Honors Algebra

MATH-SHU 348

Yao Xiao

Fall 2023

This course is taught by Professor Nadir Matringe.

Contents

8/28 Lecture

1 Group Theory

1.1 Permutations of a Set

Definition 1.1. Let X be a set. $f : X \to X$ is a **bijection** if $\forall y \in X$, there exists a unique $x \in X$, such that $f(x) = y$.

Remark 1.2. We observe that $f : X \to X$ is bijective if and only if there exists $g : X \to X$, such that $f \circ g = g \circ f = \mathrm{Id}_X$. Such a mapping g is unique when it exists, denoted as f^{-1}, the inverse mapping of f. We commonly write $\mathfrak{S}(X)$ or $\mathfrak{S}_X$ as the set of bijections from X to X, namely the set of **permutations** of X. Specifically, $\mathfrak{S}_n := \mathfrak{S}(\{1, \ldots, n\})$.

Definition 1.3. Let G be a set, and we say that $\cdot$ is a **binary operation** on G if $\forall x, y \in G$, we have that $x \cdot y \in G$.

1.2 Groups

Definition 1.4. A couple $(G, \cdot)$, where G is a set and $\cdot$ is a binary operation on G, is called a **group** if the operation $\cdot$ satisfies:

(1) Associativity: $\forall g, h, f \in G$, one has $(g \cdot h) \cdot f = g \cdot (h \cdot f)$.

(2) Identity/neutral element: $\exists e \in G$, such that $e \cdot g = g \cdot e = g$, $\forall g \in G$.

(3) Inverse: $\forall g \in G$, $\exists h \in G$, such that $g \cdot h = h \cdot g = e$, *i.e.*, every element in G has an inverse in G.

Remark 1.5. Suppose $(G, \cdot)$ is a group with neutral element e and e', we can see that $e = e \cdot e' = e'$, so that the neutral element e is unique. We denote it by e_G or $\mathbb{1}_G$. Now take $g \in G$ and suppose h and h' are both inverse of g. We can show that

$$h = h \cdot e_G = h \cdot (g \cdot h') = h \cdot g \cdot h' = (h \cdot g) \cdot h' = e_G \cdot h' = h', \tag{1}$$

and thus the inverse is also unique, denoted as $h = g^{-1}$. When $(G, \cdot)$ is a group, the group operation $\cdot$ can also be called as group law or the multiplication on G.

Theorem 1.6. (1) Let $(G, \cdot)$ be a group and $g \in G$, then $(g^{-1})^{-1} = g$.

(2) Take $g, h \in G$ where $(G, \cdot)$ is a group, then $(g \cdot h)^{-1} = h^{-1} \cdot g^{-1}$.

Proof. (1) We can easily see that

$$g \cdot g^{-1} = g^{-1} \cdot g = e_G \implies (g^{-1})^{-1} = g. \tag{2}$$

(2) We can easily see that

$$(h^{-1} \cdot g^{-1}) \cdot (g \cdot h) = h^{-1} \cdot (g^{-1} \cdot g) \cdot h = h^{-1} \cdot e_G \cdot h = h^{-1} \cdot h = e_G, \tag{3}$$

so we can conclude that $(h^{-1} \cdot g^{-1}) = (g \cdot h)^{-1}$.

□

Example 1.7. (1) $(\mathbb{Z}, +)$ is a group with neutral element 0, and inverse "n^{-1}" $= -n$.

(2) $(\mathbb{N}, +)$ is not a group, because $1 \in \mathbb{N}$ does not have an inverse in $\mathbb{N}$ for $+$.

(3) $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}, +)$ are groups.

(4) $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{Q}^*, \times)$ are groups, where $K^* = K \setminus \{0\}$. We explicitly show that $(\mathbb{Q}^*, \times)$ is a group. To see this, take arbitrary elements $\frac{a}{b}$ and $\frac{c}{d}$ in $\mathbb{Q}^*$ where $a, b, c, d \in \mathbb{Z}^*$. Then $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \in \mathbb{Q}^*$. Also, $\times$ is clearly associative, 1 is the neutral element, and there exists the unique inverse element $\frac{b}{a} \in \mathbb{Q}^*$ for any $\frac{a}{b} \in \mathbb{Q}^*$.

(5) $(\mathbb{Z}^*, \times)$ is not a group, since 2 does not have an inverse in $\mathbb{Z}^*$.

(6) Let X be a set, then $(\mathfrak{S}(X), \circ)$ is a group. Indeed, $\circ$ satisfies associativity, the neutral element is Id_X, and the inverse of a mapping f is f^{-1}. It suffices to validate that $\circ$ is a binary operation. Indeed, we have that

$$(f \circ g) \circ (g^{-1} \circ f^{-1}) = f \circ (g \circ g^{-1}) \circ f^{-1} = f \circ f^{-1} = \mathrm{Id}_X, \tag{4}$$

and similarly $(g^{-1} \circ f^{-1}) \circ (f \circ g) = \mathrm{Id}_X$. This means that $f \circ g$ is a bijection when f and g are both bijections, and thus $\circ$ is a binary operator.

(7) $(\mathfrak{M}_{n,m}(K), +)$ is a group, $K = \mathbb{R}, \mathbb{C}, \mathbb{Q}$.

(8) Let $GL_n(K) := \{\text{invertible matrices in } \mathfrak{M}_n(K)\}$, then $(GL_n(K), \times)$ is a group, $K = \mathbb{R}, \mathbb{C}, \mathbb{Q}$.

Definition 1.8. A group $(G, \cdot)$ is called **commutative** or **abelian** if $\forall g, h \in G$, $g \cdot h = h \cdot g$.

Example 1.9. (1) $(\mathbb{Z}, +)$, $(\mathbb{R}^*, \times)$, $(\mathbb{C}^*, \times)$, $(\mathbb{Q}^*, \times)$ are abelian groups.

(2) $(\mathfrak{M}_{n,m}(K), +)$ is an abelian group, $K = \mathbb{R}, \mathbb{C}, \mathbb{Q}$.

(3) $(GL_n(K), \times)$ is not commutative for $n \geq 2$, $K = \mathbb{R}, \mathbb{C}, \mathbb{Q}$. Clearly high-dimensional matrix multiplication is not commutative.

(4) $(\mathfrak{S}(X), \circ)$ is not commutative for $|X| \geq 3$.

8/30 Lecture

1.3 Subgroups

Definition 1.10. Let $(G, \cdot)$ be a group and let $H \subseteq G$. Then H is a **subgroup** of G if:

(1) $e_G \in H$.

(2) $\forall x, y \in H$, $x \cdot y \in H$.

(3) $\forall x \in H$, $x^{-1} \in H$.

Often, one writes G instead of $(G, \cdot_G)$ and H instead of $(H, \cdot_H)$. We denote the subgroup relation by $H \leq G$.

Remark 1.11. We can easily observe the following. If $(G, \cdot_G)$ is a group and $H \leq G$, then $(H, \cdot_G)$ is a group, $e_H = e_G$, and the inverse of an element in H is equal to its inverse in G. These follow trivially from the definition, the uniqueness of neutral element, and the uniqueness of inverse.

Example 1.12. (1) $(\mathbb{R}, +) \leq (\mathbb{C}, +)$. Indeed, we can check that $0 \in \mathbb{R}$ where 0 is the neutral element of $(\mathbb{C}, +)$. Also, $\forall x, y \in \mathbb{R}$, $x + y \in \mathbb{R}$ and $-x \in \mathbb{R}$.

(2) $\mathbb{C}^*$ is not a subgroup of $\mathbb{C}$, since the neutral element of $\mathbb{C}$, 0, is not in $\mathbb{C}^*$.

(3) For $a \in \mathbb{Z}$, $a\mathbb{Z} := \{ak;\ k \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

(4) For any group G, $\{e_G\}$ and G are clearly subgroups of G. $\{e_G\}$ is called the trivial subgroup of G.

Example 1.13. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, and let $GL_n(K) = \{\text{invertible matrices in } \mathfrak{M}_n(K)\}$. Set

$$SL_n(K) = \{M \in GL_n(K);\ \det(H) = 1\}, \tag{5}$$

$$O_n(K) = \left\{M \in GL_n(K);\ M^\top M = I_n\right\}. \tag{6}$$

(1) Show that $SL_n(K) \leq GL_n(K)$. Indeed, the neutral element of $GL_n(K)$ is the n-dimensional identity matrix I_n. Clearly $\det(I_n) = 1$, so that $I_n \in SL_n(K)$. Moreover, taking arbitrary $A, B \in SL_n(K)$, we have that $\det(AB) = \det(A)\det(B) = 1$ and $\det(A^{-1}) = (\det(A))^{-1} = 1$, so that $AB, A^{-1} \in SL_n(K)$. The proof is done.

(2) Show that $O_n(K) \leq SL_n(K)$. Indeed, we have checked that the neutral element of $SL_n(K)$ is I_n, and clearly $I_n^\top I_n = I_n$. Therefore, $I_n \in O_n(K)$. Moreover, taking arbitrary $A, B \in O_n(K)$, we have that $(AB)^\top AB = B^\top (A^\top A)B = B^\top B = I_n$. Since $A^\top A = I_n$, we have that $A^{-1} = A^\top$. Taking transpose on both sides, we can see that $(A^{-1})^\top = (A^\top)^\top = A$. By multiplying A^{-1} from the right on both sides, we can conclude that $(A^{-1})^\top A^{-1} = AA^{-1} = I_n$. The proof is done.

Lemma 1.14. Let $(G, \cdot)$ be a group. If $K \leq G$ and $H \leq K$, then $H \leq G$.

Proof. We have observed that the neutral element of a group and its subgroup is the same, so that $e_H = e_K = e_G \in H$. Now take arbitrary $x, y \in H$, we have that $x \cdot y \in H$ and $x^{-1} \in H$ because $H \leq K$ (for the inverse it is important to also note that the inverse of x in H and G are equal). Therefore it follows that $H \leq G$, and the proof is complete. □

Lemma 1.15. If $K \leq G$, $H \leq G$, and $H \subseteq K$, then $H \leq K$.

Proof. Similar to above, we can see that $e_H = e_G = e_K \in H$. Take arbitrary $x, y \in H$, then $x \cdot y \in H$ and $x^{-1} \in H$ because $H \leq G$. Therefore it follows that $H \leq K$, and the proof is complete. □

Proposition 1.16. Let $(G, \cdot)$ be a group and $H_i \leq G$, $\forall i \in I$, where I is a (possibly infinite) indexing set. Then $\bigcap_{i \in I} H_i \leq G$.

Proof. We have that $e_G \in H_i$, $\forall i \in I$, so that $e_G \in \bigcap_{i \in I} H_i$. Moreover, taking arbitrary $x, y \in \bigcap_{i \in I} H_i$, $x, y \in H_i$, $\forall i \in I$. Then $x \cdot y, x^{-1} \in H_i$, $\forall i \in I$. This implies that $x \cdot y, x^{-1} \in \bigcap_{i \in I} H_i$, so the proof is complete. □

1.4 Groups Generated by a Subset

Definition 1.17. Let $(G, \cdot)$ be a group and $S \subseteq G$. One sets

$$\langle S \rangle = \bigcap_{H \leq G, S \subseteq H} H = \{\text{intersection of all subgroups containing } S\}, \tag{7}$$

where $\langle S \rangle$ is called the **subgroup generated by** S.

Remark 1.18. We observe that $\langle S \rangle \leq H$ by the previous proposition, and $\langle S \rangle$ is in fact the smallest subgroup of G containing S.

Lemma 1.19. Let $(G, \cdot)$ be a group and $H \leq G$. Then $S \subseteq H$ if and only if $\langle S \rangle \subseteq H$.

Proof. $\Longrightarrow$ H is a subgroup of G containing S, and $\langle S \rangle$ is the smallest subgroup of G containing S. Therefore, $\langle S \rangle \subseteq H$ trivially. In fact, $\langle S \rangle \leq H$ by Proposition 1.16.

$\Longleftarrow$ Clearly, $S \subseteq \langle S \rangle$ so this direction is trivial. □

Proposition 1.20. Let $(G, \cdot)$ be a group and $S \subseteq G$, then

$$\langle S \rangle = \{e_G\} \cup \{s_1^{\epsilon_1} \dots s_n^{\epsilon_n};\ n \in \mathbb{N}^*,\ \epsilon_i = \pm 1,\ s_i \in S\}. \tag{8}$$

Proof. $\subseteq$ Denote the right-hand side by A. We need to check that A is a subgroup of G containing S, so it will definitely contain the smallest subgroup of G containing S, *i.e.*, $\langle S \rangle$. Clearly for each $s \in S$, we can take $n = 1$ and $s = s_1^{\epsilon_1}$ with $s_1 = s$ and $\epsilon_1 = 1$, so $S \subseteq A$. Now it suffices to check that $A \leq G$. By definition $e_G \in A$. Take arbitrary $a, b \in A$, we can see that $a \cdot b \in A$. This can be discussed in two cases. If one of the elements is e_G, then the product is simply the other element. Otherwise, the two sequences of products can be concatenated into a longer sequence of product, still falling into A. Finally $a^{-1} \in A$, because clearly $e_G^{-1} = e_G \in A$, and for any other element, we can simply revert the signs of the ϵ_i's which falls back to A. Thus we have shown that A is a subgroup of G containing S, and this direction is done.

$\supseteq$ Since $\langle S \rangle \leq G$, we have that $e_G \in \langle S \rangle$. Moreover, each $s_i \in S$, so all their inverses and all possible products of their inverses and themselves are in $\langle S \rangle$. This direction is thus done. □

9/4 Lecture

1.5 Group Homomorphisms

Definition 1.21. Let $(G, \cdot)$ and $(G', *)$ be two groups. A mapping $f : G \to G'$ is called a **group homomorphism** if $f(x \cdot y) = f(x) * f(y)$, $\forall x, y \in G$.

Remark 1.22. If $f : G \to G'$ is a group isomorphism, then $f(e) = e'$. Indeed, we can see that $f(e) = f(e \cdot e) = f(e) * f(e)$. Multiplying on the left by $(f(e))^{-1}$ on both sides of the equation, we have that $e' = f(e)$. Moreover, $f(x^{-1}) = (f(x))^{-1}$, $\forall x \in G$. Indeed, we can see that $e' = f(e) = f(x \cdot x^{-1}) = f(x) * f(x^{-1})$, so $f(x^{-1}) = (f(x))^{-1}$.

Remark 1.23. We denote the set of homomorphisms from G to G' by $\mathrm{Hom}(G, G')$. We further define the set of **endomorphisms** on G to be $\mathrm{End}(G) := \mathrm{Hom}(G, G)$, the homomorphisms from G to iteself. For $f \in \mathrm{Hom}(G, G')$, if it is furthermore bijective, we say that $f \in \mathrm{Iso}(G, G')$, the set of **isomorphisms** from G to G'. In what follows, we write the group law $\cdot$ for abstract groups. In particular, writing $(G, \cdot)$ and $(G', \cdot)$ does not mean that $\cdot_G = \cdot_{G'}$. It is an abuse of notation and may sometimes be omitted.

Example 1.24. (1) $\det : GL_n(K) \to K^*$ belongs to $\mathrm{Hom}(GL_n(K), K^*)$. Indeed, $\det(AB) = \det(A)\det(B)$.

(2) For a fixed $a \in \mathbb{Z}$, the mapping $m_a : \mathbb{Z} \to \mathbb{Z}$ such that $x \mapsto ax$, belongs to $\mathrm{End}(\mathbb{Z})$. Indeed, $m_a(x + y) = a(x+y) = ax+ay = m_a(x)+m_a(y)$. Check that $\mathrm{End}(\mathbb{Z}) = \{m_a;\ a \in \mathbb{Z}\}$. Check that if $f \in \mathrm{End}(\mathbb{Z})$, then $f = m_{f(1)}$.

(3) If G and G' are groups, then the **trivial isomorphism** $\mathbb{1}_{G,G'} : G \to G'$ defined by $\mathbb{1}_{G,G'}(x) = e'$, $\forall x \in G$, is a group homomorphism from G to G'. In particular, $\mathrm{Hom}(G, G') \neq \varnothing$ because it always contains $\mathbb{1}_{G,G'}$.

(4) $\mathrm{Id}_{G,G'} : x \mapsto x$ is a endomorphism of G. In particular, $\mathrm{End}(G)$ contains at least two elements $\mathbb{1}_{G,G}$ and Id_G as long as $G \neq \{e\}$.

Proposition 1.25. If $f_1 \in \mathrm{Hom}(G_1, G_2)$ and $f_2 \in \mathrm{Hom}(G_2, G_3)$, then $f_2 \circ f_1 \in \mathrm{Hom}(G_1, G_3)$.

Proof. Take arbitrary $x, y \in G_1$, then we have that

$$(f_2 \circ f_1)(x \cdot y) = f_2(f_1(x \cdot y)) = f_2(f_1(x) \cdot f_1(y)) = f_2(f_1(x)) \cdot f_2(f_1(y)) = (f_2 \circ f_1)(x) \cdot (f_2 \circ f_1)(y), \tag{9}$$

so the proof is complete. □

Proposition 1.26. For $f \in \mathrm{Hom}(G, G')$, if $H \leq G$ and $H' \leq G'$, then $f(H) \leq G'$ and $f^{-1}(H') \leq G$.

Proof. Since $e \in H$, $e' = f(e) \in f(H)$. Take arbitrary $x', y' \in f(H)$, then there exists $x, y \in H$, such that $f(x) = x'$ and $f(y) = y'$. Clearly $(x')^{-1} = (f(x))^{-1} = f(x^{-1}) \in f(H)$ because $x^{-1} \in H$. Also, $x' \cdot y' = f(x) \cdot f(y) = f(x \cdot y) \in f(H)$ because $x \cdot y \in H$. Up till now we have shown that $f(H) \leq G$. Similarly, since $e' = f(e) \in H'$, $e \in f^{-1}(H')$. Take arbitrary $x, y \in f^{-1}(H')$, then $f(x), f(y) \in H'$. Clearly $x^{-1} \in f^{-1}(H')$ because $f(x^{-1}) = (f(x))^{-1} \in H'$. Also, $x \cdot y \in f^{-1}(H')$ because $f(x \cdot y) = f(x) \cdot f(y) \in H'$. Now we have also shown that $f^{-1}(H') \leq G$, so the proof is complete. □

Definition 1.27. For $f \in \mathrm{Hom}(G, G')$, one sets $\mathrm{Ker}(f) := \{x \in G;\ f(x) = e'\} = f^{-1}(\{e'\})$ as the **kernel** of f, and $\mathrm{Im}(f) := f(G)$ as the **image** of f.

Example 1.28. (1) $\mathrm{Im}(\det) = K^*$ and $\mathrm{Ker}(\det) = SL_n(K)$, where $\det \in \mathrm{Hom}(GL_n(K), K^*)$. Recall that $SL_n(K)$ is given by $SL_n(K) = \{M \in GL_n(K);\ \det(H) = 1\}$.

(2) $\mathrm{Im}(\exp) = \mathbb{R}_{>0}$ and $\mathrm{Ker}(\exp) = \{0\}$, where $\exp \in \mathrm{Hom}(\mathbb{R}, \mathbb{R}_{>0})$ is the real exponential mapping.

(3) $\mathrm{Im}(\exp) = \mathbb{C}^*$ and $\mathrm{Ker}(\exp) = 2i\pi\mathbb{Z}$, where $\exp \in \mathrm{Hom}(\mathbb{C}, \mathbb{C}^*)$ is the complex exponential mapping.

