Math 3121, Sections 13, 14, 16, 18, 19, 20, 21, 26

This note includes all the lecture notes after the quiz.

Section 13. Homomorphisms.

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

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

Example 1. $\phi : \mathbb{R} \to \mathbb{R}^*$ given by

$$\phi(x) = e^x$$

is a homomorphism. Notice that the operation for $\mathbb{R}$ is $+$ and the operation for $\mathbb{R}^*$ is the multiplication $\cdot$, the fact that ϕ is a homomorphism follows from the identity $e^{a+b} = e^a\, e^b$. Similarly, for arbitrary base $c > 0$, the map $f : \mathbb{R} \to \mathbb{R}^*$, $f(x) = c^x$ is a homomorphism. The map $g : \mathbb{C} \to \mathbb{C}^*$ given by $g(z) = e^z$ is a homomorphism.

Example 2. Let $\mathbb{R}_{>0}$ be the multiplicative group of positive real numbers. The map $\phi : \mathbb{R}_{>0} \to \mathbb{R}$ given by

$$\phi(x) = \log\, x$$

is a homomorphism, this follows from identity

$$\log(ab) = \log a + \log b.$$

Example 3. The map $\phi : \mathbb{R}^* \to \mathbb{R}^*$ given by

$$\phi(x) = x^n$$

is a homomorphism, where n is a fixed integer. Notice that both G and G' are multiplicative groups (both are $\mathbb{R}^*$). The homomorphism property follows from the identity $(ab)^n = a^n b^n$.

Example 4. The map $\phi : GL(2, \mathbb{R}) \to \mathbb{R}^*$ given by

$$\phi(A) = \mathrm{Det}(A)$$

is a homomorphism, where $\mathrm{Det}(A)$ is the determinant of 2×2 matrix A. The homomorphism property follows from the following identity about determinant: $\mathrm{Det}(AB) = \mathrm{Det}(A)\mathrm{Det}(B)$. Similarly, the map $\phi : GL(n, \mathbb{R}) \to \mathbb{R}^*$ given by $\phi(A) = \mathrm{Det}(A)$ is a homomorphism.

Example 5. Let V and V' be vector spaces, a map $f : V \to V'$ is called a linear map if (1) $f(u + v) = f(u) + f(v)$ for all $u, v \in V$ and (2) $f(kv) = kf(v)$ for every $k \in \mathbb{R}$ and $v \in V$. The first condition implies that f is a homomorphism of the additive group $(V, +)$ to $(V', +)$.

Example 6. Let G be an arbitrary group, $g \in G$ be a given element. Then the map $\phi : G \to G$ given by $\phi(a) = gag^{-1}$ is a homomorphism. Proof: We need to prove the identity $\phi(ab) = \phi(a)\phi(b)$.

$$\text{Right} = \phi(a)\phi(b) = gag^{-1}gbg^{-1} = gabg^{-1} = \phi(ab) = \text{Left}.$$

Example 7. The map $\phi : G \to G'$ given by $\phi(x) = e'$ (where e' is the identity element of G') for all $x \in G$ is a homomorphism, We call it the **trivial homomorphism**. The map $I : G \to G$ given by $I(x) = x$ is a homomorphism, it is called the identity homomorphism of G.

Example 8. $\phi : \mathbb{R} \to \mathbb{R}$ given by $\phi(x) = 100x$ is a homomorphism from the group $\mathbb{R}$ to itself, because

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

Example 9. $\phi(a) = \ln(|a|)$ is a homomorphism from $\mathbb{R}^*$ to $\mathbb{R}$, bacause

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

Example 10. $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ given by $\gamma(m) = r$, where r is the remainder of m divided by n, is a homomorphism.

Definition 13.11. If $\phi : X \to Y$ is a map. Let $A \subset X$ and $B \subset Y$. The **image** $\phi[A]$ is defined as

$$\phi[A] = \{\phi(a) \mid a \in A\}$$

which is a subset of Y. The **inverse image** $\phi^{-1}[B]$ is defined as

$$\phi^{-1}[B] = \{a \in A \mid \phi(a) \in B\},$$

which is a subset of X.

Theorem 13.12. Let $\phi : G \to G'$ be a homomorphism.Then
(1). $\phi(e) = e'$.
(2). $\phi(a^{-1}) = \phi(a)^{-1}$.
(3). If H is a subgroup of G, then $\phi[H]$ is a subgroup of G'.
(4). If K' is a subgroup of G', then $\phi^{-1}[K']$ is a subgroup of G.

Because $\{e'\}$ is a subgroup G', so

$$\phi^{-1}[e'] = \{a \in G \mid \phi(a) = e'\}$$

is a subgroup of G. We call $\phi^{-1}[e']$ the **kernel** of ϕ and denote it by $Ker(\phi)$. That is, $Ker(\phi) = \phi^{-1}[e'] = \{a \in G \mid \phi(a) = e'\}$.

