‘

Math 311, A Summary of Sections 10,11,13,14,16,18,19,20,21,22,26

Section 10. Cosets and the Theorem of Lagrange

Basic concepts

Left coset of a subgroup, right coset of a subgroup (**Definition 10.2**). Index $(G : H)$ (**Definition 10.13**).
For example, $U_4 = \{1, i, -1, -i\}$ is a subgroup of $\mathbb{C}^*$. The left coset $2U_4$, $10U_4$ are

$$2U_4 = \{2h \,|\, h \in U_4\} = \{2, 2i, -2, -2i\}, \;\; 10U_4 = \{10, 10i, -10, -10i\}.$$

And since $\mathbb{C}^*$ is abelian, each left coset is also a right coset: $aU_4 = U_4 a$.
Another example: $H = 3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, H has three left cosets (they are also right cosets as $\mathbb{Z}$ is abelian):

$$3\mathbb{Z}, \;\; 1 + 3\mathbb{Z}, \;\; 2 + 3\mathbb{Z}.$$

A very important of property of left cosets: for two left cosets aH and bH, then either $aH = bH$ or $aH \cap bH$ is empty.

Theorems

Theorem 10.10 (Lagrange Theorem). If G is a finite group and $H \subseteq G$ is a subgroup. Then $|H|$ is a divisor of $|G|$.
Sketch of Proof. Let $a_1H, a_2H, \ldots, a_rH$ be the complete list of all left cosets of H. Step 1. Prove each left coset a_iH has exactly $|H|$ elements. Step 2. $a_1H, a_2H, \ldots, a_rH$ forms a patition of G. Step 3. By steps 1 and 2, we have $|G| = |a_1H| + \cdots + |a_rH| = r|H|$, so $|H|$ is a divisor of $G|$.

Corollary 10.11. Let G be a group, if $|G|$ is a prime, then G is cyclic.

Theorem 10.12 The order of an element of a finite group G is a divisor of $|G|$.

Theorem 10.14. If H and K are subgroups of a finite group G, and $K \subseteq H$, then $(G : K) = (G : H)(H : K)$.

Problems

Suppose $n \geq 2$. Prove that the set of all odd permutations in S_n is a left coset and also a right coset of A_n. Find $(S_n : A_n)$.

Section 11. Direct Products of Finitely Generated Abelian Groups

Basic concepts

Cartesian product of sets $S_1, S_2, \dots, S_n$ (**Definition 11.1**). Direct product of groups $G_1, G_2, \dots, G_n$ (**Theorem 11.2**).
For example, the direct product of two groups G_1 and G_2 is

$$G_1 \times G_2 = \{(a_1, a_2) \mid a_1 \in G_1, a_2 \in G_2.\}$$

with the binary operation given by $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$.

Theorems

Theorem 11.5. The group $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if m and n are relatively prime.

Theorem 11.12. Every finitely generated abelian group is isomorphic to a direct product of cyclic groups in the form

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where the p_i are primes, not necessarily distinct, and r_i are positive integers. The direct product is unique except for possible rearrangement of the factors.

Section 13. Homomorphisms

Basic concepts

Homomorphism (Definition 13.1). Let $(G, *)$ and $(G', \star)$ be groups, a map $\phi : G \to G'$ is a homomorphism if for all $a, b \in G$,

$$\phi(a * b) = \phi(a) \star \phi(b).$$

The map $\phi : G \to G'$ given by $\phi(x) = e'$ for all $x \in G$ is a homomorphism, We call it the trivial homomorphism (page 126). Image $\phi[A]$, inverse image $\phi^{-1}[B]$ (Definition 13.11). Kernel of a homomorphism $\phi : G \to G'$ (Definition 13.13), denoted by $Ker(\phi)$, is

$$Ker(\phi) = \{x \in G \mid \phi(x) = e'\}.$$

Normal subgroup (Definition 13.19). Isomorphism (page 132): $\phi : G \to G'$ is called an isomorphism if (1). ϕ is a homomorphism. (2). ϕ is one-to-one. (3). ϕ is onto.

Examples

(1). $\phi : \mathbb{R} \to \mathbb{R}$ given by $\phi(x) = 100x$ is a homomorphism from the group $\mathbb{R}$ to itself, because

$$\phi(a + b) = \phi(a) + \phi(b), \quad \longleftrightarrow 100(a + b) = 100a + 100b.$$

(2). $\phi : \mathbb{R} \to \mathbb{R}^*$ given by $\phi(x) = e^x$ is homomorphism from $\mathbb{R} \to \mathbb{R}^*$, because

$$\phi(a + b) = \phi(a)\phi(b), \quad \longleftrightarrow e^{a+b} = e^a e^b.$$

(3). $\phi : \mathbb{R}^* \to \mathbb{R}$ given by $\phi(a) = \ln(|a|)$ is a homomorphism from $\mathbb{R}^*$ to $\mathbb{R}$, bacause

$$\phi(ab) = \phi(a) + \phi(b), \quad \longleftrightarrow \ln(|ab|) = \ln(|a|) + \ln(|b|).$$

(4). **Example 13.10**. $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ given by $\gamma(m) = r$, where r is the remainder of m divided by n.

