PMATH 336: INTRODUCTION TO GROUP THEORY WITH APPLICATIONS
NOTES FOR WEEK 1

INSTRUCTOR: ARUNDHATHI KRISHNAN

1. Preliminaries

We recap some preliminaries that will be used widely in this course.

1.1. Well-Ordering Principle and Mathematical Induction.

Axiom 1.1.1 (Well-Ordering Principle)**.** *Every non-empty set of positive integers has a least element.*

The principle of induction will commonly be used to prove results in this course. Let's look at two forms of mathematical induction.

Theorem 1.1.2 (First Principle of Induction)**.** *Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then $n+1 \in S$ also holds. Then S contains every integer greater than or equal to a.*

In some cases, the following equivalent form of the principle of induction may be more useful.

Theorem 1.1.3 (Second/ Strong Principle of Induction)**.** *Let S be a set of integers containing a. Suppose S has the property that whenever each integer m with $a \leq m \leq n$ belongs to S, then $n+1 \in S$ also holds. Then S contains every integer greater than or equal to a.*

1.2. Equivalence Relations.

Definition 1.2.1. An equivalence relation on a set S is a subset $R \subset S \times S$ satisfying the following properties:

(i) $(a,a) \in R$ for all $a \in S$ (reflexive);

(ii) $(a,b) \in R \implies (b,a) \in R$ (symmetric);

(iii) $(a,b) \in R, (b,c) \in R \implies (a,c) \in R$ (transitive).

For each $a \in S$, the set

$$[a] = \{x \in S \mid (a,x) \in R\}$$

is called the equivalence class of a.

Definition 1.2.2. A partition of a set S is a collection of non-empty disjoint subsets of S whose union is S.

Theorem 1.2.3. *The equivalence classes of an equivalence relation on a set S constitute a partition of S. Conversely, for any partition P of S, there is an equivalence relation whose equivalence classes are the elements of P.*

1.3. **Functions.**

Definition 1.3.1. A function φ from a set A to a set B is a rule that assigns to each element a of A exactly one element of B.

A function $\varphi : A \to B$ is called

(i) *injective* or one-to-one or $1-1$ if $\varphi(a_1) = \varphi(a_2) \implies a_1 = a_2$.
(ii) *surjective* or onto if for every $b \in B$, there exists $a \in A$ with $\varphi(a) = b$.

Suppose A, B and C are sets and $\varphi : A \to B$ and $\psi : B \to C$ are functions. Then we can define the composition of φ and ψ as

$$\psi\varphi(a) = \psi(\varphi(a)) \quad (a \in A).$$

Proposition 1.3.2. *Suppose A, B, C, D are sets and $\alpha : A \to B, \beta : B \to C, \gamma : C \to D$ are functions. Then the following hold:*

(i) $\gamma(\beta\alpha) = (\gamma\beta)\alpha$;

(ii) If α and β are $1-1$, then so is $\beta\alpha$;

(iii) If α and β are onto, then so is $\beta\alpha$;

(iv) If α is $1-1$ and onto, then there exists a function $\alpha^{-1} : B \to A$ such that $\alpha^{-1}\alpha(a) = a \ \forall a \in A$ and $\alpha\alpha^{-1}(b) = b \ \forall b \in B$.

Hence, given a set A, we can consider the set $\{\alpha : A \to A \mid \alpha \text{ is one-to-one and onto}\}$ which has a product on it given by composition of functions. This is an important example that we will return to when we consider permutation groups.

1.4. **Basic Number Theory.**

Definition 1.4.1. Let $m, n \in \mathbb{Z}$. Then we say that m divides n, and write $m|n$ if there exists $k \in \mathbb{Z}$ such that $n = km$. The integer m is called a divisor of n.

Theorem 1.4.2. *Let $a, b, c \in \mathbb{Z}$.*

(i) If $a|b$ and $b|c$, then $a|c$,

(ii) If $a|b$ and $a|c$, then $a|(bx + cy)$ for all $x, y \in \mathbb{Z}$.

(iii) If $a|b$ and $b \neq 0$, then $|\,a\,| \leq |\,b\,|$.

Theorem 1.4.3 (Division Algorithm)**.** *If a, b are integers and $b > 0$, then there exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$. The integers q and r are called the quotient and remainder respectively.*

Definition 1.4.4. The greatest common divisor of two non-zero integers a and b is the largest of all common divisors of a and b, and is denoted by $\gcd(a, b)$. If $\gcd(a, b) = 1$, then a and b are called *relatively prime*.

