MA 212: Algebra I

Naman Mishra

August 2024

Contents

The course

Grading

This is tentative.

- Quizzes: 30%
- Midterm: 30%
- Final: 40%

Lecture 1.
Friday
August 2

Chapter 1

Groups

Definition 1.1 (Binary operation)**.** A *binary operation* $\cdot$ on a set A is any map from $A \times A \to A$, written $(a, b) \mapsto a \cdot b$.

We say that $\cdot$ is *associative* if for all $a, b, c \in A$,

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

and *commutative* if for all $a, b \in A$,

$$a \cdot b = b \cdot a.$$

Examples.

- Addition and multiplication are associative and commutative binary operations on $\mathbb{R}$.
- Subtraction, division and exponentiation are non-associative and non-commutative binary operations.
- Composition is an associative but non-commutative binary operation on X^X.

Definition 1.2 (Group)**.** A *group* is a set G equipped with a binary operation $\cdot$ satisfying the following properties:

(G1) **associativity:** $\cdot$ is associative;

(G2) **identity:** there exists an element $1_G = e \in G$ such that $1_G \cdot x = x \cdot 1_G = x$ for all $x \in G$;

(G3) **inverse:** for every $x \in G$, there exists an element $y \in G$ such that $x \cdot y = y \cdot x = 1_G$. We write y as x^{-1}.

If $\cdot$ is also commutative, we say that G is an *abelian group.*

A subset $H \subseteq G$ is a *subgroup* of G if H is a group with respect to the same binary operation $\cdot$. We write $H \leq G$.

Examples.

- $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$ are abelian groups.
- $(\mathbb{R}^\times, \cdot)$ is a group but $(\mathbb{R}, \cdot)$ is not.
- $(\mathrm{GL}_n(\mathbb{R}), \cdot)$ is a non-abelian group, where
$$\mathrm{GL}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det A \neq 0\}.$$
- For any $n \in \mathbb{N}^+$, $(S_n, \circ)$ is a group, where
$$S_n = \{\sigma \colon [n] \to [n] \mid \sigma \text{ is bijective}\}.$$
$$\begin{aligned} S_1 &= \{1\}, \\ S_2 &= \{1, (12)\}, \\ S_3 &= \{1, (12), (13), (23), (123), (132)\}. \end{aligned}$$
S_1 and S_2 are abelian, but S_3 is not. Let $x = (12)$ and $y = (13)$, then
$$(x \circ y)(1) = x(3) = 3, \quad (x \circ y)(2) = x(2) = 1, \quad (x \circ y)(3) = x(1) = 2,$$
but
$$(y \circ x)(1) = y(2) = 2, \quad (y \circ x)(2) = y(1) = 3, \quad (y \circ x)(3) = y(3) = 1.$$
- Let $H = \left\{ \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \mid x \in \mathbb{R} \right\}$. Then H is an abelian subgroup of the non-abelian $\mathrm{GL}_2(\mathbb{R})$.

Remarks (New groups from old).

- Let $(A, \cdot)$ and $(B, *)$ be groups. The cartesian product $A \times B$ is a group with respect to the operation
$$(a_1, b_1) \star (a_2, b_2) = (a_1 \cdot a_2, b_1 * b_2).$$
defined componentwise.
- Let X be a set and $S = \mathbb{R}^X$. Then S is an abelian group under addition (pointwise). In fact, if $(G, \cdot)$ is a group, then G^X is a group under the operation
$$(f \cdot g)(x) = f(x) \cdot g(x).$$
If G is abelian, then so is G^X.
- Given any set A, we can form the group $S(A)$ of all bijections from A to itself, under composition.

Proposition 1.3. *Let $(G, \cdot)$ be a group. Then* *(i) the identity element 1_G is unique;*

(ii) the inverse of each element $x \in G$ is unique;

(iii) $(x^{-1})^{-1} = x$ for all $x \in G$;

(iv) $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$ for all $x, y \in G$;

(v) The product $a_1 a_2 \dots a_n$ does not depend on bracketing.

Proof.

(i) Suppose e and f are both identities of G. Then

$$e = e \cdot f = f.$$

(ii) Suppose y and y' are both inverses of x. Then

$$xy = 1_G \implies y'xy = y' \implies y' = y.$$

(iii) We have

$$x \cdot x^{-1} = 1_G = x^{-1} \cdot x.$$

reinterpreted in the context of x^{-1}.

(iv) Checking

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = 1_G.$$

Alternatively, let $z = (xy)^{-1}$. Then

$$\begin{aligned} (xy)z &= 1_G \\ (x^{-1}x)yz &= x^{-1} \\ yz &= x^{-1} \\ (y^{-1}y)z &= y^{-1}x^{-1} \\ z &= y^{-1}x^{-1}. \end{aligned}$$

(v) Induct on n. Look at the rightmost left bracket

$$a_1 \dots a_n = (a_1 \dots a_k) \cdot (a_{k+1} \dots a_n).$$

■

Corollary 1.4 (Cancellation law)**.** *Let $(G, \cdot)$ be a group. If $x, y, z \in G$ and $xy = xz$, then $y = z$.*

Proof. Multiply by x^{-1} on the left. ■

Lecture 2. Monday August 5

Definition 1.5 (Order)**.** The order of an element $x \in G$ is the smallest $n \in \mathbb{N}$ such that $x^n = 1_G$ if it exists, and ∞ otherwise.

Examples.

- $G = \mathbb{Z}/n\mathbb{Z} = \{\bar{a} \mid 0 \leq a < n\}$ where $\bar{a} = \{a + kn \mid k \in \mathbb{Z}\}$ under the operation $\bar{a} + \bar{b} = \overline{a+b}$.

- $G = \mathbb{C}^\times$. All roots of unity have finite order.

- $G = \mathrm{GL}_2(\mathbb{R})$. The matrix
$$\alpha_\theta = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$$
has order n if $\theta = \frac{2\pi}{n}$. [This is a homomorphism from $(\mathbb{R}, +)$ to $(G, \cdot)$]

- $G = \mathrm{GL}_2(R)$ where R is a ring. Elements of the following set may have finite order.
$$\{g \in M_2(R) \mid \det(g) \text{ is a unit in } R\}$$

Proposition 1.6 (Crystallographic restriction)**.** *Let* $x \in \mathrm{GL}_2(\mathbb{Z})$*. Then* $\operatorname{ord} x \in \{1, 2, 3, 4, 6, \infty\}$.

Definition 1.7 (Subgroup)**.** A set $H \subseteq G$ is a *subgroup* of G if it is a group under the same operation. We write $H \leq G$.

Examples.

- $G = \mathbb{Z}$. Then $H \leq G \iff H = n\mathbb{Z}$ for some $n \in \mathbb{N}$.