Proposition 1.29. If $f \in \mathrm{Hom}(G, G')$, then $\mathrm{Ker}(f) \leq G$ and $\mathrm{Im}(f) \leq G'$.

Proof. This is a direct consequence of Proposition 1.26. □

Proposition 1.30. If $f \in \mathrm{Hom}(G, G')$, then f is injective if and only if $\mathrm{Ker}(f) = \{e\}$, and f is surjective if and only if $\mathrm{Im}(f) = G$.

Proof. The second point is obvious, so we only prove the first point. If f is injective, then there can only be a unique element mapped to e'. Since $f(e) = e'$, we have that $\mathrm{Ker}(f) = \{e\}$. Conversely assume that $\mathrm{Ker}(f) = \{e\}$. Take arbitrary $x, y \in G$ such that $f(x) = f(y)$, then $f(x \cdot y^{-1}) = f(x) \cdot (f(y))^{-1} = e'$. This implies that $x \cdot y^{-1} = e$ since $\mathrm{Ker}(f) = \{e\}$. But then by uniqueness of inverse, $x = y$, so f is indeed injective. □

Proposition 1.31. If $f \in \mathrm{Iso}(G, G')$, then $f^{-1} \in \mathrm{Iso}(G', G)$.

Proof. Take arbitrary $x', y' \in G'$, then since f is a bijection, we can set $x = f^{-1}(x')$ and $y = f^{-1}(y')$. Then $f^{-1}(x' \cdot y') = f^{-1}(f(x) \cdot f(y)) = f^{-1}(f(x \cdot y)) = x \cdot y = f^{-1}(x') \cdot f^{-1}(y')$, which implies that $f^{-1} \in \mathrm{Hom}(G', G)$. Clearly f^{-1} is a bijection because f is a bijection, so $f^{-1} \in \mathrm{Iso}(G', G)$ and the proof is complete. □

Definition 1.32. We say that two groups G and G' are **isomorphic** if $\mathrm{Iso}(G, G') \neq \varnothing$.

Example 1.33. The real exponential mapping $\exp : \mathbb{R} \to \mathbb{R}_{>0}$ belongs to $\mathrm{Iso}(\mathbb{R}, \mathbb{R}_{>0})$. This amounts to say that studying $(\mathbb{R}_{>0}, \times)$ as a group is equivalent to studying $(\mathbb{R}, +)$ as a group, which is more familiar.

9/6 Lecture

1.6 Automorphisms

Definition 1.34. Let $\mathrm{Aut}(G) := \mathrm{Iso}(G, G)$. We call an element in $\mathrm{Aut}(G)$ an **automorphism** of G.

Proposition 1.35. We have that $(\mathrm{Aut}(G), \circ) \leq (\mathfrak{S}(G), \circ)$.

Proof. Clearly the neutral element $\mathrm{Id}_G \in \mathrm{Aut}(G)$. Take arbitrary $f, g \in \mathrm{Aut}(G)$, then $f \circ g \in \mathrm{Aut}(G)$ by Proposition 1.25 since automorphism are homomorphisms. Also, $f^{-1} \in \mathrm{Aut}(G)$ by Proposition 1.31 since automorphisms are isomorphisms. Therefore $(\mathrm{Aut}(G), \circ) \leq (\mathfrak{S}(G), \circ)$, so the proof is complete. □

Example 1.36. $\mathrm{Aut}(\mathbb{Z}) = \{m_1, m_{-1}\} = \{\pm \mathrm{Id}_{\mathbb{Z}}\}$. Indeed, $\forall m \in \mathbb{Z}$, we have that $f(m) = f(1) + \ldots + f(1) = f(1)m$, which means that any $f \in \mathrm{Aut}(\mathbb{Z})$ must be such that $m \mapsto f(1)m$. Now f must also be bijective. Suppose $f(1)m = 1$, then since $f(1), m \in \mathbb{Z}$, the only possibilities are $f(1) = \pm 1$. Therefore, either $m \mapsto m$ or $m \mapsto -m$, and we can check that they are indeed automorphisms of $\mathbb{Z}$.

Remark 1.37. For x in a group G, we define $\iota_x : G \to G$, such that $g \mapsto x \cdot g \cdot x^{-1}$. Then for $x \in G$, we can see that $\iota_x \in \mathrm{Aut}(G)$. Indeed, take arbitrary $f, g \in G$, we have that

$$\iota_x(f \cdot g) = x \cdot (f \cdot g) \cdot x^{-1} = x \cdot f \cdot (x^{-1} \cdot x) \cdot g \cdot x^{-1} = (x \cdot f \cdot x^{-1}) \cdot (x \cdot g \cdot x^{-1}) = \iota_x(f) \cdot \iota_x(g). \tag{10}$$

To see that ι_x is bijective, we claim that $\iota_{x^{-1}}$ is its inverse. Indeed, we can see that

$$(\iota_x \circ \iota_{x^{-1}})(f) = \iota_x(\iota_{x^{-1}}(f)) = \iota_x(x^{-1} \cdot f \cdot x) = x \cdot (x^{-1} \cdot f \cdot x) \cdot x^{-1} = f, \qquad \forall f \in G. \tag{11}$$

The case is the same for $\iota_{x^{-1}} \circ \iota_x$, both equal to Id_G. This implies that ι_x is bijective, and an automorphism of G.

Remark 1.38. The mapping $\iota : G \to \mathrm{Aut}(G)$ such that $x \mapsto \iota_x$ is a group homomorphism. Indeed, take arbitrary $x, y \in G$, we can check that

$$\begin{aligned} \iota(x \cdot y)(g) &= \iota_{x \cdot y}(g) = (x \cdot y) \cdot g \cdot (x \cdot y)^{-1} = x \cdot (y \cdot g \cdot y^{-1}) \cdot x^{-1} \\ &= x \cdot \iota_y(g) \cdot x^{-1} = \iota_x(\iota_y(g)) = (\iota_x \circ \iota_y)(g) = (\iota(x) \circ \iota(y))(g), \qquad \forall g \in G. \end{aligned} \tag{12}$$

Definition 1.39. We set $\mathrm{Inn}(G) := \iota(G)$. An element in $\mathrm{Inn}(G)$ is called an **inner automorphism** of G. We call ι_x **the conjugation by** x.

Definition 1.40. Two elements $x, y \in G$ are said to be **conjugate** if there exists $g \in G$, such that $y = \iota_g(x) = gxg^{-1}$.

Proposition 1.41. Conjugation on the group G, denoted $\sim$, is an equivalence relation.

Proof. We have that $\iota_x(x) = xxx^{-1} = x$ so $x \sim x$, which means that conjugation is reflexive. If $x \sim y$ and $y \sim z$, we assume that $y = \iota_f(x)$ and $z = \iota_g(y)$. Then $x = \iota_f^{-1}(y) = \iota_{f^{-1}}(y)$ so $y \sim x$, which means that conjugation is symmetric. Moreover, $z = \iota_g(\iota_f(x)) = \iota_{gf}(x)$ so $x \sim z$, which means that conjugation is transitive. These three properties show that conjugation on the group G is an equivalence relation. □

Remark 1.42. We denote by $Cl_G(x)$ the **conjugacy class** of x in G.

Lemma 1.43. Take σ and $c = \begin{pmatrix} a_1 & \dots & a_m \end{pmatrix}$ in $\mathfrak{S}_n$. Then

$$\sigma \circ c \circ \sigma^{-1} = \iota_\sigma(c) = \begin{pmatrix} \sigma(a_1) & \dots & \sigma(a_m) \end{pmatrix}. \tag{13}$$

Proof. Note that c here is a specific type of permutation where elements are cyclically permuted within the cycle, and all other elements are fixed. There are thus two cases.

- If $x \notin \{\sigma(a_1), \dots, \sigma(a_m)\}$, then $\sigma^{-1}(x) \notin \{a_1, \dots, a_m\}$. Therefore, $\sigma^{-1}(x)$ remain fixed when permuted, *i.e.*, $c(\sigma^{-1}(x)) = \sigma^{-1}(x)$. This means that $(\sigma \circ c \circ \sigma^{-1})(x) = \sigma(\sigma^{-1}(x)) = x$. Indeed, in this case x should be fixed under the cyclic permutation $\begin{pmatrix} \sigma(a_1) & \dots & \sigma(a_m) \end{pmatrix}$, so we are done.
- If $x \in \{\sigma(a_1), \dots, \sigma(a_m)\}$, then $\sigma^{-1}(x) \in \{a_1, \dots, a_m\}$. Therefore, $\sigma^{-1}(x)$ will be cyclically permuted within the cycle $\begin{pmatrix} a_1 & \dots & a_m \end{pmatrix}$. Suppose $x = \sigma(a_i)$, $1 \le i \le m-1$. Then $(\sigma \circ c \circ \sigma^{-1})(x) = \sigma(c(a_i)) = \sigma(a_{i+1})$. Indeed, $x = \sigma(a_i)$ will be cyclically permuted as $\sigma(a_{i+1})$ under $\begin{pmatrix} \sigma(a_1) & \dots & \sigma(a_m) \end{pmatrix}$ when $1 \le i \le m$. Otherwise, $x = \sigma(a_m)$. Then $(\sigma \circ c \circ \sigma^{-1})(x) = \sigma(c(a_m)) = \sigma(a_1)$. Indeed, $x = \sigma(a_m)$ will be cyclically permuted as $\sigma(a_1)$ under $\begin{pmatrix} \sigma(a_1) & \dots & \sigma(a_m) \end{pmatrix}$. We have checked all cases up till now, so the proof is complete. □

9/11 Lecture

1.7 Normal Subgroups

Definition 1.44. Let $(G, \cdot)$ be a group and $H \le G$. One says that H is a **normal subgroup** of G and writes $H \trianglelefteq G$, if $xhx^{-1} \in H$ for all $x \in G$ and $h \in H$. An equivalent formulation of the definition is that $\iota_x(H) \subseteq H$ for all $x \in G$.

Remark 1.45. Let $H \le G$, then $H \trianglelefteq G$ if and only if $\iota_x(H) = H$ for all $x \in G$. Indeed, if $\iota_x(H) = H$ necessarily means that $\iota_x(H) \subseteq H$, so the $\Longleftarrow$ direction is trivial. For the other direction, suppose that $H \trianglelefteq G$, then $\iota_x(H) \subseteq H$ for all $x \in G$. But then $x^{-1} \in G$, so that $\iota_x^{-1}(H) = \iota_{x^{-1}}(H) \subseteq H$. Hence $H \subseteq \iota_x(H)$, so the proof is complete.

Proposition 1.46. If $f \in \mathrm{Hom}(G, G')$ and $H' \trianglelefteq G'$, then $f^{-1}(H') \trianglelefteq G$.

Proof. We want to show that $xhx^{-1} \in f^{-1}(H')$ for all $x \in G$ and $h \in f^{-1}(H')$. To see this, we observe that

$$f(xhx^{-1}) = \underbrace{f(x)}_{\in G'}\underbrace{f(h)}_{\in H'}\underbrace{f(x^{-1})}_{\in G'} \quad \underbrace{\in H'}_{\text{since } H' \trianglelefteq G'} \quad . \tag{14}$$

Therefore, $xhx^{-1} \in f^{-1}(H')$ for all $x \in G$ and $h \in f^{-1}(H')$, so the proof is complete. □

Corollary 1.47. If $f \in \mathrm{Hom}(G, G')$, then $\mathrm{Ker}(f) \trianglelefteq G$.

Proof. We check that $\{e'\} \trianglelefteq G'$. Indeed, $xe'x^{-1} = xx^{-1} = e' \in \{e'\}$ for all $x \in G'$. Now since $\mathrm{Ker}(f) = f^{-1}(\{e'\})$, we can conclude directly by Proposition 1.46. □

Example 1.48. Since $\det \in \mathrm{Hom}(GL_n(K), K^*)$, and $SL_n(K) = \mathrm{Ker}(\det)$, we have that $SL_n(K) \trianglelefteq GL_n(K)$.

Definition 1.49. For $(G, \cdot)$ a group, we denote by $Z(G)$ or Z_G the set $Z(G) = \{z \in G;\ xz = zx, \forall x \in G\}$, called the **center** of G. It is the subset of G the elements of which commute with all $x \in G$.

Proposition 1.50. *$Z(G) \leq G$ and if $H \leq Z(G)$, then H is commutative and $H \trianglelefteq G$. In particular, $Z(G) \trianglelefteq G$.*

Proof. Clearly $e \in Z(G)$ because $ex = xe = x$ for any $x \in G$. Now take arbitrary $z, z_1, z_2 \in Z(G)$, then for any $x \in G$, we have that

$$xz^{-1} = (z^{-1}z)(xz^{-1}) = z^{-1}(zx)z^{-1} = z^{-1}(xz)z^{-1} = (z^{-1}x)(zz^{-1}) = z^{-1}x, \tag{15}$$

$$x(z_1z_2) = \underbrace{(xz_1)}_{\in G} z_2 = z_2(xz_1) = \underbrace{(z_2x)}_{\in G} z_1 = z_1(z_2x) = (z_1z_2)x. \tag{16}$$

Therefore, we have shown that $Z(G) \leq G$. Now further assume that $H \leq Z(G)$. Now for any $h_1, h_2 \in H$, clearly $h_1, h_2 \in Z(G)$, and thus $h_1h_2 = h_2h_1$ which implies that H is commutative. Furthermore, take arbitrary $h \in H$ and $x \in G$, we can see that $xhx^{-1} = (xh)x^{-1} = (hx)x^{-1} = h \in H$, indicating that H is stable under G-conjugation, and hence $H \trianglelefteq G$. The proof is thus complete. Note that in particular, $Z(G) \leq Z(G)$ so that $Z(G) \trianglelefteq G$. □

Remark 1.51. A group G is commutative if and only if $G = Z(G)$. The $\Longleftarrow$ direction is trivial, since then for all $x \in G$, it commutes with all $z \in G$, meaning that $xz = xz$ for all $x, z \in G$. The other direction is also trivial. Assume that G is commutative, then for any $x \in G$, $xz = zx$ for any $z \in G$ so $x \in Z(G)$. Clearly $Z(G) \subseteq G$, and thus $Z(G) = G$ and the proof is complete.

Corollary 1.52. If A is a commutative group, then all its subgroups are normal.

Remark 1.53. We can show that $Z(G) = \mathrm{Ker}(\iota)$, where we recall that $\iota : G \to \mathrm{Inn}(G)$ such that $x \mapsto \iota_x$. Indeed, for any $z \in Z(G)$, we have that $zx = xz$ for all $x \in G$. Then $\iota(z)(x) = \iota_z(x) = zxz^{-1} = xzz^{-1} = x$ for all $x \in G$, meaning that $\iota(z) = \mathrm{Id}_G$, the neutral element in $\mathrm{Inn}(G)$. Hence $z \in \mathrm{Ker}(\iota)$, implying that $Z(G) \subseteq \mathrm{Ker}(\iota)$. On the other hand, for any $z \in \mathrm{Ker}(\iota)$, we have that $\iota(z) = \mathrm{Id}_G$. This means that for any $x \in G$, we have

$$x = \iota(z)(x) = \iota_z(x) = zxz^{-1} \implies xz = zx. \tag{17}$$

Hence $z \in Z(G)$, and thus $\mathrm{Ker}(\iota) \subseteq Z(G)$. Both directions of inclusion hold, so $Z(G) = \mathrm{Ker}(\iota)$.

Remark 1.54. We can show that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. Indeed, for any $f \in \mathrm{Inn}(G)$ and $g \in \mathrm{Aut}(G)$, we can write $f = \iota_z$ for some $z \in G$. Then for any $x \in G$, we have that

$$\begin{aligned}(g \circ \iota_z \circ g^{-1})(x) &= g(\iota_z(g^{-1}(x))) = g(g^{-1}(x)z(g^{-1}(x))^{-1}) \\ &= g(g^{-1}(x)z\underbrace{g^{-1}(x^{-1})}_{g \in \mathrm{Aut}(G)}) = \underbrace{g(g^{-1}(x))g(z)g(g^{-1}(x^{-1}))}_{g \in \mathrm{Aut}(G)} = xg(z)x^{-1} = \iota_{g(z)}(x),\end{aligned} \tag{18}$$

which implies that $g \circ \iota_z \circ g^{-1} = \iota_{g(z)} \in \mathrm{Inn}(G)$. Clearly $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$, so that $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

1.8 Quotient Groups

Remark 1.55. Let X be a set and $\sim$ be an equivalence relation on X, then we denote by $Cl(x) = \{y \in X;\ y \sim x\}$ the equivalence class of x. We recall that for $x, x' \in X$, either $Cl(x) \cap Cl(x') = \varnothing$ or $Cl(x) = Cl(x')$. Hence the equivalence classes form a partition of X.

Definition 1.56. We denote by $\frac{X}{\sim}$ the set of classes for $\sim$, which is called the **quotient set** of X by $\sim$. For each $C \in \frac{X}{\sim}$, we pick on element $x_C \in C$ (hence $C = Cl(x_C)$), then the set $R = \left\{x_C;\ C \in \frac{X}{\sim}\right\}$ is called the **set of representatives** for $\sim$. In particular X is the disjoint union $X = \bigsqcup_{x\in\mathbb{R}} Cl(x)$.

Remark 1.57. A subset $R \subseteq X$ is a set of representatives for $\sim$ if and only if the mapping $Cl : R \to \frac{X}{\sim}$ is a bijection.

9/13 Lecture

Remark 1.58. Let G be a group. For $A \subseteq G$ and $x, y \in G$, we set the notations $xAy = \{xay;\ a \in A\}$, $xA = xAe = \{xa;\ a \in A\}$, and $Ay = eAy = \{ay;\ a \in A\}$. From now on, $H \leq G$.

Proposition 1.59. The relations $y_H \sim x \iff y \in Hx$ and $y \sim_H x \iff y \in xH$ are equivalence relations on G.

Proof. We prove that $_H\sim$ is an equivalence relation on G, and the proof for $\sim_H$ would be analogous. First, we have that $x = ex \in Hx$ so $x_H \sim x$, which means that $_H\sim$ is reflexive. Second, if $x_H \sim y$, then there exists $h \in H$ such that $y = hx$. Then $x = h^{-1}y$ where $h^{-1} \in H$ because H is a subgroup. Therefore, $x \in Hy$ and thus $y_H \sim x$, which means that $_H\sim$ is symmetric. Finally, if $x_H \sim y$ and $y_H \sim z$, then there exists $h_1, h_2 \in H$ such that $y = h_1x$ and $z = h_2y$. Hence $z = h_2(h_1x) = (h_2h_1)x$ where $h_2h_1 \in H$ because H is a subgroup. Therefore, $z \in Hx$ and thus $x_H \sim z$, which means that $_H\sim$ is transitive. Now we can conclude that $_H\sim$ is an equivalence relation on G. □

Remark 1.60. Note that xH is the equivalence class $Cl_H(x) = \{y \in G;\ y_H \sim x\}$, and Hx is the equivalence class $_HCl(x) = \{y \in G;\ y_H \sim x\}$.

Definition 1.61. We call xH the **right H-coset** of x, and Hx the **left H-coset** of x. We denote by G/H the set of right H-cosets $G/H = \frac{G}{\sim_H}$ and $H\backslash G$ the set of left H-cosets $H\backslash G = \frac{G}{_H\sim}$.

