

Algebra

September 26, 2016

1 Group theory

1.1 Week 1

Def 1. A non-empty set G with a binary function $f : G \times G \rightarrow G, (a, b) \mapsto ab$ is a **group** if it satisfies

1. $(ab)c = a(bc)$.
2. $\exists 1 \in G$ s.t. $1a = a1 = a, \forall a \in G$.
3. $\exists a^{-1} \in G$ s.t. $aa^{-1} = a^{-1}a = 1$.

CONCON

Def 2. Let G be a group. Then G is said to be **abelian** if $\forall a, b \in G, ab = ba$.

Def 3. Let G be a group and $H \subseteq G, H \neq \emptyset$. Then H is said to be a subgroup of G , denoted by $H \leq G$, if

1. $\forall a, b \in H, ab \in H$.
2. $1 \in H$.
3. $\forall a \in H, a^{-1} \in H$.

useful criterion: $H \leq G \iff \forall a, b \in H, ab^{-1} \in H$.

pf:

\Rightarrow $b \in H \implies b^{-1} \in H$, and $a \in H$, so $ab^{-1} \in H$.

\Leftarrow

1. $H \neq \emptyset \implies \exists a \in H \implies aa^{-1} = 1 \in H$.
2. $1, a \in H \implies 1a^{-1} = a^{-1} \in H$.
3. $a, b^{-1} \in H \implies a(b^{-1})^{-1} = ab \in H$. □

Eg 1.1.1. $(\mathbb{Z}, +, 0) \leq (\mathbb{Q}, +, 0) \leq (\mathbb{R}, +, 0) \leq (\mathbb{C}, +, 0) ; (\mathbb{Q}^\times, \times, 1) \leq (\mathbb{R}^\times, \times, 1) \leq (\mathbb{C}^\times, \times, 1)$

Eg 1.1.2.

- Special linear group $\text{SL}(n, \mathbb{F}) = \{ A \in \text{GL}(n, \mathbb{F}) \mid \det A = 1 \}$
- Orthogonal group $\text{O}(n) = \{ A \in \text{GL}(n, \mathbb{R}) \mid A^t A = I_n \}$
- Unitary group $\text{U}(n) = \{ A \in \text{GL}(n, \mathbb{C}) \mid A^* A = I_n \}$
- Special orthogonal group $\text{SO}(n) = \text{SL}(n, \mathbb{R}) \cap \text{O}(n)$
- Special unitary group $\text{SU}(n) = \text{SL}(n, \mathbb{C}) \cap \text{U}(n)$

Def 4. Let $f : G_1 \rightarrow G_2$. f is called an **isomorphism** if

1. f is 1-1 and onto.
2. $\forall a, b \in G_1, f(ab) = f(a)f(b)$. (**homomorphism**)

, denoted by $G_1 \cong G_2$.

Remark 1. (practice)

1. $f(1) = 1$.

2. $f(a^{-1}) = f(a)^{-1}$.
3. If f is an isomorphism, then $\exists f^{-1}$ is also a homomorphism.

Eg 1.1.3.

- $U(1) = \{ z \in \mathbb{C}^\times \mid \bar{z}z = 1 \}, z = \cos \theta + \sin \theta i$
- $SO(2) = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} : \theta \in \mathbb{R} \right\}$

notice that $U(1) \cong SO(2)$. $S^1 = \{ (a, b) \in \mathbb{R}^2 \mid a^2 + b^2 = 1 \}$, 可被賦予群的結構.

Eg 1.1.4. Let $A \in SU(2) \implies A = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \alpha\bar{\alpha} + \beta\bar{\beta} = 1, \alpha, \beta \in \mathbb{C}$.

Quaternion(四元數): $\mathbb{H} = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \}$ with $i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j (\implies ij = -ji)$.