  Proof. Ignore the trivial case $H = \{0\}$. Let n be the smallest positive element of H. Then $n\mathbb{Z} \subseteq H$ by closure under addition. For any $m \in H$, write $m = qn + r$ with $0 \leq r < n$. Then $r = m - qn \in H$. Since n is the smallest positive element of H, $r = 0$. Thus $H \subseteq n\mathbb{Z}$. ■

- Let $|G| = 2k < \infty$. Then G has an element of order 2.

  Proof. Suppose not. Then for any $x \in G \setminus \{1\}$, $x^{-1} \neq x$. Thus $G \setminus \{1\}$ is a disjoint union of pairs $\{x, x^{-1}\}$. This would imply $|G|$ is odd. ■

- Let G be a group such that $x^2 = 1$ for all $x \in G$. Then G is abelian.

  Proof. Let $x, y \in G$. Then
$$\begin{aligned} &(xy)^2 = 1 \\ \implies &xyxy = 1 \\ \implies &xy = y^{-1}x^{-1} = yx \end{aligned}$$
■

- Let G be a finite group where each element is its own inverse. What can be said about $|G|$?

  $(G, \cdot)$ can be viewed as a vector space over $(\mathbb{F}_2, +, \cdot)$ with the scalar product of $x \in G$ and $c \in \mathbb{F}_2$ given by x^c. Let $n = \dim_{\mathbb{F}_2} G$ (possibly zero). Then $(G, \cdot) \cong (\mathbb{F}_2^n, +)$ and thus $|G| = 2^n$. (ref. structure theorem for finitely generated abelian groups)

  Furthermore, $\mathbb{F}_2^n$ is a group of this form for all n. Thus the groups of this form are precisely $\{\mathbb{F}_2^n \mid n \in \mathbb{N}\}$ (up to isomorphism).

Proposition 1.8. *Let $H \subseteq G$. Then $H \leq G$ iff $H \neq \varnothing$ and H is closed under the operation $(x, y) \mapsto xy^{-1}$.*

Proof. The "only if" direction is trivial.

Suppose $H \neq \varnothing$ and H is closed under the operation. Let x be any element of H. Then $1 = xx^{-1} \in H$. Now for any $y \in H$, $y^{-1} = 1y^{-1} \in H$. Now for any $x, y \in H$, $xy = x(y^{-1})^{-1} \in H$. ■

Proposition 1.9. *Let $H \subseteq G$ be finite. Then $H \leq G$ iff $H \neq \varnothing$ and H is closed under multiplication.*

Proof. Let ■

1.1 Cyclic groups

Given $x \in G$, look at the set $\langle x \rangle = \{x^n \mid n \in \mathbb{Z}\}$. This is a cyclic subgroup of G.

We wish to classify all cyclic subgroups (up to isomorphism).

Example. Let $H \leq G$ with $|G| = n > 2$, $|H| = n - 1$. Is this possible?

No. Let $G \setminus H = \{x\}$. Then $x^{-1} = x$. Let $h \neq 1 \in H$. Then $xh = h' \in H$, so $x \in H$ (closure).

Generalising gives the following proposition.

Proposition 1.10. *No group can be the union of two proper subgroups.*

Proof. Suppose $G = H_1 \cup H_2$ where $H_1, H_2 \leq G$. Pick an $x \in H_1 \setminus H_2$ and $y \in H_2 \setminus H_1$. WLOG assume $xy \in H_1$. Then $y \in H_1$. This means at least one of $H_1 \setminus H_2$ and $H_2 \setminus H_1$ is empty. ■

Definition 1.11 (Homomorphism)**.** Let G and H be groups. A map $\varphi\colon G \to H$ is a *homomorphism* from G to H if it respects the group operation. That is,

$$\varphi(xy) = \varphi(x)\varphi(y)$$

for all $x, y \in G$.

- If φ is bijective, it is called an *isomorphism*.
- If $H = G$, it is an *automorphism*.

G and H are *isomorphic* ($G \cong H$) if there exists an isomorphism from G to H.

Definition 1.12 (Kernel)**.** The *kernel* of a homomorphism $\varphi\colon G \to H$ is the set

$$\ker\varphi = \{x \in G \mid \varphi(x) = 1_H\}.$$

The *image* of φ is the set

$$\operatorname{Im}\varphi = \{\varphi(x) \mid x \in G\}.$$

Examples.

- $\det\colon \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^\times$ is a homomorphism.
- $\mu\colon \mathbb{Z}/n\mathbb{Z} \to \mu_n$ given by
  $$\mu\left(\bar{k}\right) = \exp(\frac{2\pi k}{n})$$
  is an isomorphism, where
  $$\mu_n = \{n\text{th roots of unity}\} \subseteq \mathbb{C}.$$
- φ is injective iff $\ker\varphi = \{1_G\}$.
- $\exp\colon (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ is an isomorphism.
- $\mathbb{R}^\times \not\cong \mathbb{C}^\times$.
- Let A, B be nonempty sets. Then $S_A \cong S_B$ iff A and B are in bijection.

  Proof. Suppose τ is a bijection from A to B. Then $\sigma \mapsto \tau\sigma\tau^{-1}$ is an isomorphism from S_A to S_B. ■

If two groups are isomorphic, they are essentially the same group. An isomorphism $\varphi\colon G \to H$ is only a "re-parameterization" of G in terms of H. **Lecture 3.** Wednesday August 7

Lecture 3

Lemma 1.13. $|\langle x\rangle| = \operatorname{ord} x$.

Proof. If $\operatorname{ord} x = \infty$, then $x^n \neq x^m$ for $n \neq m$. Thus $|\langle x\rangle| = \infty$.

If $\operatorname{ord} x = n < \infty$, then $x^0, x^1, \dots, x^{n-1}$ are distinct. Let $x^m \in \langle x\rangle$. Write $x^m = x^{qn+r} = x^r$ with $0 \leq r < n$. Thus these n elements are the only ones in $\langle x\rangle$. ■

Proposition 1.14. *Let G be a cyclic group. Then*

(i) if $|G| = \infty$, then $G \cong \mathbb{Z}$;

(ii) if $|G| = n < \infty$, then $G \cong \mathbb{Z}/n\mathbb{Z}$.

Proof. Let $G = \langle x\rangle$. We want an isomorphism $\varphi\colon G \to \mathbb{Z}/n\mathbb{Z}$, where $n \in \mathbb{N} \cup \{\infty\}$. It suffices to define $\varphi(x)$ and extend it to all of G.

If $|G| = \infty$, define $\varphi(x) = 1$. Then $\varphi(x^n) = n$ for all $n \in \mathbb{Z}$. This is a bijection and $\varphi(ab) = \varphi(a) + \varphi(b)$ holds.