Example 1.62. Define $\text{inv} : G \to G$ by $\text{inv}(x) = x^{-1}$. We can easily see that $\text{inv} \circ \text{inv} = \text{Id}$, and we can check that $\text{inv}(xH) = Hx^{-1}$ and $\text{inv}(Hx) = x^{-1}H$. We want to show that inv induces a bijection between G/H and $H\backslash G$. Indeed, $\text{inv}_H : xH \mapsto \text{inv}(xH) = Hx^{-1}$ is a mapping from G/H to $H\backslash G$, and $\text{inv}^H : Hx \mapsto \text{inv}(Hx) = x^{-1}H$ is a mapping from $H\backslash G$ to G/H. Moreover, inv_H and inv^H are inverses of each other.

Lemma 1.63. For all $x \in G$, the mapping $l_x : G \to G$ such that $g \mapsto xg$ induces a bijection between H and xH, and the mapping $r_x : G \to G$ such that $g \mapsto gx$ induces a bijection between H and Hx.

Proof. We only prove for l_x, then r_x would be analogous. Indeed, the mapping $l_x : G \to G$ is bijective with inverse $l_{x^{-1}}$, and moreover $xH = l_x(H)$, so the proof is trivial. □

Corollary 1.64. If $|H| < \infty$, then $|xH| = |H|$ and $|Hx| = |H|$ for all $x \in H$.

Theorem 1.65 (Lagrange's theorem)**.** Let G be a group and $H \leq G$ be a subgroup of G. If G is finite, then $|H|$ divides $|G|$ and $|G| = |G/H| \times |H|$, and also $|G| = |H\backslash G| \times |H|$.

Proof. Let $R \subseteq G$ be a set of representatives of $G/H = \frac{G}{\sim_H}$, then $G = \bigsqcup_{r\in R} rH$. Therefore, $|G| = \sum_{r\in R} |rH|$. But by Corollary 1.64, we have that $|rH| = |H|$, and as a result $|G| = |R| \times |H|$. This implies that $|H|$ divides $|G|$, and moreover we conclude the result by observing that $|R| = |G/H|$. The other result follows an analogous proof and will not be explicitly shown here. □

Remark 1.66. If G is a finite group with prime cardinality p, then $G = \langle x\rangle$ for any $x \neq e$ in G. Indeed by Lagrange's theorem (Theorem 1.65), we know that $|\langle x\rangle|$ divides $|G|$ because $\langle x\rangle \leq G$, but since $|G|$ is prime, either $|\langle x\rangle| = 1$ or $|\langle x\rangle| = |G| = p$. However $|\langle x\rangle| \geq 2$ because it at least contains the neutral element e and $x \neq e$. Therefore, we can conclude that $G = \langle x\rangle$ because $\langle x\rangle \subseteq G$ but both have the same cardinality.

9/18 Lecture

Lemma 1.67. Let $H \leq G$, then the following are equivalent.

(1) $H \trianglelefteq G$.

(2) $gHg^{-1} = H$ for all $g \in G$.

(3) $gH = Hg$ for all $g \in G$.

Proof. We first argue that (1) and (2) are equivalent. (2) implies (1) by definition. Now assume that $H \trianglelefteq G$, so that $gHg^{-1} \subseteq H$ for all $g \in G$. Taking $g^{-1} \in G$, we also have that $g^{-1}Hg \subseteq H$ for all $g \in G$, which necessarily means that $H \subseteq gHg^{-1}$. With both inclusions, we can conclude that $gHg^{-1} = H$ for all $g \in G$ and thus (1) implies (2) as well. Now we move on to show that (2) is equivalent to (3). Indeed, multiplying by g on the right of (2) gives (3), and multiplying by g^{-1} on the right of (3) gives (2). In conclusion, the three statements are all equivalent, and the proof is complete. □

Remark 1.68. In particular, if $H \trianglelefteq G$, then $G/H = H\backslash G$. By convention, we denote $\frac{G}{H} := G/H = H\backslash G$, and we set $\overline{g}$ for $gH = Hg \in \frac{G}{H}$.

Lemma 1.69. Suppose that $H \trianglelefteq G$, then the multiplication mapping $m : \frac{G}{H} \times \frac{G}{H} \to \frac{G}{H}$, such that $m(\overline{x}, \overline{y}) = \overline{xy}$ is well-defined.

Proof. It suffices to check that if $\overline{x'} = \overline{x}$ and $\overline{y'} = \overline{y}$, then $\overline{x'y'} = \overline{xy}$. By assumption, there exists $x' = xh$ for some $h \in H$ and $y' = yk$ for some $k \in H$. As a result, we can see that $x'y' = xhyk = x(yy^{-1})hyk = xy((y^{-1}hy)k)$. Note that since $H \trianglelefteq G$, we have that $y^{-1}hy \in H$ because $y \in \frac{G}{H} \subseteq G$. Hence $\overline{x'y'} = \overline{xy}$ and the proof is complete. □

Remark 1.70. From the previous lemma, we can see that it makes sense to put $\overline{g} \cdot \overline{g'} = \overline{gg'}$.

Theorem 1.71. If $H \trianglelefteq G$, then $\left(\frac{G}{H}, \cdot\right)$ is a group with neutral element $\overline{e} = H$.

Proof. This is trivial by previous observations and will be omitted here. □

Proposition 1.72. If $H \trianglelefteq G$, then the **canonical projection/surjection** $p : G \to \frac{G}{H}$ defined by $p(g) = \overline{g}$, is a surjective homomorphism with kernel $\operatorname{Ker}(p) = H$.

Proof. Since $p(xy) = \overline{xy} = \overline{x} \cdot \overline{y} = p(x)p(y)$, clearly p is a homomorphism. The surjectivity of p is trivial. Now if $x \in \operatorname{Ker}(p)$, then $p(x) = \overline{e} = H$. Necessarily $x \in H$, since otherwise $\overline{x}$ has at least an element not in H. On the other hand, if $x \in H$, then $p(x) = \overline{x} = H = \overline{e}$, so that $x \in \operatorname{Ker}(p)$. By both directions of inclusion, we can conclude that $\operatorname{Ker}(p) = H$, and the proof is complete. □

Corollary 1.73. If $H = \{e\}$, then p is an isomorphism between G and $\frac{G}{\{e\}}$.

Proof. By the previous proposition, p is a surjective homomorphism with $\operatorname{Ker}(p) = H$, so that $\operatorname{Ker}(p) = \{e\}$, which necessarily means that p is injective as well. Therefore, p is bijective and thus an isomorphism. The proof is now complete. □

9/20 Lecture

Example 1.74. We recall that if G is commutative, then all its subgroups are normal. Also, we recall from recitations that the subgroups of $\mathbb{Z}$ are the groups $n\mathbb{Z}$, $n \in \mathbb{N}$. We can see that

$$\frac{\mathbb{Z}}{n\mathbb{Z}} \begin{cases} \simeq \mathbb{Z}, & \text{if } n = 0, \\ = \left\{\overline{0}, \ldots, \overline{n-1}\right\}, & \text{if } n \geq 1. \end{cases} \tag{19}$$

In the case $n \geq 1$, we have that $\left|\frac{\mathbb{Z}}{n\mathbb{Z}}\right| = 1$, and $R = \{0, \ldots, n-1\}$ is a system of representatives for $\frac{\mathbb{Z}}{n\mathbb{Z}}$.

Theorem 1.75 (First isomorphism theorem)**.** For $f \in \mathrm{Hom}(G, G')$ and $p : G \to \frac{G}{\mathrm{Ker}(f)}$ the canonical projection, there exists a unique $\overline{f} : \frac{G}{\mathrm{Ker}(f)} \to G'$, such that $f = \overline{f} \circ p$, *i.e.*, such that the following diagram commutes.

$$\begin{tikzcd}
G \arrow[r, "f"] \arrow[d, "p"'] & G' \\
\frac{G}{\mathrm{Ker}(f)} \arrow[ur, "\overline{f}"'] &
\end{tikzcd}$$

Moreover, $\overline{f} \in \mathrm{Hom}\left(\frac{G}{\mathrm{Ker}(f)}, G'\right)$ and is injective.

Proof. If $f = \overline{f} \circ p$ and $\overline{x} = p(x) \in \frac{G}{\mathrm{Ker}(f)}$, then the relation $\overline{f}(\overline{x}) = \overline{f}(p(x)) = (\overline{f} \circ p)(x) = f(x)$ shows that $\overline{f}$ is unique if it exists. Therefore, it suffices to prove that such $\overline{f}$ exists, *i.e.*, to check that the mapping $\overline{f} : \frac{G}{\mathrm{Ker}(f)} \to G'$ such that $\overline{x} \mapsto f(x)$ is well-defined. Indeed, if $\overline{x'} = \overline{x}$, then there exists $k \in \mathrm{Ker}(f)$, such that $x' = xk$. As a consequence, $f(x') = f(xk) = f(x)f(k) = f(x)$ because f is a homomorphism and k is in the kernel. This proves that $\overline{f}$ is well-defined. Now we prove that $\overline{f}$ is a group homomorphism. For any $\overline{x}, \overline{x'} \in \frac{G}{\mathrm{Ker}(f)}$, we have that

$$\overline{f}(\overline{x} \cdot \overline{x'}) = \overline{f}(\overline{xx'}) = f(xx') = \underbrace{f(x)f(x')}_{f \in \mathrm{Hom}(G,G')} = \overline{f}(\overline{x})\overline{f}(\overline{x'}), \tag{20}$$

so indeed $\overline{f} \in \mathrm{Hom}\left(\frac{G}{\mathrm{Ker}(f)}, G'\right)$. Finally if $\overline{x} \in \mathrm{Ker}(\overline{f})$, we have that $\overline{f}(\overline{x}) = e' \in G'$. This means that $f(x) = e'$, so $x \in \mathrm{Ker}(f)$. Note again that the quotient space is $\frac{G}{\mathrm{Ker}(f)}$, and thus $\overline{x} = \overline{e}$. Therefore, $\mathrm{Ker}(\overline{f}) \subseteq \{\overline{e}\}$. But $\overline{e} \in \mathrm{Ker}(\overline{f})$, so necessarily $\mathrm{Ker}(\overline{f}) = \{\overline{e}\}$, which implies that $\overline{f}$ is injective, so the proof is complete. □

Corollary 1.76. The mapping $\overline{f}$ induces an isomorphism between $\frac{G}{\mathrm{Ker}(f)}$ and $\mathrm{Im}(f) = f(G)$. In other words,

$$\frac{G}{\mathrm{Ker}(f)} \overset{\overline{f}}{\simeq} \mathrm{Im}(f). \tag{21}$$

In particular for finite G, we have that $|G| = |\mathrm{Ker}(f)| \times |\mathrm{Im}(f)|$.

Proof. This is a direct consequence of the first isomorphism theorem (Theorem 1.75), *i.e.*, the quotient space of G divided by $\mathrm{Ker}(f)$ is isomorphic to $\mathrm{Im}(f)$ if f is a group homomorphism from G. Moreover if G is finite, we have that $|G|/|\mathrm{Ker}(f)| = \left|\frac{G}{\mathrm{Ker}(f)}\right| = |\mathrm{Im}(f)|$ by the Lagrange's theorem (Theorem 1.65), and thus $|G| = |\mathrm{Ker}(f)| \times |\mathrm{Im}(f)|$. The proof is now complete. □

Theorem 1.77. Let G be a **cyclic group**, *i.e.*, a group generated by one element, up to isomorphism. Then there exists a unique $n \in \mathbb{N}$, such that $G \simeq \frac{\mathbb{Z}}{n\mathbb{Z}}$. If $n = 0$ then $G \simeq \mathbb{Z}$ is infinite, and if otherwise $n \geq 1$, G is finite of cardinality n.

Proof. Let $G = \langle x \rangle$, then the mapping $f : \mathbb{Z} \to G$, defined by $f(k) = x^k$, is a surjective homomorphism. Indeed, we have that $f(k_1 + k_2) = x^{k_1+k_2} = x^{k_1}x^{k_2} = f(k_1)f(k_2)$ for any $k_1, k_2 \in \mathbb{Z}$ and f is clearly surjective. Since $\mathrm{Ker}(f) \leq \mathbb{Z}$, it is of the form $n\mathbb{Z}$. Therefore by Corollary 1.76 and surjectivity of f, we can conclude that $\frac{\mathbb{Z}}{n\mathbb{Z}} = \frac{\mathbb{Z}}{\mathrm{Ker}(f)} = \mathrm{Im}(f) = G$. The rest of the theorem holds by Example 1.74, so the proof is complete. □

Example 1.78. (1) For $n \geq 1$, we check that $\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{U}_n := \{z \in \mathbb{C};\ z^n = 1\}$. Consider the mapping $\phi : \mathbb{Z} \to \mathbb{U}_n$, such that $k \mapsto (\exp(i2\pi/n))^k$, which is a surjective homomorphism. Indeed, we have that $\phi(k_1 + k_2) = (\exp(i2\pi/n))^{k_1+k_2} = (\exp(i2\pi/n))^{k_1}(\exp(i2\pi/n))^{k_2} = \phi(k_1)\phi(k_2)$ for any $k_1, k_2 \in \mathbb{Z}$ and ϕ is clearly surjective because it maps to all powers of the nth root of unity. Since $\mathrm{Ker}(\phi) \leq \mathbb{Z}$, it is of the form $n\mathbb{Z}$. Therefore by Corollary 1.76 and surjectivity of ϕ, we can conclude that $\frac{\mathbb{Z}}{n\mathbb{Z}} = \frac{\mathbb{Z}}{\mathrm{Ker}(\phi)} \simeq \mathrm{Im}(\phi) = \mathbb{U}_n$ for some $n \in \mathbb{N}$.

(2) We check that $\frac{\mathbb{R}}{\mathbb{Z}} \simeq \mathbb{C}_u := \{z \in \mathbb{C};\ |z| = 1\}$. Consider the mapping $\phi : \mathbb{R} \to \mathbb{C}_u$, such that $x \mapsto \exp(i2\pi x)$, which is a surjective homomorphism. Indeed, we have that $\phi(x_1+x_2) = \exp(i2\pi(x_1+x_2)) = \exp(i2\pi x_1)\exp(i2\pi x_2) = \phi(x_1)\phi(x_2)$ for any $x_1, x_2 \in \mathbb{R}$ and ϕ is clearly surjective because it maps to the whole unit circle. Now we check that $\operatorname{Ker}(\phi) = \mathbb{Z}$. Indeed, if $x \in \operatorname{Ker}(\phi)$, we necessarily have that $\phi(x) = \exp(i2\pi x) = 1$, the rightmost point of the unit circle in the complex plane. Hence $2\pi x \in 2\pi\mathbb{Z}$, *i.e.*, $x \in \mathbb{Z}$, which implies that $\operatorname{Ker}(\phi) \subseteq \mathbb{Z}$. The other direction of inclusion is trivial, so we can conclude that $\operatorname{Ker}(\phi) = \mathbb{Z}$. Now by Corollary 1.76 and surjectivity of ϕ, we can conclude that $\frac{\mathbb{R}}{\mathbb{Z}} = \frac{\mathbb{Z}}{\operatorname{Ker}(\phi)} \simeq \operatorname{Im}(\phi) = \mathbb{C}_u$.

(3) We check that $\frac{GL_n(K)}{SL_n(K)} \simeq K^*$. Recall that $GL_n(K)$ is the group of all $n\times n$ invertible matrices and $SL_n(K)$ is the group of all $n \times n$ matrices with determinant 1 (and thus invertible). Consider the mapping $\det : GL_n(K) \to K^*$, which is a surjective homomorphism. Indeed, we have that $\det(M_1M_2) = \det(M_1)\det(M_2)$ for any $M_1, M_2 \in GL_n(K)$ and det is clearly surjective because K^* does not include 0 determinant and we can always find invertible matrices with any non-zero determinant. Now recall that $\operatorname{Ker}(\det) = SL_n(K)$, which is trivial. Therefore by Corollary 1.76 and surjectivity of det, we can conclude that $\frac{GL_n(K)}{SL_n(K)} = \frac{GL_n(K)}{\operatorname{Ker}(\det)} \simeq \operatorname{Im}(\det) = K^*$.

9/25 Lecture

Lemma 1.79. Take $f \in \operatorname{Hom}(G, G')$. If $K \trianglelefteq G'$ then $f^{-1}(K) \trianglelefteq G$, whereas if $H \trianglelefteq G$ then $f(H) \trianglelefteq f(G)$.

Proof. For the first part, take arbitrary $x \in f^{-1}(K)$ and $x' \in G$. Then we have that $x \in G$ and thus $x'x(x')^{-1} \in G$. By arbitrariness of x and x', we can conclude that $f^{-1}(K) \trianglelefteq G$. Now for the second part, take arbitrary $y \in f(H)$ and $y' \in f(G)$, there exists $h \in H$ and $g \in G$ such that $y = f(h)$ and $y' = f(g)$. Then we have that $y'y(y')^{-1} = f(g)f(h)(f(g))^{-1} = f(ghg^{-1}) \in f(H)$ because f is a group homomorphism and $H \trianglelefteq G$. Hence by arbitrariness of g and h, we can conclude that $f(H) \trianglelefteq f(G)$. The proof is now complete. □

Remark 1.80. Though $H \trianglelefteq G$ implies $f(H) \trianglelefteq f(G)$, it does *not* imply that $f(H) \trianglelefteq G'$ in general.

Theorem 1.81. If $f \in \operatorname{Hom}(G, G')$, then the mapping $H \mapsto f(H)$ is a bijection from the set $\{H;\ \operatorname{Ker}(f) \leq H \leq G\}$ to the set $\{K;\ K \leq \operatorname{Im}(f)\}$ of subgroups of $\operatorname{Im}(f)$, with inverse $K \mapsto f^{-1}(K)$. Moreover, this bijection and its inverse preserve normal subgroups.

Proof. Denote $\mathscr{A} = \{H;\ \operatorname{Ker}(f) \leq H \leq G\}$ and $\mathscr{B} = \{K;\ K \leq \operatorname{Im}(f)\}$. Also denote the mappings $m : H \mapsto f(H)$ and $n : K \mapsto f^{-1}(K)$. We want to show that m and n are bijective and are inverses of each other. First we show that $m \circ n = \operatorname{Id}_{\mathscr{B}}$, *i.e.*, for any $K \in \mathscr{B}$, we claim that $K = m(n(K)) = f(f^{-1}(K))$.

$\subseteq$ Fix arbitrary $k \in K$. Since $K \leq \operatorname{Im}(f)$, we have that $k \in \operatorname{Im}(f)$, so by definition of image there exists $x \in G$ such that $f(x) = k$. Then by definition of preimage $x \in f^{-1}(K)$, and thus $k = f(x) \in f(f^{-1}(K))$.

$\supseteq$ Fix arbitrary $k \in f(f^{-1}(K))$, then there exists $h \in f^{-1}(K)$ such that $k = f(h)$. By definition of preimage, we can see that $k = f(h) \in K$.

Next we show that $n \circ m = \operatorname{Id}_{\mathscr{A}}$, *i.e.*, for any $H \in \mathscr{A}$, we claim that $H = n(m(H)) = f^{-1}(f(H))$.

$\subseteq$ Fix arbitrary $h \in H$, then $f(h) \in f(H)$. By definition of preimage, $h \in f^{-1}(f(H))$.

