Chapter 2 Subgroups

Contents

1 Definition and Examples

Definition. ***(Subgroup)***

1. ***(subgroup)*** *Let G be a group. The subset H of G is a subgroup of G, denoted as $H \leq G$ if*

   (a) *H is nonempty*

   (b) *H is closed under products and inverses, i.e. $x, y \in G$ implies $x^{-1}, xy \in H$*

   If $H \leq G$ and $H \neq G$, then $H < G$. $H \leq G$ implies operation on H is the operation on G restricted to H. So any equation in H can also be viewed as equation in G

2. ***(The Subgroup Criterion)*** *$H \subset G$ is a subgroup if and only if*

   (a) *$H \neq \emptyset$*

   (b) *for all $x, y \in H$, $xy^{-1} \in H$*

   Furthermore, if H is finite, then suffice to check H is nonempty and closed under multiplication

- *(examples)*
  - *$G \leq G$ and $\{1\} \leq G$ (latter is called the trivial subgroup)*
  - *$\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$ under operation of addition*
  - *$\left\{1, r, r^2, \cdots, r^{n-1}\right\} \leq D_{2n}$*
  - *$2\mathbb{Z} \leq \mathbb{Z}$*
  - *$(\mathbb{Q}^\times, \times) \not\leq (\mathbb{R}, +)$ (operation are different)*
  - *$\mathbb{Z}^+ \leq \mathbb{Z}$ and $(\mathbb{Z}^+)^\times \not\leq \mathbb{Q}^\times$ (not closed under inverses and does not contain identity)*
  - *$D_6 \not\leq D_8$ ($D_6 \not\subset D_8$)*
- ***(theorem)*** *subgroup is a transitive relation, i.e. $K \leq H, H \leq G$, then $K \leq G$*

2 Centralizers and Normalizers, Stabilizers and Kernels

Definition. ***(Centralizers and Normalizers)*** *Let G be a group and $A \subset G$ be nonempty*

1. ***(centralizer)*** *The centralizer of A in G is a subset of G which commute with every element of A*

$$C_G(A) = \left\{g \in G \mid gag^{-1} = a \text{ for all } a \in A\right\}$$

   - *$ga = ag \iff gag^{-1} = a$*

2. ***(center)*** *The center of G is a subset of G which commutes with all the elements of G*

$$Z(G) = C_G(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$$

3. ***(normalizer)*** *The normalizer of A in G are subsets of G that fixes A by conjugation*

$$N_G(A) = \left\{g \in G \mid gAg^{-1} = A\right\}$$

   where $gAg^{-1} = \left\{gag^{-1} \mid a \in A\right\}$

- *(convention) For $A = \{a\}$, write $C_G(a)$ instead of $C_G(\{a\})$. Note $a^n \in C_G(a)$ for all $n \in \mathbb{Z}^+$*
- ***(theorem)*** *$Z(G) \leq C_G(A) \leq N_G(A) \leq G$*

  Proof. proofs for $C_G(A)$ and $N_G(A)$ are subgroups of G are similar. For now want to show $N_G(A) \leq G$. Note $1 \in N_G(A)$ so $N_G(A) \neq \emptyset$. Let $g_1, g_2 \in N_G(A)$, then $g_1 A g_1^{-1} = A$ and $g_2 A g_2^{-1} = A$. therefore

$$g_1 g_2^{-1} A (g_1 g_2^{-1})^{-1} = g_1 g_2^{-1} (g_2 A g_2^{-1}) g_2 g_1^{-1} = g_1 A g_1^{-1} = A$$

  hence $g_1 g_2^{-1} \in N_G(A)$. So $N_G(A) \leq G$. ■

- *(examples)*
  - *If G is abelian*
    - $Z(G) = G$
    - $C_G(A) = N_G(A) = G$ *for any subset* A $(gag^{-1} = gg^{-1}a = a$ *for all* $a \in A$, $g \in G)$
  - $C_{Q_8}(i) = \{\pm 1, \pm i\}$
  - *Let* $G = D_8$ *and* $A = \{1, r, r^2, r^3\} \le G$ *be subgroup of rorations*
    - $C_{D_8}(A) = A$
    - $N_{D_8}(A) = D_8$
    - $Z(D_8) = \{1, r^2\}$