If $|G| = \{1, x, \dots, x^{n-1}\}$, define $\varphi(x) = \overline{1} \in \mathbb{Z}/n\mathbb{Z}$. Then $\varphi(x^m) = \overline{m}$ for all $m \in \mathbb{Z}$. It is clearly a surjection. The kernel is $\{x^m \in G : n \mid m\} = \{1\}$, so it is injective. Finally, $\varphi(x^m x^k) = \varphi(x^{m+k}) = \overline{m+k} = \overline{m} + \overline{k}$. ■

Cyclic groups are generated by a single element. What about groups generated by multiple elements?

Let $S \subseteq G$. Define two sets

$$\begin{aligned}
\langle S\rangle_1 &= \{s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k} \mid s_i \in S, \varepsilon_i \in \{\pm 1\}\} \\
&= \{s_1^{\alpha_1} \dots s_k^{\alpha_k} \mid s_i \in S, \alpha_i \in \mathbb{Z}\} \\
\langle S\rangle_2 &= \bigcap_{S \subseteq H \leq G} H.
\end{aligned}$$

Lemma 1.15. $\langle S\rangle_1 = \langle S\rangle_2 =: \langle S\rangle$.

Proof. $\langle S\rangle_2 \leq G$ since the intersection of subgroups is a subgroup. We first check that $\langle S\rangle_1 \leq G$ under multiplication (which is essentially concatenation). Inverses are given by $s_1^{\varepsilon_1} \dots s_k^{\varepsilon_k} \mapsto s_k^{-\varepsilon_k} \dots s_1^{-\varepsilon_1}$.

Moreover, $S \subseteq \langle S\rangle_1$. Thus $\langle S\rangle_2 \subseteq \langle S\rangle_1$.

Since $\langle S\rangle_2$ is a group containing S, closure under products and inverses implies $\langle S\rangle_1 \subseteq \langle S\rangle_2$. ■

Examples.

- S_n is generated by transpositions.

- $\mathrm{GL}_n(\mathbb{R})$ is generated by the elementary matrices
$$E_{ij}(\lambda) = I_n + \lambda e_{ij},$$
where $e_{pq} = (\delta_{ip}\delta_{jq})_{i,j=1}^n$, taken together with the diagonal matrices. [swapping is done by $(a, b) \mapsto (a, a + b) \mapsto (-a, a + b) \mapsto (b, a + b) \mapsto (b, a)$]

- $\mathbb{Q}^\times$ is not finitely generated. Take any finite set $S \subseteq \mathbb{Q}^\times$ and look at the numerators. There are finitely many primes in the numerators of S, so any prime not in the numerators of S is not in $\langle S \rangle$.

- $\mathrm{SL}_n(\mathbb{R}) = \{M \in M_n(\mathbb{R}) \mid \det M = 1\}$ is generated by
$$E_{ij}(\lambda) = I_n + \lambda e_{ij}, \quad \text{with } i \neq j.$$

- Let F be any infinite field. Then $(F^\times, \cdot)$ is not finitely generated. If $\operatorname{char} F = p$, then p is prime and

  Suppose $\operatorname{char} F = 0$. Then F contains (an isomorphic copy of) $\mathbb{Q}$. For $F^\times$ to be finitely generated, $Q^\times$ would have to be finitely generated. We will later see that subgroups of finitely generated groups are finitely generated. We will also see that $\mathbb{Q}^\times$ is not finitely generated. Thus $F^\times$ is not finitely generated.

Lecture 4. Friday August 9

- $\mathrm{GL}_n(F)$ is not finitely generated for any infinite field F.
  - There is an isomorphic copy of $F^\times$ in $\mathrm{GL}_n(F)$. If $\mathrm{GL}_n(F)$ were finitely generated, so would $F^\times$.
  - $\det\colon \mathrm{GL}_n(F) \to F^\times$ is a surjective homomorphism. If $\mathrm{GL}_n(F)$ were finitely generated, so would $F^\times$.

  However, $\mathbb{F}^\times$ is not finitely generated since it contains $\mathbb{Q}^\times$.

- In the non-abelian setting, a subgroup of a finitely generated group is not necessarily finitely generated. Let
$$G = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \leq \mathrm{GL}_2(\mathbb{R}).$$
Let
$$H = \left\{ g \in G \;\middle|\; g = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \right\} \leq G.$$
Check that
$$H = \left\{ \begin{pmatrix} 1 & n/2^m \\ 0 & 1 \end{pmatrix} \;\middle|\; n, m \in \mathbb{Z} \right\}.$$

This is not finitely generated. H is isomorphic to the additive group of rationals with power-of-2 denominators. The span of any finite set

$$S = \{\frac{n_1}{2^{m_1}}, \dots, \frac{n_k}{2^{m_k}}\},$$

cannot contain any rational with a denominator larger than $2^{\max m_i}$.

Exercise 1.16. *Can any non-empty finite set S be given the structure of a group? What if S is countable? What if it is any set?*

Solution. In the case $|S| = n$, there is an obvious isomorphism to $\mathbb{Z}/n\mathbb{Z}$. If $|S| = \aleph_0$, there is an obvious isomorphism to $\mathbb{Z}$.

If S is a set of sets, the symmetric difference $A \Delta B = (A \setminus B) \cup (B \setminus A)$ gives a group structure. Thus in pure set theory, any set can be given the structure of a group.

What if the elements of S are not sets? ∎

1.2 Orders of Elements

Lemma 1.17. *Let G be a group. If $x^m = x^n = 1$, then $x^{(m,n)} = 1$.*

Proof. Bezout's identity. ∎

Corollary 1.18. *If $x^\alpha = 1$, then $\operatorname{ord} x \mid \alpha$.*

Proof. $(\operatorname{ord} x, \alpha) \leq \operatorname{ord} x$ by elementary number theory. But $x^{(\operatorname{ord} x, \alpha)} = 1$ (by the previous lemma) gives $(\operatorname{ord} x, \alpha) \geq \operatorname{ord} x$ by minimality of $\operatorname{ord} x$. Thus $(\operatorname{ord} x, \alpha) = \operatorname{ord} x$ so $\operatorname{ord} x \mid \alpha$. ∎

Lemma 1.19. *Let G be a group.*

(i) If $\operatorname{ord} x = \infty$, then $\operatorname{ord} x^k = \infty$ for every $k \in \mathbb{Z}^\times$.

(ii) If $\operatorname{ord} x = n < \infty$, then $\operatorname{ord} x^k = n/(n,k)$.

Proof. It suffices to prove the second statement. Let $y = x^k$ and $d = (n,k)$. Write $n = \tilde{n}d$ and $k = \widetilde{k}d$. Suppose $y^m = 1$. Then by the previous corollary, $n \mid mk$ and so $\tilde{n} \mid m\widetilde{k} \implies \tilde{n} \mid m$.

