Suns

Eric Liu

Contents

Chapter 1

Groups

1.1 Group action

Let M be a set equipped with a binary operation $M \times M \to M$. We say M is a **monoid** if the binary operation is associative and there exists a two-sided identity $e \in M$.

Example 1.1.1. Defining $(x, y) \mapsto y$, we see that the operation is associative and every element is a left identity, but no element is a right identity unless $|M| = 1$. This is an example why identity must be two-sided.

Because the identity of a monoid is defined to be two-sided, clearly it must be unique. Suppose every element of monoid M has a left inverse. Fix $x \in M$. Let $x^{-1} \in M$ be a left inverse of x. To see that x^{-1} is also a right inverse of x, let $(x^{-1})^{-1} \in M$ be a left inverse of x and use

$$(x^{-1})^{-1} = (x^{-1})^{-1}e = (x^{-1})^{-1}(x^{-1}x) = ((x^{-1})^{-1}x^{-1})x = ex = x$$

to deduce

$$xx^{-1} = (x^{-1})^{-1}x^{-1} = e$$

In other words, if we require every element of a monoid M to has a left inverse, then immediately every left inverse upgrades to a right inverse. In such case, we call M a **group**. Notice that inverses of elements of a group are clearly unique.

Unlike the category of monoids, the category of groups behaves much better. Given two groups G, H and a function $\varphi : G \to H$, if φ respects the binary operation, then φ also respects the identity:

$$e_H = (\varphi(x)^{-1})\varphi(x) = (\varphi(x)^{-1})\varphi(xe_G) = (\varphi(x)^{-1}\varphi(x))\varphi(e_G) = \varphi(e_G)$$

which implies that φ must also respect inverse. In such case, we call φ a **group homomorphism**. Given a subset $H \subseteq G$ closed under the binary operation, if H forms a group itself, then since the set inclusion $H \hookrightarrow G$ forms a group homomorphism, we have $e_H = e_G$, and thus x^{-1} in H, G are the same element.

In this note, by a **subgroup** H of G, we mean an injective group homomorphism $H \hookrightarrow G$. Clearly, a subset of G forms a subgroup if and only it is closed under both the binary operation and inverse. Note that one of the key basic property of subgroup $H \subseteq G$ is that if $g \notin H$, then $hg \notin H$, since otherwise $g = h^{-1}hg \in H$.

Let S be a subset of G. The group of **words** in S is clearly the smallest subgroup of G containing S. We say this subgroup is **generated** by S. If G is generated by a single element, we say G is **cyclic**. Let $x \in G$. The **order** of G is the cardinality of G, and the order of x is the cardinality of the cyclic subgroup $\langle x \rangle \subseteq G$, or equivalently the infimum of the set of natural numbers n that makes $x^n = e$. Clearly, finite cyclic groups of order n are all isomorphic to $\mathbb{Z}_n$.

Let G be a group and H a subgroup of G. The **right cosets** Hx are defined by $Hx \triangleq \{hx \in G : h \in H\}$. Clearly, when we define an equivalence relation in G by setting:

$$x \sim y \overset{\triangle}{\iff} xy^{-1} \in H$$

the equivalence class $[x]$ coincides with the right coset Hx. Note that if we partition G using **left cosets**, the equivalence relation being $x \sim y \iff x^{-1}y \in H$, then the two partitions need not to be identical.

