Theory of Numbers

Eric Liu

Contents

Chapter 1 **Groups** ____ Page 2
1.1 Subgroups 2
1.2 Group homomorphisms 4
1.3 Normal subgroups 5

Chapter 1

Groups

1.1 Subgroups

Let G be a group, a **subgroup** of G is a group H together with an injective group homomorphism $H \hookrightarrow G$. Clearly, if $H \subseteq G$ satisfies:

(i) $e \in H$

(ii) $xy \in H$ for all $x, y \in H$

(iii) $x^{-1} \in H$ for all $x \in H$

then the set inclusion makes H a subgroup of G. The easiest spotted subgroups of a group G are perhaps the **cyclic subgroups**:

$$\langle x \rangle \triangleq \{x^n \in G : n \in \mathbb{Z}\}$$

namely, the smallest subgroup of G containing x. Note that G is said to be **cyclic** if $G = \langle x \rangle$ for some $x \in G$. 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 1.1.1. 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

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

$\blacksquare$

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**:

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

Theorem 1.1.2. (Structure theorems of finite groups) Let G be a group and $x \in G$. The **order** of G and x are respectively the cardinality G and $\langle x \rangle$. We denote them by $|G|, \text{ord}(G)$, and $\text{ord}(x)$. We have the followings:

(i) If the order of x is finite, then it is the smallest natural number n that makes $x^n = e$.

(ii) If G is finite, then $\text{ord}(x)$ divides $|G|$.

(iii) If G is finite cyclic $\langle x \rangle$, then for all

(iv) If $|G| = p$, then it is cyclic.

Proof. $\blacksquare$

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.

Equivalent Definition 1.1.3. (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) $xNx^{-1} \subseteq N$ for all $x \in G$.

(ii) $xNx^{-1} = N$ for all $x \in G$

Proof. $\blacksquare$

1.2 Group homomorphisms

Let G be a group. There are essentially two ways to embed G into $\mathrm{Aut}(G)$:

$$x \mapsto \left(y \mapsto xyx^{-1}\right) \quad \text{and} \quad x \mapsto \left(y \mapsto x^{-1}yx\right)$$

For all $x \in G$, we say the image of x under the homomorphism

$$z \mapsto y^{-1}zy$$

is the **conjugate** of x by y.

1.3 Normal subgroups