Let $x = a + bi + cj + dk, \bar{x} = a - bi - cj - dk$, then $N(x) = x\bar{x} = a^2 + b^2 + c^2 + d^2$, For $x \neq 0, N(x) \neq 0, x^{-1} = \frac{1}{N(x)}\bar{x}$

Now, for $x = a + bi + cj + dk = (a + bi) + (c + di)j$. So $SU(2) \cong \{ x \in \mathbb{H}^\times \mid N(x) = 1 \}$. $S^3 = \{ (a, b, c, d) \in \mathbb{R}^4 \mid a^2 + b^2 + c^2 + d^2 = 1 \}$, 可被賦予群的結構.

★ The only spheres with continuous group law are S^1, S^3 .

Def 5 (symplectic group). $Sp(n, \mathbb{F}) = \{ A \in GL(2n, \mathbb{F}) \mid A^t J A = J \}$ where $J = \begin{pmatrix} O & I_n \\ -I_n & O \end{pmatrix}$.

($A^t J A = J$ preserving non-degenerate skew-symmetric forms)

$Sp(n) = \{ A \in GL(n, \mathbb{H}) \mid A^* A = I_n \}$.

Ques: Find the smallest subgroup of $SU(2)$ containing $\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$.

Ex 1.1.1. Let G be a semigroup. Then TFAE (the following are equivalent)

1. G is a group.
2. For all $a, b \in G$ and the equations $bx = a, yb = a$, each of them has a solution in G .
3. $\exists e \in G$ s.t. $ae = a \forall a \in G$ and if we fix such e , then $\forall b \in G \exists b' \in G$ s.t. $bb' = e$.

Ex 1.1.2. Let G be a group. Show that

1. $\forall a \in G, a^2 = 1$, then G is abelian.
2. G is abelian $\iff \forall a, b \in G, (ab)^n = a^n b^n$ for three consecutive integer n .

Ex 1.1.3. Find a way to regard $M_{n \times n}(\mathbb{H})$ as a subset of $M_{2n \times 2n}(\mathbb{C})$, which preserves addition and multiplication, and then there is a way to characterize $GL(n, \mathbb{H})$.

Ex 1.1.4. Show $Sp(n) \cong U(2n) \cap Sp(n, \mathbb{C})$.

1.2 Week 2

1.2.1 Permutation groups and Dihedral groups

Def 6. A permutation of a set B is a 1-1 and onto function from B to B .

Let $S_B :=$ the set of permutations of B . Then $(S_B, \cdot, \text{Id}_B)$ forms a group.

If $B = \{a_1, \dots, a_n\}$, then $S_B \cong S_{\{1, \dots, n\}}$ and write $S_n = S_{\{1, \dots, n\}}$, called the symmetric group of degree n .

Theorem 1 (Cayley theorem). Any group is isomorphic to a subgroup of some permutation group.

(Hint): Let G be a group. Set $B = G$. Consider $a \in G$ as $\sigma_a : G \rightarrow G, x \mapsto ax$. Then $\sigma_a \in S_G \implies G \leq S_G$.

Fact 1.2.1. S_n is a finite group of order $n!$, i.e. $|S_n| = n!$.

pf: EASY =O

□

Cyclic notation: $\sigma \in S_5$, say $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 1 & 2 \end{pmatrix}$. Write $\sigma = (1\ 4)(2\ 3\ 5)$.

\Rightarrow Any permutation can be written as a product of disjoint cycles.

Eg 1.2.1. In S_7 , $\sigma_1 = (1\ 2\ 3)(4\ 5\ 6)(7)$, $\sigma_2 = (1\ 3\ 5\ 6)(2\ 4\ 7)$.

Then $\sigma_1\sigma_2 = (2\ 5\ 4\ 7\ 3\ 6)$, $\sigma_1^{-1} = (1\ 3\ 2)(4\ 6\ 5)$.

Def 7. A 2 cycle is called a **transposition**.

Eg 1.2.2. $(1\ 2\ 3) = (1\ 3)(1\ 2)$, $(1\ 2\ 3\ 4\ 5) = (1\ 5)(1\ 4)(1\ 3)(1\ 2)$.