Example 1.1.2. Let $H \triangleq \{e, (1,2)\} \subseteq S_3$. The right cosets are

$$H(2,3) = \{(2,3), (1,2,3)\} \quad \text{and} \quad H(1,3) = \{(1,3), (1,3,2)\}$$

while the left cosets being

$$(2,3)H = \{(2,3), (1,3,2)\} \quad \text{and} \quad (1,3)H = \{(1,3), (1,2,3)\}$$

■

However, as one may verify, we have a well-defined bijection $xH \mapsto Hx^{-1}$ between the sets of left cosets and right cosets of H. Therefore, we may define the **index** $|G : H|$ of H in G to be the cardinality of the collection of left cosets of H, without falling into the discussion of left and right. Moreover, by axiom of choice, there exists a set $T \subseteq G$ such that $|T \cap xH| = 1$ for all $x \in G$. Such T clearly makes the set map $T \times H \to G$ defined by:

$$(t, h) \mapsto th$$

a bijection. This proves the **Lagrange's theorem**:

$$|G| = |G : H| \cdot |H|$$

Consider a group G of prime order. If $x \neq e \in G$, then clearly the cyclic subgroup $\langle x \rangle$ must be G by Lagrange's theorem.

Let G be a group and X a set. If we say G **acts on** X **from left** we are defining a function $G \times X \to X$ such that

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

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

Note that there is a difference between left action and right action, as gh means $g \circ h$ in left action and means $h \circ g$ in right action.

Because groups admit inverses, a G-action is in fact a group homomorphism $G \to \mathrm{Sym}(X)$. The trivial action then correspond to the trivial group homomorphism. An action is **faithful** if it is injective.

Show that $Z(G) \subseteq \operatorname{Ker} \theta$ if and only if θ is faithful.

An action is **free** if $g \cdot x = x$ for a $x \in X$ implies $g = e$. Note that the isomorphism $\mathrm{Sym}(X) \to \mathrm{Sym}(X)$ is always injective but never free unless $|X| \leq 2$. The action is **transitive** if for any $x, y \in X$, there always exists some $g \in G$ such that $y = g \cdot x$. An action is **regular** if it is both free and transitive.

Let $x \in X$. We call the set $G \cdot x \triangleq \{g \cdot x \in X : g \in G\}$ the **orbit** of x. Clearly the set G_x of all elements of G that fixes x forms a group, called the **stabilizer subgroup** of G with respect to x. Consider the action left. The fact that the obvious mapping between the set of left cosets of stabilizer subgroups of G with respect to x to the orbit of x:

$$\{g(G_x) \subseteq G : g \in G\} \longleftrightarrow G \cdot x$$

forms a bijection is called the **orbit-stabilizer theorem**.

Theorem 1.1.3. (Cauchy's theorem for finite group) Let G be a finite group whose order is divided by some prime p. Then the number of solutions to the equation $x^p = e$ is a positive multiple of p.

Proof. The set X of p-tuples $(x_1, \ldots, x_p)$ that satisfies $x_1 \cdots x_p = e$ clearly has cardinality $|G|^{p-1}$.

Consider the group action $\mathbb{Z}_p \to \mathrm{Sym}(X)$ defined by

$$g \cdot (x_1, \ldots, x_p) \triangleq (x_p, x_1, \ldots, x_{p-1})$$

Then by orbit-stabilizer theorem and Lagrange theorem, an orbit in X either has cardinality p or 1.

$$p|\,|G|^{p-1} = m + kp$$

with m the number of cardinality 1 orbits and k the number of cardinality p orbits.

This implies $p|m$, as desired.
Notice that $x^p = e$ if and only if $(x, \ldots, x) \in X$. Therefore the number of cardinality 1 orbit equals to number of solution to $x^p = e$.

■

1.2 Normalizer and centralizer

Because the inverse of an injective group homomorphism forms a group homomorphism, we know the set $\text{Aut}(G)$ of automorphisms of G forms a group. We say $\phi \in \text{Aut}(G)$ is an **inner automorphism** if ϕ takes the form $x \mapsto gxg^{-1}$ for some fixed $g \in G$. We say two elements $x, y \in G$ are **conjugated** if there exists some inner automorphism that maps x to y. Clearly conjugacy forms a equivalence relation. We call its classes **conjugacy classes**.