A map $\phi : G \to G'$ is called an **isomorphism** if (1). ϕ is a homomorphism. (2). ϕ is one-to-one and onto. Examples 2, 6 , 8 above are isomorphisms.

Theorem 13.5. Let $G : G \to G'$ be a homomorphism, and $H = \text{Ker}(\phi)$. Let $b \in G'$. Then $\phi^{-1}(b) = \{x \in G \mid \phi(x) = b\}$ is either empty or $\phi^{-1}(b) = aH$ for any $a \in \phi^{-1}(b)$.

Corollary 13.18. Let $G : G \to G'$ be a homomorphism, ϕ is one-to-one iff $\text{Ker}(\phi) = \{e\}$.

Definition 13.19. A subgroup H of a group G is called a **normal subgroup** if $aH = Ha$ for all $a \in G$.

It can be proved that a subgroup H of G is normal iff for every $h \in H$ and $a \in G$, $aha^{-1} \in H$.

Corollary 13.20. Let $G : G \to G'$ be a homomorphism, then $\text{Ker}(\phi)$ is a normal subgroup of G.

Exercises

Problem 1. Find a homomorphism from $\mathbb{C}^*$ to U that is onto.

Problem 1. 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).

Problem 3. Find an isomorphism $\phi : \mathbb{Z}_n \to U_n$.

Problem 4. Prove that there is a unique homomorphism $\phi : S_{100} \to U_2 = \{1, -1\}$ that is onto.

Problem 5. Find a homomorphism of $\phi : S_3 \to S_5$ that is 1-1.

Section 14. Factor Groups.

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.

Proof. To prove the product is well-defined, we need to prove that $aH = a'H$ and $bH = b'H$ imply that $(ab)H = (a'b')H$. Recall that $cH = c'H$ iff $c' = ch$ for some $h \in H$. Because $aH = a'H$ and $bH = b'H$, we have $a' = ah_1$, $b' = bh_2$ for some $h_1, h_2 \in H$. Then $a'b' = ah_1bh_2 = ab(b^{-1}h_1bh_2)$. Since H is normal, the conjugate $b^{-1}h_1b \in H$, so $b^{-1}h_1bh_2 \in H$. This proves $a'b' = abh_3$ with $h_3 = b^{-1}h_1bh_2 \in H$. So $(a'b')H = (ab)H$. This proves the well-definess of the coset multiplication. The proof of the remaining part of the theorem is straightforward.

The group G/H in Theorem 14.9 is called the **factor group** of G by H, also called the **quotient group** of G by H. If G is finite, then G/H is also finite, we have $|G/H| = \frac{|G|}{|H|}$.

Theorem 14.9. If H is a normal subgroup of group G, then $\gamma : G \to G/H$ given by $\gamma(x) = xH$ is a homomorphism with kernel H.

The proof is straightforward.

Theorem 14.11. (**The Fundamental Homomorphism Theorem.**) Let $\phi : G \to G'$ be a homomorphism with $\text{Ker}(\phi) = H$. Then (1) $\Phi[G]$ is a subgroup of G'. (2). $\mu : G/H \to \phi[G]$ given by

$$\mu(aH) = \phi(a)$$

is well-defined and is an isomorphism. (3). $\phi = \mu \circ \gamma$, where γ is as in Theorem 14.9.

This Theorem is often used to identify the factor group G/H with other known groups.

Example. $G = \mathbb{C}^*$, $U_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$ is a normal subgroup of $\mathbb{C}^*$. Since $\mathbb{C}^*$ is abelian, U_n is a normal subgroup. We now use Theorem 14.11 to identify the factor group $\mathbb{C}^*/U_n$. Consider $\phi : \mathbb{C}^* \to \mathbb{C}^*$ given by $\phi(z) = z^n$. $\phi[\mathbb{C}^*] = \mathbb{C}^*$ and $\text{Ker}(\phi) = U_n$. By Theorem 14.11, $\mathbb{C}^*/U_n$ is isomorphic to $\mathbb{C}^*$.

Exercises.

Problem 1. Let $SL(2,\mathbb{R}) = \{A \in GL(2,\mathbb{R}) \mid \text{Det}\,(A) = 1\}$.
(1). Prove that $SL(2,\mathbb{R})$ is a normal subgroup of $GL(2,\mathbb{R})$.
(2). Prove that the factor group $GL(2,\mathbb{R})/SL(2,\mathbb{R})$ is isomorphic to $\mathbb{R}^*$.

Section 16. Group Action on a Set

The notion of group action provides an abstract model to study symmetries. We give an example before formally introducing this notion.