Theorems

Theorem 13.12. **Theorem 13.15. Corollary 13.18. Corollary 13.20.**

Problems

1. Find a homomorphism from $\mathbb{C}^*$ to U that is onto.
2. Find a homomorphsim from $\mathbb{C}^*$ to $GL(2, \mathbb{R})$ that is one-to-one (hint: it is related to Exercise 23 page 27).
2. Find an isomorphism $\phi : \mathbb{Z}_n \to U_n$.

Section 14. Factor Groups

Basic concepts

Factor group (or quotient group) (Definition 14.6). Automorphism, inner automorphism.

Theorems

Theorem 14.4, Corollary 14.5. Let H be a normal subgroup of G. Let G/H denote the set of all left cosets of H. Then the left coset multiplication

$$(aH)(bH) = (ab)H$$

is well-defined and G/H is a group under this binary operation.

Theorem 14.9. Theorem 14.11. Theorem 14.13.

Example . For each positive integer n, $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$ consists of n-elements:

$$n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \dots, n - 1 + n\mathbb{Z}.$$

The quotient group $\mathbb{Z}/n\mathbb{Z}$ is the same as $\mathbb{Z}_n$.

Section 16. Group Action on a Set

Basic concepts

The concept of "group action" is very important, which provides an abstract model to study symmetries.

Definition 16.1 Let X be a set and G a grouop. An **action of** G **on** X is a map $*: G \times X$ (we write the image of (g, x) as $g * x$ or often as gx) such that
(1). $e * x = x$ for all $x \in X$. (2). $(g_1 g_2) * x = g_1 * (g_2 * x)$ for all $g_1, g_2 \in G$ and all $x \in X$.

Faithful action, transitive action (page 155). Isotropy subgroup (Definition 16.13). Orbit (Definition 16.14), if G acts on X, $x \in X$, the orbit of a, denoted by Gx, is the set

$$Gx = \{gx \mid g \in G\}.$$

Examples
(1). S_n acts on $X = \{1, 2, \ldots, n\}$ by $\sigma * k = \sigma(k)$. This action is faithful and transitive.
(2). $GL(n, \mathbb{R})$ acts on $\mathbb{R}^n$ by matrix multiplication. This action is faithful but not transitive.

Theorems

Theorem 16.3. Let G be a group and X a set. An action of G on X is equivalent to a homomorphism from G to S_X.

Theorem 16.12. Let G act on X, for $x \in X$, put

$$G_x = \{g \in G \,|\, gx = x\}.$$

Then G_x is a subgroup of G (G_x is called the isotropy subgroup of x).

Theorem 16.14. Let X be a G-set. For $x_1, x_2 \in X$, let $x_1 \sim x_2$ if and only if there exists $g \in G$ such that $bx_1 = x_2$. Then $\sim$ is an equivalence relation on X.

Theorem 16.16. Let G act on X, suppose G is finite, then $|Gx| = (G : G_x) = \frac{|G|}{|G_x|}$. In particular $|Gx|$ is a divisor of $|G|$.

Section 18. Rings and Fields

Basic concepts

Ring (Definition 18.1). A ring $(R, +, \cdot)$ is a set together with two binary operations $+$ and $\cdot$, such that the following axioms are satisfied:
(1). $(R, +)$ is an abelian group.
(2). Multiplication $\cdot$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
(3). Distributive laws: for all $a, b, c \in R$,

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$$

Direct product of rings $R_1 \times R_2 \times \cdots \times R_n$ (page 169).
Ring homomorphism (Definition 18.9). For rings R and R', a map $\phi : R \to R'$ is called a ring homomorphism if

$$\phi(a + b) = \phi(a) + \phi(b), \quad \phi(ab) = \phi(a)\phi(b)$$

for all $a, b \in R$.
Kernel of a ring homomorphism (page 171). Isomorphism of rings (Definition 18.12).
Commutative ring. A ring R is called commutative ring if $ab = ba$ for all $a, b \in R$.
Unity. Ring with unity (Definition 18.14). Unit, division ring, field (Definition 18.16). Subring (page 173). Subfield (page 173).

Examples

(1). $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are commutative rings. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, but $\mathbb{Z}$ is not a field.
(2). Let R be any ring, $M_n(R)$ be the set of all $n \times n$ matrices with all entries in R. Then $M_n(R)$ is a ring. In particular, $M_n(\mathbb{Z}), M_n(\mathbb{Q}), M_n(\mathbb{R}), M_n(\mathbb{C})$ are rings. They are not commutative if $n \geq 2$.
(3). For a given positive integer, $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$ is a commutative ring. For example $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, the multiplication is

$$0 \cdot 0 = 0, \ 0 \cdot 1 = 0, \ 0 \cdot 2 = 0, \ 0 \cdot 3 = 0, \ 1 \cdot 1 = 1, \ 1 \cdot 2 = 2, \ 1 \cdot 3 = 3,$$

$$2 \cdot 2 = 4 = 0, \ 2 \cdot 3 = 6 = 2, \ 3 \cdot 3 = 9 = 1.$$

Theorems

Theorem 18.8.