$\supseteq$ Fix arbitrary $h \in f^{-1}(f(H))$, then $f(h) \in f(H)$ by definition of preimage. This means that there exists $h' \in H$, such that $f(h) = f(h')$. Since f is a group homomorphism, we have that $f(h(h')^{-1}) = f(h)(f(h'))^{-1} = e'$, so $h(h')^{-1} \in \operatorname{Ker}(f)$. Since $\operatorname{Ker}(f) \leq H$, we have that $h(h')^{-1} \in H$, and thus $h \in Hh' = \{xh';\ x \in H\}$. But we claim that $Hh' = H$.

  $\subseteq$ Fix arbitrary $h \in Hh'$, then there exists $x \in H$ such that $h = xh'$. But $x \in H$ and $h' \in H$, so $h = xh' \in H$.

  $\supseteq$ Fix arbitrary $h \in H$, then take $x = h(h')^{-1}$. Indeed $x \in H$ since $h \in H$ and $h' \in H$, and clearly $h = xh'$ so that $h \in Hh'$.

  Therefore, we can see that $h \in Hh' = H$.

Up till now, we have shown that $m \circ n = \operatorname{Id}_{\mathscr{B}}$ and $n \circ m = \operatorname{Id}_{\mathscr{A}}$, which prove that m and n are inverses of each other, and thus automatically bijective. Moreover, they both preserve normal subgroups by Lemma 1.79, so the proof is complete. □

Corollary 1.82 (Subgroups of quotients)**.** Assume that $N \trianglelefteq G$ and $p \in \operatorname{Hom}\left(G, \frac{G}{N}\right)$ the canonical projection, then the mapping $H \mapsto p(H) = \frac{H}{N}$ is a bijection from the set $\{H;\ N \leq H \leq G\}$ to the set $\left\{K;\ K \leq \frac{G}{N}\right\}$, with inverse $K \mapsto p^{-1}(K)$. Moreover, this bijection and its inverse preserve normal subgroups.

Proof. This is a direct consequence of the previous theorem by taking $G = G$ and $G' = \frac{G}{N}$. Note that $\operatorname{Ker}(p) = N$. □

Remark 1.83. In the corollary above, if $N \leq H$, then automatically $N \trianglelefteq H$ because $N \trianglelefteq G$. Hence $\frac{H}{N}$ is indeed a group.

Example 1.84. Take $n \geq 1$, then we can check that the subgroups of $\frac{\mathbb{Z}}{n\mathbb{Z}}$ are exactly those of the form $\frac{d\mathbb{Z}}{n\mathbb{Z}}$ where $d \in D(n) = \{d \in \mathbb{N}^*;\ d \mid n\}$. First of all, if $n\mathbb{Z} \leq H \leq \mathbb{Z}$, then H must be of the form $d\mathbb{Z}$ because $H \leq \mathbb{Z}$ and necessarily $d \mid n$ because it needs to contain all elements of $n\mathbb{Z}$. Taking $N = n\mathbb{Z}$ and $G = \mathbb{Z}$ in Corollary 1.82, we can see that the mapping $m : \{d\mathbb{Z};\ d \in D(n)\} \to \left\{K;\ K \leq \frac{\mathbb{Z}}{n\mathbb{Z}}\right\}$, such that $d\mathbb{Z} \mapsto p(d\mathbb{Z}) = \frac{d\mathbb{Z}}{n\mathbb{Z}}$ is a bijection. Clearly all $\frac{d\mathbb{Z}}{n\mathbb{Z}}$ with $d \in D(n)$ would then be subgroups of $\frac{\mathbb{Z}}{n\mathbb{Z}}$. Moreover by the surjectivity of m, we can then see that for any $K \leq \frac{\mathbb{Z}}{n\mathbb{Z}}$, there exists $d\mathbb{Z}$ with $d \mid n$, such that $K = m(d\mathbb{Z}) = \frac{d\mathbb{Z}}{n\mathbb{Z}}$. We can thus conclude that the subgroups of $\frac{\mathbb{Z}}{n\mathbb{Z}}$ are exactly those of the form $\frac{d\mathbb{Z}}{n\mathbb{Z}}$ with $d \in D(n)$.

9/27 Lecture

Proposition 1.85 (Digression on cyclic groups)**.** A subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group and assume that it is generated by a. Also let H be an arbitrary subgroup of G. If $H = \{e\}$, then $H = \langle e \rangle$ and thus is cyclic so we are done. Therefore we assume that $H \neq \{e\}$. This means that $a^n \in H$ for some $n \in \mathbb{N}^*$. Let m be the smallest integer in $\mathbb{N}^*$ such that $a^m \in H$, then we claim that $H = \langle a^m \rangle$. To see this, we need to show that every $b \in H$ is some positive integer power of a^m. Now since $b \in H$ and $H \leq G$, there exists $n \in \mathbb{N}$ such that $b = a^n$. Then by Euclidean division property, there exists unique integers q and r such that $n = mq + r$, with $0 \leq r < m$. Consequently, $b = a^{mq+r} = (a^m)^q \cdot a^r$, and thus $a^r = b \cdot (a^m)^{-q}$. We note that $b \in H$ and $a^m \in H$, so that $a^r \in H$. But m is the smallest integer in $\mathbb{N}^*$ such that $a^m \in H$, so necessarily $r = 0$ (otherwise $a^r \in H$ with $0 < r < m$ leads to a contradiction). Therefore, each b can be written as $b = (a^m)^q$, which means that $H = \{a^m\}$. By arbitrariness of H, we can hence conclude that every subgroup of a cyclic group G is cyclic, and the proof is complete. □

Alternative proof. If G is cyclic, it is isomorphic to $\frac{\mathbb{Z}}{n\mathbb{Z}}$ for some $n \in \mathbb{N}$ (Theorem 1.77). Hence, it is sufficient to prove that the statement holds for subgroups H of $\frac{\mathbb{Z}}{n\mathbb{Z}}$. If $n = 0$, then $\frac{\mathbb{Z}}{n\mathbb{Z}} \simeq \mathbb{Z}$, so any subgroup H must be of the form $H = m\mathbb{Z} = \langle m \rangle$ for some $m \in \mathbb{N}$, thus being cyclic. Otherwise if $n \geq 1$, we have just shown in a previous example that any subgroup H must be of the form $H = \frac{d\mathbb{Z}}{n\mathbb{Z}} = \langle \overline{d} \rangle$ for some $d \in D(n)$, also being cyclic. The proof is thus complete. □

Example 1.86. We shall check that for $d \in D(n)$, we have that $\frac{d\mathbb{Z}}{n\mathbb{Z}} \simeq \frac{\mathbb{Z}}{\frac{n}{d}\mathbb{Z}}$. How to do this?

Theorem 1.87 (Second isomorphism theorem)**.** Take $f \in \operatorname{Hom}(G, G')$, and fix $N \trianglelefteq G$ with $N \subseteq \operatorname{Ker}(f)$. If p is the canonical projection from G to $\frac{G}{N}$, then there is a unique mapping $\overline{f} : \frac{G}{N} \to G'$ such that $f = \overline{f} \circ p$. Moreover, $\overline{f}$ is a group homomorphism such that $\operatorname{Im}(\overline{f}) = \operatorname{Im}(f)$ and $\operatorname{Ker}(\overline{f}) = \frac{\operatorname{Ker}(f)}{N}$.

Proof. If $\overline{f}$ exists, it is unique by the formula $\overline{f}(\overline{g}) = \overline{f}(p(g)) = (\overline{f} \circ p)(g) = f(g)$. Therefore, it suffices to prove that such $\overline{f}$ exists, *i.e.*, to check that the mapping $\overline{f} : \frac{G}{N} \to G'$ such that $\overline{g} \mapsto f(g)$ is well-defined. Indeed, if $\overline{g'} = \overline{g}$, then there exists $n \in N$ such that $g' = gn$. As a consequence, $f(g') = f(gn) = f(g)f(n) = f(g)$ because f is a homomorphism and $n \in N \subseteq \operatorname{Ker}(f)$. This proves that $\overline{f}$ is well-defined. Now we prove that $\overline{f}$ is a group homomorphism. For any $\overline{g}, \overline{g'} \in \frac{G}{N}$, we have that

$$\overline{f}(\overline{g} \cdot \overline{g'}) = \overline{f}(\overline{gg'}) = f(gg') = \underbrace{f(g)f(g')}_{f \in \operatorname{Hom}(G,G')} = \overline{f}(\overline{g})\overline{f}(\overline{g'}), \tag{22}$$

so indeed $\overline{f} \in \mathrm{Hom}\left(\frac{G}{N}, G'\right)$. Finally, $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$ directly follows from the formula $\overline{f}(\overline{g}) = f(g)$, and we note that

$$\overline{g} \in \mathrm{Ker}(\overline{f}) \iff \overline{f}(\overline{g}) = e' \iff f(g) = e' \iff g \in \mathrm{Ker}(f) \iff \overline{g} \in \frac{\mathrm{Ker}(f)}{N}. \tag{23}$$

This necessarily means that $\mathrm{Ker}(\overline{f}) = \frac{\mathrm{Ker}(f)}{N}$, and the proof is now complete. □

Corollary 1.88. With the same notations as in Theorem 1.87, we have that

$$\frac{\frac{G}{N}}{\frac{\mathrm{Ker}(f)}{N}} \overset{\overline{(\overline{f})}}{\simeq} \mathrm{Im}(f). \tag{24}$$

Proof. By the second isomorphism theorem (Theorem 1.87), we have that $\overline{f} \in \mathrm{Hom}\left(\frac{G}{N}, G'\right)$. By Corollary 1.76, we then have that

$$\frac{\frac{G}{N}}{\mathrm{Ker}(\overline{f})} \overset{\overline{(\overline{f})}}{\simeq} \mathrm{Im}(\overline{f}). \tag{25}$$

Again by the second isomorphism theorem (Theorem 1.87), we have that $\mathrm{Ker}(\overline{f}) = \frac{\mathrm{Ker}(f)}{N}$ and $\mathrm{Im}(\overline{f}) = \mathrm{Im}(f)$, so the proof is now complete by substituting these results into the relation above. □

Corollary 1.89. Suppose that N and H are two normal subgroups of G with $N \subseteq H$, then $\frac{H}{N}$ is a normal subgroup of $\frac{G}{N}$ and we have that

$$\frac{\frac{G}{N}}{\frac{H}{N}} \simeq \frac{G}{H}. \tag{26}$$

Proof. Since H is a normal subgroup of G, clearly $\frac{H}{N}$ is a normal subgroup of $\frac{G}{N}$. Let $f := p_H$ be the canonical projection from G to $\frac{G}{H}$. Then by the previous corollary we can conclude that

$$\frac{\frac{G}{N}}{\frac{H}{N}} = \frac{\frac{G}{N}}{\frac{\mathrm{Ker}(f)}{N}} \simeq \mathrm{Im}(f) = \frac{G}{H}. \tag{27}$$

The proof is thus complete. □

Example 1.90. If $d \in D(n)$, then $d\mathbb{Z}$ and $n\mathbb{Z}$ are both normal subgroups of $\mathbb{Z}$ and $n\mathbb{Z} \subseteq d\mathbb{Z}$. Then $\frac{d\mathbb{Z}}{n\mathbb{Z}}$ is a normal subgroup of $\frac{\mathbb{Z}}{n\mathbb{Z}}$, and that

$$\frac{\frac{\mathbb{Z}}{n\mathbb{Z}}}{\frac{d\mathbb{Z}}{n\mathbb{Z}}} \simeq \frac{\mathbb{Z}}{d\mathbb{Z}}. \tag{28}$$

10/9 Lecture

1.9 Group Actions

Definition 1.91. Let G be a group and X be a set. One says that a map $G \times X \to X$ defined by $(g, x) \mapsto g \cdot x$ is a **group action** if:

(1) $e \cdot x = x$ for all $x \in X$.

(2) $g \cdot (h \cdot x) = (gh) \cdot x$ for all $g, h \in G$ and $x \in X$.

Example 1.92. (1) If V is a k-vector space, then $GL(V)$ acts on V by $g \cdot v = g(v)$.

(2) The group $\mathfrak{S}(X)$ acts on X by $\sigma \cdot x = \sigma(x)$.

(3) If $H \leq G$, the one can define at least three natural actions of H on G: the action by **left translation** $h \cdot_1 g := hg$, the action by **right translation** $h \cdot_2 g := gh^{-1}$, and the action by **conjugation** $h \cdot_3 g = hgh^{-1}$.

Proposition 1.93. (1) If $(g, x) \mapsto g * x$ is an action of the group G and the set X, then for any fixed $g \in G$ the mapping $\phi_*(g) : X \to X$ such that $x \mapsto g * x$ belongs to $\mathfrak{S}(X)$. The mapping $\phi_* : G \to \mathfrak{S}(X)$ is a homomorphism from G to $\mathfrak{S}(X)$.

(2) Conversely if $\phi : G \to \mathfrak{S}(X)$ is a homomorphism and if we set $g *_\phi x := \phi(g)(x)$, then the mapping $G \times X \to X$ such that $(g, x) \mapsto g *_\phi x$ is a group action.

(3) Both constructions above are "inverse" of each other.

Proof. (1) For fixed $g \in G$, the mapping $\phi_*(g)$ is bijective with inverse $\phi_*(g^{-1})$. Indeed for any $x \in X$, we have

$$(\phi_*(g) \circ \phi_*(g^{-1}))(x) = \phi_*(g)(\phi_*(g^{-1})(x)) = \phi_*(g)(g^{-1} * x) = \underbrace{g * (g^{-1} * x) = (gg^{-1}) * x}_{\text{by group action}} = x, \tag{29}$$

so that $\phi_*(g) \circ \phi_*(g^{-1}) = \mathrm{Id}_X$, and analogously we can see that $\phi_*(g^{-1}) \circ \phi_*(g) = \mathrm{Id}_X$ as well. Hence, $\phi_*(g) \in \mathfrak{S}(X)$. Moreover for arbitrary $g, h \in G$ and $x \in X$, we have that

$$(\phi_*(g) \circ \phi_*(h))(x) = \phi_*(g)(\phi_*(h)(x)) = \phi_*(g)(h * x) = \underbrace{g * (h * x) = (gh) * x}_{\text{by group action}} = \phi_*(gh)(x), \tag{30}$$

so that $\phi_*(g) \circ \phi_*(h) = \phi_*(gh)$, and by arbitrariness of g and h we can conclude that $\phi_* \in \mathrm{Hom}(G, \mathfrak{S}(X))$.

(2) Since $\phi \in \mathrm{Hom}(G, \mathfrak{S}(X))$, for any $g, h \in G$ and $x \in X$ we have that

$$g *_\phi (h *_\phi x) = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))(x) = \phi(gh)(x) = (gh) *_\phi x, \tag{31}$$

so $(g, x) \mapsto g *_\phi x$ is indeed a group action.

(3) We need to check that if $(g, x) \mapsto g * x$ is an action of G on X then $*_{\phi_*} = *$, and that if $\phi \in \mathrm{Hom}(G, \mathfrak{S}(X))$ then $\phi_{*_\phi} = \phi$. First, if $(g, x) \mapsto g * x$ is an action of G on X, then for any $g \in G$ and $x \in X$, by definition we have that $g *_{\phi_*} x = \phi_*(g)(x) = g * x$, so $*_{\phi_*} = *$. On the other hand, if $\phi \in \mathrm{Hom}(G, \mathfrak{S}(X))$, then for any $g \in G$ and $x \in X$, we have that $\phi_{*_\phi}(g)(x) = g *_\phi x = \phi(g)(x)$, so $\phi_{*_\phi} = \phi$ as well. The proof is thus complete. □

10/11 Lecture

Example 1.94. (1) Recall in a previous example that, if V is a k-vector space, then $GL(V)$ acts on V by $g \cdot v = g(v)$. The corresponding homomorphism is the tautological homomorphism, *i.e.*, the natural inclusion of $GL(V)$ into $\mathfrak{S}(V)$.

(2) Recall in a previous example that, the group $\mathfrak{S}(X)$ acts on X by $\sigma \cdot x = \sigma(x)$. The corresponding homomorphism is again the tautological homomorphism, *i.e.*, the identity mapping from $\mathfrak{S}(X)$ to itself.

Definition 1.95. For $x \in X$ and G acting on X, one calls the **orbit** of x the set $\mathscr{O}_x := G \cdot x = \{g \cdot x;\ g \in G\}$.

Theorem 1.96. If G acts on X, the relation $x \sim y$ if there exists $g \in G$ such that $y = g \cdot x$, is an equivalence relation on X, and for this relation $Cl(X) = G \cdot x$. In particular, the orbits of G in X form a partition of X.

Example 1.97. (1) For the natural action of $GL(V)$ on V, there are two orbits, *i.e.*, $\{0\}$ and $V \setminus \{0\}$.

(2) For the action of the rotations group $SO(\mathbb{R}^2) = \left\{Q \in GL_2(\mathbb{R});\ Q^\top Q = QQ^\top = I\right\}$ on $\mathbb{R}^2$, the orbit of $v \in \mathbb{R}^2$ is the circle $C(0, \|v\|)$ of center 0 and radius $\|v\|$ the Euclidean norm of v.

10/16 Lecture

Definition 1.98. One says that an action of G on X is **transitive** if it has a single orbit, which must be X. In other words $X = G \cdot x$ for some $x \in X$ or equivalently $X = G \cdot x$ for all $x \in X$.

Proposition 1.99. Let $G \times X \to X$ such that $(g, x) \mapsto g \cdot x$ be an action of G on X, and suppose that $A \subseteq X$ is G-stable, *i.e.*, for any $x \in A$ and $g \in G$, necessarily $g \cdot x \in A$. Then the mapping $G \times A \to A$ such that $(g, x) \mapsto g \cdot x$ obtained by restriction of the second variable is an action of G on A.

Example 1.100. The most basic example of the above situation is when you start with a group action $G \times X \to X$ such that $(g, x) \mapsto g \cdot x$, and take $A := G \cdot x$ to be the orbit of an element $x \in X$. Clearly $G \cdot x$ is G-stable because of the property $g \cdot (g' \cdot x) = (gg') \cdot x$. Then by restriction (of the second variable) one gets an action of G on $G \cdot x$. *Such a restricted action to one orbit is automatically transitive by definition.* For instance, the natural action of $GL(V)$ on $V \setminus \{0\}$ is transitive as we saw that $V \setminus \{0\}$ is the orbit of any nonzero vector.

Definition 1.101. If G acts on X and $x \in X$, we set $\mathrm{Stab}_G(x) = \{g \in G;\ g \cdot x = x\}$ and call this set the **stabilizer subgroup** of x in G.

Remark 1.102. Clearly $\mathrm{Stab}_G(x) \leq G$, so indeed it can be called a subgroup. Indeed, $e_G \in \mathrm{Stab}_G(x)$ because $e_G \cdot x = x$. Associativity clearly holds because $\mathrm{Stab}_G(x) \subseteq G$. Finally, if $g \in \mathrm{Stab}_G(x)$, then $g \cdot x = x$, and multiplying both sides by g^{-1} on the left, we can see that $x = g^{-1} \cdot x$, and thus $g^{-1} \in \mathrm{Stab}_G(x)$.

Example 1.103. We shall check that the action of $\mathfrak{S}_n$ on $\{1, \ldots, n\}$ is transitive, and that $\mathrm{Stab}_{\mathfrak{S}_n}(1) \simeq \mathfrak{S}_{n-1}$. Indeed, for any $i \in \{1, \ldots, n\}$, we have that $\mathfrak{S}_n \cdot i = \{1, \ldots, n\}$. Moreover, $\mathfrak{S}_n$ contains all possible permutations over $\{1, \ldots, n\}$, so the set of those permutations which fix 1 are simply the ones that permute the set $\{2, \ldots, n\}$ in every possible way, thus $\mathrm{Stab}_{\mathfrak{S}_n}(1) \simeq \mathfrak{S}_{n-1}$.

