II.K. Generators and relations

The abelian case. Let G be an abelian group. We will write the group operation as "$+$". Note that for $g \in G$ and $a \in \mathbb{Z}$, the notation ag means adding g to itself a times (or, if $a < 0$, its inverse $-g$ to itself $|a|$ times). So it is the equivalent of exponentiation in the multiplicative notation.

II.K.1. PROPOSITION. *The following are equivalent:*
(i) $G = \{a_1 g_1 + \cdots + a_n g_n \mid a_i \in \mathbb{Z}\}$ *for some* $g_1, \ldots, g_n \in G$*, called a* generating set *for* G*.*
(ii) $G \cong \mathbb{Z}^n / K$ *for some* $n \in \mathbb{N}$, $K \leq \mathbb{Z}^n$*.*

PROOF. If (i) holds, define $\varphi \colon \mathbb{Z}^n \twoheadrightarrow G$ to send $\underline{a} := (a_1, \ldots, a_n) \mapsto \sum_i a_i g_i$. By the Fundamental Theorem, $G \cong \mathbb{Z}^n / \ker(\varphi)$.

Conversely, assuming (ii), write η for the composition

$$\mathbb{Z}^n \overset{\nu}{\twoheadrightarrow} \mathbb{Z}^n / K \overset{\cong}{\to} G,$$

and set $g_i := \eta(\underline{e}_i)$ (where $\underline{e}_i$ is the i^{th} standard basis vector). Every element of $\mathbb{Z}^n$ is of the form $\sum_i a_i \underline{e}_i$, and η is surjective; thus, every element of G is of the form $\eta(\sum_i a_i \underline{e}_i) = \sum_i a_i \eta(\underline{e}_i) = \sum_i a_i g_i$. □

II.K.2. DEFINITION. (i) If the equivalent conditions of II.K.1 hold, G is **finitely generated (f.g.)**.
(ii) K is called the **relations subgroup** for G.
(iii) If $G \cong \mathbb{Z}^m$ (for some m), G is (f.g.) **free abelian** of rank m. The image of the standard basis $\{\underline{e}_i\}_{i=1}^m \subset \mathbb{Z}^m$ under the isomorphism is called a **basis** of G.

II.K.3. EXAMPLES. (i) $\mathbb{Z}_n$ is f.g. (with one generator: $\bar{1}$), and isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

(ii) $\mathbb{Q}$ is *not* f.g.: if you pick $\frac{r_1}{s_1}, \ldots, \frac{r_n}{s_n}$ then any $\sum_{i=1}^n a_i \frac{r_i}{s_i}$ can be represented with denominator $\prod_i s_i$ — clearly not possible for an arbitrary rational number.

(iii) Suppose $G \cong \mathbb{Z}^3/K$, and $K \cong \mathbb{Z}^2$ with basis $(11, -21, -10)$, $(1, -6, -5)$. Then we can write G in terms of "generators and relations":[21]

$$G \cong \frac{\mathbb{Z}\langle X, Y, Z\rangle}{\langle 11X - 21Y - 10Z,\ X - 6Y - 5Z\rangle}.$$

The key here is using the fact that K is free, and further, having a basis for K. The next result and its proof generalize this:

II.K.4. THEOREM. *Every subgroup of a free f.g. abelian group is free f.g.; more precisely, any $K \leq \mathbb{Z}^n$ is $\cong \mathbb{Z}^m$ for some $m \leq n$.*

PROOF. If $n = 1$, let $a \in \mathbb{N} \cap K$ be as small as possible. If $b \in K \backslash \{0\}$ is not a multiple of a, then $\gcd(a, b) = \ell_1 a + \ell_2 b \in K$, and is less than a, a contradiction. So $K = \langle a \rangle \cong \mathbb{Z}$.

Now, assuming the statement for $n - 1$, consider the projection $\pi\colon K \to \mathbb{Z}$ to the first $\mathbb{Z}$-factor. If $\pi(K) = \{0\}$, we're done by induction (as $\ker(\pi) \leq \mathbb{Z}^{n-1}$). Otherwise, $\pi(K)\,(\leq \mathbb{Z})$ consists of multiples of some $a = \pi(\alpha)$, $\alpha \in K$. Hence any $\beta \in K$ is of the form

$$(\beta - \tfrac{\pi(\beta)}{a}\alpha) + \tfrac{\pi(\beta)}{a}\alpha \ \in\ ker(\pi) + \langle \alpha \rangle\,,$$

and $\ker(\pi) \cap \langle \alpha \rangle = \{0\}$. So by (say) II.E.11(iii), $K \cong \ker(\pi) \times \langle \alpha \rangle$, and applying the inductive assumption to $\ker(\pi) \leq \mathbb{Z}^{n-1}$, we are done. (Note that the proof also yields a method for constructing a basis, starting with α.) □