Thus $m \geq \tilde{n}$. But $y^{\tilde{n}} = x^{k\tilde{n}} = x^{n\widetilde{k}} = 1$. Thus $\operatorname{ord} y = \tilde{n}$. ∎

Lemma 1.20. *Let $H = \langle x \rangle$.*

(i) If $\operatorname{ord} x = \infty$, then H is generated by x^a iff $a = \pm 1$.

(ii) If $\operatorname{ord} x = n$, then H is generated by x^a iff $(a,n) = 1$.

Proof. For the first case, assume $H = \mathbb{Z}$ by isomorphism. $\mathbb{Z} = a\mathbb{Z} \implies \exists n \in \mathbb{Z}$ s.t. $an = 1$. Then $|a| = 1$. The converse is by inspection.

For the second, assume $H = \mathbb{Z}/n\mathbb{Z}$ by isomorphism. Let $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ be a generator. Then $\operatorname{ord}\bar{a} = n$. By the previous lemma, $\operatorname{ord}\bar{a} = n/(n,a)$ (since $\operatorname{ord}\bar{1} = n$). ■

Lecture 5. Monday August 12

1.3 Generation of groups

Lemma 1.21. *Let G be a group and let $a, b \in G$ commute. Let $\operatorname{ord} a = m$, $\operatorname{ord} b = n$, $\operatorname{lcm}(m,n) = \ell$. Then $\operatorname{ord} ab \mid \ell$. If $(m,n) = 1$, then $\operatorname{ord} ab = \ell$.*

Proof. $(ab)^\ell = a^\ell b^\ell = 1$.

Now suppose that $(m,n) = 1$. Let $d = \operatorname{ord} ab \implies d \mid \ell$. Now

$$\begin{aligned}(ab)^d = 1 &\implies a^d b^d = 1\\ &\implies a^d = b^{-d}.\end{aligned}$$

Raising to the power m gives $a^{dm} = 1 = b^{-dm}$. Thus $n \mid md \implies n \mid d$ (coprime). Similarly $m \mid d$. Thus $nm = \ell \mid d$. Together with $d \mid \ell$, we get $d = \ell$. ■

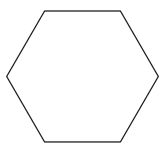
Examples.

- If $(a,b) \neq 1$, we can't say anything. For example, $b = a^{-1}$ gives $\operatorname{ord} ab = 1$.
- If $ab \neq ba$, things can go crazy. For example, $a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & 1/2 \\ 2 & 0 \end{pmatrix}$. Then $a^2 = b^2 = 1$ but $ab = \begin{pmatrix} 1/2 & 0 \\ 0 & 2 \end{pmatrix}$ has infinite order.

Definition 1.22 (Presentation)**.**

Definition 1.23 (the dihedral group)**.** For $n \geq 3$, the dihedral group D_{2n} is the group of rigid motions of a regular n-gon R_n in $\mathbb{R}^2$.

Remark. A "rigid motion" is an isoemtry: a distance preserving bijection. For example, reflections and rotations. Note how rigid motions being a bijection (when restricted to the n-gon) implies that only those isometries that preserve the n-gon are allowed.



Rigid motions in $\mathbb{R}^n$ are given by $x \mapsto Ax + b$ where $A \in O_n$, the set of orthogonal matrices in M_n.

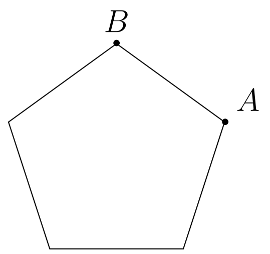
$$(A_1, b_1) \circ (A_2, b_2) = (A_1 A_2, A_1 b_2 + b_1).$$

$A_1 A_2 \in O_n$ so the product is closed. Associativity is inherited from function composition. The identity is $(1, 0)$ and the inverse of (A, b) is $(A^\top, -A^\top b)$.

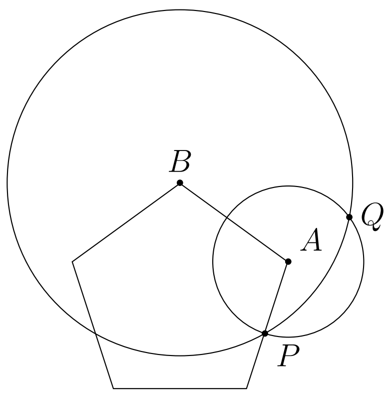
Lemma 1.24. *Every point P on R_n is determined, among all other points on R_n, by its distance from* any *two fixed adjacent vertices of R_n.*

That is, let A and B be adjacent vertices of R_n. Then for any $d_A, d_B \in \mathbb{R}^+$, there is at most one point P on R_n such that $d(P, A) = d_A$ and $d(P, B) = d_B$.

Proof. Look at the edge $\overline{AB}$.



Draw a circle of radius d_A around A and a circle of radius d_B around B. They intersect in at most two points, but they are on opposite sides of $\overline{AB}$. R_n is convex, so every point on R_n lies on one of only one side of $\overline{AB}$. Thus only one of these two points can lie on R_n.



■

Proposition 1.25. $|D_{2n}| = 2n$.

Proof. We first show that $|D_{2n}| \leq 2n$. Start with any two vertices A and B of R_n. Let $g \in D_{2n}$.

Claim. *g takes vertices to vertices.*

To see this, note that the vertices are special in that they are distinguised from all other points on R_n as follows:

> Let $P \in \mathbb{R}_n$ and $r > 0$ be small. We can find two points P_r' and P_r'' on R_n such that $d(P, P_r') = d(P, P_r'') = r$. If P is *not* a vertex, then $d(P_r', P_r'') = 2r$. If P *is* a vertex, then $d(P_r', P_r'') < 2r$.

Thus we can distinguish between P being a vertex or not solely by the distance function. Since g is an isometry (even Lipschitz), this property is preserved. Thus g takes vertices to vertices.

Claim. *g preserves adjacency of vertices.*

Fix a vertex A on R_n. Then $d(P, A)$ for a vertex distinct from A is minimized when P is adjacent to A. Since g preserves distances, g must take adjacent vertices to adjacent vertices.

Combining these two claims, we have proven that for any $P \in R_n$, $g(P)$ is uniquely determined by its distance from $g(A)$ and $g(B)$, where A and B are any two adjacent vertices. Thus g is determined by $g(A)$ and $g(B)$.

By the first claim, there are n possible choices for $g(A)$. By the second claim, there are 2 possible choices for $g(B)$. Thus there are at most $2n$ possible g's.

Finally, we can produce $2n$ distinct elements as follows.

