{s_i}, then it is trivial that

$$\rho_w(1) = w,$$

so distinct w's produce distinct ρ_w's, which proves the freeness. The uniqueness is clear: reduced words go to the corresponding reduced word. The multiplication in G is accomplished by juxtaposition and cancellation, although that was not our definition of it.

Theorem. *Let S be a set and F be a free group on S. Let G be a group and $\psi : S \to G$ be a mapping (of sets). Then there is a unique homomorphism $\Psi : F \to G$ such that $\Psi | S = \psi$.*

Indeed if $w \in G$ there is a unique way to write $w = s_1^{\epsilon_1} s_2^{\epsilon_2} \cdots s_n^{\epsilon_n}) \in G$, the word being reduced, and we set $\Psi(w) = \psi(s_1)^{\epsilon_1} \cdots \psi(s_n)^{\epsilon_n}$. This is the only choice for Ψ, and in fact it gives a homomorphism.

This leads to the following alternative definition of a free group, essentially equivalent to the first.

Definition. *Let S be a set. A free group on S is a group F, together with a mapping $i : S \to F$, with the following universal mapping property: For every group G and every mapping $j : S \to G$ there is a unique homomorphism $\phi : F \to G$ such that $\phi i = j$.*

From this definition it follows easily that i is injective, and that any two free groups $i : S \to F$ and $i' : S \to F'$ are isomorphic, i.e., there is an isomorphism $\phi : F \to F'$ such that $i' = \phi i$ (in fact, a unique isomorphism).

4b. Presentations

A free group on S can be informally described as having a certain set (S) of generators which satisfy no relations (other than those entailed by the group axioms). Here a relation means an equation between two words in S, more precisely between the group elements which they represent. If one is willing to impose relations, we can describe other groups in a similar way. Indeed every group can be described in this way, although infinitely many generators and infinitely many relations may be involved. This is the content of the following trivial theorem:

Theorem. *Let G be a group and S a subset of G such that $G = \langle S \rangle$. Let F be a free group on S. Then there is a normal subgroup $R \triangleleft F$ and an isomorphism $F/R \to G$ such that $sR \mapsto s$ for each $s \in S$.*

Proof The universal mapping property above provides a homomorphism $\phi : F \to G$ mapping $s \mapsto s$ for all $s \in S$. Since $G = \langle S \rangle$, ϕ is surjective. Let $R = \ker \phi$; the first isomorphism theorem completes the proof.

A consequence of the theorem is that

Every group is a homomorphic image of a free group;

in fact of many free groups. Thus homomorphic images of free groups are totally arbitrary groups.

(Remark: Subgroups, however, are not:

Theorem (Schreier). *Subgroups of free groups are free.*

However, they may require more generators than the group.)

Returning to the isomorphism $F/R \cong G$, we say that G is generated by S, with defining relations given by R. Or, G is presented by the generators S and relations R.

Of course R is too large, and it can be replaced by any subset which generates R. Even less is required: a subset R_0 of R such that R is the smallest normal subgroup of F containing R_0.

Lemma. *The intersection of normal subgroups of a group G is a normal subgroup of G.*

Thus given a set $X \subseteq G$, the intersection of all normal subgroups of G containing X is the smallest normal subgroup of G containing X. It is written $\langle X^G \rangle$, the reason being that it is the group generated by the union of all the G-conjugates of X.

In many cases R_0 may be taken to be quite small.

Definition. *Let S be a set and R_0 a set of words in S. Then*

$$gp\langle S \mid R_0 \rangle = F/\langle R_0^F \rangle.$$

Here on the right side, F is a free group on S and R_0 is interpreted as a subset of F. Notice that for each $s \in S$ there is an element $s\langle R_0^F \rangle$ of this group, which we could call $\overline{s}$. The mapping $s \mapsto \overline{s}$ is not necessarily injective, though it frequently is. This group is presented by generators S with relators R_0.

By the uniqueness of free groups, this definition is okay up to isomorphism (preserving S).

Theorem. *Let S and R_0 be as in the previous definition. Let G be a group and $i : S \to G$ a mapping such that for each word $w = w(s_1, \ldots, s_n)$ in S, the corresponding*

word $w(i(s_1), \ldots, i(s_n))$ represents the identity element of G. Then there is a unique homomorphism

$$\phi : gp\langle S \,|\, R_0\rangle \to G$$

such that $\phi(\overline{s}) = i(s)$ for all $s \in S$.