  Proof. **(1)** Since all powers of r commutes with each other, $A \le C_{D_8}(A)$. since $sr^i = r^{-i}s \neq r^i s$, s does not commute with any rotation, so $s \notin C_{D_8}(A)$. In fact, any $sr^i \notin C_{D_8}(A)$ where $i \in \{0, 1, 2, 3\}$. If assume for contradiction, $s = (sr^i)(r^{-i}) \in C_{D_8}(A)$, a contradiction. Hence $C_{D_8} = A$. **(2)** Note, $A \le N_{D_8}(A)$ by fact that centeralizer is contained in normalizer. Now consider

  $$sAs^{-1} = \{s1s^{-1}, srs^{-1}, sr^2s^{-1}, sr^3s^{-1}\} = \{1, r^3, r^2, r\} = A$$

  so that $s \in N_{D_8}$. Since $r, s \in N_{D_8}(A)$ and N_{D_8} is closed under multiplication (its a subgroup!), $s^i r^j \in N_{D_8}$ for all i, j. $D_8 \le N_{D_8}$, hence $N_{D_8}(A) = D_8$ **(3)** Note, $Z(D_8) \le A$ by fact that center is contained in the centralizer. Note $sr = r^{-1}s = r^3 s \neq rs$ and $sr^3 = r^{-3}s = rs \neq r^3 s$ hence $r, r^3 \notin Z(D_8)$ (but $sr^2 = r^{-2}s = r^2 s$). Therefore $Z(D_8) \le \{1, r^2\}$. The reverse inclusion holds by 1 (and r^2) commutes with r and s. Since r, s generates D_8, every element of D_8 commutes with 1 (and r^2) hence $\{1, r^2\} \le Z(D_8)$ and so equality holds. ∎

  - *Let* $G = S_3$ *and* $A = \{1, (1\ 2)\}$,
    - $C_{S_3}(A) = A$
    - $N_{S_3}(A) = A$
    - $Z(S_3) = \{1\}$

  Proof. **(1)** Both 1 and $(1\ 2)$ commutes with all of A hence $A \le C_{S_3}(A)$ (for $a, g = (1\ 2)$, $gag^{-1} = (1\ 2)(1\ 2)(2\ 1) = (1\ 2)$, commutativity with $a = 1$ or $g = 1$ is trivial). To show $C_{S_3}(A) \le A$, enough to show that both $(2\ 3)$ and $(1\ 3)$ do not commute with all elements of A, specifically $(1\ 2)$ (by fact that transpositions generates S_3). $(2\ 3)(1\ 2) = (1\ 3\ 2) \neq (1\ 2\ 3) = (1\ 2)(2\ 3)$ similarly for $(1\ 3)$. Alternatively, by Lagrange theorem, $|C_{S_3}(A)| \mid |S_3| = 6$ and $2 = |A| \mid |C_{S_3}(A)|$. Possible values for $|C_{S_3}(A)|$ are 2 or 6. If latter is true, then $C_{S_3}(A) = S_3$ but this is a contradiction since $(2\ 3)$ does not commute with $(1\ 2)$. So $|C_{S_3}(A)| = 2$ hence $C_{S_3}(A) = A$. **(2)** Note $N_{S_3}(A) = A$ because $\sigma \in N_{S_3}(A)$ if and only if

  $$\sigma A \sigma^{-1} = \{\sigma 1 \sigma^{-1}, \sigma(1\ 2)\sigma^{-1}\} = \{1, (1\ 2)\} = A$$

  if and only if $\sigma(1\ 2)\sigma^{-1} = (1\ 2)$, i.e. $\sigma \in C_{S_3}(A) = A$. **(3)** $Z(S_3) \le C_{S_3}(A) = A$ and $(1\ 2) \notin Z(S_3)$ ∎

Definition. ***(Stabilizers and Kernels of Group Actions)***

1. ***(stabilizer)*** *If G is a group acting on a set S and $s \in S$ is a fixed element, the stabilizer of s in G is*

   $$G_s = \{g \in G \mid g \cdot s = s\}$$

2. ***(kernel)*** *of action of G on S is defined as*

   $$\ker \varphi = \{g \in G \mid g \cdot s = s \textit{ for all } s \in S\}$$

3. ***(centralizers and normalizers as kernels of some group action)***

(a) *(normalizer) Let $G \curvearrowright \mathcal{P}(G)$ by conjugation, i.e. for any $g \in G$ and $B \subset G$*

$$g : B \to gBg^{-1} \quad \text{where} \quad gBg^{-1} = \left\{gbg^{-1} \mid b \in B\right\}$$