- Consider the n rotations: rotate by $2\pi k/n$ for $k \in n$.
- The n reflections:
  - For odd n, reflect over the line through a vertex and the midpoint of the opposite edge.
  - For even n, reflect over the line through two opposite vertices or through two opposite midpoints.

Each reflection fixes exactly two points. Any non-trivial rotation fixes no points. Thus the $2n$ elements are distinct. ■

Notation. Let r denote the counter-clockwise rotation by $2\pi/n$ and let s denote the reflection over the line through some fixed vertex V_0.

Then $r^n = s^2 = 1$.

Observe that $\{1, r, r^2, \ldots, r^{n-1}\}$ gives all the rotations in D_{2n}.

Lemma 1.26. *All reflections in D_{2n} are given by $\{s, rs, r^2 s, \ldots, r^{n-1} s\}$.*

Proof. All of these elements are distinct, since $r^k \neq 1$ for $0 < k < n$. None of these elements are rotations, since if $r^k s = r^m$ for some $k, m \in n$, then $s = r^{m-k}$, which is a contradiction. ■

Theorem 1.27. $|D_{2n}| = 2n$ *and* $D_{2n} = \{1, r, \ldots, r^{n-1}, s, rs, \ldots, r^{n-1}s\}$.

Proposition 1.28. *In* D_{2n}, $sr = r^{-1}s$.

Proof. From lemma 1.26, we know that rs is a reflection. Thus $(rs)(rs) = 1$, which immediately gives $sr = r^{-1}s$. ∎

Next lecture: $D_{2n} = \langle r, s \mid r^n = s^2 = 1, sr = r^{-1}s\rangle$.

Lecture 7. Monday August 19

Definition 1.29 (Action)**.** We say that a group $(G, *)$ *acts* on a set X if there is a map $\theta\colon G \times X \to X$, such that if we write $\theta(g, x)$ as $g \cdot x$ then for every $g_1, g_2 \in G$ and $x \in X$,

(i) $g_1 \cdot (g_2 \cdot x) = (g_1 * g_2) \cdot x$;

(ii) $1_G \cdot x = x$.

We say that $x \in X$ is *moved* by $g \in G$ to $g \cdot x$.

Examples.

- The trivial action $(g, x) \mapsto x$.
- The interesting action of $\mathrm{GL}_n(F)$ on F^n (columns) by matrix-vector multiplication.
- The left regular action of G on itself. $(g, x) \mapsto gx$
- The conjugating action of G on itself. $(g, x) \mapsto gxg^{-1}$

Remark. Given a right action of G on X, we can define a left action as

$$g \cdot x = x \cdot g^{-1}.$$

It thus suffices to study left actions.

Proposition 1.30. *The set of actions of* G *on* X *is isomorphic to* $\hom(G, S_X)$*. The associated map is*

$$\theta \mapsto (g \mapsto (x \mapsto \theta(g, x))).$$

Proof. For an action $\cdot$, define for each $g \in G$ the map $\sigma_g\colon X \to X$ by $\sigma_g(x) = g \cdot x$.

Notice that σ_g is a bijection, since

$$(\sigma_{g^{-1}} \circ \sigma_g)(x) = g^{-1} \cdot (g \cdot x) = x.$$

Thus $g \mapsto \sigma_g$ is a homomorphism from G to S_X.

$\hom(G, S_X)$ is a group under composition.

For a homomorphism $\sigma\colon G \to S_X$, define the group action

$$g \cdot x = \sigma_g(x).$$ ∎

Remark. This is essentially a juggling between the set of functions $(A, B) \to C$ and the set of curried functions $A \to B \to C$.

Definition 1.31 (Orbits and stabilizers)**.** Let G act on X. Then for $x \in X$, we define the *orbit* of x as

$$\mathcal{O}_x = Gx = \{gx \mid g \in G\} \subseteq X,$$

and the *stabilizer* of x as

$$\mathrm{Stab}_x = G_x = \{g \in G \mid g \cdot x = x\} \leq G.$$

We say that the action is *faithful* if

$$\bigcap_{x \in X} G_x = \{1\}.$$

Examples.

- For the trivial action, $\mathcal{O}_x = \{x\}$ and $G_x = G$.
- For the action of $\mathrm{GL}_n(\mathbb{R})$ on $\mathbb{R}^n$, the orbit of x is

  $$\mathcal{O}_x = \begin{cases} \{0\} & \text{if } x = 0, \\ \mathbb{R}^n \setminus \{0\} & \text{if } x \neq 0. \end{cases}$$

  To see this, **challenge:** prove by induction.

  The stabilizer of x is all matrices which have x as an eigenvector with eigenvalue 1.
- For the left regular action of G on itself, $\mathcal{O}_x = G$ and $G_x = \{1\}$.
- For the conjugating action of G on itself, $\mathcal{O}_x = \{gxg^{-1} \mid g \in G\}$ and $G_x = \{g \in G \mid gxg^{-1} = x\}$. There is no simple description of either.

Definition 1.32 (Centralizer and center)**.** For $x \in G$, the *centralizer* of x is

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

The *center* of G is

$$Z_G = \bigcap_{x \in G} C_G(x) = \{g \in G \mid \forall x \in G, gx = xg\}.$$

Example. $Z_{\mathrm{GL}_n(\mathbb{R})} = \{\lambda I \mid \lambda \in \mathbb{R}^\times\}$.

Definition 1.33. Let $H \leq G$. Define the relation $\sim$ on G by $x \sim y$ if $x^{-1}y \in H$.

Lemma 1.34. $\sim$ *is an equivalence relation.*

Proof. Reflexive since $1 \in H$. Symmetric since H is closed under inverses, so

$$x^{-1}y \in H \implies (x^{-1}y)^{-1} = y^{-1}x \in H.$$

Transitive by closure under products,

$$x^{-1}y, y^{-1}z \in H \implies x^{-1}yy^{-1}z = x^{-1}z \in H. \qquad \blacksquare$$

Notice that the equivalence class of $x \in G$ is

$$[x] = \{y \in G \mid yx^{-1} \in H\} = Hx.$$

Definition 1.35 (Coset)**.** Let $H \leq G$. The *left coset* of $x \in G$ is

$$xH = \{xh \mid h \in H\}.$$

The *right coset* of $x \in G$ is

$$Hx = \{hx \mid h \in H\}.$$

We will only write left cosets, but the same results hold for right cosets.

Corollary 1.36. *$xH \cap yH \neq \varnothing$ iff $x \sim y$.*

Definition 1.37. The set of (left) cosets of H in G is denoted by G/H.

Examples.