Any permutation is a product of 2 cycles.

Useful formula: $\sigma \in S_n$, $\sigma(j_1 \dots j_m)\sigma^{-1} = (\sigma(j_1) \dots \sigma(j_m))$.

Eg 1.2.3. Let $\sigma = (1\ 2\ 3)(4\ 5\ 6\ 7)$, $\sigma(2\ 3\ 4)\sigma^{-1} = (3\ 1\ 5)$.

pf: Note that both sides are functions. For $i \in \{1, \dots, n\}$,

Case 1: $\exists k$ s.t. $\sigma(j_k) = i$, CONCON

Case 2: Otherwise, CONCON

□

Fact 1.2.2. $S_n = \langle (1\ 2), \dots, (1\ n) \rangle$.

pf: $(1\ i)^{-1} = (1\ i)$ and $(i\ j) = (1\ i)(1\ j)(1\ i)^{-1}$.

□

Def 8. Let G be a group and $S \subset G$. The subgroup generated by S defined to be the smallest subgroup of G which contains S , denoted by $\langle S \rangle$.

Def 9. $A_n = \{\text{even permutations of } S_n\} \leq S_n, |A_n| = \frac{n!}{2}$.

Remark 2. $\langle S \rangle = \bigcap_{S \subseteq H \leq G} H = \{a_1 a_2 \dots a_k \mid k \in \mathbb{N}, a_i \in S \cup S^{-1}\} \cup \{1\}$

The orthogonal transformations on \mathbb{R}^2 : $O(2)$.

Let $A = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} \in O(2)$.

略... (這邊討論旋轉和反射的矩陣)

Case 1: $A = \begin{pmatrix} \cos \alpha & -\sin \alpha \\ \sin \alpha & \cos \alpha \end{pmatrix}$ is counterclockwise rotation w.r.t. α .

Case 2: $A = \begin{pmatrix} \cos \alpha & \sin \alpha \\ \sin \alpha & -\cos \alpha \end{pmatrix}$ is the reflection. $A^2 = I_2 \implies$ eigenvalues are ± 1 .

Easy to show that $L_A(v) = v - 2\langle v, v_2 \rangle v_2$.

$O(2) = \{\text{rotations}\} \cup \{\text{reflections}\}$.

Def 10. The dihedral group D_n is the group of symmetries of a regular n -gon. In general, $D_n = \langle T, R \mid T^n = 1, R^2 = 1, TR = RT^{-1} \rangle \leq O(2) \leq S_n, |D_n| = 2n$.

Def 11. Let T be a linear transformation from $\mathbb{R}^n \rightarrow \mathbb{R}^n$.

- T is called a rotation if \exists a T -invariant subspace $W \subseteq \mathbb{R}^n$ with $\dim W = 2$ s.t. $\begin{cases} T|_W \text{ is a rotation} \\ T|_{W^\perp} = \text{id}_{W^\perp} \end{cases}$
- T is called a reflection if \exists a T -invariant subspace $W \subseteq \mathbb{R}^n$ with $\dim W = 1$ s.t. $\begin{cases} T|_W = -\text{id}_W \\ T|_{W^\perp} = \text{id}_{W^\perp} \end{cases}$

Main result: the group of orthogonal transformations $= \langle \text{rotations, reflections} \rangle$.

Prop 1.2.1. For $T : \mathbb{R}^n \rightarrow \mathbb{R}^n$, \exists a T -invariant subspace $W \subseteq \mathbb{R}^n$ with $1 \leq \dim W \leq 2$.

pf: Let $A = [T]_\alpha \in M_{n \times n}(\mathbb{R}) \subseteq M_{n \times n}(\mathbb{C})$. Consider $\widetilde{L}_A : \mathbb{C}^n \rightarrow \mathbb{C}^n, v \mapsto Av$.