Equivalent Definition 1.2.1. (Normalize)

From the point of view of inner automorphism, we see that it is well-defined whether an element $g \in G$ **normalize** a subset $S \subseteq G$:

$$\left\{gsg^{-1} \in G : s \in S\right\} = S$$

independent of left and right. Because of the independence, For each subset $S \subseteq G$, we see that the set of elements $g \in G$ that normalize S forms a group, called the **normalizer** of S. Note that if g normalize S, then $gS = Sg$.

Example 1.2.2. Consider $G \triangleq \text{GL}_2(\mathbb{R})$ and consider:

$$H \triangleq \left\{\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R}) : n \in \mathbb{Z}\right\} \quad \text{and} \quad g \triangleq \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \in \text{GL}_2(\mathbb{R})$$

Note that $gHg^{-1} \subset H$. In other words, inner automorphisms can maps a subgroup H into a subgroup strictly contained by H if G is infinite.

Equivalent Definition 1.2.3. (Normal subgroups) Let G be a group and N a subgroup. We say N is a **normal subgroup** of G if any of the followings hold true:

(i) $\phi(N) \subseteq N$ for all $\phi \in \text{Inn}(G)$

(ii) $\phi(N) = N$ for all $\phi \in \text{Inn}(G)$

(iii) $xN = Nx$ for all $x \in G$.

(iv) The set of all left cosets of N equals the set of all right cosets of N.

(v) N is a union of conjugacy classes.

(vi) For all $n \in N$ and $x \in G$, their **commutator** $nxn^{-1}x^{-1} \in G$ lies in N.

(vii) For all $x, y \in G$, we have $xy \in N \iff yx \in N$.

Proof. (i) $\implies$ (ii): Let $\phi \in \text{Inn}(G)$. By premise, $\phi(N) \subseteq N$ and $\phi^{-1}(N) \subseteq N$. Applying ϕ to both side of $\phi^{-1}(N) \subseteq N$, we have $\phi(N) \subseteq N \subseteq \phi(N)$, as desired.

(ii) $\implies$ (iii): Consider the automorphisms:

$$\phi_{L,x}(g) = xg \quad \text{and} \quad \phi_{L,x^{-1}}(g) = x^{-1}g \quad \text{and} \quad \phi_{R,x}(g) = gx$$

Because $\phi_{L,x^{-1}} \circ \phi_{R,x} \in \text{Inn}(G)$, by premise we have:

$$xN = \phi_{L,x}(N) = \phi_{L,x} \circ \phi_{L,x^{-1}} \circ \phi_{R,x}(N) = \phi_{R,x}(N) = Nx$$

(iii) $\implies$ (iv) is clear. (iv) $\implies$ (iii): Let $x \in G$. By premise, there exists some $y \in G$ that makes $xN = Ny$. Let $x = ny$. The proof then follows from noting

$$xN = Ny = N(n^{-1}x) = Nx$$

(iii) $\implies$ (v): Let $n \in N$ and $x \in G$. We are required to show $xnx^{-1} \in N$. Because $xN = NX$, we know $xn = \widetilde{n}x$ for some $\widetilde{n} \in N$. This implies

$$xnx^{-1} = \widetilde{n}xx^{-1} = \widetilde{n} \in N$$

(v) $\implies$ (vi): Fix $n \in N$ and $x \in G$. By premise, $xn^{-1}x^{-1} \in N$. Therefore, $n(xn^{-1}x^{-1}) \in N$, as desired.

(vi) $\implies$ (vii): Let $xy \in N$. To see yx also belong to N, observe:

$$(xy)^{-1}(yx) = (xy)^{-1}x^{-1}xyx = [xy, x] \in N$$

(viii) $\implies$ (i): Let $n \in N$ and $x \in G$. Because $(nx)x^{-1} = n \in N$, by premise we have $x^{-1}nx \in N$, as desired. ■

Equivalent Definition 1.2.4. (Normal closure) Let G be a group and $S \subseteq G$. The **normal closure** $\text{ncl}_G(S)$ of S in G refer to any one of the followings:

(i) The smallest normal subgroup of G containing S, which we know exists as the intersection of all normal subgroups of G containing S.