- G acts on the power set 2^G by $g \cdot A = gA = \{ga \mid a \in A\}$.
- Restricting this is useful. Let $H \leq G$. Then G acts on the set of left cosets G/H by $g \cdot xH = (gx)H$.
- If one wishes to define a left action on the set of *right* cosets G/H, one can define
$$g \cdot Hx = Hxg^{-1}.$$
$g \cdot Hx = Hxg$ will not obey associativity. $g \cdot Hx = Hgx$ is not necessarily well-defined.

Question: When and how can one make G/H naturally a group?

We would want $(xH)(yH) = \{xh_1yh_2 \mid h_1, h_2 \in H\}$ to be equal to $(xy)H$. This would require for all $h_1, h_2 \in H$ that $xh_1yh_2 = xyh_3$ for some $h_3 \in H$.

If $hy = yh$ for all $y \in G$ and $h \in H$, then $xh_1yh_2 = (xy)h_1h_2 \in (xy)H$.

Example. Let $\varphi\colon G \to H$ be a group homomorphism. Let $K = \ker\varphi = \{g \in G \mid \varphi(g) = 1\}$. Then G/K is a group under the operation

$$(xK) \cdot (yK) = (xy)K.$$

This is well-defined, since $xK = x'K$ iff $\varphi(x) = \varphi(x')$. Thus whenever $xK = x'K$ and $yK = y'K$, we have

$$\varphi(x'y') = \varphi(x')\varphi(y') = \varphi(x)\varphi(y) = \varphi(xy),$$

so that $(xy)K = (x'y')K$.

Obviously this defines a group operation on G/K. Associativity, identity, inverses are borrowed from G.

Note that for any $x \nsim y$, $xK \neq yK$. Thus $G = \bigsqcup_{xH \in G/H} xH$.

Lecture 8. Wednesday August 21

Theorem 1.38 (orbit-stabilizer theorem)**.** *Let G act on a set X. Then G/G_x and $\mathcal{O}_x$ are in natural bijection (as sets) via the map $gG_x \mapsto gx$.*

Proof. We first show that the map is well-defined.

$$\begin{aligned} gG_x = g'G_x &\iff g^{-1}g' \in G_x \\ &\iff g^{-1}g'x = x \\ &\iff gx = g'x \end{aligned}$$

This also shows that the map is injective. Surjection is simply since for any $gx \in \mathcal{O}_x$ (everything in the orbit is of this form), we have $gG_x \mapsto gx$. ■

Theorem 1.39 (Lagrange's theorem)**.** *If G is finite and $H \leq G$, then $|G| = |H| \cdot |G/H|$.*

Proof. First note that each coset of H has the same size as H, since $xh \mapsto h$ is a bijection. No two distinct cosets overlap, since whenever $xh = yh'$, $y^{-1}x = h'h^{-1} \in H$, so $xH = yH$.

Finally $G = \bigsqcup_{S \in G/H} S$ gives

$$|G| = |H| \cdot |G/H|.$$ ■

Corollary 1.40. *Let $x \in G$. Then* $\operatorname{ord} x \mid |G|$.

Proof. $\langle x \rangle$ is a subgroup of G of order $\operatorname{ord} x$. ■

Corollary 1.41 (Cauchy's theorem)**.** *Let G be a finite group and $p \mid |G|$ be a prime. Then G has an element of order p.*

We will be largely relying on group actions, so we will attempt to prove this using group actions.

Lemma 1.42. *Let G be a p-group, i.e. $|G| = p^m$ for some $m \in \mathbb{Z}^+$, acting on a finite set X. Then the set of all fixed points*

$$X^G = \{x \in X \mid \forall g \in G, g \cdot x = x\}$$

satisfies $|X^G| \equiv |X| \pmod p$.

Proof. Notice that $x \in X^G \iff \mathcal{O}_x = \{x\}$. By the orbit-stabilizer theorem and Lagrange's theorem, we have

$$|\mathcal{O}_x| = \frac{|G|}{|G_x|}.$$

Whenever $z \notin X^G$, $|\mathcal{O}_x| > 1$ so it is a power of p.

Now since orbits are disjoint,

$$|X| = |X^G| + \sum_{x \notin X^G} |\mathcal{O}_x|$$

gives the result. ∎

Proof of Cauchy's theorem. Let $X = \{\underline{x} \in G^p \mid x_1 \cdots x_p = 1_G\}$. Clearly $|X| = |G|^{p-1}$, since we can choose $x_1, \ldots, x_{p-1}$ freely and then x_p is determined.

Let $\mathbb{Z}/p\mathbb{Z}$ act on X by cyclic permutations.

$$\bar{i} \cdot (x_1, \ldots, x_p) := (x_{i+1}, \ldots, x_p, x_1, \ldots, x_i)$$

Inverses commute, so the product is still identity. We have to check that this is a group action.

- $\bar{0} \cdot (x_0, \ldots, x_{p-1}) = (x_0, \ldots, x_{p-1})$.
- $$\begin{aligned} \bar{i} \cdot (\bar{j} \cdot (x_0, \ldots, x_{p-1})) &= \bar{i} \cdot (x_{j \bmod p}, \ldots, x_{p-1+j \bmod p}) \\ &= (x_{i+j \bmod p}, \ldots, x_{p-1+i+j \bmod p}) \\ &= \overline{i+j} \cdot (x_0, \ldots, x_{p-1}). \end{aligned}$$

Notice that $|X^{\mathbb{Z}/p\mathbb{Z}}| \neq 0$, since $(1, 1, \ldots, 1) \in X^{\mathbb{Z}/p\mathbb{Z}}$. Thus $|X^{\mathbb{Z}/p\mathbb{Z}}| \geq p$. Let $(a, a, \ldots, a) \in X^{\mathbb{Z}/p\mathbb{Z}}$ where $a \neq 1$. Then $a^p = 1$, so $\operatorname{ord} x = p$. ∎

Corollary 1.43. *Every finite group is a subgroup of S_n for some n.*

Proof. Look at the left regular action of G on itself $(g, x) \mapsto gx$. This is obviously faithful. Consider the homomorphism $\sigma\colon G \to S(G)$

$$\sigma_g = x \mapsto gx.$$

Since the kernel is just $\{1\}$, this is an embedding. ■

Examples.

- S_n acts on $X = [n]$ by permuting the elements.
- S_n acts on $\mathbb{R}[T_1, \ldots, T_n]$, the polynomial ring in n variables, by permuting the variables.

  $$(\sigma \cdot f)(T_1, \ldots, T_n) = f(T_{\sigma(1)}, \ldots, T_{\sigma(n)}).$$

  The identity permutation fixes all polynomials. For associativity,

  $$\begin{aligned}(\sigma \cdot (\tau \cdot f))(T_1, \ldots, T_n) &= (\sigma \cdot f)(T_{\tau(1)}, \ldots, T_{\tau(n)}) \\ &= f(T_{\sigma(\tau(1))}, \ldots, T_{\sigma(\tau(n))}) \\ &= (\sigma\tau) \cdot f(T_1, \ldots, T_n).\end{aligned}$$

  Polynomials that are fixed by all permutations are called *symmetric polynomials*. See the fundamental theorem of symmetric polynomials for an interesting result.