In fact, the group in Ex. II.K.3(iii) is $\cong \mathbb{Z}_{45} \times \mathbb{Z}$, which inspires the next statement:

II.K.5. PROPOSITION-DEFINITION. (*Let G be abelian.*) *The subset $G_{\text{tor}} \subseteq G$ comprising elements of finite order is a* subgroup, *the* ***torsion part*** *of G; while G/G_{tor} is a free abelian group* (*all nonzero elements are of infinite order*), *the* ***free part*** *of G.* (*If G is f.g., this is $\cong \mathbb{Z}^m$ for some m.*)

PROOF. Given $g_1, g_2 \in G_{\text{tor}}$, we have $a_i \in \mathbb{N}$ with $a_i g_i = 0$. Then $\text{lcm}(a_1, a_2) \cdot (g_1 + g_2) = 0 \implies g_1 + g_2 \in G_{\text{tor}}$. (So it's closed under addition — the rest is trivial.)

[21]The notation $\mathbb{Z}\langle X, Y, Z\rangle$ means the free abelian group with basis X, Y, Z; the denominator means the subgroup generated by those two elements.

Given $g \in G \backslash G_{\text{tor}}$, if $ag \in G_{\text{tor}}$ for some $a \in \mathbb{N}$, then there exists $b \in \mathbb{N}$ such that $0 = b(ag) = (ba)g$, making $g \in G_{\text{tor}}$, a contradiction. So g has infinite order in G/G_{tor}. (I skip the proof of the parenthetical for now; we will return to f.g. abelian groups in the context of modules.) $\square$

II.K.6. REMARK. Prop. II.K.5 is false for nonabelian groups. There is no reason, if g_1 and g_2 don't commute, why $g_1^a = 1$ and $g_2^b = 1$ should imply that $g_1 g_2$ has finite order. One example is[22] $\mathrm{PSL}_2(\mathbb{Z})$, which is generated by $R = \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ and $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. These elements satisfy $R^3 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) = S^2$ (i.e. have finite order), but their product $RS = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ has infinite order.

The general (non-abelian) case. We return to multiplicative notation. Given a subset $S \subseteq G$, we defined the subgroup generated by S as

$$\langle S \rangle := \text{smallest subgroup of } G \text{ containing } S.$$

For later use, also write

$$\langle\!\langle S \rangle\!\rangle := \text{smallest } \textit{normal} \text{ subgroup of } G \text{ containing } S.$$

A set of **generators** for G is a subset S such that $\langle S \rangle = G$ (and it is **minimal** if for all $S' \subsetneq S$, we have $\langle S' \rangle < G$). We say that G is **finitely generated** iff there exists a finite set S with $G = \langle S \rangle$. Having a (small) generating set is useful because of the following

II.K.7. PROPOSITION. *A homomorphism $\varphi\colon G \to H$ is defined by its behavior on a generating set. That is, if $G = \langle S \rangle$ and φ, η are homomorphisms with $\varphi(s) = \eta(s)$ ($\forall s \in S$), then $\varphi = \eta$.*

PROOF. Any $g \in G$ may be written in the form $g = s_1 \cdots s_N$ with $s_i \in S$ (and possible repetitions). Hence, $\varphi(g) = \varphi(s_1) \cdots \varphi(s_N) = \eta(s_1) \cdots \eta(s_N) = \eta(g)$. $\square$

II.K.8. PROPOSITION. *Given $\varphi\colon H \to G$, if $\varphi(H) \supset S$ and $\langle S \rangle = G$, then φ is surjective.*

[22] $\mathrm{SL}_2(\mathbb{Z})$ quotiented by the normal 2-element subgroup generated by $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$.

PROOF. Since $\varphi(H)$ is a group, $\langle S\rangle \leq \varphi(H)$. □

Now let $\mathcal{S}$ be a set, not a subset of a group, just a set. Consider the set of *words* on $\mathcal{S}$, by which we mean the set of expressions

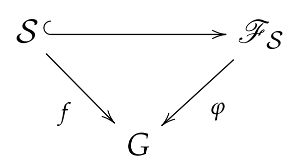
$$s_1^{m_1} s_2^{m_2} \cdots s_k^{m_k} \quad (k \geq 0,\, s_i \in \mathcal{S},\, m_i \in \mathbb{Z})$$

subject only to the (equivalence) relation $s^a s^b = s^{a+b}$ (for each $s \in \mathcal{S}$). Denote this set by[23] $\langle \mathcal{S} \rangle$, and introduce the binary operation of "concatenating words" together with the obvious inverses $s_k^{-m_k} \cdots s_1^{-m_1}$ to put a group structure on it. (Clearly the subset $\mathcal{S}$ generates the resulting group $\langle \mathcal{S} \rangle$!!) More intrinsically, we have the