Example 1.104. Let $H \leq G$, then the mapping $G \times G/H \to G/H$ such that $(g, g'H) \mapsto gg'H$ defines a transitive action of G on G/H. For this action $\mathrm{Stab}_G(eH) = H$. Indeed, for any $\overline{g} \in G/H$, there exists $g \in G$ such that $\overline{g} = gH$, so we have that $G \cdot gH = \{g'gH;\ g' \in G\} = \{g'H;\ g' \in G\} = G/H$. Moreover, for $g \in G$, if $g \cdot eH = geH = gH = eH$, then necessarily $g \in H$. Hence we can conclude that $\mathrm{Stab}_G(eH) = H$.

Theorem 1.105 (Orbit-stabilizer theorem)**.** If G acts on X, then the mapping $\phi_x : G/\mathrm{Stab}_G(x) \to G \cdot x$ such that $g\mathrm{Stab}_G(x) \mapsto g \cdot x$ is well-defined and bijective. In particular if G is finite, then $|G \cdot x| = |G|/|\mathrm{Stab}_G(x)|$.

Proof. To see that ϕ_x is well-defined, we need to prove that if $g\mathrm{Stab}_G(x) = g'\mathrm{Stab}_G(x)$ then $g \cdot x = g' \cdot x$. Indeed, if $g\mathrm{Stab}_G(x) = g'\mathrm{Stab}_G(x)$, then there exists $h \in \mathrm{Stab}_G(x)$ such that $g' = gh$, and thus $g' \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$, where the last equality is because of stability. Hence we have shown that ϕ_x is well-defined. Now clearly ϕ_x is surjective by its definition, so it suffices to prove that ϕ_x is injective as well. Suppose that $\phi_x(\overline{g}) = \phi_x(\overline{g}')$, then $g \cdot x = g' \cdot x$. Acting by g^{-1} on both sides, we can see that $x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g' \cdot x) = (g^{-1}g') \cdot x$. This further implies that $g^{-1}g' \in \mathrm{Stab}_G(x)$, and thus $g' \in g\mathrm{Stab}_G(x)$. This necessarily means that $g\mathrm{Stab}_G(x) = g'\mathrm{Stab}_G(x)$, *i.e.*, $\overline{g} = \overline{g'}$, so the proof of injectivity is done. Hence, we can conclude that ϕ_x is bijective. Finally if G is finite, Lagrange's theorem (Theorem 1.65) implies that $|G \cdot x| = |G/\mathrm{Stab}_G(x)| = |G|/|\mathrm{Stab}_G(x)|$, and the proof is thus complete. □

Remark 1.106. In particular if the action of G on X is transitive, we obtain a natural bijection $G/\mathrm{Stab}_G(x) \simeq X$.

10/18 Lecture

Corollary 1.107 (Class formula)**.** If X is finite and the partition of X into G-orbits is given by $X = \bigsqcup_{i=1}^{r} G \cdot x_i$, then $|X| = \sum_{i=1}^{r} |G \cdot x_i|$. If G is moreover finite, then $|X| = \sum_{i=1}^{r} |G|/|\mathrm{Stab}_G(x_i)|$.

Proof. This is trivial. □

Definition 1.108. Let G be a group, then we say that a set X is a G**-space** if G acts on X. If X and Y are both G-spaces, then we say that a mapping $\phi : X \to Y$ is G**-equivariant** if $\phi(g \cdot x) = g \cdot \phi(x)$ for all $(g, x) \in G \times X$.

Remark 1.109. One can observe that the bijection $\phi_x : G/\mathrm{Stab}_G(x) \to G \cdot x$ in the statement of the orbit-stabilizer theorem (Theorem 1.105) is G-equivariant for the action of G on $G/\mathrm{Stab}_G(x)$ defined in Example 1.104, and the natural action of G on $G \cdot x$ is defined by restriction of the second variable. Indeed, for all $(g', \overline{g}) \in G \times G/\mathrm{Stab}_G(x)$, there exists $g \in G$ such that $\overline{g} = g\mathrm{Stab}_G(x)$, so we have that

$$\phi_x(g' \cdot \overline{g}) = \phi_x(g'g\mathrm{Stab}_G(x)) = (g'g) \cdot x = g' \cdot (g \cdot x) = g' \cdot \phi_x(g\mathrm{Stab}_G(x)) = g' \cdot \phi_x(\overline{g}). \tag{32}$$

Definition 1.110. If p is a prime number, one calls G a p**-group** if it is finite of cardinality of $|G| = p^a$ for some $a \in \mathbb{N}$.

Remark 1.111. By Lagrange's theorem (Theorem 1.65), a subgroup of a p-group is again a p-group.

Definition 1.112. If X is a G-space, we set $X^G := \{x \in X;\ g \cdot x = x,\ \forall g \in G\}$. In other words, X^G denotes the fixed points of the action of G on X.

Lemma 1.113. Let G be a p-group for some prime number p, and X be a finite set. Then $|X| \equiv |X^G| \mod p$.

Proof. If $X = X^G$ then the result is obvious, so we assume that $X \neq X^G$. Note that

$$x \in X^G \iff G \cdot x = \{x\} \iff |G \cdot x| = 1 \iff |\mathrm{Stab}_G(x)| = |G|, \tag{33}$$

where the last equivalence follows from the orbit-stabilizer theorem (Theorem 1.105). We can write $X = \bigsqcup_{i=1}^{r} G \cdot x_i$ and up to renumbering, suppose that the first s orbits are those of cardinality 1, *i.e.*, $X^G = \{x_1, \ldots, x_s\}$. Our assumption that $X \neq X^G$ further ensures that $s < r$. By the class formula (Corollary 1.107), we can see that

$$|X| = \sum_{i=1}^{r} |G \cdot x_i| = s + \sum_{i=s+1}^{r} |G \cdot x_i| = |X^G| + \sum_{i=s+1}^{r} |G \cdot x_i|. \tag{34}$$

Hence, we are reduced to proving that $\sum_{i=s+1}^{r} |G \cdot x_i|$ is a multiple of p, which will follow from the fact that each $|G \cdot x_i|$ is a multiple of p for $i \geq s+1$. Indeed, for $i \geq s+1$, we have that $|G \cdot x_i| = |G|/|\mathrm{Stab}_G(x_i)|$ and $|G| = p^a$ for some $a \in \mathbb{N}^*$ (a cannot be zero since otherwise G would be trivial, contradicting our assumption that $X \neq X^G$), so by primality of p, it is clearly that $|G \cdot x_i|$ must also be a multiple of p given that it is not 1. The proof is thus complete. □

Corollary 1.114. If G is a non-trivial p-group for some prime number p, then $Z(G)$ is not reduced to $\{e\}$.

Proof. Take $X := G$ is the previous proposition and G acts on itself by conjugation (*i.e.*, $g \cdot x = gxg^{-1}$, $g \in G$, $x \in X = G$), then we have that $|G| \equiv |G^G| \mod p$. Note that $G^G = Z(G)$ in this case. Indeed if $x \in G^G$, then $g \cdot x = gxg^{-1} = x$ for all $g \in G$, which means that $gx = xg$ for all $g \in G$, so $x \in Z(G)$. On the other hand, if $x \in Z(G)$, then $gx = xg$ for all $g \in G$, and thus then $g \cdot x = gxg^{-1} = xgg^{-1} = x$ for all $g \in G$, so $x \in G^G$. Hence, we can conclude that $|G| \equiv |Z(G)| \mod p$. Since G is a non-trivial p-group, we have that $|G| \equiv 0 \mod p$, and thus $|Z(G)| \equiv 0 \mod p$ as well. This necessarily implies that $|Z(G)| \neq 1$, so $Z(G)$ cannot be reduced to $\{e\}$, and thus the proof is complete. □

Example 1.115. Let G be a group of order p^2 for some prime number p, then G is commutative. Indeed, by the previous corollary, we have that $Z(G) \neq \{e\}$, so either $|Z(G)| = p$ or $|Z(G)| = p^2$. The latter case is trivial since then $Z(G) = G$, meaning that G is commutative. In the former case, by Lagrange's theorem (Theorem 1.65) $|G/Z(G)| = p$, and further since p is prime by the remark of the same theorem $G/Z(G) = \langle \overline{g} \rangle$ for any $\overline{g} \in G/Z(G)$ with $\overline{g} \neq \overline{e}$. Without loss of generality we assume that $G/Z(G) = \langle xZ(G) \rangle$ with $x \in G$ and $x \neq e$. For any $g \in G$, there exists $m \in \mathbb{N}$ such that $gZ(G) = x^m Z(G)$. This means that $g(x^m)^{-1} \in Z(G)$, so there exists $z \in Z(G)$ such that $g(x^m)^{-1} = z$, or in other words, $g = zx^m$. Now for any $g_1, g_2 \in G$, suppose that $g_1 = x^{m_1} z_1$ and $g_2 = x^{m_2} z_2$, where $m_1, m_2 \in \mathbb{N}$ and $z_1, z_2 \in Z(G)$. We can thus compute that

$$g_1 g_2 = x^{m_1} z_1 x^{m_2} z_2 = x^{m_1+m_2} z_1 z_2 = x^{m_2+m_1} z_2 z_1 = x^{m_2} z_2 x^{m_1} z_1 = g_2 g_1, \tag{35}$$

so G is commutative, and the proof is thus complete. To summarize what we have shown, $G/Z(G)$ being of prime order p implies that it is cyclic, and this necessarily means that G is commutative.

10/23 Lecture

1.10 Decomposition of Permutations

Definition 1.116. Let $\{a_1, \dots, a_r\}$ be a subset of $\{1, \dots, n\}$ with $r \geq 1$ different elements, then the permutation $\begin{pmatrix} a_1 & a_2 & \dots & a_r \end{pmatrix} \in \mathfrak{S}_n$ fixes by definition any $i \in \{1, \dots, n\} \setminus \{a_1, \dots, a_r\}$, sends a_i to a_{i+1} for $i \in \{1, \dots, r-1\}$, and sends a_r to a_1. A permutation of this form is called an r**-cycle** or a **cycle of length** r.

Definition 1.117. A permutation in $\mathfrak{S}_n$ is called a **cycle** if it is an r-cycle for some $1 \leq r \leq n$.

Example 1.118. By definition, a 1-cycle is the identity of $\mathfrak{S}_n$. For this reason we usually do not consider 1-cycles as they are all equal to the identity.

Definition 1.119. If $\sigma \in \mathfrak{S}_n$, one denotes by $\mathrm{Fix}(\sigma)$ its set of **fixed points**, *i.e.*, we have that

$$\mathrm{Fix}(\sigma) := \{x \in \{1, \dots, n\}\, ;\, \sigma(x) = x\}\,. \tag{36}$$

Example 1.120. If $c := \begin{pmatrix} a_1 & a_2 & \dots & a_r \end{pmatrix} \in \mathfrak{S}_n$, then $\mathrm{Fix}(c) = \{1, \dots, n\} \setminus \{a_1, \dots, a_r\}$.

Remark 1.121. For $\sigma \in \mathfrak{S}_n$, we have that $\mathrm{Fix}(\sigma) \subseteq \mathrm{Fix}(\sigma^k)$ for any $k \in \mathbb{Z}$. In particular, $\sigma^k(\mathrm{Fix}(\sigma)) = \mathrm{Fix}(\sigma)$. Indeed, if $x \in \mathrm{Fix}(\sigma)$, then $\sigma(x) = x$, and composing both sides by σ^{-1} we also have $x = \sigma^{-1}(x)$. For any $k_1 \geq 1$ and $k_2 \leq -1$, inductively we have that

$$\sigma^{k_1}(x) = \sigma^{k_1 - 1}(x) = \ldots = \sigma(x) = x = \sigma^{-1}(x) = \sigma^{-2}(x) = \ldots = \sigma^{k_2}(x), \tag{37}$$

so $\sigma^k(x) = x$ for any $k \in \mathbb{Z}$. This proves that $\mathrm{Fix}(\sigma) \subseteq \mathrm{Fix}(\sigma^k)$ for any $k \in \mathbb{Z}$. It is then clear that σ^k acts like the identity on $\mathrm{Fix}(\sigma)$, so $\sigma^k(\mathrm{Fix}(\sigma)) = \mathrm{Fix}(\sigma)$.

Definition 1.122. The **support** $\mathrm{Supp}(\sigma)$ of a permutation $\sigma \in \mathfrak{S}_n$ is by definition the set of non-fixed points of σ, such that

$$\mathrm{Supp}(\sigma) := \{1, \dots, n\} \setminus \mathrm{Fix}(\sigma) = \{x \in \{1, \dots, n\}\, ;\, \sigma(x) \neq x\}\,. \tag{38}$$

Example 1.123. If $c := \begin{pmatrix} a_1 & a_2 & \dots & a_r \end{pmatrix} \in \mathfrak{S}_n$, then $\mathrm{Supp}(c) = \{a_1, \dots, a_r\}$.

Remark 1.124. For $\sigma \in \mathfrak{S}_n$, we have that $\mathrm{Supp}(\sigma^k) \subseteq \mathrm{Supp}(\sigma)$ for any $k \in \mathbb{Z}$. In particular, $\sigma^k(\mathrm{Supp}(\sigma)) = \mathrm{Supp}(\sigma)$. Indeed since $\mathrm{Fix}(\sigma) \subseteq \mathrm{Fix}(\sigma^k)$, the first conclusion is trivial by taking complements. The second conclusion follows since $\sigma^k(\mathrm{Fix}(\sigma)) = \mathrm{Fix}(\sigma)$ and σ^k is bijective.

Lemma 1.125. If c_1 and c_2 are two cycles in $\mathfrak{S}_n$ with disjoint support, then $c_1 \circ c_2 = c_2 \circ c_1$.

Proof. Write $c_1 = \begin{pmatrix} a_1 & \dots & a_r \end{pmatrix}$ and $c_2 = \begin{pmatrix} b_1 & \dots & b_s \end{pmatrix}$, with respective supports $S_1 = \{a_1, \dots, a_r\}$ and $S_2 = \{b_1, \dots, b_s\}$. By assumption $S_1 \cap S_2 = \varnothing$. We consider three cases:

- If $i \notin S_1 \cup S_2$, then $c_1(i) = c_2(i) = i$, so $(c_1 \circ c_2)(i) = c_1(c_2(i)) = c_1(i) = i = c_2(i) = c_2(c_1(i)) = (c_2 \circ c_1)(i)$.
- If $i \in S_1$, then $c_1(i) \in S_1$ and $c_2(i) = i$. Hence $c_2(c_1(i)) = c_1(i)$ because $c_1(i) \notin S_2$. Therefore, we can deduce that $(c_1 \circ c_2)(i) = c_1(c_2(i)) = c_1(i) = c_2(c_1(i)) = (c_2 \circ c_1)(i)$.
- If $i \in S_2$, then $c_2(i) \in S_2$ and $c_1(i) = i$. Hence $c_1(c_2(i)) = c_2(i)$ because $c_2(i) \notin S_1$. Therefore, we can deduce that $(c_1 \circ c_2)(i) = c_1(c_2(i)) = c_2(i) = c_2(c_1(i)) = (c_2 \circ c_1)(i)$.

By arbitrariness of i, we can conclude that $c_1 \circ c_2 = c_2 \circ c_1$, and the proof is thus complete. □

Theorem 1.126. In $\mathfrak{S}_n$, any permutation σ can be written $\sigma = c_1 \circ \ldots \circ c_d$ for some $d \in \mathbb{N}$ (by convention $\sigma = \mathrm{Id}$ if $d = 0$), where each c_i is a cycle of length at least 2, and all cycles c_i have disjoint supports. Moreover, the decomposition is unique up to the reordering of the cycles c_i.

Proof. The group $G := \langle \sigma \rangle$ acts on $\{1, \ldots, n\}$, so we have a decomposition of $\{1, \ldots, n\}$ into G-orbits, such that

$$\{1, \ldots, n\} = \bigsqcup_{k=1}^{m} G \cdot i_k. \tag{39}$$

Up to renumbering, we suppose that $l_k := |G \cdot i_k| \geq 2$ for $1 \leq k \leq d$, whereas $l_k = 1$ for $d+1 \leq k \leq m$. We note that $l_k = 1$ if and only if $\sigma(i_k) = i_k$. To see this, if $\sigma(i_k) = i_k$ then $\sigma_p(i_k) = i_k$ for any $p \in \mathbb{Z}$, meaning that $G \cdot i_k = \{i_k\}$ and so $l_k = 1$. On the other hand if $l_k = 1$, then $G \cdot i_k = \{i_k\}$ so that $\sigma(i_k) = i_k$. We can thus write that

$$\mathrm{Fix}(\sigma) = \bigsqcup_{k=d+1}^{m} G \cdot i_k = \{i_{d+1}, \ldots, i_m\}. \tag{40}$$

On the other hand, for $k = 1, \ldots, d$, one shall be able to check that $G \cdot i_k = \left\{i_k, \sigma(i_k), \ldots, \sigma^{l_k - 1}(i_k)\right\}$ and $\sigma^{l_k}(i_k) = i_k$. WHY? From this, it follows that $\sigma = c_1 \circ \ldots \circ c_d$ where $c_k := \begin{pmatrix} i_k & \sigma(i_k) & \ldots & \sigma^{l_k-1}(i_k) \end{pmatrix}$ for $1 \leq k \leq d$. WHY? This proves the existence of the decomposition. To prove the uniqueness, suppose that $\sigma = c'_1 \circ \ldots \circ c'_d$ is another such decomposition. One can easily check that $G \cdot a_i = \mathrm{Supp}(c'_i)$ if $a_i \in \mathrm{Supp}(c'_i)$, and $G \cdot x = \{x\}$ if x is not in the support of any c'_i. WHY? By uniqueness of the decomposition of $\{1, \cdots, n\}$ into G-orbits, we deduce that $d = d'$, and that up to reordering, $\mathrm{Supp}(c'_i) = \mathrm{Supp}(c_i)$. WHY? Finally because σ decomposes over both families of cycles and by disjointness of the supports, for any $a_i \in \mathrm{Supp}(c'_i) = \mathrm{Supp}(c_i)$, we can see that $c_i = \begin{pmatrix} a_i & \sigma(a_i) & \ldots & \sigma^{l_i - 1}(a_i) \end{pmatrix} = c'_i$, where l_i is the common length of c_i and c'_i. WHY? The proof is thus complete. □

Example 1.127. In $\mathfrak{S}_8$, the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 5 & 6 & 2 & 4 & 1 & 8 & 7 \end{pmatrix} \tag{41}$$

has the commuting decomposition $\sigma = \begin{pmatrix} 1 & 3 & 6 \end{pmatrix} \circ \begin{pmatrix} 2 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 7 & 8 \end{pmatrix}$.

10/25 Lecture

Proposition 1.128. Let σ and σ' be two permutations in $\mathfrak{S}_n$, and let $\sigma = c_1 \circ \ldots \circ c_d$ and $\sigma' = c'_1 \circ \ldots \circ c'_{d'}$ be their two decompositions into (commuting) cycles with disjoint support (of length at least 2). We order the cycles by length, such that $2 \leq l_1 \leq \ldots \leq l_d$ and $2 \leq l'_1 \leq \ldots \leq l'_{d'}$, where $l_i = l(c_i)$ and $l'_j = l(c'_j)$. Then σ and σ' are conjugate in $\mathfrak{S}_n$ if and only if $d = d'$ and $l_i = l'_i$ for all $i = 1, \ldots, d$.