- S_n acts on $\mathbb{R}^n$ by permuting the coordinates.

  $$\sigma \cdot (x_1, \ldots, x_n) = (x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

  Or does it? Consider $n = 3$, $\sigma = (12)$ and $\tau = (23)$. Then $\sigma\tau = (123)$, but

  $$\sigma \cdot (\tau \cdot (v_1, v_2, v_3)) = \sigma \cdot (v_1, v_3, v_2) = (v_3, v_1, v_2),$$

  but $(\sigma\tau) \cdot (v_1, v_2, v_3) = (v_{\sigma\tau(1)}, v_{\sigma\tau(2)}, v_{\sigma\tau(3)}) = (v_2, v_3, v_1)$.

  The correct definition is to invert the permutation.

  $$\sigma \cdot (x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)}).$$

  Let $v = (v_1, \ldots, v_n)$ and $w = \sigma \cdot v = (v_{\sigma^{-1}(1)}, \ldots, v_{\sigma^{-1}(n)})$. For each i, $w_i = v_{\sigma^{-1}(i)}$. Then

  $$\begin{aligned}\tau \cdot w &= (w_{\tau^{-1}(1)}, \ldots, w_{\tau^{-1}(n)}) \\ &= (v_{\sigma^{-1}(\tau^{-1}(1))}, \ldots, v_{\sigma^{-1}(\tau^{-1}(n))})\end{aligned}$$

  Thus $\tau(\sigma v) = (\sigma\tau)v$.

We continue with examples.

Lecture 9.
Monday
August 26

Examples.

- Let G act on X. Let S be a set. Consider the set $Fn(X,S) = S^X = \{\text{all function from } X \text{ to } S\}$ Define the group action G on S^X by
$$(g \cdot f)(x) \coloneqq f(g \cdot x).$$

1.4 Normal subgroups

Proposition 1.44. *Let $N \leq G$. Consider the set of left cosets G/N with the operation $(uN) \cdot (vN) = (uv)N$.*

(i) The above operation is well-defined.

(ii) $gng^{-1} \in N$ for all $g \in G$ and $n \in N$.

(iii) $gNg^{-1} = N$ for all $g \in G$.

If the operation is well-defined, then G/N is a group with identity $1N$ and inverse $(gN)^{-1} = g^{-1}N$.

Proof. First notice that (ii) is equivalent to $gNg^{-1} \subseteq N$ for all $g \in G$. Thus (ii) immediately follows from (iii). Conversely, if (ii) holds, then $gNg^{-1} \subseteq N$ and

Recall that $uN = vN$ if and only if $u^{-1}v \in N$.

Suppoe (i) holds. Let $g \in G$ and $n \in N$. Note that $nN = 1N$, so $gnN = gN$, which gives $gng^{-1} \in N$.

Suppose (ii) holds. Let $u_1N = u_2N$ and $v_1N = v_2N$. Let $u_2 = u_1m$ and $v_2 = v_1n$ for some $m, n \in N$. Then $u_2v_2 = u_1mv_1n = u_1v_1(v_1^{-1})mv_1n \in u_1v_1N$ since $v_1^{-1}mv_1 \in N$. ■

Definition 1.45 (normal subgroup)**.** A subgroup $N \leq G$ is *normal* if $gNg^{-1} = N$ for all $g \in G$. We write $N \trianglelefteq G$.

Definition 1.46 (normalizer)**.** Let $S \subseteq G$. The *normalizer* of S in G is the set
$$N_G(S) = \{g \in G \mid gSg^{-1} = S\}.$$

Exercise 1.47 (self)**.** *When is the normalizer*

- *a subgroup?*
- *normal?*

Proof. Let S be any subset of G. Note that $1 \in N_G(S)$. Suppose $g, h \in N_G(S)$. That is, $gSg^{-1} = S$ and $hSh^{-1} = S$. Then
$$(gh)S(gh)^{-1} = g(hSh^{-1})g^{-1} = gSg^{-1} = S,$$
so $N_G(S)$ is closed under products.

However, closure under inverses is not guaranteed. Consider ■

Exercise 1.48. *The following are equivalent.*

(i) $N \trianglelefteq G$.

(ii) $N_G(N) = G$.

(iii) $gN = Ng$ *for all* $g \in G$.

(iv) G/N *is a group.*

Proof. ■

Examples.

- Consider $\mathrm{SL}_n(\mathbb{R}) \leq \mathrm{GL}_n(\mathbb{R})$. Since $\det(gng^{-1}) = \det(n)$, we get $\mathrm{SL}_n(\mathbb{R}) \trianglelefteq \mathrm{GL}_n(\mathbb{R})$.

Theorem 1.49. $N \trianglelefteq G$ *if and only if* N *is the kernel of some homomorphism from* G *to some group.*

Proof. Suppose $N = \ker \varphi$, where $\varphi \colon G \to H$ is a homomorphism. Let $g \in G$ and $n \in N$. Then $\varphi(gng^{-1}) = \varphi(g)\varphi(n)\varphi(g)^{-1} = 1$, so $gng^{-1} \in N$.

Suppose $N \trianglelefteq G$. Consider the map $\pi \colon G \to G/N$ given by $\pi(g) = gN$. This is a homomorphism since $\pi(1) = 1N$ is the identity, and

$$\pi(xy) = (xy)N = xN \cdot yN = \pi(x)\pi(y).$$

Moreover, $\ker(\pi) = N$ since $\pi(x) = 1N \iff xN = 1N \iff x \in N$. ■

1.5 Products

We have already defined the direct product of two groups in **??**.

Definition 1.50 (direct product)**.** Given any index set I and for each $i \in I$ a group A_i, we can give a group structure to the direct product $\prod_{i \in I} A_i$ by defining the operation componentwise.

Definition 1.51 (direct sum)**.** Given any index set I and for each $i \in I$ a group A_i, we define the *direct sum* of the groups A_i as

$$\bigoplus_{i \in I} A_i = \left\{ (a_i) \in \prod_{i \in I} A_i \;\middle|\; \text{all but finitely many } a_i \text{ are } 1 \right\}.$$

This is a group since the union of two finite sets (the support) is finite.

Exercise 1.52. *Suppose* $H, K \leq G$. *When is* $HK \leq G$? *When is* $HK \cong H \times K$?

Proof.