This is a group action.
The normalizer of G on A is the stabilizer of A when G acts on $\mathcal{P}(G)$ by conjugation, i.e. $N_G(A) = G_s$ where $s = A \subset \mathcal{P}(G)$. Therefore $N_G(A) \leq G$

(b) *(centralizer) Let $N_G(A) \curvearrowright A$ by conjugation, i.e. for any $g \in N_G(A)$ and $a \in A$*

$$g : a \to gag^{-1}$$

which maps A to A by definition of $N_G(A)$ fixing A and so gives an action on A.
The centralizer of G on A is simply the kernel of $N_G(A)$ acting on A by conjugation.

$$\ker(G \curvearrowright S) = \{g \in G \mid g \cdot s = s \text{ for all } s \in S\} = \left\{g \in G \mid gsg^{-1} = s \text{ for all } s \in S\right\} = C_G(S)$$

Since $C_G(A) \leq N_G(A)$ and $N_G(A) \leq G$, we have $C_G(A) \leq G$

(c) *(center) The center of G is the kernel of G acting on $S = G$ by conjugation*

- ***(theorem)*** $\ker(G \curvearrowright S) \leq G$
- ***(theorem)*** $G_s \leq G$ *($1 \in G_s$ and $(xy^{-1}) \cdot s = (xy^{-1}) \cdot (y \cdot s) = x \cdot s = s$ for any $x, y \in G_s$)*
- *(examples)*
  - *Let $G = D_8$ and $A = \{1, 2, 3, 4\}$ the vertices of a square. Then the stabilizer of any vertex $a \in A$ is the subgroup $\{1, t\} \leq D_8$, where t is the reflection about line of symmetry passing through a and center of the square. The kernel of the action is just the identity*
  - *Let $G = D_8$ and $A = \{\{1, 3\}, \{2, 4\}\}$ be the two unordered pairs of opposite vertices. The kernel of the action of G on A is the subgroup $\left\{1, s, r^2, sr^2\right\}$ and for any $a \in A$, the stabilizer of a in D_8 is equal to the kernel of the action*

3 Cyclic Groups and Cyclic Subgroups

Definition. ***(cyclic group)*** *A group H is cyclic if H can be generated by a single element, i.e. there is some element $x \in H$ such that $H = \{x^n \mid n \in \mathbb{Z}\}$ in multiplicative notation (or that $H = \{nx \mid n \in \mathbb{Z}\}$ in additive notation). We write $H = \langle x \rangle$ and say H is* ***generated by*** *x and x is a* ***generator****. For any $n \in \mathbb{Z}^+$, let Z_n be the cyclic group of order n (written multiplicatively)*

- *(fact) A cyclic group may have more than one generator ($H = \langle x \rangle$ implies $H = \left\langle x^{-1} \right\rangle$)*
- *(fact) not all powers of the generator are distinct, i.e. possibly $x^n = x^m$ where $n \neq m$*
- *(fact) cyclic group is abelian (law of exponent)*
- *(examples)*
  - *all rotations of a regular n-gon $H = \langle r \rangle = \left\{1, r, r^2, \cdots, r^{n-1}\right\}$ is a cyclic subgroup of D_{2n}*
    - $|H| = |r| = n$
    - *we can reduce arbitrary powers of a generator in a finite cyclic group to the least residual power, i.e. $r^t = r^{nq+k} = (r^n)^q r^k = 1^q r^k = r^k$ for some $0 \leq k < n$*
  - *$H = \mathbb{Z} = \langle 1 \rangle$ is a cyclic group, since any element in H can be written as $n \cdot 1$.*
    - $|H| = |1| = \infty$
- ***(proposition)*** *order of a cyclic group is the order of its generator, i.e. if $H = \langle x \rangle$, then $|H| = |x|$*
  1. *($|H| = n < \infty$): $x^n = 1$ and $1, x, x^2, \cdots, x_{n-1}$ are distinct*
  2. *($|H| = \infty$): $x^n \neq 1$ for all $n \neq 0$ and $x^a \neq x^b$ for all $a \neq b \in \mathbb{Z}$*