Proof. TO BE DONE... □

Remark 1.129. In particular, if c is an r-cycle in $\mathfrak{S}_n$, then its conjugacy class consists of all r-cycles in $\mathfrak{S}_n$.

Remark 1.130. The r-cycle $\begin{pmatrix} a_1 & \ldots & a_r \end{pmatrix} \in \mathfrak{S}_n$ is can be decomposed as

$$\begin{pmatrix} a_1 & \ldots & a_r \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \end{pmatrix} \circ \begin{pmatrix} a_2 & a_3 \end{pmatrix} \circ \ldots \circ \begin{pmatrix} a_{r-1} & a_r \end{pmatrix}. \tag{42}$$

Definition 1.131. A **transposition** is a 2-cycle.

Corollary 1.132. The group $\mathfrak{S}_n$ is generated by the transpositions.

Proof. This is trivial because we have seen that every permutation is a product of cycles, and that every cycle is a product of transpositions. □

1.11 The Sign Map

Definition 1.133. Let $\sigma \in \mathfrak{S}_n$, we say that $(i,j) \in \{1,\dots,n\}^2$ with $i<j$ is an **inversion** of σ if $\sigma(i) > \sigma(j)$. We denote by $\mathrm{Inv}(\sigma)$ the set of inversions of σ, and by $l(\sigma)$ its cardinality.

Definition 1.134. For $\sigma \in \mathfrak{S}_n$, we set $\epsilon(\sigma) := (-1)^{l(\sigma)}$, and call it the **sign** of σ.

Remark 1.135. For $x \in \mathbb{R}^\times$, we set $\mathrm{sgn}(x) = x/|x|$. Then by definition, for any $\sigma \in \mathfrak{S}_n$, we have that

$$\epsilon(\sigma) = \prod_{1 \le i < j \le n} \mathrm{sgn}(\sigma(j) - \sigma(i)). \tag{43}$$

This formula is very useful in practice for computing the sign of a permutation.

Remark 1.136. We give another familiar (though not very useful) formula for the sign of a permutation. For $\sigma \in \mathfrak{S}_n$, we have that

$$\epsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}. \tag{44}$$

To see this, from the useful formula we have that

$$\epsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{|\sigma(j) - \sigma(i)|} = \frac{\prod_{1 \le i < j \le n}(\sigma(j) - \sigma(i))}{\prod_{1 \le i < j \le n}|\sigma(j) - \sigma(i)|}. \tag{45}$$

But note that $\prod_{1 \le i < j \le n}|\sigma(j) - \sigma(i)| = \prod_{1 \le j < i \le n}|\sigma(j) - \sigma(i)|$, so that

$$\left(\prod_{1 \le i < j \le n}|\sigma(j) - \sigma(i)|\right)^2 = \prod_{1 \le i \ne j \le n}|\sigma(j) - \sigma(i)|. \tag{46}$$

Moreover, by the bijectivity of σ, we can see that

$$\prod_{1 \le i \ne j \le n}|\sigma(j) - \sigma(j)| = \prod_{1 \le k \ne l \le n}|l - k| = \prod_{1 \le i \ne j \le n}|j - i| = \left(\prod_{1 \le i < j \le n}|j - i|\right)^2 = \left(\prod_{1 \le i < j \le n}(j - i)\right)^2, \tag{47}$$

so we arrive at the conclusion that

$$\epsilon(\sigma) = \frac{\prod_{1 \le i < j \le n}(\sigma(j) - \sigma(i))}{\prod_{1 \le i < j \le n}(j - i)} = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}, \tag{48}$$

as desired.

Theorem 1.137. $\epsilon : \mathfrak{S}_n \to \{\pm 1\}$ is a group homomorphism, which is surjective if $n \ge 2$.

Proof. We prove this by the original definition of the sign map. If $A \subseteq \left\{(i,j) \in \{1,\dots,n\}^2 ;\ i<j\right\}$, we set

$$A^C := \left\{(i,j) \in \{1,\dots,n\}^2 ;\ i<j\right\} \setminus A. \tag{49}$$

Take $\sigma_1, \sigma_2 \in \mathfrak{S}_n$ and set $I_1 := \mathrm{Inv}(\sigma_1)$, $J_1 = I_1^C$, $I_2 := \mathrm{Inv}(\sigma_2)$, and $J_2 := I_2^C$. We observe that $(i,j) \in \mathrm{Inv}(\sigma_1 \circ \sigma_2)$ if and only if $\sigma_1(\sigma_2(i)) > \sigma_1(\sigma_2(j))$, *i.e.*, if and only if we have one of the two disjoint cases (a) $(i,j) \in I_2$ and $(\sigma_2(j), \sigma_2(i)) \in J_1$, or (b) $(i,j) \in J_2$ and $(\sigma_2(j), \sigma_2(i)) \in I_1$. In particular, we can see that

$$l(\sigma_1 \circ \sigma_2) = |(i,j) \in I_2,\ (\sigma_2(j), \sigma_2(i)) \in J_1| + |(i,j) \in J_2,\ (\sigma_2(j), \sigma_2(i)) \in I_1|. \tag{50}$$

However, we know that

$$|(i,j) \in I_2,\ (\sigma_2(j), \sigma_2(i)) \in J_1| + |(i,j) \in I_2,\ (\sigma_2(j), \sigma_2(i)) \in I_1| = |(i,j) \in I_2| = |I_2| = l(\sigma_2), \tag{51}$$

$$|(i,j) \in J_2,\ (\sigma_2(j), \sigma_2(i)) \in I_1| + |(j,i) \in I_2,\ (\sigma_2(j), \sigma_2(i)) \in I_1| = |(\sigma_2(j), \sigma_2(i)) \in I_1| = |I_1| = l(\sigma_1), \tag{52}$$

so that

$$\begin{aligned} l(\sigma_1)+l(\sigma_2) &= l(\sigma_1\circ\sigma_2)+|(i,j)\in I_2,\ (\sigma_2(j),\sigma_2(i))\in I_1|+|(j,i)\in I_2,\ (\sigma_2(j),\sigma_2(i))\in I_1| \\ &= l(\sigma_1\circ\sigma_2)+2|(i,j)\in I_2,\ (\sigma_2(j),\sigma_2(i))\in I_1|. \end{aligned} \tag{53}$$

Hence, by definition we can deduce that

$$\epsilon(\sigma_1\circ\sigma_2)=(-1)^{l(\sigma_1\circ\sigma_2)}=(-1)^{l(\sigma_1)+l(\sigma_2)+\text{some even number}}=(-1)^{l(\sigma_1)}(-1)^{l(\sigma_2)}=\epsilon(\sigma_1)\epsilon(\sigma_2), \tag{54}$$

which proves that σ is a group homomorphism by arbitrariness of σ_1 and σ_2. To prove surjectivity, we note that the identity has sign 1 and the transposition has sign -1. The proof is thus complete. □

Proposition 1.138. If τ is a transposition, then always $\epsilon(\tau)=-1$. More generally, if c is a r-cycle with $r\geq 2$, then $\epsilon(c)=(-1)^{r-1}$.

Proof. If τ is a transposition, then it is conjugate to $\begin{pmatrix}1 & 2\end{pmatrix}$ by some $\sigma\in\mathfrak{S}_n$, *i.e.*, $\tau=\sigma\circ\begin{pmatrix}1 & 2\end{pmatrix}\circ\sigma^{-1}$. Since ϵ is a group homomorphism, we thus have that $\epsilon(\tau)=\epsilon(\sigma)\epsilon(\begin{pmatrix}1 & 2\end{pmatrix})\epsilon(\sigma^{-1})=\epsilon(\begin{pmatrix}1 & 2\end{pmatrix})=-1$. Then if $c=\begin{pmatrix}a_1 & \dots & a_r\end{pmatrix}$ is an r-cycle, we can write it as the composition of $r-1$ transpositions, such that $c=\begin{pmatrix}a_1 & a_2\end{pmatrix}\circ\dots\circ\begin{pmatrix}a_{r-1} & a_r\end{pmatrix}$. Hence since ϵ is a group homomorphism, we can conclude that $\epsilon(c)=(-1)^{r-1}$, and the proof is thus complete. □

Proposition 1.139. If $\sigma=c_1\circ\dots\circ c_d$, with each c_i being a l_i-cycle, then $\epsilon(\sigma)=(-1)^{\sum_{i=1}^d(l_i-1)}$.

Proof. This is trivial using the previous proposition and the fact that ϵ is a group homomorphism. □

Example 1.140. We can compute that

$$\epsilon\left(\begin{pmatrix}1 & 2 & 3 & 4 & 5 & 6 & 7 & 8\\ 3 & 5 & 6 & 2 & 4 & 1 & 8 & 7\end{pmatrix}\right)=\epsilon\left(\begin{pmatrix}1 & 3 & 6\end{pmatrix}\circ\begin{pmatrix}2 & 5 & 4\end{pmatrix}\circ\begin{pmatrix}7 & 8\end{pmatrix}\right)=(-1)^{2+2+1}=-1. \tag{55}$$

10/30 Lecture

2 Ring Theory

2.1 Rings

Definition 2.1. A triple $(A,+,\times)$ where $+$ and $\times$ are two binary operations on the set A is called a **ring** if:

(1) $(A,+)$ is a commutative group (we denote 0_A or 0 its neutral element).

(2) $\times$ is associative, and has a neutral element (denoted 1_A or 1).

(3) $\times$ is distributive with respect to $+$, *i.e.*, $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$ for any $a,b,c\in A$ (here we have omitted $\times$ and we will often do it).

Definition 2.2. A ring A is said to be **commutative** if $\times$ is commutative.

Remark 2.3. (1) $0_A\times x=x\times 0_A=0_A$ for any $x\in A$. Indeed, $0_A\times x=(0_A+0_A)\times x=0_A\times x+0_A\times x$, so $0_A\times x=0$. Analogously we can obtain that $x\times 0_A=0$.

(2) $(-1_A)\times x=x\times(-1_A)=-x$ (where $-x$ is the inverse of x for $+$). Indeed, $(-1_A)\times x+1_A\times x=(-1_A+1_A)\times x=0_A\times x=0_A$, so $(-1_A)\times x=-1_A\times x=-x$. Analogously we can obtain that $x\times(-1_A)=-x$.

(3) $a(b-c)=ab-ac$ and $(b-c)a=ba-ca$ for any $a,b,c\in A$.

Example 2.4. (1) The triples $(K,+,\times)$, $K=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ are commutative rings.

(2) The triples $(\mathfrak{M}_n(K),+,\times)$, $K=\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ are non-commutative rings when $n\geq 2$.

Definition 2.5. Let $f : A \to B$ be a mapping between two rings. One says that f is a **ring homomorphism** if:

(1) $f : (A, +) \to (B, +)$ is a group homomorphism (in particular, this implies that $f(0_A) = 0_B$).

(2) $f(xy) = f(x)f(y)$ for any $x, y \in A$.

(3) $f(1_A) = 1_B$.

Definition 2.6. A ring homomorphism $f : A \to B$ is called an **isomorphism** if f is bijective.

Remark 2.7. If $f : A \to B$ is a ring isomorphism, then its inverse $f^{-1} : B \to A$ is a ring isomorphism as well.

Proposition 2.8. A ring A has only one element if and only if $0_A = 1_A$. Such a ring is unique up to isomorphism and is called the **trivial ring**.

Proof. Clearly if A has only one element, then $A = \{0_A\} = \{1_A\}$ and this is indeed a ring. Conversely, if $0_A = 1_A$, then for any $x \in A$, we have that $x = x \times 1_A = x \times 0_A = 0_A$, so A has only one element. Now suppose that A and B are two rings with $0_A = 1_A$ and $0_B = 1_B$. Then for any $x \in A$, we have that $x = x \times 1_A = x \times 0_A = 0_A$, so $A = \{0_A\} = \{1_A\}$. The uniqueness up to isomorphism is trivial. □

2.2 Subrings

Definition 2.9. A subset B of a ring A is called a **subring** of A, denoted $B \leq A$, if:

(1) B is stable under $+$ and $(B, +)$ is a subgroup of A.

(2) B is stable under $\times$.

(3) $1_A \in B$.

Remark 2.10. If A is a ring and $B \leq A$, then $(B, +, \times)$ is a ring, and $0_B = 0_A$ and $1_B = 1_A$. Indeed, $(B, +)$ is a commutative group because $(A, +)$ is a commutative group and $(B, +) \leq (A, +)$. The associativity of $\times$ and distributivity of $\times$ with respect to $+$ are inherited from A. Hence we can conclude that B is indeed a ring. The uniqueness of neutral elements is trivial.

Example 2.11. (1) $(\mathbb{Z}, +, \times) \leq (\mathbb{Q}, +, \times) \leq (\mathbb{R}, +, \times) \leq (\mathbb{C}, +, \times)$.

(2) $(\mathfrak{M}_n(\mathbb{Z}), +, \times) \leq (\mathfrak{M}_n(\mathbb{Q}), +, \times) \leq (\mathfrak{M}_n(\mathbb{R}), +, \times) \leq (\mathfrak{M}_n(\mathbb{C}), +, \times)$.

(3) The trivial ring $\{0\}$ is contained in every ring *but* $\{0\} \leq A$ if and only if $A = \{0\}$. This is the consequence of the third requirement in the definition of a subring. For instance, $\{0\}$ is not a subring of $\mathbb{Z}$ because $1_{\mathbb{Z}} = 1 \notin \{0\}$, even though $\{0\}$ is a ring contained in $\mathbb{Z}$.

Definition 2.12. If A is a ring, we set $Z(A) := \{z \in A;\ zx = xz,\ \forall x \in A\}$, called the **center** of A.

Proposition 2.13. If A is a ring, then $Z(A) \leq A$ and $Z(A) = A$ if and only if A is commutative.

Proof. We prove that $Z(A)$ is stable under both $+$ and $\times$. For any $z_1, z_2 \in Z(A)$ and any $x \in A$, we have that

$$(z_1 z_2)x = z_1(z_2 x) = (z_2 x)z_1 = z_2(x z_1) = (x z_1)z_2 = x(z_1 z_2), \tag{56}$$

where the second equality follows from the fact that $z_1 \in Z(A)$ and that $z_2 x \in A$, and the fourth equality is similar. Hence we can conclude that $z_1 z_2 \in Z(A)$. On the other hand, we also have that

$$(z_1 + z_2)x = z_1 x + z_2 x = x z_1 + x z_2 = x(z_1 + z_2), \tag{57}$$

which means that $z_1 + z_2 \in Z(A)$ as well. Hence $Z(A)$ is stable under both $+$ and $\times$ by arbitrariness of z_1 and z_2. It is trivial that $(Z(A), +) \leq (A, +)$. Moreover, $1_A x = x 1_A$ for any $x \in A$ so $1_A \in Z(A)$. We have now completed the proof that $Z(A)$ is a subring of A. The second part of the proof is trivial and will be omitted here. □

Example 2.14. $Z(\mathbb{R}) = \mathbb{R}$ and $Z(\mathfrak{M}_n(\mathbb{R})) = \{tI_n, ; t \in \mathbb{R}\} \simeq \mathbb{R}$.

11/1 Lecture

2.3 Fields

Definition 2.15. (1) An element x of a ring A is called **invertible** if there is an element $y \in A$, such that $xy = yx = 1_A$.

(2) The element y above is unique and we denote it by x^{-1}, and call it the **multiplicative inverse** of x.

(3) We denote by $A^\times$ the set of invertible elements in A.

Remark 2.16. If A is a ring, then $(A^\times, \times)$ is a group, so we are using the same notation as before. Indeed, if $x, y \in A^\times$ with respective inverses u and v, we can easily see that $(xy)(vu) = x(yv)u = xu = 1_A$ so $xy \in A$ with inverse vu, and thus $xy \in A^\times$, meaning that $\times$ *does* define a binary operation on $A^\times$. By definition, it is associative. Moreover, 1_A is the neutral element for this law, and each element in $A^\times$ has an inverse in $A^\times$ by definition of $A^\times$. Therefore, we can conclude that $(A^\times, \times)$ is a group.

Definition 2.17. A ring F is called a **field** if $F \neq \{0\}$ and all its nonzero elements are invertible for $\times$, *i.e.*, if $F^\times = F \setminus \{0\}$.

Example 2.18. (1) $(\mathbb{Z}, +, \times)$ is a commutative ring and $\mathbb{Z}^\times = \{\pm 1\} \neq \mathbb{Z} \setminus \{0\}$, so $\mathbb{Z}$ is not a field.

(2) $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative fields.

(3) $\mathfrak{M}_n(\mathbb{R})^\times = GL_n(\mathbb{R})$ hence it is not a field when $n \geq 2$.

2.4 Polynomial Rings

Remark 2.19. If A is a commutative ring, we set

$$A[X] = \left\{ \sum_{k=0}^{\infty} a_k X^k;\ a_k \in A \text{ and there exists } k_0 \in \mathbb{N} \text{ such that } a_k = 0 \text{ for all } k \geq k_0 \right\}. \tag{58}$$

This definition is formal but not totally rigorous. One just needs to remember that for $P = \sum_{k=0}^{\infty} a_k X^k \in A[X]$ and $Q = \sum_{k=0}^{\infty} b_k X^k \in A[X]$, by definition $P = Q$ if and only if $a_k = b_k$ for all $k \in \mathbb{N}$.

Definition 2.20. Let A be a commutative ring. For $P = \sum_{k=0}^{\infty} a_k X^k$ and $Q = \sum_{k=0}^{\infty} b_k X^k$ in $A[X]$, we set

$$P + Q = \sum_{k=0}^{\infty} (a_k + b_k) X^k, \qquad PQ = P \times Q = \sum_{k=0}^{\infty} c_k X^k, \tag{59}$$

where $c_n = \sum_{k=0}^{n} a_k b_{n-k} = \sum_{k=0}^{n} a_{n-k} b_k$ for $n \in \mathbb{N}$.

Remark 2.21. Let A be a commutative ring, then $(A[X], +, \times)$ is also a commutative ring with $1_{A[X]} = 1_A \times X^0$ and $0_{A[X]} = 0_A \times X^0$. For $k, l \in \mathbb{N}$ we have the relation $X^k \times X^l = X^{k+l}$.

Definition 2.22. Let A be a commutative ring, then the ring $A[X]$ is called the **ring of polynomials** with coefficients in A.

Definition 2.23. Let A be a commutative ring. Let the mapping $d^\circ : A[X] \to \mathbb{N} \cup \{-\infty\}$ be such that $d^\circ(0) = -\infty$ and $d^\circ(P) = d \in \mathbb{N}$ if $P \neq 0$ and $P = \sum_{k=0}^{d} a_k X^k$ with $a_d \neq 0$. The mapping $d^\circ(P)$ the **degree mapping**.

Definition 2.24. We denote by $A_d[X]$ the set of polynomials of degree at most d in $A[X]$.

Remark 2.25. The set $A_0[X]$ is in fact a subring of A, and the mapping $i : A \to A_0[X]$ such that $i(a) = a \times X^0$ is a ring isomorphism.

Remark 2.26. In view of the above remark, we will simply identify A with $A_0[X]$ and make the confusions that $1_{A[X]} = 1_A = X^0$ and $0_{A[X]} = 0_A$. We also extend the addition on $\mathbb{N}$ to $\mathbb{N} \cup \{-\infty\}$ such that $-\infty + n = n + -\infty = -\infty$, which shall allow us to state some useful properties of the degree mapping.