(ii) The subgroup of G generated by

$$\bigcup_{\phi \in \text{Inn}(G)} \{\phi(x) \in G : x \in S\}$$

Proof. We are required to prove the subgroup of G from (ii) is normal. Clearly, it is the set:

$$\left\{g_1^{-1}x_1^{\epsilon_1}g_1 \cdots g_n^{-1}x_n^{\epsilon_n}g_n \in G : n \geq 0, x_i \in S, \epsilon_i = \pm 1, g_i \in G\right\}$$

Fix $g \in G$. The proof then follows from noting

$$g^{-1}\left(g_1^{-1}x_1^{\epsilon_1}g_1 \cdots g_n^{-1}x_n^{\epsilon_n}g_n\right)g = \Big(\left(g_1g\right)^{-1}x_1^{\epsilon_1}\left(g_1g\right)\Big)\cdots\Big(\left(g_ng\right)^{-1}x_n^{\epsilon_n}\left(g_ng\right)\Big)$$

■

We denote the **centralizer** $C_G(S) \triangleq \left\{g \in G : gsg^{-1} = s \text{ for all } s \in S\right\}$. We call the centralizer of the whole group $Z(G) \triangleq C_G(G)$ **center**. Clearly $Z(G)$ forms an abelian subgroup of G, and every element of the center form a single conjugacy classes.

For finite group G, we have the **class equation**

$$|G| = |Z(G)| + \sum |G : C_G(x)|$$

where x runs through conjugacy classes outside of $Z(G)$.

Clearly $C_G(S) \subseteq N_G(S)$.

1.3 Isomorphism theorems

Let G be a group and $N \subseteq G$ a normal subgroup. We say a group homomorphism $\pi : G \to G/N$ satisfies the **universal property of quotient group** G/N if

(i) it vanishes on N. **(Group condition)**

(ii) for all group homomorphism $f : G \to H$ that vanishes on N there exist a unique group homomorphism $\widetilde{f} : G/N \to H$ that makes the diagram:

$$\begin{tikzcd} G \arrow[r, two heads, "\pi"] \arrow[dr, "f"'] & G/N \arrow[d, "\widetilde{f}"] \\ & H \end{tikzcd}$$

commute. **(Universality)**

Theorem 1.3.1. (The first isomorphism theorem for groups) The group homomorphism $\pi : G \to G/N$ is always surjective with kernel N. Let $f : G \to H$ be a group homomorphism. Then $\ker f$ is normal in G, and the induced homomorphism $\widetilde{f} : G/\ker f \to H$ is injective.

Proof. The first part is an immediate consequence of construction of G/N. However, it should be noted that such construction can be avoided. The fact that $\ker(\pi) = N$ can be proved by considering the permutation representation $G \to \mathrm{Sym}(\Omega)$, where Ω is the set of the cosets of N, and the fact that π is surjective is a consequence of $\widetilde{\pi} = \mathbf{id}_{G/N}$.

We clearly have $\ker f \trianglelefteq G$. The fact that $\widetilde{f} : G/\ker f \to H$ is injective follows from $\pi : G \to G/\ker f$ being surjective with kernel $\ker f$. ∎

Because the kernel of a group homomorphism is clearly normal, if N is not normal, then there can not be a pair $G \to G/N$ that satisfies the universal property. If any things, this is the "reason" why normal subgroups are what meant to be quotiented in the category of group.

Given $x, y \in G$, we often write

$$[x, y] \triangleq xyx^{-1}y^{-1} \quad \text{or} \quad [x, y] \triangleq x^{-1}y^{-1}xy$$

and call $[x, y]$ the **commutator** of x and y. Independent of differences of the definition, we have $[x, y] \in N$ if and only if $xyN = yxN$. Again, independent of the definition, the **commutator subgroup** $[G, G]$ of G is the subgroup generated by the commutators.