Then \exists an eigenvalue $\lambda \in \mathbb{C}$ and an eigenvector $v \in \mathbb{C}^n$ for \widetilde{L}_A . Let $\lambda = \lambda_1 + \lambda_2 i, v = v_1 + v_2 i$. By definition, we have

$$Av = \widetilde{L}_A(v) = \lambda v = (\lambda_1 + \lambda_2 i)(v_1 + v_2 i) \implies \begin{cases} Av_1 = \lambda_1 v_1 - \lambda_2 v_2 \\ Av_2 = \lambda_2 v_1 + \lambda_1 v_2 \end{cases},$$

so $W = \langle v_1, v_2 \rangle$. □

For $n = 3, A \in O(3)$, we have $A \sim \begin{pmatrix} \cos \alpha & -\sin \alpha & \\ \sin \alpha & \cos \alpha & \\ & & \pm 1 \end{pmatrix}$.

1.2.2 Cyclic groups and internal direct product

Def 12. If $G = \langle a \rangle = \{\dots, a^{-2}, a^{-1}, a, 1, a, a^2, \dots\} = \{a^n \mid n \in \mathbb{Z}\}$, then G is a cyclic group generated by a .

Eg 1.2.4. $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

Eg 1.2.5. Let $A = \begin{pmatrix} \cos \frac{2\pi}{n} & -\sin \frac{2\pi}{n} \\ \sin \frac{2\pi}{n} & \cos \frac{2\pi}{n} \end{pmatrix} \in SO(2)$. Then $\langle A \rangle = \{I_2, A, A^2, \dots, A^{n-1}\}$ and $A^n = I_2, A^m = A^r$ where $m \equiv r \pmod{n}$.

Eg 1.2.6. $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{(n-1)}\}$ with $\bar{j} = \{m \in \mathbb{Z} \mid m \equiv j \pmod{n}\}$.

Define $\bar{i} + \bar{j} = \begin{cases} \overline{i+j} & \text{if } 0 \leq i+j \leq n \\ \overline{i+j-n} & \text{otherwise} \end{cases} \implies (\mathbb{Z}/n\mathbb{Z}, +, \bar{0}) \text{ forms a group.}$

Remark 3. $\bar{i} \times \bar{j} = \overline{i \times j}$.

- 略

- If $\gcd(j, n) = d, \exists h, k \in \mathbb{Z}$ s.t. $hj + kn = d$.

Def 13. $(\mathbb{Z}/n\mathbb{Z})^\times = \{j \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(j, n) = 1\} \implies ((\mathbb{Z}/n\mathbb{Z})^\times, \times, \bar{1})$ forms a group.

Eg 1.2.7. 略... 简化剩余系, 原根 (generator) $(1, 2, 4, p^k, 2p^k, p \text{ is an odd prime})$

Def 14.

- The **order** of a finite group G is the number of elements in G , denoted by $|G|$.
- Let $a \in G$, the order of a is defined to be the least positive integer n s.t. $a^n = 1$, denoted by $\text{ord}(a) = n$.
- If $a^n \neq 1 \quad \forall n \in \mathbb{N}$, then we call “ a has infinite order”.

Prop 1.2.2. Let $G = \langle a \rangle$ with $\text{ord}(a) = n$. Then

1. $a^m = 1 \iff n \mid m$.

pf:

\Leftarrow : Let $m = dn$, then $a^m = (a^n)^d = 1$.

\Rightarrow : Let $m = qn + r, 0 \leq r < n$. If $r \neq 0$, then $a^r = a^{m-qn} = (a^m)(a^n)^{-q} = 1$. But $r < n$, which is a contradiction. Hence $r = 0 \implies n \mid m$. \square

2. $\text{ord}(a^r) = n / \gcd(r, n)$.

pf: Let $\gcd(r, n) = d, n = dn', r = dr'$ with $\gcd(n', r') = 1$. Plan to show “ $\text{ord}(a^r) = n'$ ”

- $(a^r)^{n'} = a^{r'dn'} = (a^n)^{r'} = 1 \implies \text{ord}(a^r) \mid n'$.
- $1 = (a^r)^{\text{ord}(a^r)} = a^{r \cdot \text{ord}(a^r)} \implies n \mid r \cdot \text{ord}(a^r) \implies n' \mid r' \cdot \text{ord}(a^r) \implies n' \mid \text{ord}(a^r)$.