Proposition 2.27. Let A be a commutative ring, and let $P, Q \in A[X]$. We have that

(1) $d^\circ(P + Q) \leq \max(d^\circ(P), d^\circ(Q))$.

(2) $d^\circ(P \times Q) \leq d^\circ(P) + d^\circ(Q)$.

Definition 2.28. Let A be a nonzero commutative ring. If $P \in A[X] \setminus \{0\}$ and $P = \sum_{k=0}^{d} a_k X^k$ for $d = d^\circ(P)$ (*i.e.*, $a_d \neq 0$), we call a_d the **leading term** of P.

Remark 2.29. Note that surprisingly the second inequality in the previous proposition is not an equality in general. This is because the product of the leading terms of P and Q might be zero.

Definition 2.30. Let A be a commutative ring. We say that $x \in A$ is a **zero divisor** if $x \neq 0$ and there exists $y \neq 0 \in A$ such that $xy = 0$.

Definition 2.31. A commutative ring is called an **integral domain** if it is not reduced to $\{0\}$ but has no zero divisors. The latter requirement is equivalent to the implication $xy = 0 \implies x = 0$ or $y = 0$.

Remark 2.32. By considering the leading term of polynomials, we see that if A is an integral domain and $P, Q \in A[X]$, then $d^\circ(P \times Q) = d^\circ(P) + d^\circ(Q)$.

Proposition 2.33. If A is an integral domain, then $A[X]$ is an integral domain.

Proof. If $PQ = 0 \in A[X]$, then $-\infty = d^\circ(PQ) = d^\circ(P) + d^\circ(Q)$, so either $d^\circ(P) = -\infty$ or $d^\circ(Q) = -\infty$. This means that either $P = 0$ or $Q = 0$, so $A[X]$ is an integral domain. □

11/6 Lecture

2.5 Properties of Ring Homomorphisms

Remark 2.34. We denote by $\mathrm{Hom}(A, B)$ the set of ring homomorphisms from a ring A to a ring B.

Remark 2.35. If $f \in \mathrm{Hom}(A, B)$, then $\mathrm{Im}(f) \leq B$. Indeed by group theory, we have $(\mathrm{Im}(f), +) \leq (B, +)$. Moreover, $f(1_A) = 1_B$ hence $1_B \in \mathrm{Im}(f)$. Finally, the property $f(x)f(y) = f(xy)$ for any $x, y \in A$ shows that $\mathrm{Im}(f)$ is stable under multiplication, so we can conclude that $\mathrm{Im}(f)$ is a subring of B.

Definition 2.36. If $f \in \mathrm{Hom}(A, B)$, we set the **kernel** of f as $\mathrm{Ker}(f) := \{x \in A;\ f(x) = 0_B\}$.

Remark 2.37. Note that the kernel of f above is almost never a subring of A due to the condition $f(1_A) = 1_B$, which prevents 1_A to belong to the kernel of f unless $B = \{0_A\}$.

Remark 2.38. (1) $(\mathrm{Ker}(f), +) \leq (A, +)$. This comes from the fact that f is an additive group homomorphism.

(2) If $x, y \in A$ and $x \in \mathrm{Ker}(f)$ or $y \in \mathrm{Ker}(f)$, then $xy \in \mathrm{Ker}(f)$. Indeed, without loss of generality we assume that $x \in \mathrm{Ker}(f)$, then $f(xy) = f(x)f(y) = 0_B f(y) = 0_B$, meaning that $xy \in \mathrm{Ker}(f)$.

(3) f is injective if and only if $\mathrm{Ker}(f) = \{0_A\}$. This again comes from the fact that f is an additive group homomorphism.

2.6 Ideals of Commutative Rings

Definition 2.39. A subset $I \subseteq A$ of a commutative ring A is called an **ideal** of A, denoted $I \trianglelefteq A$, if:

(1) I is an additive subgroup of $(A, +)$.

(2) If $x \in I$ and $y \in I$, then $xy \in I$.

Example 2.40. (1) Let A be a commutative ring and $f : A \to B$ be a ring homomorphism, then $\mathrm{Ker}(f) \trianglelefteq A$.

(2) If $I \trianglelefteq \mathbb{Z}$, then in particular it is a subgroup of $(\mathbb{Z}, +)$, hence of the form $n\mathbb{Z}$. Therefore, there exists $n \in \mathbb{N}$ such that $I = n\mathbb{Z}$. Conversely, it is immediate to check that if $n \in \mathbb{N}$, then $n\mathbb{Z}$ fulfills all the requirements to be an ideal ot $\mathbb{Z}$. Hence, the ideals of $\mathbb{Z}$ are exactly the sets $n\mathbb{Z}$, $n \in \mathbb{N}$. Beware that this is a completely exceptional situation, and that in general not all subgroups of $(A, +)$ are automatically ideals of a commutative ring A.

Remark 2.41. Let A be a commutative ring and let $x \in A$, we set $(x) := \{xa;\ a \in A\}$. We can also use the notation xA for this subset of A, *i.e.*, $(x) = xA$. We shall be able to check that (x) is an ideal of A. Indeed, (x) is an additive subgroup of A because $0_{(x)} = x0_A = 0_A \in A$, $-xa_1 = x(-a_1) \in (x)$ when $xa_1 \in (x)$, and $xa_1 + xa_2 = x(a_1 + a_2) \in (x)$ when $xa_1, xa_2 \in (x)$. Moreover, if $xa_1, xa_2 \in (x)$, then $xa_1xa_2 = x(a_1xa_2) \in (x)$ because $a_1xa_2 \in A$. Hence, we can conclude that $(x) \trianglelefteq A$.

Definition 2.42. (1) For A a commutative ring and $x \in A$, we call (x) the **ideal generated by** A.

(2) We call an ideal of this form a **principal ideal** of A, *i.e.*, an ideal is called **principal** if it is generated by one element.

Example 2.43. We observe that all ideals of $\mathbb{Z}$ are principal.

Remark 2.44. Let A be a commutative ring. Let $I \trianglelefteq A$ and $x \in A$. Then $x \in I$ if and only if $(x) \subseteq I$.

Example 2.45. Let A be a commutative ring, then $(0_A) = \{0_A\}$ and $(1_A) = A$. In particular, a nonzero ring has at least two different ideals, namely the two listed above.

Remark 2.46. Let A be a commutative ring and $x \in A$. We shall be able to check that $(x) = A$ if and only if $x \in A^\times$, the set of invertible elements of A. Indeed, if $x \in A^\times$, then $1_A = xx^{-1} \in (x)$, and thus $(1_A) \subseteq (x)$. But $(1_A) = A$, so that $A \subseteq (x)$, and thus $(x) = A$. Conversely, if $(x) = A$, then $1_A \in (x)$, so there exists $a \in A$ such that $1_A = xa$. This means that x is invertible with inverse a, so $x \in A^\times$.

Proposition 2.47. Let A be a commutative ring, then A is a field if and only if it has two different ideals (which must be $\{0_A\}$ and A).

Proof. $\Longrightarrow$ If A is a field, let $I \trianglelefteq A$. Suppose that $I \neq \{0_A\}$ and take $x \neq 0_A \in I$. We know that $x \in A^\times$ because A is a field. But on one hand $x \in I$ so $(x) \in I$, and on the other hand $(x) = A$ as we have shown in the previous remark, so that $I = A$. Therefore, A has exactly two ideals $\{0_A\}$ and A, which are different because a field is never the zero ring by definition.

$\Longleftarrow$ If A has exactly two ideals, they must be $\{0_A\}$ and A and this implicitly implies that A is not reduced to zero. Take $x \neq 0_A \in A$, then (x) is a nonzero ideal of A, so $(x) = A$. Again by the previous remark $x \in A^\times$, so the proof is complete by arbitrariness of $x \neq 0_A$. □

A Recitations

9/1 Recitation

Example A.1. For n a positive integer, count the number of elements in $\mathfrak{S}_n$.

Solution. $n!$.

Example A.2. Let $(G, \cdot)$ be a group and let $x \in G$. For $k \geq 1$, put $x^k = \underbrace{x \dots x}_{k\times}$. Put $x^0 := 1$ and for $k < 0$ put $x^k := (x^{-1})^{-k}$. Finally let $\langle x \rangle := \langle \{x\} \rangle$. These are standard notations to be always used later.

(1) Check that $x^a \cdot x^b = x^{a+b}$, $\forall a, b \in \mathbb{Z}$.

(2) Check that $\langle x \rangle = \left\{x^k;\ k \in \mathbb{Z}\right\}$.

Proof. The first equality is trivial but discussing each case separately. As for the second equality, we have that

$$\langle x \rangle = \langle \{x\} \rangle = \{1\} \cup \{x_1^{\epsilon_1} \dots x_n^{\epsilon_n};\ n \in \mathbb{N}^*,\ \epsilon_i = \pm 1,\ x_i \in \{x\}\} \tag{60}$$

$$= \{1\} \cup \left\{x^{\epsilon_1 + \dots + \epsilon_n};\ n \in \mathbb{N}^*,\ \epsilon_i = \pm 1\right\} = \left\{x^k;\ k \in \mathbb{Z}\right\}, \tag{61}$$

so the proof is complete. □

Example A.3. Let G be a group such that $x^2 = e$ for all $x \in G$.

(1) Check that G is commutative.

(2) Suppose that such a group G is a subgroup of $GL_n(\mathbb{R})$. Show that every element in G is diagonalizable with eigenvalues ± 1.

(3) Set $H_n := \{\mathrm{diag}(\epsilon_1, \dots, \epsilon_n);\ \epsilon_i = \pm 1\} \subseteq GL_n(\mathbb{R})$. With the same assumption as above, show that $H_n \leq G$.

(4) With the same assumptions as above, prove that there exists $P \in GL_n(\mathbb{R})$, such that for every $M \in G$, $PMP^{-1} \in H_n$ (this can be written as $PGP^{-1} \subseteq H_n$ in short).

Proof. (1) $\forall a, b \in G$, we have that $ab \in G$. Therefore, $(ab)^2 = abab = e$. Multiplying by a on the left and b on the right on both sides of the equation, we can see that $ba = a^2bab^2 = ab$, so G is commutative.

(2) Since for each $A \in G$, $A^2 = I$. This means that the minimal polynomial is $\lambda^2 - 1$ which has two distinct roots, so A is diagonalizable. Now suppose $A\mathbf{v} = \lambda\mathbf{v}$. Multiplying by A on the left on both sides of the equation, we have that $\mathbf{v} = A^2\mathbf{v} = \lambda A\mathbf{v} = \lambda^2\mathbf{v}$. This implies that $\lambda = \pm 1$, so the proof is complete.

(3) The neutral element of H_n is $I \in G$. Take arbitrary $A = \mathrm{diag}(a_1, \dots, a_n) \in H_n$ and $B = \mathrm{diag}(b_1, \dots, b_n) \in H_n$. Clearly $AB = \mathrm{diag}(a_1b_1, \dots, a_nb_n) \in H_n$ because $a_ib_i = \pm 1$, and $A^{-1} = \mathrm{diag}(a_1^{-1}, \dots, a_n^{-1}) \in H_n$ because $a_i^{-1} = \pm 1$. Hence we can conclude that $H_n \leq G$.

(4) To be done... □

9/8 Recitation

Example A.4. Let $G \leq \mathbb{Z}$ and suppose that $G \neq \{0\}$.

(1) Prove that the positive integer $m := \min(G \cap \mathbb{N} \setminus \{0\})$ is well-defined.

(2) Prove that $G = m\mathbb{Z}$.

Hence the only subgroups of $\mathbb{Z}$ are the groups $m\mathbb{Z}$ for $m \in \mathbb{N}$.

Proof. (1) We recall the following theorems. *$S \subseteq \mathbb{N}$ has a minimum if and only if $S \neq \varnothing$; $S \subseteq \mathbb{Z}$ has a minimum if and only if $S \neq \varnothing$ and $\exists x \in \mathbb{Z}$ such that $\forall s \in S$, $x \leq s$.* By assumption, there exists $y \in G \setminus \{0\}$ since $0 \in G$ and $G \neq \{0\}$. There are two cases. If $y > 0$, then $y \in \mathbb{N}$, so we have found $y \in G \cap \mathbb{N} \setminus \{0\}$. Otherwise, $-y \in \mathbb{N}$, so we have found $-y \in G \cap \mathbb{N} \setminus \{0\}$. Therefore, $G \cap \mathbb{N} \setminus \{0\}$ has a well-defined minimum.

(2) We recall the Euclidean division lemma. *Given two integers a and b with $b \neq 0$, there exist unique integers q and r such that $a = bq + r$ and $0 \leq r < |b|$.* Now take arbitrary $x \in G$, then we have that $x = mq + r$ for some $(q, r) \in \mathbb{Z} \times [0, |m| - 1]$. Note that m is the smallest positive integer in $G \cap \mathbb{N} \setminus \{0\}$, so $r = 0$. This means that $x = mq$ for some $q \in \mathbb{Z}$. Up till now we have checked that $G \subseteq m\mathbb{Z}$. Now take arbitrary $x \in m\mathbb{Z}$, there exists $y \in \mathbb{Z}$ such that $x = my$. Now since $m \in G$ and G is a group, clearly $x \in G$ (add $m \in G$ for y times). This has shown that $m\mathbb{Z} \subseteq G$, so we can conclude that $G = m\mathbb{Z}$ and the proof is complete.

□

Example A.5. Let A be a commutative group and $a_1, \ldots, a_r \in A$. Show that $\langle a_1, \ldots, a_r \rangle = \{a_1^{m_1} \ldots a_r^{m_r};\ m_i \in \mathbb{Z}\}$.

Proof. $\supseteq$ All a_i's belong to $\langle a_1, \ldots, a_r \rangle$, and since $\langle a_1, \ldots, a_r \rangle$ is stable under "multiplication" and inverse, clearly $a_1^{m_1} \ldots a_r^{m_r} \in \langle a_1, \ldots, a_r \rangle$, $m_i \in \mathbb{Z}$.

$\subseteq$ Denote $H := \{a_1^{m_1} \ldots a_r^{m_r};\ m_i \in \mathbb{Z}\}$. Each $a_i = a_1^0 \ldots a_i^1 \ldots a_r^0 \in H$, so $\{a_1, \ldots, a_r\} \subseteq H$. Now we check that H is a group. Clearly $e = a_1^0 \ldots a_r^0 \in H$. Now take arbitrary $x, y \in H$ and assuming that $x = a_1^{x_1} \ldots a_r^{x_r}$ and $y = a_1^{y_1} \ldots a_r^{y_r}$, we can see that $x \cdot y = a_1^{x_1 + y_1} \ldots a_r^{x_r + y_r} \in H$ and $x^{-1} = a_1^{-x_1} \ldots a_r^{-x_r} \in H$. This proves that H is a group, and in particular a group containing $\{a_1, \ldots, a_r\}$. Note that $\langle a_1, \ldots, a_r \rangle$ is the smallest group containing $\{a_1, \ldots, a_r\}$, so $\langle a_1, \ldots, a_r \rangle \subseteq H$. □

Example A.6. Let G and G' be two finite groups with the same cardinality n. Prove that if $n = 2, 3$, we have that $G' \simeq G$ (*i.e.*, G' and G are isomorphic). Find a counterexample for $n = 4$.

Proof. For this question we make use of the Cayley table (Appendix B). If $n = 2$, we write the Cayley table for $G = \{e, x\}$ as

$$T_{e,x} = \begin{array}{c|c|c} \cdot & e & x \\ \hline e & e & x \\ \hline x & x & \end{array} \tag{62}$$

We can see that the $(2, 2)$th entry of $T_{e,x}$ can only be e because each row or column must have distinct elements. This means that the Cayley table for $G' = \{e', x'\}$ will be of exactly the same form, so by Theorem B.4, $G \simeq G'$ when $n = 2$. Now if $n = 3$, we write the Cayley table for $G = \{e, x, y\}$ as

$$T_{e,x,y} = \begin{array}{c|c|c|c} \cdot & e & x & y \\ \hline e & e & x & y \\ \hline x & x & & \\ \hline y & y & & \end{array} \tag{63}$$

We can see that the $(2, 2)$th entry of $T_{e,x,y}$ can only be y, because it cannot be x and the $(2, 3)$th entry that is in the same column as it cannot be y. Therefore the $(2, 3)$th and the $(3, 2)$th entry must be e, and thus the $(3, 3)$th entry must be x. The table is again uniquely determined, which means that the Cayley table for $G' = \{e', x', y'\}$ will be of exactly the same form, so again by Theorem B.4, $G \simeq G'$ when $n = 3$. Now if $n = 4$, we can write the Cayley tables for $G = \{e, x, y, z\}$ and $G' = \{e', z', y', z'\}$ respectively as

$$T_{e,x,y,z} = \begin{array}{c|c|c|c|c} \cdot & e & x & y & z \\ \hline e & e & x & y & z \\ \hline x & x & e & z & y \\ \hline y & y & z & e & x \\ \hline z & z & y & x & e \end{array} \qquad T_{e',z',y',z'} = \begin{array}{c|c|c|c|c} \cdot & e & x & y & z \\ \hline e & e & x & y & z \\ \hline x & x & y & z & e \\ \hline y & y & z & e & x \\ \hline z & z & e & x & y \end{array} \tag{64}$$

These two Cayley tables are clearly not isomorphic. By the contrapositive of Theorem B.4, we can conclude that $G \not\simeq G'$, and thus the above is a counterexample for the case $n = 4$. □

9/15 Recitation

Example A.7. For G a group and $x, y \in G$, we denote by $[x, y]$ the element $[x, y] := xyx^{-1}y^{-1}$ of G. It is called the **commutator** of x and y. We denote by $D(G)$ or $[G, G]$ the **commutator subgroup**, also called the **derived subgroup** of G, which is by definition generated by all the commutators in G, *i.e.*,

$$D(G) = [G, G] := \langle [x, y];\ x, y \in G \rangle\,. \tag{65}$$

(1) Let $f \in \mathrm{Hom}(G, G')$, and suppose that $S \subseteq G$. Show that $f(\langle S \rangle) = \langle f(S) \rangle$.

(2) Suppose that S is stable under conjugation, *i.e.*, $\iota_x(S) \subseteq S$ for any $x \in G$, prove that $\langle S \rangle \trianglelefteq G$.

(3) Prove that $[G, G] \trianglelefteq G$.

(4) Prove that $[G, G] = \{e\}$ if and only if G is commutative.

Proof. (1) $\subseteq$ Take any $y \in f(\langle S \rangle)$, then there exists $x \in \langle S \rangle$ such that $y = f(x)$. By Proposition 1.20, either $x = e$ or $x = \prod_{i=1}^n s_i^{\epsilon_i}$ for some $n \in \mathbb{N}$, $\epsilon_i = \pm 1$, and $s_i \in S$. In the former case, $y = f(e) = e' \in \langle f(S) \rangle$. In the latter case, since f is a group homomorphism, we have that $y = f\left(\prod_{i=1}^n s_i^{\epsilon_i}\right) = \prod_{i=1}^n f(s_i)^{\epsilon_i}$. This means that $y \in \langle f(S) \rangle$ because $f(s_i) \in f(S)$ and $\epsilon_i = \pm 1$ and we can apply the other direction of Proposition 1.20.

