

MATH 403 LECTURE NOTE

WEEK 7

DAESUNG KIM

1. GROUPS (SEC 2.6)

Definition 1.1. Let G be a set equipped with an operation $(x, y) \mapsto xy \in G$ for all $x, y \in G$. We say G is a group with the operation if

- (1) There exists an element e in G such that $ex = xe = x$ for all $x \in G$. We call e the identity.
- (2) For every $x \in G$, there is an element $x^{-1} \in G$ such that $xx^{-1} = x^{-1}x = e$.
- (3) For all $x, y, z \in G$, we have $x(yz) = (xy)z$.

Example 1.2. (1) The real numbers \mathbb{R} with addition is a group.
(2) The positive real numbers \mathbb{R}_+ with multiplication is a group.
(3) The integers \mathbb{Z} with addition is a group.
(4) The even integers $2\mathbb{Z}$ with addition is a group.

Example 1.3. (1) The natural numbers \mathbb{N} with addition is NOT a group.
(2) The real numbers \mathbb{R} with multiplication is NOT a group.
(3) The odd integers with addition is NOT a group.

Definition 1.4. A group G is called commutative or abelian if $xy = yx$ for all $x, y \in G$.

Example 1.5. Let A be a set and G be the collection of all bijections $f : A \rightarrow A$. Then, G with composition is a non-abelian group. (Exercise)

Definition 1.6. Let $n \in \mathbb{N}$ and $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$. Define the addition and the multiplication on \mathbb{Z}_n by the residues left after division by n .

Example 1.7. One can see that \mathbb{Z}_n with addition is a group.

Proposition 1.8. Let G be a group and $x \in G$. Then, the identity and the inverse of x are unique.

Proposition 1.9. Let G be a group and $a, b \in G$.

- (1) The equation $ax = b$ has a unique solution x .
- (2) The equation $ya = b$ has a unique solution y .

Proposition 1.10 (Cancellation rules). Let G be a group.

- (1) $ax = ax'$ implies $x = x'$.
- (2) $ya = y'a$ implies $y = y'$.

Example 1.11. In \mathbb{Z}_{12} , $3x = 5$ has no solution.

2. SUBGROUPS, CYCLIC GROUPS, AND ISOMORPHISM

Definition 2.1. Let G be a group and H a subset of G . If H is also a group itself, we call H a subgroup of G .

Example 2.2. (1) If G is a group and $e \in G$ is the identity, then $\{e\}$ is a subgroup. This is called the trivial subgroup.
(2) The even integers $2\mathbb{Z}$ is a subgroup of \mathbb{Z} .

Lemma 2.3. Let G be a group and H a subset of G . Then H is a subgroup if and only if $ab^{-1} \in H$ for all $a, b \in H$.

Proof. Suppose H is a subgroup, then $ab^{-1} \in H$ for all $a, b \in H$ by definition. Suppose we know that $ab^{-1} \in H$ for all $a, b \in H$. If $a = b$, then $e \in H$. If $a = e$, then every element in H has the inverse in H . The associativity works in H . For any $a, b \in H$, $ab = a(b^{-1})^{-1} \in H$. Thus H is a group. ■

For an element x in a group G , we use the notation

$$x^m := x \cdot x \cdots x \quad (m \text{ times})$$

for $m \in \mathbb{N}$. If $m = 0$, $x^m := E$. If $m < 0$, then $x^m = (x^{-1})^m$.

Definition 2.4. Let G a group and $x \in G$. The cyclic group $\langle x \rangle$ generated by x is a subgroup of G consists of x^m , $m \in \mathbb{Z}$.

Example 2.5. Let $G = \mathbb{Z}$ be a group with addition. What is $\langle 2 \rangle$?

Proposition 2.6. Let G a group and $x \in G$. The cyclic group $\langle x \rangle$ is the smallest subgroup containing x .

Definition 2.7. Let G, H be groups and $\varphi : G \rightarrow H$ a map. The map φ is called a homomorphism if it preserves the group structure, in a sense that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in G$.

Proposition 2.8. If φ is a homomorphism from G to H , then it maps the identity and inverses in G to the inverse and inverses in H .

Example 2.9. Consider a map $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}$ defined by $x \mapsto 2x$. One can see that φ is a homomorphism.

Definition 2.10. An isomorphism is a bijective homomorphism. We say two groups are isomorphic if there is an isomorphism between the groups.

3. GROUPS OF TRANSFORMATIONS

Let \mathcal{V} a set. We have seen that the set of all bijections $\alpha : \mathcal{V} \rightarrow \mathcal{V}$ with compositions is a group, say G . In this section, we will see several subgroups of G . In particular, we are interested in the case $\mathcal{V} = \mathbb{R}^2$.

Theorem 3.1. Let \mathcal{T} be the set of all translations $\tau_A : \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $A \in \mathbb{R}^2$. Then, \mathcal{T} with compositions is a group.

Proof. By the lemma, it suffices to show that for any $A, B \in \mathbb{R}^2$, $\tau_A \tau_B^{-1} \in \mathcal{T}$. ■

Definition 3.2. We call a bijection map $\alpha : \mathbb{R}^2 \rightarrow \mathbb{R}^2$ a dilatation if α is either a translation or a central dilatation.

Definition 3.3. We call a bijection map collineation if it maps a line to a parallel line.

As we have seen before, dilatations are collineation.

Theorem 3.4. The set of all dilatations \mathcal{D} with compositions forms a group.

Proof. Since $(\tau_A)^{-1} = \tau_{-A}$ and $(\delta_{C,r})^{-1} = \delta_{C,1/r}$, it suffices to show that

- (1) $\tau_A \tau_B \in \mathcal{D}$,
- (2) $\tau_A \delta_{C,r} \in \mathcal{D}$,
- (3) $\delta_{C,r} \tau_A \in \mathcal{D}$,
- (4) $\delta_{C,r} \delta_{D,s} \in \mathcal{D}$.

We know that (1) is trivial and (3) follows from (2). Thus, it is enough to show (2) and (4). We first have

$$\begin{aligned} \tau_A \delta_{C,r}(X) &= \tau_A((1-r)C + rX) \\ &= (1-r)\left(\frac{1}{1-r}A + C\right) + rX \\ &= \delta_{P,r}(X) \end{aligned}$$

where $P = \frac{1}{1-r}A + C$. Also,

$$\delta_{C,r} \delta_{D,s}(X) = (1-r)C + r(1-s)D + rsX = \begin{cases} \tau_{(1-r)(C-D)}(X), & rs = 1, \\ \delta_{Q,rs}(X), & rs \neq 1, \end{cases}$$

where $Q = (1-rs)^{-1}((1-r)C + r(1-s)D)$. ■

REFERENCES

[T] Philippe Tondeur, *Vectors and Transformations in Plane Geometry*, Publish Or Perish, Inc. 1993

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN
E-mail address: daesungk@illinois.edu