Example 1. Consider the group $GL(2,\mathbb{R})$, the group of 2×2 invertible matrices with matrix multiplication. Every element g in $GL(2,\mathbb{R})$ is a linear transformation of $\mathbb{R}^2$: g transforms every vector $v\in\mathbb{R}^2$ to a vector $gv\in\mathbb{R}^2$. So we have a map $GL(2,\mathbb{R})\times\mathbb{R}^2\to\mathbb{R}^2$, which sends every pair $(g,v)\in GL(2,\mathbb{R})\times\mathbb{R}^2$ to $gv\in\mathbb{R}^2$. The map satisfies the properties that

$$ev=v,\quad (g_1g_2)v=g_1(g_2v) \tag{1}$$

where e is the identity element of $GL(2,\mathbb{R})$, i.e., $e=\begin{pmatrix}1&0\\0&1\end{pmatrix}$. This is an example of the group $GL(2,\mathbb{R})$ action on the set $\mathbb{R}^2$. The identities in (1) are well-known facts about matrix multiplication.

Definition 16.1 Let X be a set and G a group. 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 the following two identities are satisfied:

$$\text{(Axiom 1).}\quad e*x=x\quad \text{for all } x\in X. \tag{2}$$

$$\text{(Axiom 2).}\quad (g_1g_2)*x=g_1*(g_2*x)\quad \text{for all } g_1,g_2\in G, x\in X \tag{3}$$

We also call G acts on X or X is a G-set.

In Example 1 above, $G=GL(2,\mathbb{R}), X=\mathbb{R}^2$, $g*x$ is just the matrix multiplication, i.e., the multiplication of 2×2 matrix g with 2×1 matrix x. The result $g*x=gx$ is a 2×1 matrix, a vector in $\mathbb{R}^2$.

Example 2. Example 1 can be generalized to the case $G=GL(n,\mathbb{R})$, where n is a given positive integer, $X=\mathbb{R}^n$ (vector space of column vectors with n components). The action of $G=GL(n,\mathbb{R})$ on $X=\mathbb{R}^n$ is given by the map $GL(n,\mathbb{R})\times\mathbb{R}^n\to\mathbb{R}^n$, which sends every pair $(g,v)\in GL(n,\mathbb{R})\times\mathbb{R}^n$ to $gv\in\mathbb{R}^n$.

Example 3. The permutation group S_3 acts on $X=\{1,2,3\}$. $g\in S_3$, $i\in X$, the action is $\sigma*i=\sigma(i)$. For example,

$$\sigma=(132), \sigma*1=3,\quad \sigma*2=1,\quad \sigma*3=2.$$

Example 4. More generally, for a given positive integer n, S_n acts on $X=\{1,2,\dots,n\}$. $\sigma*i=\sigma(i)$. In Example 3 and 4, Axiom 1 follows from the definition of $e\in S_n$ (e leaves every element fixed); Axiom 2 follows from the definition of the operation of S_n.

Example 5. This is a more abstract example. Let G be a group, H be a subgroup, let G/H be the set of all left cosets of H, then G acts on G/H by

$$g*(aH)=(ga)H.$$

Example 6. You may ignore this example for the time being. Let G be the symmetry group of some geometric figure (for example, a regular triangle) let X be a set associated to the geometric figure (for example, X is the set of vertices of the triangle). Then G acts on X, because $g\in G$, as a motion preserving the shape of the geometric figure, transforms $x\in X$, to gx (outcome of x after applying g to x).

Example 7. $G=S_5$, $X=\{(i,j)\mid 1\le i,j\le 5\}$. G acts on X by

$$\sigma(i,j)=(\sigma(i),\sigma(j)).$$

For example, $\sigma=(15423)$ (cycle of length 5),

$$\sigma(5,4)=(4,2),$$

as σ transforms 5 to 4, 4 to 2.

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).

Sketch of Proof. Step 1. Prove G_x is closed. Step 2. Prove $e \in G_x$ (this is obvious), Step 3. Prove $\sigma \in G_x$ implies $\sigma^{-1} \in G_x$. □

Example 8. In Example 3 above, the isotropy subgroup of 2 is

$$G_2 = \{e, (13)\},$$

because e and (13) are the only elements that leave 2 fixed, the other 4 elements $(23), (12), (123), (132)$ move 2 to $3, 1, 3, 1$ respectively.

Definition. Let G act on X, $x \in X$, **the orbit containing** x (also called the orbit of x) is the subset of X, denoted by Gx, given by

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

Example 9. In Example 3 above, the orbit containing 2 is $\{1, 2, 3\}$, because every element in $\{1, 2, 3\}$ can be obtained by applying some permutation to 2, $(12)2 = 1, (23)2 = 3, e2 = 2$. The orbits of 1 and 3 are also $\{1, 2, 3\}$. There are only one orbit for this case.

Example 10. In Example 3 above, the orbit containing 2 is $\{1, 2, 3\}$, because every element in $\{1, 2, 3\}$ can be obtained by applying some permutation to 2, $(12)2 = 1, (23)2 = 3, e2 = 2$. X. The orbits of 1 and 3 are also $\{1, 2, 3\}$. There are only one orbit for this case.