Theorem 1.3.2. **()**

$$G/N \text{ is abelian} \iff [G,G] \subseteq N$$

Proof. ($\implies$):

$$(xyx^{-1}y^{-1})N = xN \cdot yN \cdot (x^{-1})N \cdot (y^{-1})N = N$$

($\impliedby$): ■

Example 1.3.3. $G \triangleq S_3$. $S \triangleq \langle(1,2)\rangle$ and $H \triangleq \langle(2,3)\rangle$. SH doesn't form a group. $(2,3)(1,2) \notin SH$.

Theorem 1.3.4. **(Second isomorphism theorem)** Let $H \leq G$. If K is a subgroup of normalizer of H, then their product:

$$HK \triangleq \{hk \in G : h \in H \text{ and } k \in K\}$$

forms a group and is defined independent of left and right. Moreover, $H \trianglelefteq HK$ with $hkH = kH$, and $H \cap K \trianglelefteq K$ with

$$HK/H \cong K/H \cap K \quad \text{via} \quad kH \longleftrightarrow k(H \cap K)$$

Proof. ■

Third isomorphism theorem.
Correspondence theorem.
Because $\varphi \circ \phi_g \circ \varphi^{-1} = \phi_{\varphi(g)}$, we know $\text{Inn}(G)$ forms a normal subgroup of $\text{Aut}(G)$.

1.4 Sylow theorems

Let $o(G) \triangleq p^m q$ with $\gcd(p, q) = 1$, and let $n \leq m$. Because

$$\binom{p^m q}{p^m} = \frac{p^m q(p^m q - 1) \cdots (p^m q - p^m + 1)}{p^m(p^m - 1) \cdots 1}$$

and clearly

$$p^k | p^m q - i \iff p^k | i \iff p^k | p^m - i, \qquad \text{for all } i \text{ and } k$$

Let $\mathcal{S}$ be the set of subsets of G with cardinality p^n. Clearly $|\mathcal{S}| = \binom{o(G)}{p^n}$ and we may define a left G-action on $\mathcal{S}$ by

$$g \cdot \{h_1, \ldots, h_{p^n}\} \triangleq \{gh_1, \ldots, gh_{p^n}\}$$

we

1.5 Exercises

Question 1

Show that

(i) If $H/Z(H)$ is cyclic, then H is abelian.

(ii) If H is of order p^2, then H is abelian.

From now on, suppose G is non-abelian with order p^3.

(iii) $|Z(G)| = p$.

(iv) $Z(G) = [G, G]$.

Proof. Let $a, b \in H$ and $H/Z(H) = \langle hZ \rangle$. Write $a = h^n z_1$ and $b = h^m z_2$. Because $z_1, z_2 \in Z(H)$, we may compute:

$$ab = h^n z_1 h^m z_2 = h^{n+m} z_1 z_2 = ba$$

as desired.

Let $|H| = p^2$. Because H is a p-group, we know $Z(H)$ is nontrivial, therefore either $|Z(H)| = p$ or $|Z(H)| = p^2$. To see the former is impossible, just observe that if so, then $|H/Z(H)| = p$, which implies $H/Z(H)$ is cyclic, which by part (i) implies $Z(H) = H$.

Because G is non-abelian, we know $|Z(G)| \neq p^3$. Because G is a p-group, we know $|Z(G)| \neq 1$. Therefore, either $|Z(G)| = p$ or $|Z(G)| = p^2$. Part (i) tell us that $|Z(G)| \neq p^2$, otherwise G is abelian, a contradiction. We have shown $|Z(G)| = p$, as desired.