Theorem 1.4.5. *For any non-zero integers a and b, there exist integers s and t such that $\gcd(a, b) = as + bt$. Moreover, $\gcd(a, b)$ is the smallest positive integer of the form $as + bt$.*

Corollary 1.4.6. *If a and b are relatively prime, there exist integers s and t such that $as + bt = 1$.*

Corollary 1.4.7 (Euclid's Lemma)**.** *If p is a prime that divides ab, then p divides a or p divides b.*

Proof. If $p \not| a$, then $\gcd(a,p) = 1$. Hence by Corollary 1.4.6 there exist $s,t \in \mathbb{Z}$ such that $at + ps = 1$. Multiplying both sides by b, we get $bat + bps = b$. As p divides both terms on the left hand side, it divides the sum, and thus $p|b$. □

Theorem 1.4.8 (Fundamental Theorem of Arithmetic)**.** *Every integer greater than* 1 *is a prime or a product of primes. This product is unique, except for the order in which factors appear.*

1.5. **Modular Arithmetic.** Let n be a fixed positive integer. If $a, b \in \mathbb{Z}$, we say that a is congruent to b modulo n and write

$$a \equiv b \mod n,$$

if n divides $(a - b)$.

Theorem 1.5.1. *Let $n \in \mathbb{N}$ and $R = \{(a,b) \mid a \equiv b \mod n\}$. Then R is an equivalence relation.*

Proof. Let $a, b, c \in \mathbb{Z}$.

(i) $a \equiv a \mod n$ as $n|0$.

(ii) $a \equiv b \mod n \implies n|(a-b) \implies n|(b-a) \implies b \equiv a \mod n$.

(iii) $a \equiv b \mod n, b \equiv c \mod n \implies n|(a-b)$ and $n|(b-c)$, hence $n|(a-b)+(b-c)$, that is, $n|(a-c)$ so that $a \equiv c \mod n$.

□

Definition 1.5.2. Let $n \in \mathbb{N}$. The congruence class modulo n of the integer a is the set $[a] := \{x \in \mathbb{Z} \mid x \equiv a \mod n\}$.

Definition 1.5.3. Let $n \in \mathbb{N}$. The integers modulo n, denoted by $\mathbb{Z}_n$ is the set of n congruence classes

$$\mathbb{Z}_n := \{[0], [1], \ldots, [n-1]\}.$$

We can define two operations on $\mathbb{Z}_n$, addition and multiplication as follows:

$$[a] + [b] = [a+b], [a][b] = [ab].$$

Theorem 1.5.4. *For $[a], [b], [c] \in \mathbb{Z}_n$ we have*

(i) $[a] + [b] = [b] + [a], [a][b] = [b][a]$ *(commutativity);*

(ii) $([a] + [b]) + [c] = [a] + ([b] + [c]), ([a][b])[c] = [a]([b][c])$ *(associativity);*

(iii) $[a]([b] + [c]) = [a][b] + [a][c]$ *(distributivity);*

(iv) $[a] + [0] = [a] = [0] + [a]$ *(additive identity);*

(v) $[a][1] = [1][a] = [a]$ *(multiplicative identity);*

(vi) $[a] + [-a] = [-a] + [a] = 0$ *(additive inverse).*

Theorem 1.5.5. *Let $n \in \mathbb{N}$ and $[a] \in \mathbb{Z}_n$. Then $[a]$ has a multiplicative inverse if and only if* $\gcd(a,n) = 1$.

Proof. Suppose there exists $[s] \in \mathbb{Z}_n$ such that $[a][s] = [1]$. This means that $as \equiv 1 \mod n \implies 1 = as + nt$ for some $t \in \mathbb{Z}$. By Theorem 1.4.5, this means that $\gcd(a,n) = 1$.

Conversely, suppose $\gcd(a, n) = 1$. By Theorem 1.4.5, there exist $s, t \in \mathbb{Z}$ such that $1 = as + nt$. Hence $as \equiv 1 \mod n$, so that $[s]$ is a multiplicative inverse of $[a]$.

□

Henceforth we will write $\mathbb{Z}_n$ as $\{0, 1, \ldots, n-1\}$ and drop the square brackets when it is clear that we consider $1, \ldots, n$ as elements of $\mathbb{Z}_n$ rather than of $\mathbb{Z}$.

2. Groups

In this section, we give the definition of a group, some examples of groups, and finally consider some basic properties of groups.

2.1. **Basic Definitions.**

Definition 2.1.1. Let G be a set. A binary operation on G is a function that assigns to each ordered pair of elements of G a unique element of G.

The convention used is to denote the unique element resulting from an ordered pair (a, b) as ab. In some cases, we write $a + b$ if the binary operation is an addition.

Example 2.1.2.

(i) Addition, multiplication and subtraction on $\mathbb{Z}$ are all binary operations. What about division?
(ii) Addition and multiplication on $\mathbb{Z}_n$.

Definition 2.1.3. A set G together with a binary operation on G is called a group if the following hold:

(i) Associativity: $(ab)c = a(bc)$ for all $a, b, c \in G$.
(ii) Existence of identity: There is an element $e \in G$ such that $ae = ea = a$ for all $a \in G$.
(iii) Existence of inverse: For each $a \in G$, there is an element $b \in G$ such that $ab = ba = e$.