\square

Prop 1.2.3. Any subgroup of a cyclic group is cyclic.

pf: Let $G = \langle a \rangle$ and $H \leq G$. If $H = \{1\}$, then $H = \langle 1 \rangle$, done!

Otherwise, $d = \min\{m \in \mathbb{N} \mid a^m \in H\}$, by well-ordering axiom. Claim $H = \langle a^d \rangle$.

\supset : $a^d \in H$ by the definition of d .

\subset : $\forall a^m \in H$, write $m = qd + r, 0 \leq r < d$. If $r \neq 0$, then $a^r = a^{m-qd} = a^m(a^d)^{-q} \in H$, which is a contradiction. Hence $r = 0 \implies d \mid m$.

\square

Prop 1.2.4. Let $G = \langle a \rangle$. Then

1. $\text{ord}(a) = n \implies G \cong \mathbb{Z}/n\mathbb{Z}$
2. $\text{ord}(a) = \infty \implies G \cong \mathbb{Z}$

Def 15. Let $G_1, G_2 \leq G$. G is the internal direct product of G_1, G_2 if $G_1 \times G_2 \rightarrow G, (g_1, g_2) \mapsto g_1 g_2$ is an isom.

Remark 4. In this case, we find that

- $G = G_1 G_2 = \{g_1 g_2 \mid g_1 \in G_1, g_2 \in G_2\}$.
- $G_1 \cap G_2 = \{1\}$. (consider $a \neq 1 \in G_1 \cap G_2$, then $(1, a) \mapsto a, (a, 1) \mapsto a$, but the function is 1-1, which is a contradiction.)
- If $a \in G$ with $a = g_1 g_2 = g'_1 g'_2$, then $(g'_1)^{-1} g_1 = (g'_2) g_2^{-1} \in G_1 \cap G_2 = \{1\} \implies \begin{cases} g_1 = g'_1 \\ g_2 = g'_2 \end{cases}$.
- For $g_1 \in G_1, g_2 \in G_2, (g_1, g_2) = (g_1, 1)(1, g_2) = (1, g_2)(g_1, 1) \implies g_1 g_2 = g_2 g_1$.

Eg 1.2.8.

1. $G = \mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}, G_1 = \{\bar{0}, \bar{3}\}, G_2 = \{\bar{0}, \bar{2}, \bar{4}\}$. We have $G \cong G_1 \times G_2$.
2. $G = S_3, G_1 = \langle (1\ 2) \rangle, G_2 = \langle (1\ 2\ 3) \rangle$. We have $G_1 \times G_2 \not\cong G$ since $(1\ 2)(1\ 2\ 3) \neq (1\ 2\ 3)(1\ 2)$.

Eg 1.2.9. $G = S_3, G_1 = \langle (1\ 2) \rangle, G_2 = \langle (2\ 3) \rangle, G_1 G_2 = \{1, (1\ 2), (2\ 3), (1\ 2\ 3)\} \not\subseteq G$ since $(1\ 3\ 2) = (1\ 2\ 3)^{-1} \notin G_1 G_2$.

Prop 1.2.5. Let $H, K \leq G$. Then $HK \leq G \iff HK = KH$.

pf:

$$\begin{aligned} \Rightarrow: \begin{cases} H \leq HK \\ K \leq HK \end{cases} &\implies KH \subseteq HK; \forall hk \in HK, \exists h'k' \in HK \text{ s.t. } (hk)(h'k') = 1 \implies hk = \\ &(k')^{-1}(h')^{-1} \in KH \implies HK \subseteq KH. \end{aligned}$$

$$\Leftarrow: \text{For } h_1 k_1, h_2 k_2 \in HK, (h_1 k_1)(h_2 k_2)^{-1} = h_1 k_1 k_2^{-1} h_2^{-1} = h_1 h' k' \in HK.$$

□

Ex 1.2.1.