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

Sketch of Proof. We define the map $\phi : G/G_x \to Gx$ by $\phi(gG_x) = gx$. First we prove this map is well-defined (because the way to write a left coset gG_x is not unique). Then we prove ϕ is one-to-one and onto. SO G/G_x and Gx have the same cardinality, $|G/G_x| = |Gx|$. By the result in Section 10, we have $|G/G_x| = \frac{|G|}{|G_x|}$.

Exercises.

Problem 1. Find the order of the isotropy subgroups of $(1, 2)$ and $(1, 1)$ in Example 7.

Problem 2. In Example 7, how many elements are in the orbit of $(1, 2)$ and $(1, 1)$. How many orbits are there?

Problem 3. Prove that the following is a G-action on G:

$$g * x = gxg^{-1}.$$

that is, to prove Axiom 1 and Axiom 2,

$$e * x = x, \quad (g_1 g_2) * x = g_1 * (g_2 * x).$$

Section 18. Rings and Fields

The algebraic structure with two binary operations that is studied in this section is called a ring. All the well-known number systems such as integers, rational numbers, real numbers, complex numbers are examples of rings. Examples of rings also appear in linear algebra and analysis.

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

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

We often denote $a \cdot b$ by ab. The identity element of $+$ is denoted by 0. The additive inverse of a is denoted by $-a$, i.e., $a + (-a) = 0$.

Example 1. The set of integers $\mathbb{Z}$ is a ring with the usual addition and multiplication. Similarly $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ (the set of rational numbers, real numbers, complex numbers) are rings with the usual addition and multiplication.

Example 2. The set $C[0, 1]$ of continuous functions on $[0, 1]$ is a ring with the (function) addition and multiplication. Notice that $C[0, 1]$ is closed under the addition because the sum (product) of two continuous functions is a continuous function (a well-known result in calculus). Similarly for arbitrary domain D in $\mathbb{R}^n$, the set of continuous functions on D is a ring.

Example 3. The set $\mathbb{Z}_3 = \{0, 1, 2\}$, the modulo 3 integer system, is a ring. The operation $+$ is studied in Section 2. The multiplication $\cdot$ is the modulo 3 multiplication: $0 \cdot a = a \cdot 0 = 0$ for all $a \in \mathbb{Z}_3$; $1 \cdot a = a \cdot 1 = a$ for all $a \in \mathbb{Z}_3$; $2 \cdot 2 = 1$, because the multiplication of any two numbers in $2 + 3\mathbb{Z}$ is in $1 + 3\mathbb{Z}$.

$\mathbb{Z}_4 = \{0, 1, 2, 3\}$, the multiplication is

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

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

The rule can be summarized as follows: for $i, j \in \mathbb{Z}_4$, choose an element a in $i + 4\mathbb{Z}$ and an element $b \in j + 4\mathbb{Z}$, the multiplication ab is in $k + 4\mathbb{Z}$, we define $i \cdot j = k$. This k is independent of the choices of a and b.

For a given positive integer n, $\mathbb{Z}_n = \{0, 1, \ldots, n - 1\}$ is a ring under the modulo n addition and multiplication. 0 is the identity element for $+$ and 1 is the identity element for $\cdot$. $i \cdot j = k$ has the following meaning: any element in $i + n\mathbb{Z}$ multiplying any element in $j + n\mathbb{Z}$ gives an element in $k + n\mathbb{Z}$.

Example 4. Let n be a positive integer, $M_n(\mathbb{R})$ be the set of all $n \times n$ matrices with all entries in $\mathbb{R}$. Then $M_n(\mathbb{R})$ is a ring under the matrix addition and multiplication.

Example 5. Let $R_1, \ldots, R_n$ be rings, then the direct product $R_1 \times R_2 \times \cdots \times R_n$ is a ring under the following pointwise addition and multiplication

$$(a_1, \ldots, a_n) + (b_1, \ldots, b_n) = (a_1 + b_1, \ldots, a_n + b_n), \quad (a_1, \ldots, a_n) \cdot (b_1, \ldots, b_n) = (a_1 \cdot b_1, \ldots, a_n \cdot b_n).$$

A ring R is called a **commutative ring** if the multiplication is commutative, i.e., $a \cdot b = b \cdot a$ for all $a, b \in R$. Notice that by Axiom 1 in the definition of a ring, $+$ is always commutative. The rings in Examples 1, 2, 3, 5 are all commutative rings. In Example 4, for $n \geq 2$, $M_2(\mathbb{R})$ is NOT a commutative ring, as the matrix multiplication is not commutative.

If the multiplication for a ring R has an identity element (then it is unique), we call the identity element **the unity** of R. And we call R is a **ring with unity**. All the rings in Example 1, 2, 3, 4 are rings with unity.