Note that the existence of an identity element implies that a group must be non-empty; further, the existence of a binary operation implies that that a group G must be closed under the operation. In addition, if $ab = ba$ for all $a, b \in G$, then G is called *abelian* or *commutative*.

Example 2.1.4.

(i) $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +)$ are all abelian groups under usual addition.
(ii) $(\mathbb{Q}^+, \cdot)$ and $(\{1, -1, i, -i\}, \cdot) \subset \mathbb{C}$ are abelian groups under usual multiplication.
(iii) $M_n(\mathbb{C})$, the set of $n \times n$ matrices with complex entries, equipped with the operation of matrix addition is an abelian group.
(iv) $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ under addition mod n is an abelian group.
(v) $GL(n, \mathbb{R})$, the set of $n \times n$ matrices with non-zero determinant, is a non-abelian (for $n > 1$) group under matrix multiplication. It is called the general linear group of degree n.
(vi) $SL(n, \mathbb{R})$, the set of $n \times n$ matrices with determinant 1, is a non-abelian (for $n > 1$) group under matrix multiplication. It is called the special linear group of degree n. Note that $SL(n, \mathbb{R}) \subset GL(n, \mathbb{R})$.

For $n > 1$, define the set $U(n) := \{m \in \mathbb{N} \mid m < n \text{ and } \gcd(m, n) = 1\}$.

Proposition 2.1.5. *For $n > 1$, $U(n)$ is a group under multiplication modulo n.*

Proof. First, we show that $U(n)$ is closed under multiplication modulo n, that is, if $m_1, m_2 \in U(n)$, then $(m_1 m_2) \mod n \in U(n)$. Indeed, we have that $\gcd(m_i, n) = 1$ for $i = 1, 2$. Hence, by Theorem 1.4.5, there exist x_i, y_i such that $m_i x_i + n y_i = 1$ for $i = 1, 2$. This gives that $m_i x_i \equiv 1 \mod n$ for $i = 1, 2$, and hence $m_1 m_2 (x_1 x_2) \equiv 1 \mod n$. This gives finally that $\gcd(m_1 m_2, n) = 1$, so that $m_1 m_2 \mod n \in U(n)$.

The associativity of multiplication mod n was mentioned in part (ii) of Theorem 1.5.4 (prove it!). Clearly, $1 \in U(n)$ plays the part of the identity element. Finally, the existence of an inverse for each $a \in U(n)$ follows from Theorem 1.5.5.

□

Hence $\{1, 3\} = U(4)$ is a group under multiplication modulo 4.

Exercise 2.1.6. Prove that $\{0, 1, 2, 3\}$ is not a group under multiplication modulo 4.

Exercise 2.1.7. Prove that the set $\{1, 2, \ldots, n-1\}$ is a group under multiplication mod n if and only if n is a prime.

2.2. **Elementary Properties of Groups.**

Theorem 2.2.1 (Uniqueness of identity)**.** *There exists a unique element $e \in G$ such that $ae = ea = a$ for every $a \in G$.*

Proof. The existence of an element e is guaranteed by the definition of a group. Suppose e and f are both identity elements. Then $e = ef = f$. □

Theorem 2.2.2 (Uniqueness of inverse element)**.** *For each $a \in G$, there exists a unique element $b \in G$ such that $ab = ba = e$.*

Proof. Suppose there exist $b, c \in G$ such that $ab = ba = e$ and $ac = ca = e$. Then $c = ce = c(ab) = (ca)b = eb = b$.

□

We thus write the unique inverse of an element $a \in G$ as a^{-1}.

Theorem 2.2.3 (Cancellative property)**.** *Let $a, b, c \in G$. Then $ba = ca \implies b = c$ and $ab = ac \implies b = c$.*

Proof. Suppose $ba = ca$. Then multiplying both sides on the right by the inverse of a gives $b = c$, so we have right cancellativity. Left cancellativity follows similarly. □

The associative property means that we can unambiguously write the product

$$\underbrace{a \cdot \cdots \cdot a}_{n \text{ times}}$$

as a^n for $n \in \mathbb{N}$. For $n < 0$, we take a^n to be the $(-n)$-fold product of a^{-1} and $a^0 := e$.

In general, it is not true in a non-abelian group G that $(ab)^n = a^n b^n$ for $a, b \in G$ and $n \in \mathbb{Z}$. However, we have the following result that expresses the inverse of a product as a reversed product of inverses.

Theorem 2.2.4. *Let G be a group and $a, b \in G$. Then $(ab)^{-1} = b^{-1} a^{-1}$.*

Proof. The proof follows in a straightforward way by verifying that $(ab) b^{-1} a^{-1} = e = b^{-1} a^{-1} ab$. □

References

[1] Gallian, Joseph. Contemporary abstract algebra. Nelson Education, 2012.