1. $S_n = \langle (1\ 2), (2\ 3), \dots, (n-1\ n) \rangle, \quad n \geq 2$.
2. $S_n = \langle (1\ 2), (1\ 2 \dots n) \rangle, \quad n \geq 2$.

Ex 1.2.2.

1. $A_n = \langle (1\ 2\ 3), (1\ 2\ 4), \dots, (1\ 2\ n) \rangle, n \geq 3$.
2. $A_n = \langle (1\ 2\ 3), (2\ 3\ 4), \dots, (n-2\ n-1\ n) \rangle, n \geq 3$.

Ex 1.2.3.

1. If T is orthogonal, then W^\perp is also T -invariant.
2. Use induction on n to show the main result.

Ex 1.2.4.

1. $\text{ord}(a) = \text{ord}(a^{-1}) = n$.
2. $\langle a^r \rangle = \langle a^{\gcd(n, r)} \rangle$.
3. $\langle a^{r_1} \rangle = \langle a^{r_2} \rangle \iff \gcd(n, r_1) = \gcd(n, r_2)$.
4. $\forall m \mid n, \exists! H \leq \langle a \rangle$ s.t. $|H| = m$. Conversely, if $H \leq \langle a \rangle$, then $|H| \mid n$.

Ex 1.2.5. Show Prop 1.2.4.

Ex 1.2.6. TFAE

1. G is the internal direct product of G_1, G_2 .
2. $\forall a \in G, \exists! g_1 \in G_1, g_2 \in G_2$ s.t. $a = g_1 g_2$; $\forall g_1 \in G_1, g_2 \in G_2, g_1 g_2 = g_2 g_1$.
3. $G_1 \cap G_2 = \{1\}$; $G = G_1 G_2$; $\forall g_1 \in G_1, g_2 \in G_2, g_1 g_2 = g_2 g_1$.

1.3 Week 3

1.3.1 Coset and Quotient Group

Let $f : G_1 \rightarrow G_2$ be a group homo. Define $\text{Im } f := f(G_1)$.

Notice that $\text{Im } f \leq G_2$.

pf: Let $z_1 = f(a_1), z_2 = f(a_2)$, then $z_1 z_2^{-1} = f(a_1) f(a_2)^{-1} = f(a_1) f(a_2^{-1}) = f(a_1 a_2^{-1}) \in \text{Im } f$. \square

Def 16. $\text{Ker } f := \{x \in G_1 \mid f(x) = 1\} \leq G_1$.

Fact 1.3.1.

1. $x \in (\text{Ker } f)a \iff f(x) = f(a)$.
2. $\text{Ker } f = \{1\} \iff f$ is 1-1.

Def 17. Let $H \leq G, \forall a \in G, Ha$ is called a **right coset** of H in G .

Fact 1.3.2.

1. For 2 right cosets Ha, Hb , either $Ha = Hb$ or $Ha \cap Hb = \phi$ must hold.
2. $\{Ha : a \in G\}$ forms a partition of G .

Theorem 2 (Lagrange). Let $|G| < \infty$ and $H \leq G, |H| \mid |G|$.

pf:

\square

Remark 5. r is called the **index** of H in G , denoted by $[G : H]$. (The concept of index can be extended to infinite G, H .)

Coro 1.3.1. If $|G| = p$ is a prime in \mathbb{Z} , then G is cyclic.

pf:

\square

Coro 1.3.2. If $|G| < \infty, a \in G$, then $a^{|G|} = 1$.

pf:

\square

Remark 6.

1. Let $H \leq G, a \in G, aH$ is called a **left coset**.
2. $\{\text{right cosets of } H\} \leftrightarrow \{\text{right cosets of } H\}$ by $Ha \mapsto a^{-1}H$.