Example. Let

$$G = \mathrm{gp}\langle x, y \,|\, x^2, y^5, xyxy\rangle \text{ or equivalently} G = \mathrm{gp}\langle x, y \,|\, x^2 = 1, y^5 = 1, xyx = y^{-1}\rangle$$

Recall that D_{10} has generators a, b (a rotation of order 5 and a reflection) such that $b^2 = 1$, $a^5 = 1$ and $bab = a^{-1}$. Therefore there exists a homomorphism

$$\phi : G \to D_{10},\ \phi(x) = b,\ \phi(y) = a,$$

which we shall show is an isomorphism. As a result we will be able to say that the relations we have given on a and b are defining relations for D_{10}, or present D_{10}.

Since a and b generate D_{10}, ϕ is surjective. To prove that ϕ is injective is harder. We shall do it in this case by proving that $|G| \leq 10$. Namely, G contains elements $\overline{x}$ and $\overline{y}$ satisfying the given relations. Let us be sloppy and call them x and y. The relation $xyx = y^{-1}$ means that $xy = y^{-1}x$, and hence in G any product $x^i y^j$ may be rewritten as a product $y^k x^l$ for some k, l. The set of products $x^i y^j$ is therefore closed under multiplication (and inversion) in G, and contains x and y, so equals G. Finally there are at most 5 distinct powers of x and 2 of y in G, so $|G| \leq 10$. Therefore ϕ is an isomorphism.

Another example: let

$$G = \mathrm{gp}\langle x \,|\, x^7 = 1\rangle.$$

Then $G \cong Z_7$.

A more surprising example:

$$G = \mathrm{gp}\langle x, y \,|\, xyx^{-1} = y^2,\ yxy^{-1} = x^3\rangle.$$

In G we have $[x, y] = xyx^{-1}y^{-1} = y$ and $[y, x] = yxy^{-1}x^{-1} = x^2$. But always $[x, y] = [y, x]^{-1}$, and so $y = x^{-2}$. Consequently y and x commute, so $y = y^2$ and $x = x^3$. Therefore $y = 1$ and $x^2 = 1$. The group Z_2 does satisfy the relations (with $y = 1$ and $x \neq 1$), so $G \cong Z_2$. If we imposed the additional condition $x^{79} = 1$, for instance, then G would be 1.

The moral is that collapse is hard to detect *a priori*.

One upside of considering groups by presentations is that convenient presentations make homomorphisms easy to define. By the theorem above, for instance, since we know that $D_{10} \cong \mathrm{gp}\langle x, y \,|\, x^5 = y^2 = (xy)^2 = 1\rangle$, in order to define a homomorphism $\phi : D_{10} \to H$ for any H, it suffices to specify the elements $\phi(a)$ and $\phi(b)$ of H, as long as they satisfy $(\phi(a))^5 = (\phi(b))^2 = (\phi(a)\phi(b))^2 = 1$. For example, there is a homomorphism $D_{10} \to \Sigma_5$ taking $a \mapsto (1\,2\,3\,4\,5)$ and $b \mapsto (1\,4)(2\,3)$.

Another is that it quickly gives lots of examples of groups; for example,

$$G(m, n, p) = \mathrm{gp}\langle x, y, z \,|\, x^m = y^n = z^p = xyz = 1\rangle.$$

It is known for example that $G(2,2,p) \cong D_{2p}$; $G(2,3,2) \cong \Sigma_3$, $G(2,3,3) \cong A_4$, $G(2,3,4) \cong \Sigma_4$, $G(2,3,5) \cong A_5$, and $G(2,3,p)$ is infinite for $p > 5$.

A downside is that it can be tricky to obtain a convenient presentation of a given group. Nevertheless for many examples of groups, nice presentations have been discovered.