We now prove $Z(G) = [G, G]$. Because $|Z(G)| = p$, by part (ii) we know $G/Z(G)$ is abelian. This implies $[G, G] \leq Z(G)$, which implies $[G, G]$ is either trivial or equal to $Z(G)$. Because G is non-abelian, we know $[G, G]$ can not be trivial. This implies $Z(G) = [G, G]$, as desired. ■

Question 2

(i) Let M, N be two normal subgroups of G with $MN = G$. Prove that

$$G/(M \cap N) \cong (G/M) \times (G/N)$$

(ii) Let H, K be two distinct subgroups of G of index 2. Prove that $H \cap K$ is a normal subgroup with index 4 and $G/(H \cap K)$ is not cyclic.

Proof. The map $G/(M \cap N) \to (G/M) \times (G/N)$ defined by

$$g(M \cap N) \mapsto (gM, gN) \tag{1.1}$$

is clearly a well-defined group homomorphism, since if $gM = hM$ and $gN = hN$, then $gh^{-1} \in M$ and $gh^{-1} \in N$, which implies $gh^{-1} \in M \cap N$, which implies $g(M \cap N) = h(M \cap N)$. Let $gM = M$ and $gN = N$. Then $g \in M \cap N$ and $g(M \cap N) = M \cap N$. Therefore map 1.1 is also injective. It remains to show map 1.1 is surjective. Fix $g, h \in G$. Write $g = mn$ and $h = \widetilde{m}\widetilde{n}$. Clearly $gM = nM = \widetilde{m}nM$ and $hN = \widetilde{m}N = \widetilde{m}nN$. This implies that mapping 1.1 maps $\widetilde{m}n$ to (gM, hN), as desired.

Because H, K are both of index 2 in G, we know they are both normal in G. This by second isomorphism theorem implies HK forms a subgroup of G. Because $H \neq K$, we know HK properly contains H, which by finiteness of G implies the index of HK is strictly less than H, i.e., $HK = G$. Note that $H \cap K$ is normal since it is the intersection of normal subgroups. By part (i), we now have $G/(H \cap K) \cong (G/H) \times (G/K) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$, which shows that $H \cap K$ has index 4 and $G/(H \cap K)$ is cyclic. ∎

Question 3

Let G be a group of order pq, where $p > q$ are prime.

(i) Show that there exists a unique subgroup of order p.

(ii) Suppose $a \in G$ with $o(a) = p$. Show that $\langle a \rangle \subseteq G$ is normal and for all $x \in G$, we have $x^{-1}ax = a^i$ for some $0 < i < p$.

Proof. The third Sylow theorem stated that the number n_p of Sylow p-subgroups satisfies

$$n_p \equiv 1 \pmod{p} \quad \text{and} \quad n_p \mid q$$

Because $p > q$, together they implies $n_p = 1$. Since Sylow p-subgroups of G are exactly subgroups of order p, we have proved (i).

The third Sylow theorem also stated that $n_p = |G : N_G(P)|$ for any Sylow p-subgroup $P \leq G$. Therefore, $N_G(\langle a \rangle) = G$, i.e., $\langle a \rangle$ is normal in G. Fix $x \in G$. It remains to prove $xax^{-1} \neq e$, which is a consequence of the fact that conjugacy (automorphism) preserves order. ∎

Question 4

Let H, K be two subgroups of G of coprime finite indices m, n. Show that

$$\operatorname{lcm}(m, n) \leq |G : H \cap K| \leq mn$$

Proof. Let $\Omega_{H\cap K}, \Omega$, and Ω_K respectively denote the set of left cosets of $H \cap K, H$, and K. The map $\Omega_{H\cap K} \to \Omega_H \times \Omega_K$ defined by

$$g(H \cap K) \mapsto (gH, gK) \tag{1.2}$$

is well defined since

$$g(H \cap K) = l(H \cap K) \implies g^{-1}l \in H \cap K \implies gH = lH \text{ and } gK = lK$$

such set map is injective since if $gH = lH$ and $gK = lK$, then $g^{-1}l \in H$ and $g^{-1}l \in K$, which implies $g(H \cap K) = l(H \cap K)$, as desired. From the injectivity of map 1.2, we have shown index of $H \cap K$ indeed have upper bound mn.

■