When R is a ring with unity 1, $a \in R$ is called a **unit** if a is multiplicatively invertible, that is, there exists $a' \in R$ such that $aa' = a'a = 1$.

A ring R is called a **field** if the following three conditions are satisfied: (1) R is a commutative ring, (2) R has unity 1 and $1 \neq 0$, (3) every nonzero element is a unit.

$\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields. For ring $\mathbb{Z}$, (1) (2) are satisfied, but not (3), the units of $\mathbb{Z}$ are 1 and -1, so $\mathbb{Z}$ is NOT a field.

A subset S of a ring R is called a **subring** if S is closed under the addition and multiplication, and S is a ring under the induced addition and multiplication. To prove S is a subring of R, Step 1. we prove S is nonempty and it is closed under $+$ and $\cdot$. Step 2. we prove $a \in S$ implies that $-a \in S$.

Example. In any pair of the chain $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, the smaller ring is a subring of the bigger ring. For example. $\mathbb{Q}$ is a subring of $\mathbb{C}$.

Theorem 18.8. If R is a ring with additive identity 0, then for any $a, b \in R$ we have
(1) $a0 = 0a = 0$.
(2) $a(-b) = (-a)b = -(ab)$.
(3) $(-a)(-b) = ab$

All these identities are well-known for Example 1,2,3,4. The proof should use only the axioms in the definition of a ring. We give here the proof of (1). Since $0 + 0 = 0$, multiply a to both sides, we get

$$a(0 + 0) = a0. \tag{4}$$

By Axiom 2, $a(0 + 0) = a0 + a0$, so (1) implies that

$$a0 + a0 = a0 = a0 + 0 \tag{5}$$

Since $(R, +)$ is an abelian group (Axiom 1), we have cancellation law, cancelling $a0$ in the left side of (2) with $a0$ in the right side of (2), we get $a0 = 0$.

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 $a, b \in R$.

Notice that a ring homomorphism is also an abelian group homomorphism. The Kernel of a ring homomorphism ϕ is defined as

$$Ker(\phi) = \{a \in R \mid \phi(a) = 0\}.$$

This is the same as the kernel of group homomorphism if we consider ϕ as a group homomorphism.

Exercises.

Problem 1. If p is a prime, prove that $\mathbb{Z}_p$ is a field.

Problem 2. Determine if each of the following maps is a ring homomorphism.
(1). $\phi : \mathbb{C} \to \mathbb{C}$ given by $\phi(a + bi) = a - bi$.
(2). $\phi : \mathbb{C} \to \mathbb{C}$ given by $\phi(x) = -x$.
(3). $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ given by $\phi((a, b)) = b$.
(4). Let g be given 2×2 invertible matrix, $\phi : M_2(\mathbb{R}) \to M_2(\mathbb{R})$ given by $\phi(X) = gXg^{-1}$.
(5). $\phi : \mathbb{R} \to M_2(\mathbb{R})$ given by $\phi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

Problem 3. Determine if each of the following set is a subring of $M_2(\mathbb{R})$.
(1). The set of all 2×2 upper triangular matrices.
(2). The set of all 2×2 diagonal matrices.
(3). The set of all 2×2 diagonal matrices with non-negative diagonal entries.

Problem 4. Find all the units of the ring $\mathbb{Z}_6$.

Problem 5. Find a surjective ring homomorphism of $\mathbb{Z}$ onto $\mathbb{Z}_5$ and finds its kernel.

Section 19. Integral Domains

It is well-known that the product of two non-zero real numbers (or complex numbers) is non-zero, that is, $a, b \in \mathbb{R}$ ($\mathbb{C}$), $a \neq 0, b \neq 0$ imply $ab \neq 0$. But the same is NOT true for general rings. For example, $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, $3 \neq 0, 4 \neq 0$, but the product $3 \cdot 4 = 0$. We say that a and b are 0 **divisors**.

Definition. If a and b are two non-zero elements of a ring R such that $ab = 0$, then a and b are **divisors of zeros** (or 0 **divisors**).

This concept is used mostly for commutative rings.

Example 1. In $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, $2, 3, 4$ are the all 0-divisors.

Definition . 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.

Example 2. A field F is an integral domain. Proof. if $ab = 0$, $a \neq 0$, since F is a field, a has an inverse a^{-1}. Multiple the both sides of the equation $ab = 0$ by a^{-1}, we have $a^{-1}ab = a^{-1}0$, $1 \cdot b = 0$, $b = 0$. This proves F has no zero divisors. So the condition (3) is satisfied. Conditions (1) (2) are also satisfied because of the definition of a field.

In particular, $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are integral domains, because they are fields. $\mathbb{Z}$ is an integral domain, but not a field.