Ques: How to make $\{aH : a \in G\}$ to be a group? For aH, bH , we must have $(aH)(bH) = abH$. In general, $(aH)(bH) = abH$ is not well-defined.

Ex 1.3.1. Let $H = \langle (1\ 2) \rangle \leq S_3, a_1 = (1\ 3), a_2 = (1\ 2\ 3), b_1 = (1\ 3\ 2), b_2 = (2\ 3)$. 出慘點

If we hope $a_1 b_1 H = a_2 b_2 H$, then we need $(a_1 b_1)^{-1} a_2 b_2 \in H$.

$$b_1^{-1} a_1^{-1} a_2 b_2 = b_1^{-1} b_2 b_2^{-1} a_1^{-1} a_2 b_2$$

Notice that $b_1^{-1} b_2, a_1^{-1} a_2 \in H$, so we need $b_2^{-1} a_1^{-1} a_2 b_2 \in H$.

Def 18. Let $H \leq G$. H is said to be **normal subgroup** of G if $\forall g \in G, h \in H, g^{-1} h g \in H$ (or $g^{-1} H g \subseteq H$), denoted by $H \triangleleft G$.

Def 19. Let $H \triangleleft G$. The set $\{aH \mid a \in G\}$ forms a group under $(aH)(bH) = abH, a, b \in G$. We call it the **quotient group** of G by H , denoted by G/H .
(Note: The identity is $H = eH$ and $(aH)^{-1} = a^{-1}H$.)

Remark 7. Define $q : G \rightarrow G/H, a \mapsto aH$, called the quotient homomorphism.

Ques: How to find a normal subgroup of G ?

Prop 1.3.1.

1. If G is abelian, then $\forall H \leq G \rightsquigarrow H \triangleleft G$. (done by (c))
2. If $H \leq G$ with $[G : H] = 2$, then $H \triangleleft G$.

Eg 1.3.2. $n \leq 3, [S_n : A_n] = 2 \implies A_n \triangleleft S_n$.

pf: We can write $G = H \cup Ha = H \cup aH \implies aH = Ha, \forall a \notin H$. □

Def 20. Define the center of G to be $Z_G = \{a \in G \mid ax = xa, \forall x \in G\} \leq G$.

Prop 1.3.2.

1. $Z_G \triangleleft G$. (by (c) and def.)
2. If G/Z_G is cyclic, then G is abelian.

pf: Let $G/Z_G = \langle aZ_G \rangle$, (let $\bar{a} := aZ_G$) for some $a \in G$. For $x_1, x_2 \in G$, let $x_1 = a^{k_1}z_1, x_2 = a^{k_2}z_2$, then $x_1x_2 = a^{k_1+k_2}z_1z_2 = x_2x_1$. (z_i 可以各種交換) □

Def 21. The commutator of G is define to be $[G, G] = \langle xyx^{-1}y^{-1} \mid x, y \in G \rangle$.

Prop 1.3.3. $[G, G] \triangleleft G ; [G, G] = 1 \iff G$ is abelian.

pf: $\forall x \in G, a \in [G, G], xax^{-1} = xax^{-1}a^{-1}a$ and $xax^{-1}a^{-1}, a \in [G, G]$. □

Ex 1.3.1. no subgroup of A_4 has order 6. (converse of Lagrange thm. is false.)

Ex 1.3.2. Let $H \leq G$. Then TFAE

- (a) $H \triangleleft G$.
- (b) $\forall x \in G, xHx^{-1} = H$.
- (c) $\forall x \in G, xH = Hx$.
- (d) $\forall x, y \in G, (xH)(yH) = (xy)H$.

Ex 1.3.3. If $H \leq S_n$ and $\exists \sigma \in H$ is odd, then $[H : H \cap A_n] = 2$.

Ex 1.3.4. Let $H \leq G$. Then $H \triangleleft G$ and G/H is abelian $\iff [G, G] \leq H$. (hint: $G/[G, G]$ is "max" among all abelian quotient groups)