Exercise. *Consider the integers*

$$m_{ij} = \begin{cases} 1 & \text{if } i = j \\ 3 & \text{if } |i-j| = 1 \\ 2 & \text{otherwise} \end{cases}, \text{ for } i,j = 1,2,\ldots.$$

Show that for any $n \geq 1$,

$$gp\langle t_1, \ldots, t_n \,|\, (t_i t_j)^{m_{ij}} = 1 \ \forall i,j = 1,\ldots,n\rangle \cong \Sigma_{n+1}.$$

There has been considerable computational research on finitely presented groups, i.e., those which have a presentation consisting of finitely many generators and finitely many relators. Not every group, indeed even not every countable group, is finitely presented. But finite groups of course are finitely presented.

4c. Some Universal Mapping Properties

The critical properties of many algebraic constructions can be formulated as "universal mapping properties". Examples:

1. Given a set S, a free group on S is a mapping i from the set S into the group F such that for every mapping from the set S into an arbitrary group G,

$$\begin{array}{ccc} S & \overset{i}{\longrightarrow} & F \\ \downarrow & & \\ G & & \end{array}$$

there exists a unique group homomorphism $F \to G$ making the diagram commute. We usually speak of F as being the free group, but the objects S and F and the mapping i are really all part of the concept.

2. Given a group G and a normal subgroup $K \lhd g$, the quotient group G/K of G, the canonical projection $\pi_K : G \to G/K$ has the following property. It contains K in its kernel, and for any homomorphism $\phi : G \to H$ from G to an arbitrary group such that $K \leq \ker \phi$,

$$\begin{array}{ccc} G & \overset{\pi_K}{\longrightarrow} & G/K \\ \downarrow & & \\ H & & \end{array}$$

there exists a unique group homomorphism $G/K \to H$ making the diagram commute. We usually speak of G/K as being the quotient group, but the projection π_K is an integral part of this notion, as the multiplication in G/K has been defined as

$$gKg'K = gg'K, \text{ or equivalently } \pi_K(g)\pi_K(g') = \pi_K(gg').$$

Two remarks: of course the kernel of π_K is exactly K, but the above property is that among all homomorphisms whose kernel contains K, it is universal. Second, the mapping from $G/K \to H$ which makes the above diagram commute is the mapping ψ defined by

$$\psi(gK) = \phi(g).$$

Since $K \leq \ker \phi$, we have $\phi(g) = \phi(g)\phi(k)$ for all $k \in K$, and so ψ is well-defined. That it is a homomorphism and makes the diagram commute is then easy to check.

3. By combining these two we get a universal property of groups given by a presentation (i.e. generators and relations). Suppose that we are given a set S and a set R of reduced words in S. The group $\mathrm{gp}\langle S|R\rangle$, or more precisely the natural map $j : S \to \mathrm{gp}\langle S|R\rangle$, has the property that if $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \in R$, then the corresponding expression in $j(s_1), \ldots, j(s_n)$ represents the identity element of $\mathrm{gp}\langle S|R\rangle$. It is universal with this property, namely, for any group G and any mapping $f : S \to G$ such that $f(s_1)^{\epsilon_1} \cdots f(s_n)^{\epsilon_n} = 1$ for every word $s_1^{\epsilon_1} \cdots s_n^{\epsilon_n} \in R$,

$$\begin{array}{ccc} S & \xrightarrow{j} & \mathrm{gp}\langle S|R\rangle \\ \downarrow & & \\ G & & \end{array}$$

there is a unique homomorphism $\mathrm{gp}\langle S|R\rangle \to G$ making the diagram commute. This can be proved by noting that $\mathrm{gp}\langle S|R\rangle = F/\langle {}^F R\rangle$ by definition, where F is a free group on S, and j is the composite $\pi_{\langle {}^F R\rangle} : S \to F \to F/\langle {}^F R\rangle$; the previous two universal properties show that the given map $S \to G$ lifts uniquely by example 1 to a homomorphism $F \to G$ (which sends all words in R to the identity, and therefore contains R in its kernel, and therefore contains $\langle {}^F R\rangle$ in its kernel), and then lifts uniquely by example 2 to a homomorphism $F/\langle {}^F R\rangle \to G$.

The "same" proof shows in each case that given two universal objects, there is a unique "isomorphism" between them. Here "isomorphism" means not just an isomorphism in the ordinary sense, but one making an appropriate diagram commute. For instance, given two free groups

$$S \to F \text{ and } S \to F'$$

on S, we use

a) the universal property of $S \to F$ to get a homomorphism $\phi : F \to F'$ making diagram a) commute;

b) the universal property of $S \to F'$ to get a homomorphism $\psi : F' \to F$; making diagram b) commute;

c) the universal property of $S \to F$, and the observation that both $\psi\phi$ and id_F make diagram c) commute, to conclude that $\psi\phi = id_F$;

d) the universal property of $S \to F'$ and a similar argument to get $\phi\psi = id_{F'}$.