II.K.9. PROPOSITION-DEFINITION. *There exists a unique group*

$$\mathscr{F}_{\mathcal{S}} \supset \mathcal{S}$$

with the (*universal*) *property that:* for all groups G and maps $f\colon \mathcal{S} \to G$, there exists a unique homomorphism $\varphi\colon \mathscr{F}_{\mathcal{S}} \to G$ making the diagram

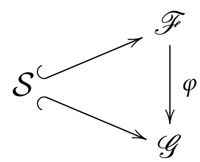


commute. *In fact, $\mathscr{F}_{\mathcal{S}} \cong \langle \mathcal{S} \rangle$. It is called the **free group** on $\mathcal{S}$.*

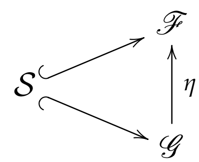
PROOF. First we prove existence by showing that $\langle \mathcal{S} \rangle$ has this property. Define $\varphi\colon \langle \mathcal{S} \rangle \to G$ by $\varphi(s_1^{m_1} \cdots s_k^{m_k}) = f(s_1)^{m_1} \cdots f(s_k)^{m_k}$. This is clearly well-defined and a homomorphism, and any other homomorphism η making the diagram commute must have $\eta(s) = f(s)$ for all $s \in \mathcal{S}$, hence (by II.K.7) $\eta = \varphi$.

[23]This designation is temporary, as — while standard — it is likely to get confused with the other meaning of $\langle S \rangle$ for a subset of a group. After II.K.9 we will be using $\mathscr{F}_{\mathcal{S}}$ instead.

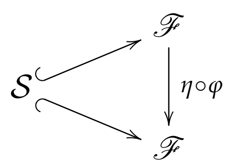
For uniqueness, suppose $\mathscr{F}$ and $\mathscr{G}$ are two groups containing $\mathcal{S}$ as a subset and satisfying the universal property. Then there are homomorphisms φ and η making



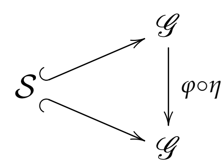
and



commute. But then



and



commute as well, and then the uniqueness in the universal property gives $\eta \circ \varphi = \mathrm{id}_{\mathscr{F}}$ and $\varphi \circ \eta = \mathrm{id}_{\mathscr{G}}$. So $\mathscr{F} \cong \mathscr{G}$ and we are done. □

Henceforth I will drop $\langle \mathcal{S} \rangle$ for free groups and use it only for subgroups generated by a subset.

II.K.10. REMARK. A similar characterization exists for the free abelian group $\mathscr{A}_{\mathcal{S}}$ on $\mathcal{S}$. In II.K.9, wherever "group(s)" occurs, replace it by "abelian group(s)", and replace $\langle \mathcal{S} \rangle$ by the group of finite formal sums $m_1 s_1 + \cdots + m_k s_k$ with $k \geq 0$, $m_i \in \mathbb{Z}$ and $s_i \in \mathcal{S}$. In the (modified) first paragraph of the proof, $\varphi(m_1 s_1 + \cdots + m_k s_k) := f(s_1)^{m_1} \cdots f(s_k)^{m_k}$ is well-defined and a homomorphism precisely because G is abelian.

Now let $\mathcal{S} \subset G$ be a *finite* generating set. We have by II.K.8-II.K.9 a (surjective) homomorphism

$$\varphi \colon \mathscr{F}_{\mathcal{S}} \twoheadrightarrow G$$

with $\varphi(s) = s$ for each $s \in \mathcal{S}$. By the Fundamental Theorem,

$$G \cong \mathscr{F}_{\mathcal{S}} / \ker(\varphi),$$

where of course $\ker(\varphi)$ is normal; and if $\ker(\varphi) = \langle\langle \mathcal{R} \rangle\rangle$ for some subset $\mathcal{R} \subset \mathscr{F}_{\mathcal{S}}$, this becomes

(II.K.11) $$G \cong \mathscr{F}_{\mathcal{S}} / \langle\langle \mathcal{R} \rangle\rangle$$

— a **presentation** of G in terms of generators $\mathcal{S}$ and relations $\mathcal{R}$. If $|\mathcal{R}| < \infty$, we say that G is **finitely presented**. We conclude with some