Example 3. $C[0, 1]$, the ring of continuous functions on $[0, 1]$ is NOT an integral domain. Conditions (1) (2) are satisfied, (3) is NOT satisfied, we can find two **non-zero functions** f, g such that $f(x) = 0$ for $x \in [0, \frac{1}{2}]$, and $g(x) = 0$ for $x \in [\frac{1}{2}, 1]$. Then $f(x)g(x) = 0$ for all $x \in [0, 1]$. So $f(x)$ and $g(x)$ are 0 divisors.

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

Example 4. In ring $\mathbb{Z}_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Among the nine nonzero elements, $2, 4, 5, 8$ are not relatively prime to 10, so they are all the 0-divisors.

Corollary 19.4. If p is a prime, then $\mathbb{Z}_p$ has no 0 divisors.

Example 5. Since 5 is a prime, $\mathbb{Z}_5$ has no zero divisors, so $\mathbb{Z}_5$ is an integral domain. We will see that $\mathbb{Z}_5$ is a field.

Theorem 19.9. Every field is an integral domain.

This theorem is already proved in Example 2.

Theorem 19.11. Every **finite** integral domain is a field.

Proof. Let D be an integral domain, we need to prove every nonzero element $a \in D$ is invertible. Consider the list $a, a^2, a^3, \ldots$; which has infinitely many elements but D is finite, so there exist different positive integers m and n such that

$$a^m = a^n \tag{6}$$

We may assume $m > n$. The equation (1) implies that $a^n(a^{m-n} - 1) = 0$. Since D has no 0 divisor, $a^n \neq 0$, this implies $a^{m-n} - 1 = 0$. So $a^{m-n} = 1$, $aa^{m-n-1} = 1$. So a^{m-n-1} is the inverse of a.

If the finiteness condition in the theorem is dropped, the result is **not** correct. Example. $\mathbb{Z}$ is an integral domain, but it is not a field.

Corollary 19.12. If p is a prime, then $\mathbb{Z}_p$ is a field.

Summary of the main results in this section.
(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.

Exercises.

Problem 1. Which of the following rings are integral domains, which of them are fields?
$\mathbb{Z}$, $\mathbb{Z}_{21}$, $\mathbb{Z}_{19}$, $\mathbb{Z}_{50}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Problem 2. Find all the 0 divisors of the ring $\mathbb{Z}_9$.

Problem 3. Let R be a finite commutative ring with unity 1, $1 \neq 0$. If $a \in F$ is not a 0 divisor, prove that a is a unit.

Section 20. Fermat's and Euler's Theorem

In this section, we apply the results in group theory and ring theory to prove two theorems in elementary number theory, Fermat's and Euler's Theorem.

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

Example . $p = 5$, $a = 3$, $a^{p-1} - 1 = 3^4 - 1 = 80$ is a multiple of 5.

It is easy to see that Theorem 20.1 is equivalent to the following:

Theorem 20.1' (An equivalent formulation of Little Theorem of Fermat) If p is a prime, $a \in \mathbb{Z}$, then $a^p - a$ is a multiple of p.

The equivalence follows from the identity $a^p - a = a(a^{p-1} - 1)$.

An elementary proof of Theorem 20.1'. It is not hard to see that if the theorem holds for positive integers a, then it holds for all integers a. It suffices to prove it for a positive integers. We use induction on a. If $a = 1$, $1^p - 1 = 0 = 0 \cdot p$ is a multiple of p. Assume $a = n$, $n^p - n$ is a multiple of p (induction assumption), then for $a = n + 1$,

$$(n+1)^p - (n+1) = \sum_{i=0}^{p} \binom{p}{i} n^i - (n+1) = (n^p - n) + \sum_{i=1}^{p-1} \binom{p}{i} n^i. \tag{7}$$

$n^p - n$ is a multiple of p by induction assumption. For $1 \le i \le p-1$,

$$\binom{p}{i} = \frac{p!}{i!(p-i)!}$$

is a multiple of p, because it is an integer by its combinatorial meaning, and p is not a factor of the denominator. Therefore the right hand side is a multiple of p. This completes the proof.

Now we give a proof of Theorem 20.1 using group theory. First we notice that for arbitrary field F, F^*, the set of all non-zero elements in F, is a group under the multiplication. (The multiplicative groups $\mathbb{Q}^*$, $\mathbb{R}^*$ and $\mathbb{C}^*$ have already been considered before.) Consider the ring $\mathbb{Z}_p$. By Corollary 19.12, $\mathbb{Z}_p$ is a field. The set G_p of non-zero elements in $\mathbb{Z}_p$ is a group under multiplication. Since $|G_p| = p-1$, by the corollary of Lagrangian Theorem,

$$a^{p-1} = 1 \quad \text{for all } a \in G_p.$$

This implies Theorem 20.1.