Problem

If p is a prime, prove that $\mathbb{Z}_p$ is a field.

Section 19. Integral Domains

Basic concepts

Zero divisor (Definition 19.2): let R be a ring, if $a, b \in R$ satisfy

$$ab = 0, \quad a \neq 0, \quad b \neq 0,$$

then a, b are called 0 divisors (or zero divisors or divisor of 0).
Integral domain (Definition 19.6). A ring R is called an integral domain if the following conditions are satisfied: (1). R is commutative; (2). R has a unity 1 and $1 \neq 0$; (3). R has **no** zero divisors.
Characteristic of a ring R (Definition 19.13). Characteristic 0 (Definition 19.13).

Examples

(1). A field is always an integral domain. In particular, since $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields, they are integral domains. $\mathbb{Z}$ is an integral domain, but not a field.
(2). In the commutative $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, $2, 3, 4$ are 0 divisors (because $2 \cdot 3 = 0, 4 \cdot 3 = 0$). 1 and 5 are units. $\mathbb{Z}_6$ is **not** an integral domain. In general if n is **not** a prime, then $\mathbb{Z}_n$ is **not** an integral domain.
(3). The characteristic of the ring $\mathbb{Z}_n$ is n. The characteristic of the rings $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are all 0.

Theorems

Theorem 19.3. In the ring $\mathbb{Z}_n$, the 0 divisors are precisely those nonzero elements that are not relatively prime to n.

Theorem 19.5. **Theorem 19.15**.

Corollary 19.4. Theorem 19.9. Theorem 19.11. Corollary 19.12.
(1). Every field is an integral domain.
(2). Every **finite** integral domain is a field.
(3). If p is a prime, then $\mathbb{Z}_p$ is an integral domain.
(4). If p is a prime, then $\mathbb{Z}_p$ is a field.

Section 20. Fermat's and Euler's Theorems

Basic concepts

Group G_n (page 186), G_n is the set of all nonzero elements in $\mathbb{Z}_n$ that are not zero divisors, G_n is a group under multiplicatiom modulo n (Theorem 20.6). Euler phi-function (page 187) , for any positive integer n,

$$\phi(n) = |G_n| = \text{the number of elements in } \mathbb{Z}_n \text{ that are relatively prime to } n.$$

Theorems

For any field, the nonzero elements form a group under the multiplication (page 184).

Theorem 20.1 (Fermat's Little Theorem). If p is a prime, and $a \in \mathbb{Z}$ is not divisible by p, then $a^{p-1} - 1$ is a multiple of p.

Corollary 20.2. If p is a prime, $a \in \mathbb{Z}$, then $a^p - a$ is a multiple of p.

Theorem 20.6. Let G_n be the set of all nonzero elements in $\mathbb{Z}_n$ that are not zero divisors, then G_n is a group under multiplicatiom modulo n.

Theorem 20.8 (Euler's Theorem). If a is an integer relatively prime to n, then $a^{\phi(n)} - 1$ is a multiple of n.

Examples

$G_{10} = \{1, 3, 7, 9\}$, the inverse of $3^{-1} = 7$ (since $3 \cdot 7 = 21 = 1$). $\phi(10) = 4$.
$G_9 = \{1, 2, 4, 5, 7, 8, \}$, $\phi(9) = 6$.

Problems

1. If p is a prime, prove that

$$\phi(p^n) = p^n - p^{n-1}.$$

2. If m and n are reltively prime, prove that

$$\phi(mn) = \phi(m)\phi(n).$$

Section 21. The Field of Quotients of an Integral Domain

The main result of this section is **Theorem 21.5**. The proof of this theorem (i.e. a construction of a field of quotients F for an integral domain D) is given on page 191-194 (steps 1,2,3,4). The uniqueness of the field of quotients is given in **Theorem 21.6**.

Example.

If the Integral domain is $\mathbb{Z}$, its field of quotients is $\mathbb{Q}$.

Section 22. Rings of Polynomials

Basic concepts

A **polynomial** $f(x)$ with coefficients in a ring R, **degree** of $f(x)$ (Definition 22.1). The ring of polynomials $R[x]$ (Theorem 22.2). **Zeros** of $f(x)$ (Definition 22.10).

Theorems

Theorem 22.2. Theorem 22.4.

Section 26. Homomorphisms and Factor Rings

Basic concepts

Ring homomorphism (Definition 26.1). Kernel (Definition 26.4). Ideal (Definition 26.10). Quotient ring (Definition 26.14).

Theorems

Theorem 26.3. **Theorem 26.5**. **Corollary 26.6**. **Theorem 26.7**. **Theorem 26.9**. **Corollary 26.14**. **Theorem 26.16**. **Theorem 26.17**.

Problems

1. Find all the ideals of $\mathbf{Z}$.
2. Let F be a field, prove that the matrix ring $M_n(F)$ has only two ideals $\{0\}$ and $M_n(F)$ itself.