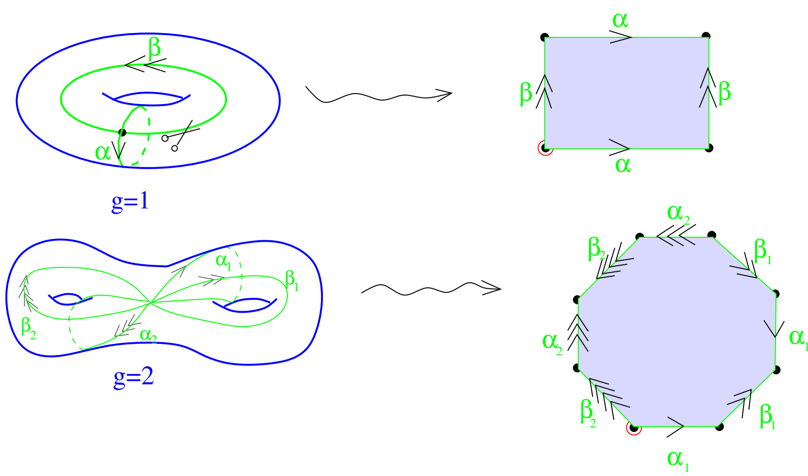
II.K.12. Examples. (i) $D_n \cong \mathscr{F}_{\{r,h\}} / \langle\langle r^n, h^2, rhrh \rangle\rangle$.

(ii) $\mathrm{PSL}_2(\mathbb{Z}) \cong \mathscr{F}_{\{S,R\}} / \langle\langle S^2, R^3 \rangle\rangle$.

(iii) [HW] $\mathscr{A}_{\mathcal{S}} \cong \mathscr{F}_{\mathcal{S}} / [\mathscr{F}_{\mathcal{S}}, \mathscr{F}_{\mathcal{S}}]$ for any set $\mathcal{S}$.

The next two examples illustrate the role these concepts play in algebraic topology and complex analysis.

(iv) A *compact Riemann surface C of genus g* is, topologically, the surface of a sphere with g handles attached, or of a donut with g holes.



Choosing a point $x \in C$, its *fundamental group* $\pi_1(C)$ is the set of closed curves starting and ending at x modulo the equivalence relation given by continuous deformation;[24] the group operation is concatenating loops and inversion is reversing the direction. In fact, it

[24]More precisely, a closed curve is a continuous map $\gamma\colon [0,1] \to C$ with $\gamma(0) = \gamma(1)$; and γ_0 and γ_1 are equivalent if there is a continuous map $\Gamma\colon [0,1] \times [0,1] \to C$ with $\gamma_0(t) = \Gamma(0,t)$ and $\gamma_1(t) = \Gamma(1,t)$.

is the quotient of a free group on certain loops (shown for $g = 1, 2$) modulo a single relation:

$$\pi_1(C) \cong \mathscr{F}_{\{\alpha_1,\beta_1,\ldots,\alpha_g,\beta_g\}} / \langle\!\langle \prod_{i=1}^{g} [\alpha_i, \beta_i] \rangle\!\rangle.$$

The relation arises from cutting open the surface as shown, then observing that the boundary can be continuously deformed to a point. (To see that the boundary curve is the product of commutators shown, start at the red dot with β resp. β_2.)

(v) Let $N \geq 3$, and set $\kappa := \frac{N^2}{2} \prod_{p|N} (1 - \frac{1}{p^2})$ (where p is prime) and $g := 1 + \frac{N-6}{12}\kappa$. Recall the *congruence subgroups*

$$\Gamma(N) := \ker\{\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})\}.$$

Let $\mathfrak{H} := \{x + \mathbf{i}y \mid x \in \mathbb{R}, y \in \mathbb{R}_{>0}\}$ denote the upper half-plane in $\mathbb{C}$. We let $\Gamma(N)$ act on $\mathfrak{H}$ by fractional linear transformations, with $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ sending $z \mapsto \frac{az+b}{cz+d}$. The "quotient set"

$$Y(N) := \mathfrak{H}/\Gamma(N)$$

obtained[25] by identifying all points related by $\Gamma(N)$, is a genus g Riemann surface with κ points removed. Moreover, writing $\gamma_1, \ldots, \gamma_\kappa$ for loops around these points, we have

$$\Gamma(N) \cong \pi_1(Y(N)) \cong \mathscr{F}_{\{\alpha_1,\beta_1,\ldots,\alpha_g,\beta_g,\gamma_1,\ldots,\gamma_\kappa\}} / \langle\!\langle \prod_{i=1}^{g} [\alpha_i, \beta_i] \prod_{j=1}^{\kappa} \gamma_j \rangle\!\rangle.$$

In particular, $\Gamma(N)$ is finitely presentable (in fact, it is also torsion-free).

[25]That is, $Y(N)$ is the set of orbits of the group action on $\mathfrak{H}$.