Then by c) and d), ϕ is an isomorphism, and by a) it is unique subject to making the diagram commute.

$$\begin{array}{ccc} S & \longrightarrow & F \\ \downarrow & & \\ F' & & \end{array} \qquad \begin{array}{ccc} S & \longrightarrow & F' \\ \downarrow & & \\ F & & \end{array} \qquad \begin{array}{ccc} S & \longrightarrow & F \\ \downarrow & & \\ F & & \end{array}$$

a) b) c)

This uniqueness is what makes it possible to define free group by the universal mapping property, as an alternative to the concrete definition we have given. (Either way, one has to prove that free groups exist!)

In category theory, the uniqueness argument just given is formalized, and is just the theorem that in any category, given any two initial objects, there is a unique isomorphism between them.

4d. Free Products

Related to free groups there is the construction of free products. Let $\{G_i \,|\, i \in I\}$ be a family of groups. The free product

$$\underset{i\in I}{\star} G_i$$

can be defined either in a "word" way or by a universal mapping property.

First a technicality: replace the G_i by isomorphic copies if necessary to insure that as sets, they are pairwise disjoint. Then define a reduced word to be a word in the alphabet

$$\bigcup_{i\in I}(G_i - \{1\})$$

such that any two adjacent terms come from two different G_i's. Informally the free product $\star_{i\in I} G_i$ is the set of all such reduced words, multiplication consisting of juxtaposition followed by reduction (reduction consisting of multiplying any two adjacent letters which happen to lie in the same G_i, and throwing out any terms which are 1, and iterating). The same problem exists here as with the definition of free group, and is finessed the same way. Let W be the set of all reduced words. For each $g \in \cup G_i - \{1\}$, let $\rho_g \in \Sigma_W$ be the permutation of W defined by "appending g on the left and reducing". Notice that for this kind of reducing, there is at most one step to be done (or two, if the word begins with g^{-1}) and there is no possible ambiguity. Then let

$$\underset{i\in I}{\star} G_i = \langle \rho_g \,|\, g \in \cup_{i\in I} G_i - \{1\} \rangle.$$

Technically this is a subgroup of Σ_W. However we may represent the element $\rho_g \rho'_g \cdots$ just by the word $gg' \cdots$, and if we do so, then the elements of the free product are just the reduced words, and distinct reduced words represent distinct group elements (as can be seen by applying the permutations to the empty word).

The free product has the following universal mapping property. It comes equipped with a family of homomorphisms $j_i : G_i \to (\star_{i \in I}\ G_i)$, one for each $i \in I$, namely $j_i(g) = g$. Then for any group H and any family of homomorphisms $f_i : G_i \to H$, one for each i, there is a unique homomorphism $(\star_{i \in I}\ G_i) \to H$ making the following diagram commute for each i:

$$\begin{array}{ccc} G_i & \longrightarrow & \underset{i \in I}{\star} G_i \\ & \searrow & \downarrow \\ & & H \end{array}$$

We leave the checking of this property to the reader.

As an example, if a group G is generated by an element a of order m and an element b of order n, then it is a quotient of $Z_m \star Z_n$. Namely there exist homomorphisms $Z_m \to G$ and $Z_n \to G$ taking generators to a and b, respectively. By the universal property there is a homomorphism $Z_m \star Z_n \to G$ taking generators of Z_m and Z_n to a and b, respectively. Since a and b generate G this homomorphism is surjective. By the first isomorphism theorem, G is a quotient of $Z_m \star Z_n$.

For instance, we know that $PSL_2(Z)$ is generated by the images of the two matrices

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix},$$

of orders 2 and 3 respectively. Hence there is a homomorphism

$$Z_2 \star Z_3 \to PSL_2(Z)$$

taking generators of Z_2 and Z_3 to the images of these matrices, and $PSL_2(Z)$ is thus a quotient of $Z_2 \star Z_3$. In this particular case this mapping turns out to be an isomorphism!