The group theory proof can be generalized to prove Euler's Theorem. Consider the ring $\mathbb{Z}_n$. We have the following theorem

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

Sketch of Proof. By the definition of G_n, G_n consists of elements a, $1 \le a \le n-1$ such that a is relatively prime to n. If $a, b \in G_n$, so a, b are relatively prime to n, so the remainder of ab divided by n is again relatively prime to n. This proves G_n is closed under the modulo n multiplication. It is obvious that $1 \in G_n$. It remains to prove every $a \in G_n$ has a multiplicative inverse in G_n. To this end, we consider the list $a, a^2, a^3, \ldots$. Since this list is infinite, but G_n is finite, we have $a^m = a^k$ for some $m > k$. This implies that $a^{m-k} = 1$, so a has inverse a^{m-k-1}.

We denote the order of G_n by $\phi(n)$. By definition of G_n, $\phi(n)$ is the number of integers a, $1 \le a \le n-1$, that is relatively prime to n. $\phi(n)$ is called **Euler phi-function**.

Example. Compute $\phi(10)$. Among the nine numbers $1, 2, 3, 4, 5, 6, 7, 8, 9$, Four of them $1, 3, 7, 9$ are relatively prime to 10, so $\phi(10) = 4$.

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.

Proof. Because a is an integer relatively prime to n, we can consider a as an element in G_n. So we have $a^{|G_n|} = 1$, that is, $a^{\phi(n)} = 1$ on G_n. This means $a^{\phi(n)} - 1$ is a multiple of n.

Example. 7 is relatively prime to 10, so $7^{\phi(10)} - 1$ is a multiple of 10, that is, $7^4 - 1$ is a multiple of 10.

The following rules can be used to compute Euler phi-function.

(1) If m and n are relatively prime, so the

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

(2). If p is a prime, then

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

Example. Find $\phi(1000)$ and prove that the last three digit of $7^{800} - 1$ are 0.
$1000 = 2^3 \cdot 5^3$. Since 2^3 and 5^3 are relatively prime, we have

$$\phi(1000) = \phi(2^3 \cdot 5^3) = \phi(2^3)\phi(5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400.$$

Since 7 is relatively prime to 1000, by Euler's Theorem, $7^{400} - 1$ is a multiple of 1000. So $7^{800} - 1 = (7^{400} - 1)(7^{400} + 1)$ is a multiple of 1000, so its last three digits are 0.

Exercises

Problem 1. List all the elements in G_6 and G_9.

Problem 2. Compute $\phi(99)$. Prove that $5^{180} - 1$ is a multiple of 99.

Problem 3. Let F be a field, prove that $F^* = \{a \in F \mid a \neq 0\}$ is a group under $\cdot$.

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**.

An example of Theorem 21.5 is $D = \mathbb{Z}$, the ring of integers. From $\mathbb{Z}$, one can construct the field $\mathbb{Q}$ of rational numbers. The construction of $\mathbb{Q}$ uses fractions $\frac{n}{m}$, $m, n \in \mathbb{Z}$, $m \neq 0$. Students learn this construction in primary school, which can be generalized to arbitrary integral integral domain as follows.

Let D be an integral domain, we consider the set of pairs (a, b) with $a, b \in D$, $b \neq 0$. One thinks a pair (a, b) as $\frac{a}{b}$. The two pairs (a, b) and (a', b') are considered equal if $ab' = a'b$. Let F be the set of all such pairs (after the above identification). We define addition $+$ and multiplication $\cdot$ on F as follows:

$$(a, b) + (c, d) = (ad + bc, bd), \quad (a, b) \cdot (c, d) = (ac, bd).$$

One checks $+$ and $\cdot$ are well-defined.

Theorem 21.5. F above is a field, it contains D as a subring.

Section 26. Homomorphisms and Factor Rings

Definition 26.1. A map ϕ of a ring R into a ring R' is a (ring) **homomorphism** if

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

for all $a, b \in R$.

Example 1. Let $R_1, \ldots, R_n$ be rings. For each i, the map $\pi_i : R_1 \times \cdots \times R_n \to R_i$ defined by $\pi_i(a_1, \ldots, a_n) = a_i$ is a homomorphism. It is called the projection onto the i-component.

Example 2. Let $\phi : \mathbb{C} \to M(2, \mathbb{R})$ be the map given by

$$\phi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}.$$

ϕ is a ring homomorphism. It is easy to check $\phi(z+w) = \phi(z) + \phi(w)$, but it is more involved to check $\phi(zw) = \phi(z)\phi(w)$ for $z, w \in \mathbb{C}$.

Example 3. Let $C[0,1]$ be the ring of continuous functions on $[0,1]$. The map $\phi : C[0,1] \to \mathbb{R}$ given by $\phi(f) = f(\frac{1}{2})$ is a ring homomorphism, it is called the evaluation homomorphism at $\frac{1}{2}$. In general, let $D \subset \mathbb{R}^n$ be a domain, $C(D)$ the ring of continuous functions on D. For a given point $p \in D$, the evaluation map $\phi : C(D) \to \mathbb{R}$, $\phi(f) = f(p)$ is a ring homomorphism.