$\supseteq$ Take any $y \in \langle f(S) \rangle$, then by Proposition 1.20, either $y = e'$ or $y = \prod_{i=1}^n {s'_i}^{\epsilon_i}$ for some $n \in \mathbb{N}$, $\epsilon_i = \pm 1$, and $s'_i \in f(S)$. In the former case, we note that $f(e) = e' = y$ so $y \in f(\langle S \rangle)$. In the latter case, there exists $s_1, \ldots, s_n \in S$, such that $f(s_i) = s'_i$ for any $1 \leq i \leq n$. Since f is a group homomorphism, we have that $y = \prod_{i=1}^n f(s_i)^{\epsilon_i} = f\left(\prod_{i=1}^n s_i^{\epsilon_i}\right)$. This means that $y \in f(\langle S \rangle)$ because $s_i \in S$ and $\epsilon_i = \pm 1$ and we can apply the other direction of Proposition 1.20 to see that $\prod_{i=1}^n s_i^{\epsilon_i} \in \langle S \rangle$.

(2) For any $x \in G$, we know that $\iota_x \in \mathrm{Inn}(G) \subseteq \mathrm{Hom}(G, G)$, so $\iota_x(\langle S \rangle) = \langle \iota_x(S) \rangle$ for any $S \subseteq G$ as is shown in the previous part. But since $\iota_x(S) \subseteq S$, we have that $\langle \iota_x(S) \rangle \subseteq \langle S \rangle$, so $\iota_x(\langle S \rangle) \subseteq \langle S \rangle$. This, by the alternative definition, concludes that $\langle S \rangle \trianglelefteq G$.

(3) For any $s \in [G, G]$, there exists $x, y \in G$ such that $s = xyx^{-1}y^{-1}$. Then for any $g \in G$, we have that

$$\begin{aligned} gsg^{-1} = gxyx^{-1}y^{-1}g^{-1} = gx(g^{-1}g)y(g^{-1}g)x^{-1}(g^{-1}g)y^{-1}g^{-1} &= (gxg^{-1})(gyg^{-1})(gx^{-1}g^{-1})(gy^{-1}g^{-1}) \\ &= \underbrace{(gxg^{-1})}_{\in G}\underbrace{(gyg^{-1})}_{\in G}(gxg^{-1})^{-1}(gyg^{-1})^{-1}, \quad (66) \end{aligned}$$

so $\iota_g(s) \in [G, G]$ for any $s \in [G, G]$ and $g \in G$. In other words, $\iota_g([G, G]) \subseteq [G, G]$ for any $g \in G$. By the previous part, we can thus conclude that $\langle [G, G] \rangle \trianglelefteq G$.

(4) $\Longrightarrow$ If $[G, G] = \{e\}$, then for any $x, y \in G$, we have that $xyx^{-1}y^{-1} = e$. In other words, $xy = yx$ so that G is commutative.

$\Longleftarrow$ If G is commutative, then for any $x, y \in G$, we have that $xyx^{-1}y^{-1} = (xx^{-1})(yy^{-1}) = e$, so $[G, G] = \{e\}$.

The proof is thus complete. □

Example A.8. Let K be a field. For $1 \leq i \neq j \leq n$ and $x \in K$, set $E_{i,j}(x) := I_n + xE_{i,j} \in \mathfrak{M}_n(K)$, where $E_{i,j}$ has all entries equal to 0 except the entry in position (i, j) which is equal to 1. For $t \in K^*$, set $d_t = \mathrm{diag}(t, I_{n-1}) \in \mathfrak{M}_n(K)$.

(1) Check that $E_{i,j}(x) \in SL_n(K)$ and $d_t \in GL_n(K)$.

(2) Prove that $SL_2(K) = \langle \{E_{i,j}(x);\ 1 \leq i \neq j \leq 2,\ x \in K\} \rangle$.

(3) Prove that $SL_n(K) = \langle \{E_{i,j}(x);\ 1 \leq i \neq j \leq n,\ x \in K\} \rangle$.

(4) Prove that $GL_n(K) = \langle \{E_{i,j}(x);\ 1 \leq i \neq j \leq n,\ x \in K\} \cup \{d_t;\ t \in K^*\} \rangle$.

Proof. (1) Note that $E_{i,j}(x)$ can either be upper triangular or lower triangular with diagonal elements all 1 because for $i \neq j$. Therefore, $\det(E_{i,j}(x)) = 1$ which means that $E_{i,j}(x) \in SL_n(K)$. On the other hand, d_t is diagonal with diagonal elements $t, 1, \ldots, 1$, so that $\det(d_t) = t \neq 0$ for $t \neq 0$. This means that $d_t \in GL_n(K)$.

(2) To be done...

(3) To be done...

(4) To be done...

□

B Cayley Table

Let G be a finite group with r elements. To a numbering $g_1, \dots, g_r$ of the elements of G, one can associate the corresponding **multiplication table** of G, also known as the **Cayley table**.

$$T_{g_1,\dots,g_r} := \tag{67}$$

$\cdot$	g_1	g_2	$\cdots$	g_{r-1}	g_r
g_1	g_1^2	$g_1 \cdot g_2$	$\cdots$	$g_1 \cdot g_{r-1}$	$g_1 \cdot g_r$
g_2	$g_2 \cdot g_1$	g_2^2	$\cdots$	$g_2 \cdot g_{r-1}$	$g_2 \cdot g_r$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
g_{r-1}	$g_{r-1} \cdot g_1$	$g_{r-1} \cdot g_2$	$\cdots$	g_{r-1}^2	$g_{r-1} \cdot g_r$
g_r	$g_r \cdot g_1$	$g_r \cdot g_2$	$\cdots$	$g_r \cdot g_{r-1}$	g_r^2

In other words, the table is of size $r \times r$, and the entry in position (i, j) contains the value $g_i \cdot g_j$. Often one chooses $g_1 = e$, the neutral element, in the numbering of G.

Example B.1. We write the multiplication table of $\mathbb{U}_5 = \{1, u, u^2, u^3, u^4\}$ where $u = \exp(2i\pi/5)$, the 5th root of unity. Using the relation $u^5 = 1$, we obtain

$$T_{1,u,u^2,u^3,u^4} = \tag{68}$$

$\cdot$	1	u	u^2	u^3	u^4
1	1	u	u^2	u^3	u^4
u	u	u^2	u^3	u^4	1
u^2	u^2	u^3	u^4	1	u
u^3	u^3	u^4	1	u	u^2
u^4	u^4	1	u	u^2	u^3

Proposition B.2. Let G be a finite group with r elements and $g_1, \dots, g_r$ be a numbering of the elements of G. Then each row and each column of $T_{g_1,\dots,g_r}$ contains distinct elements, which are exactly all elements of G in a possibly different order.

Proof. We observe that for a fixed $g \in G$, the mapping $l_g : G \to G$ such that $x \mapsto g \cdot x$ is bijective with inverse mapping $l_{g^{-1}}$. The same holds for $r_g : x \mapsto x \cdot g$ such that $x \mapsto x \cdot g$, which is bijective with inverse mapping $r_{g^{-1}}$. This implies that the elements of the ith row are $l_{g_i}(g_1), \dots, l_{g_i}(g_r)$ (from left to right), and the elements of the jth column are $r_{g_i}(g_1), \dots, r_{g_i}(g_r)$ (from top to bottom). The proof is thus complete. □

Definition B.3. Let G and G' be two finite groups of the same cardinality r, with respective elements numbering $g_1, \dots, g_r$ and $g'_1, \dots, g'_r$. We say that $T := T_{g_1,\dots,g_r}$ and $T' = T_{g'_1,\dots,g'_r}$ are **isomorphic** if for all $i, j \in \{1, \dots, r\}$, the following holds: if the entry $T_{i,j} = g_i \cdot g_j$ is equal to g_k (for some $k \in \{1, \dots, r\}$), then the entry $T'_{i,j} = g'_i \cdot g'_j$ is equal to g'_k (for the same k). We denote this as $T' \simeq T$.

Theorem B.4. Let G and G' be two finite groups, then they are isomorphic if and only if they have the same cardinatlity, say r, and if there are numberings $g_1, \dots, g_r$ of G and $g'_1, \dots, g'_r$ of G', such that $T_{g'_1,\dots,g'_r} \simeq T_{g_1,\dots,g_r}$.

Proof. $\implies$ If G and G' are isomorphic, then there exists $\phi \in \mathrm{Iso}(G, G')$. Fix an arbitrary numbering $g_1, \dots, g_r$ of G, and set $g'_i = \phi(g_i)$. Then $g'_1, \dots, g'_r$ is a numbering of G', and we observe that if $g_i \cdot g_j = g_k$, then $g'_i \cdot g'_j = \phi(g_i) \cdot \phi(g_j) = \phi(g_i \cdot g_j) = \phi(g_k) = g'_k$. Hence $T_{g'_1,\dots,g'_r} \simeq T_{g_1,\dots,g_r}$.

$\impliedby$ Assume that there are numberings $g_1, \dots, g_r$ of G and $g'_1, \dots, g'_r$ of G', such that $T_{g'_1,\dots,g'_r} \simeq T_{g_1,\dots,g_r}$. We define the mapping $\phi : G \to G'$ such that $\phi(g_i) = g'_i$ for $i = 1, \dots, r$. Clearly ϕ is a bijection and for any i, j, take the unique integer $1 \leq k \leq r$ such that $g_k = g_i \cdot g_j$, we can deduce that

$$\phi(g_i \cdot g_j) = \phi(g_k) = g'_k = g'_i \cdot g'_j = \phi(g_i) \cdot \phi(g_j). \tag{69}$$

Therefore, ϕ preserves multiplication and is thus a group homomorphism, and further since ϕ is a bijection, we can conclude that ϕ is an isomorphism. G and G' are thus isomorphic.

□

C Order of an Element

Definition C.1. Let G be a group and $x \in G$. Set $\alpha_x : \mathbb{Z} \to G$, such that $k \mapsto x^k$. Note that $\alpha_x \in \mathrm{Hom}(\mathbb{Z}, G)$, and that $\mathrm{Im}(\alpha_x) = \langle x \rangle$. We say that x has **infinite order** if $\mathrm{Ker}(\alpha_x) = \{0\}$, and that x has **finite order** if $\mathrm{Ker}(\alpha_x) \neq \{0\}$.

Proposition C.2. x has finite order if and only if $\langle x \rangle$ is finite.

Proof. $\Longleftarrow$ If x has infinite order, then $\mathbb{Z} \simeq \langle x \rangle$ so that $\langle x \rangle$ is infinite. Taking its contrapositive statement, we can see that the finiteness of $\langle x \rangle$ implies that x is of finite order.

$\Longrightarrow$ If x has finite order, then there exists a unique $n \geq 1$, such that $\mathrm{Ker}(\alpha_x) = n\mathbb{Z}$ because $\mathrm{Ker}(\alpha_x)$ is necessarily a subgroup of $\mathbb{Z}$. Moreover by the first isomorphism theorem (Theorem 1.75), we know that in this case $\frac{\mathbb{Z}}{n\mathbb{Z}} \overset{\overline{\alpha_x}}{\simeq} \langle x \rangle$. Therefore, we can see that $|\langle x \rangle| = \left|\frac{\mathbb{Z}}{n\mathbb{Z}}\right| = n$, indicating that $\langle x \rangle$ is finite. □

Definition C.3. If x has finite order, then the **order of** x is $n = |\langle x \rangle|$. It is also the unique $n \geq 1$ such that $\mathrm{Ker}(\alpha_x) = n\mathbb{Z}$. We denote by $o(x) = n$ the order of x.

Remark C.4. By convention, $o(x) = \infty$ if x has infinite order. We also use the convention that the minimal element of the empty set of $\mathbb{N}^*$ is ∞.

Proposition C.5. We have that $o(x) = \min\left\{k \in \mathbb{N}^*;\ x^k = e\right\}$.

Proof. Set $C_x := \left\{k \in \mathbb{N}^*;\ x^k = e\right\}$, then by definition, we have that $C_x = \mathrm{Ker}(\alpha_x) \cap \mathbb{N}^*$. If $\mathrm{Ker}(\alpha_x) \neq \{0\}$, then we have that $C_x = (o(x)\mathbb{Z}) \cap \mathbb{N}^*$, so clearly $\min(C_x) = o(x)$. If $\mathrm{Ker}(\alpha_x) = \{0\}$, then C_x is empty and thus by convention $\min(C_x) = \infty$, where we note that in this case x has infinite order and thus $o(x) = \infty$ as well. The proof is thus complete. □

Example C.6. (1) The order of e is $o(e) = 1$.

(2) In $\frac{\mathbb{Z}}{n\mathbb{Z}}$, we have that $o(\overline{1}) = n$. In $\mathbb{U}_n$, we have that $o(\exp(2i\pi/n)) = n$.

(3) The elements of $\mathbb{C}^*$ of finite order are the elements of $\mathbb{U}_\infty$. The elements of $\mathbb{R}^*$ of finite order are the elements $\{\pm 1\}$, where $o(1) = 1$ and $o(-1) = 2$.

(4) The order of an r-cycle in $\mathfrak{S}_n$ is r. Indeed, let the cycle be $c = (a_1, \ldots, a_r)$. Note that c^k means applying c for k times. Clearly $k < r$ does not hold, since otherwise $a_{k+1} = a_1$ which breaks the cycle. But $k = r$ clearly holds, since applying c for r times brings each a_i around the cycle back to itself, and any other element remains unchanged, so c^r is clearly the identity mapping. Therefore, the order of any r-cycle in $\mathfrak{S}_n$ is r.

Proposition C.7. Let G be a finite group and $x \in G$, then $o(x) \mid |G|$. In particular, $x^{|G|} = e$.

Proof. We note that $\langle x \rangle \leq G$ and $o(x) = |\langle x \rangle|$. By the Lagrange's theorem (Theorem 1.65), clearly $o(x) \mid |G|$. Then $|G| = ao(x)$ for some $a \geq 1$, which implies that $x^{|G|} = (x^{o(x)})^a = e^a = e$. The proof is thus complete. □

D Chinese Remainder Theorem and its Applications

Theorem D.1 (Chinese remainder theorem (CFT))**.** If a and b are two coprime positive integers, then we have that

$$\frac{\mathbb{Z}}{ab\mathbb{Z}} \simeq \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}. \tag{70}$$

Proof. Consider the mapping $f : \mathbb{Z} \to \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}$, such that $x \mapsto (\overline{x}^a, \overline{x}^b)$. Clearly $f \in \mathrm{Hom}\left(\mathbb{Z}, \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}\right)$. Moreover, we claim that $x \in \mathrm{Ker}(f)$ if and only if $ab \mid x$. Indeed, if $x \in \mathrm{Ker}(f)$, then $\overline{x}^a = \overline{0}^a$ and $\overline{x}^b = \overline{0}^b$. This necessarily means that $a \mid x$ and $b \mid x$, so that $ab \mid x$ since a and b are assumed to be coprime. On the other hand, if $ab \mid x$, then clearly $a \mid x$ and $b \mid x$, and thus $\overline{x}^a = \overline{0}^a$ and $\overline{x}^b = \overline{0}^b$. In other words, $x \in \mathrm{Ker}(f)$, thus the claim has been validated. Note that $\mathrm{Ker}(f)$ is a subgroup of $\mathbb{Z}$, so that it is of the form $n\mathbb{Z}$ for some unique n. By the claim, clearly $\mathrm{Ker}(f) = ab\mathbb{Z}$. Using the first isomorphism theorem (Theorem 1.75), we thus have that

$$\frac{\mathbb{Z}}{ab\mathbb{Z}} \xrightarrow{\overline{f}} \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}, \tag{71}$$

is injective. Moreover, since both sides have cardinality ab, this is actually bijective. Therefore, we can conclude that

$$\frac{\mathbb{Z}}{ab\mathbb{Z}} \simeq \frac{\mathbb{Z}}{a\mathbb{Z}} \times \frac{\mathbb{Z}}{b\mathbb{Z}}, \tag{72}$$

and the proof is complete. □

Theorem D.2. Let A be a finitely generated commutative group, then there exists a unique $m \in \mathbb{N}$, a unique $r \in \mathbb{N}$, and a unique sequence of positive integers $(d_1, \ldots, d_r)$ at least equal to 2 with $d_i \mid d_{i+1}$, such that

$$A \simeq \mathbb{Z}^m \times \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{d_r\mathbb{Z}}. \tag{73}$$

Here by convention, (1) $A \simeq \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{d_r\mathbb{Z}}$ if $m = 0$, (2) $A \simeq \mathbb{Z}^m$ if $r = 0$, and (3) $A \simeq \{0\}$ if $m = r = 0$.

Proof. TO BE DONE... □

Remark D.3. The d_i's above are called the **elementary divisors**.

Theorem D.4. Let A be a finite commutative group, then there exists a unique $r \in \mathbb{N}^*$ and a unique sequence of positive integers $(d_1, \ldots, d_r)$ with $d_i \mid d_{i+1}$, such that

$$A \simeq \frac{\mathbb{Z}}{d_1\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{d_r\mathbb{Z}}. \tag{74}$$

If a finite commuative group is written under this form, we say that it is under **standard form**.

Remark D.5. The method to put a product $\prod_{i=1}^{s} \frac{\mathbb{Z}}{n_i\mathbb{Z}}$ under standard form is to use the Chinese remainder theorem to decompose each $\frac{\mathbb{Z}}{n_i\mathbb{Z}}$ as much as possible. For this, write the decomposition of n_i into prime powers, such that

$$n_i = p_{1,i}^{a_{1,i}} \times \ldots \times p_{k_i,i}^{a_{k_i,i}}. \tag{75}$$

Then by the Chinese remainder theorem (Theorem D.1), we have that

$$\frac{\mathbb{Z}}{n_i\mathbb{Z}} \simeq \frac{\mathbb{Z}}{p_{1,i}^{a_{1,i}}\mathbb{Z}} \times \ldots \times \frac{\mathbb{Z}}{p_{k_i,i}^{a_{k_i,i}}\mathbb{Z}}. \tag{76}$$

One then needs to pair again these elementary pieces by the Chinese remainder theorem in order to obtain the standard form. For this, one makes a table in which each row corresponds to a given prime, and justifies the table to the right by adding 1's on the lefft if necessary. The product of the entries in each column of the table would then give the elementary divisors d_j.

Example D.6. (1) $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is already in standard form and n is the unique elementary divisor.

(2) Consider $A \simeq \frac{\mathbb{Z}}{15\mathbb{Z}} \times \frac{\mathbb{Z}}{50\mathbb{Z}}$. Decomposing the product as much as possible using the Chinese remainder theorem, we get that

$$A \simeq \left(\frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5\mathbb{Z}}\right) \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{5^2\mathbb{Z}}\right). \tag{77}$$

Therefore, for prime 2, we have powers 0 and 1; for prime 3, we have powers 1 and 0; and for prime 5, we have powers 1 and 2. Taking the smallest powers for the first divisor, we have $2^0 \times 3^0 \times 5^1 = 5$, and taking the following powers for the second divisor, we have that $2^1 \times 3^1 \times 5^2 = 150$. Therefore, applying the Chinese remainder theorem (Theorem D.1), we can obtain the standard form as

$$A \simeq \frac{\mathbb{Z}}{5\mathbb{Z}} \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{3\mathbb{Z}} \times \frac{\mathbb{Z}}{5^2\mathbb{Z}} \right) \simeq \frac{\mathbb{Z}}{5\mathbb{Z}} \times \frac{\mathbb{Z}}{150\mathbb{Z}}. \tag{78}$$