Lecture 9

Claim. *$HK \leq G$ if and only if $HK = KH$.*

Subproof. Suppose $HK \leq G$. Note that $1 \in H, K$, so $H = H1, K = 1K \subseteq HK$. Thus for any $k \in K$, $h \in H$, $kh \in HK$ by closure under products. □

Let H, K intersect only in $\{1\}$. Suppose $hk = kh$ for all $h \in H$ and $k \in K$. Then the map

$$\begin{aligned} \theta\colon H \times K &\to HK \\ (h, k) &\mapsto hk \end{aligned}$$

is an isomorphism. It is a homomorphism, since $\theta(1, 1) = 1$ and

$$\theta(h_1, k_1)\theta(h_2, k_2) = h_1k_1h_2k_2 = h_1h_2k_1k_2 = \theta(h_1h_2, k_1k_2).$$

Surjectivity is obvious. Injectivity is since

$$\begin{aligned} \theta(h_1, k_1) = \theta(h_2, k_2) &\implies h_1k_1 = h_2k_2 \\ &\implies h_1h_2^{-1} = k_1k_2^{-1} \\ &\implies h_1h_2^{-1}, k_1k_2^{-1} \in H \cap K \\ &\implies h_1 = h_2 \text{ and } k_1 = k_2. \end{aligned}$$ ■

Lecture 10. Wednesday August 28

Remark. Suppose $H_1, \ldots, H_m \leq G$ and H_{i+1} is orthogonal to $H_1H_2 \ldots H_i$ for all i. Then $H_1 \times \cdots \times H_m \leq G$ and is isomorphic to $H_1H_2 \ldots H_m$.

Lemma 1.53. *Let $H \leq G$. Then the left and right cosets of H in G are in bijection.*

Proof. Let $I \subseteq G$ be a set of representatives for the left cosets of H in G. Then

$$\begin{aligned} G &= \bigsqcup_{x \in I} xH \\ \implies G = G^{-1} &= \bigcup_{x \in I} H^{-1}x^{-1} \\ &= \bigcup_{x \in I} Hx^{-1}. \end{aligned}$$

Note that $Hx^{-1} = Hy^{-1} \iff x^{-1}y \in H \iff xH = yH$. Thus the union is still disjoint, and I^{-1} is a set of representatives for the right cosets. ■

Definition 1.54 (index)**.** Let $H \leq G$, Then $(G : H) = \#(G/H)$ is the *index* of H in G if G/H is finite. Otherwise, we say $(G : H) = \infty$.

Proposition 1.55. *Let $K \leq H \leq G$. and $G = \bigsqcup_{x \in I} xH$. Let $H = \bigsqcup_{y \in J} yK$ Then $G = \bigsqcup_{x \in I, y \in J} xyK$.*

Proof.

$$G = \bigsqcup_{x\in I} xH = \bigsqcup_{x\in I}\left(x\bigsqcup_{y\in J} yK\right) = \bigcup_{x\in I, y\in J} xyK.$$

We need to check that the union is disjoint.

$$\begin{aligned} xyK = x_1y_1K &\implies y^{-1}x^{-1}x_1y_1 \in K \\ &\implies x^{-1}x_1 \in yKy_1^{-1} \subseteq HKH^{-1} \\ &\implies x^{-1}x_1 \in H \\ &\implies xH = x_1H. \end{aligned}$$

This contradicts the disjointness of $\{xH\}_{x\in I}$. Thus

$$G = \bigsqcup_{x\in I, y\in J} xyK.$$

■

Corollary 1.56 (multiplicity of the index)**.** *Let $K \le H \le G$. Then $(G : K) = (G : H)(H : K)$, with the understanding that ∞ is absorbing.*

Example. $6\mathbb{Z} \le 2\mathbb{Z} \le \mathbb{Z}$.

$$2\mathbb{Z} = (0 + 6\mathbb{Z})\bigsqcup(2 + 6\mathbb{Z})\bigsqcup(4 + 6\mathbb{Z})$$

so $(2\mathbb{Z} : 6\mathbb{Z}) = 3$.

$$\mathbb{Z} = (0 + 2\mathbb{Z})\bigsqcup(1 + 2\mathbb{Z})$$

so $(\mathbb{Z} : 2\mathbb{Z}) = 2$. Similarly $(\mathbb{Z} : 6\mathbb{Z}) = 6$ and sure enough, $(\mathbb{Z} : 6\mathbb{Z}) = (\mathbb{Z} : 2\mathbb{Z})(2\mathbb{Z} : 6\mathbb{Z})$.

1.6 Isomorphism theorems

Theorem 1.57 (first isomorphism theorem)**.** *Let $\varphi\colon G \to H$ be a homomorphism. Let $K = \ker(\varphi)$. Then φ induces an isomorphism $\varphi_*\colon G/K \to \operatorname{Im}(\varphi)$ given by $\varphi_*(gK) = \varphi(g)$.*

Proof. This is well-defined since $gK = g'K \iff g^{-1}g' \in K \iff \varphi(g) = \varphi(g')$. This also shows injectivity.

φ_* is clearly a homomorphism. It is surjective since for any $y = \varphi(g) \in \operatorname{Im}(\varphi)$, $y = \varphi_*(gK)$. ■

Theorem 1.58 (second isomorphism theorem)**.** *Let $A, B \le G$. Suppose $A \subseteq N_G(B)$. Then $A \cap B \trianglelefteq A$ and*

$$AB/B \cong A/(A \cap B).$$

Proof. First note that AB is a group by exercise 1.52. Moreover, $B \trianglelefteq AB$ since $abB = aBb = Bab$ for each $ab \in AB$. This will also follow independently from the later half of this proof.

Moreover, $A \cap B \trianglelefteq A$ since for each $a \in A$, $a(A \cap B)a^{-1} = aAa^{-1} \cap aBa^{-1} = A \cap B$. Define

$$\begin{aligned} \varphi\colon AB &\to A/(A \cap B) \\ ab &\mapsto a(A \cap B) \end{aligned}$$

This is well-defined since $ab = a'b' \implies a^{-1}a' \in A \cap B$, so $a(A \cap B) = a'(A \cap B)$. It is a homomorphism since

$$a_1b_1a_2b_2 = a_1(a_2b')b_2 = a_1a_2b'b_2.$$

for some $b' \in B$, so

$$\varphi(a_1b_1a_2b_2) = a_1a_2(A \cap B) = a_1(A \cap B) \cdot a_2(A \cap B) = \varphi(a_1b_1)\varphi(a_2b_2).$$

- The kernel is $(A \cap B)B = B$. (Note that this proves $B \trianglelefteq AB$.)
- The image is all of $A/(A \cap B)$.

By the first isomorphism theorem, $AB/B \cong A/(A \cap B)$. ■