- ***(proposition)*** *Let G be a group. Let $m, n \in \mathbb{Z}$, then*

    1. $x^m = 1$, $x^n = 1$ *implies* $x^{(m,n)} = 1$ *(by Euclidean Algo,* $x^{(m,n)} = x^{mr+ns} = (x^m)^r + (x^n)^s = 1^r 1^s = 1$*)*
    2. $x^m = 1$ *implies* $|x| \mid m$ *(let* $n = |x|$*, by previous,* $x^{(n,m)} = 1$*,* $0 < d \leq n$ *implies* $n = d \mid m$ *by gcd)*

    We can say something about the power m when we have we know $x^m = 1$

- ***(theorem)*** *two cyclic group of same order are isomorphic (both finite and infinite case)*

    - *(examples)*
        * $(Z_n, \times) \cong (\mathbb{Z}/n\mathbb{Z}, +)$
        * $(\langle x \rangle, \times) \cong (\mathbb{Z}, +)$

    Proof.
    (finite case) if $\langle x \rangle, \langle y \rangle$ are cyclic group of order $n \in \mathbb{Z}^+$, show φ is an isomorphism

    $$\begin{aligned} \varphi : \langle x \rangle &\to \langle y \rangle \\ x^k &\mapsto y^k \end{aligned}$$

    - (well defined) let $x^r = x^s$ for some $r, s \in \mathbb{Z}$ and show $\varphi(x^r) = \varphi(x^s)$.
      $x^{r-s} = 1$, hence $n \mid r-s$ and write $r-s = tn$, then $\varphi(x^r) = \varphi(x^{tn+s}) = y^{tn+s} = (y^n)^t y^s = y^s = \varphi(x^s)$
    - (homomorphism) $\varphi(x^a x^b) = \varphi(x^{a+b}) = y^{a+b} = y^a y^b = \varphi(x^a)\varphi(x^b)$
    - (bijection) φ surjective since any y^k is image of x^k under φ. As $|\langle x \rangle| = |\langle y \rangle| = n$, φ is bijective

    (infinite case) If $\langle x \rangle$ is an infinite cyclic group, show φ is an isomorphism

    $$\begin{aligned} \varphi : \mathbb{Z} &\to \langle x \rangle \\ k &\mapsto x^k \end{aligned}$$

    - (well-defined) no ambiguity on $\mathbb{Z}$
    - (homomorphism) by law of exponent
    - (bijection) φ surjective by definition of cyclic group. φ injective by previous proposition, i.e. $x^a \neq x^b$ for all distinct $a, b \in \mathbb{Z}$.

    ∎

- ***(proposition)*** *Let G be a group, $x \in G$, and $a \in \mathbb{Z} - \{0\}$*

    1. *If* $|x| = \infty$*, then* $|x^a| = \infty$
    2. *If* $|x| = n < \infty$*, then* $|x^a| = \frac{n}{(n,a)}$
    3. *(special case to 2) if* $|x| = n < \infty$ *and* $a \mid n$ *where* $a \in \mathbb{Z}^+$*, then* $|x^a| = \frac{n}{a}$ *(*$(n,a) = a$*)*

    Intuitively, we can say something about the order of x^a when we know the order of x

    Proof. **(1)** by contradiction, assume $|x^a| = 1$, then $1 = (x^a)^m = x^{am}$, similarly, $x^{-am} = (x^{am})^{-1} = 1^{-1} = 1$. Either am or $-am$ is positive, so some positive power of x is the identity, contradicting $|x| = \infty$. **(2)** Let $y = x^a$ and $(n, a) = d$ and $n = db$ and $a = dc$. Note $(b, c) = 1$. Let $|y| = k$ we show b and k divides each other hence proving equality

    - $(k \mid b)$ $y^b = x^{ab} = x^{dcb} = x^{nc} = 1^c = 1$. by previous proposition on $\langle y \rangle$, $k \mid b$
    - $(b \mid k)$ $x^{ak} = y^k = 1$. by previous proposition on $\langle x \rangle$, $n \mid ak \Rightarrow db \mid dck \Rightarrow b \mid ck$, so $(b, c) = 1 \Rightarrow b \mid k$.

    ∎

- ***(proposition)***