Theorem 26.3. (Analog of Theorem 13.12). Let $\phi : R \to R'$ be a ring homomorphism. Then
(1) $\phi(0) = 0$.
(2) $\phi(-a) = -\phi(a)$.
(3) If $S \subset R$ is a subring, then $\phi[S]$ is a subring of R'.
(4) If $S' \subset R'$ is a subring, then $\phi^{-1}[S']$ is a subring of R.

Definition 26.4. Let $\phi : R \to R'$ be a ring homomorphism, the **kernel** of ϕ, denoted by $\mathrm{Ker}(\phi)$, is given by

$$\mathrm{Ker}(\phi) = \phi^{-1}(0) = \{a \in R \mid \phi(a) = 0\}.$$

It is clear that a ring homomorphism $\phi : R \to R'$ is a group homomorphism of $(R, +)$ into $(R', +)$. The kernel of ϕ is the same as the kernel for the additive group homomorphism.

Definition 26.10. Additive subgroup $N \subset R$ is called an **ideal** of R if it satisfies the property that $n \in N$ and $a \in R$ imply that $an \in N$ and $na \in N$.

If $\phi : R \to R'$ is a ring homomorphism, then $\mathbf{Ker}(\phi)$ is an ideal of R.

Proof. Because ϕ is an additive group homomorphism, so $\mathrm{Ker}(\phi)$ is an additive subgroup of R. For $n \in \mathrm{Ker}(\phi)$ and $a \in R$, $\phi(an) = \phi(a)\phi(n) = \phi(a)0 = 0$, this proves $an \in \mathrm{Ker}(\phi)$. Similarly, $\phi(na) = \phi(n)\phi(a) = 0\phi(a) = 0$, so $na \in \mathrm{Ker}(\phi)$.

Theorem 26.9, Corollary 26.14. Let N be an ideal of ring R, let R/N be the set of cosets $a + N$.
(1) Then the binary operations $+$ and $\cdot$ on R/N defined by

$$(a+N) + (b+N) = (a+b) + N, \quad (a+N) \cdot (b+N) = ab + N$$

are well-defined.
(2) $(R/N, +, \cdot)$ is a ring.

Proof. The well-definess of $+$ on R/N is included in Section 14 (Theorem 14.4 and Corollary 14.5). To prove $\cdot$ is well-defined, suppose $a+N = a'+N$ and $b+N = b'+N$, we need to prove $ab+N = a'b'+N$. We have $a' = a+n_1$ and $b' = b+n_2$ for some $n_1, n_2 \in N$. So $a'b' = (a+n_1)(b+n_2) = ab+an_2+n_1b+n_1n_2$. Since N is an ideal, $n_1, n_2 \in N$, we have $an_2 \in N, n_1b \in N, n_1n_2 \in N$, so $an_2 + n_1b + n_1n_2 \in N$. This proves $ab + N = a'b' + N$. The proof of Part (2) is straightforward.

The ring R/N is called the **factor ring** of R by N.

Example. $3\mathbb{Z}$ is an ideal of $\mathbb{Z}$. The set $\mathbb{Z}/3\mathbb{Z}$ has three elements:

$$\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$$

The factor ring $\mathbb{Z}/3\mathbb{Z}$ is just $\mathbb{Z}_3$. When we introduced $\mathbb{Z}_3$ earlier, we used the symbols $0, 1, 2$ to denote the elements rather than $0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}$. In general for any positive integer n, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$. The factor ring $\mathbb{Z}/n\mathbb{Z}$ is $\mathbb{Z}_n$.

Theorem 26.16. (Analog of Theorem 14.9) Let N be an ideal of a ring R. Then $\gamma : R \to R/N$ given by $\gamma(a) = a + N$ is a ring homomorphism with kernel N.

Theorem 26.17. (**Fundamental Homomorphism Theorem for Rings**, Analog of Theorem 14.11) Let $\phi : R \to R'$ be a ring homomorphism with kernel N, Then
(1) $\phi[R]$ is a subring of R'.
(2) The map $\mu : R/N \to \phi[R]$ given by $\mu(a + N) = \phi(a)$ is well-defined and is a ring isomorphism.
(3) $\phi = \mu \circ \gamma$.

(1) is included in Theorem 26.3 (3). For (2), to prove the well-definess of μ, suppose $a + N = a' + N$, then $a' = a + n$ for some $n \in N$. So

$$\mu(a' + N) = \phi(a') = \phi(a + n) = \phi(a) + \phi(n) = \phi(a) + 0 = \phi(a + N).$$

It is straightforward to prove μ is a ring homomorphism. And it is easy to see that ϕ is onto. It remains to prove μ is 1-1. By Corollary 13.18, it suffices to prove $\mathrm{Ker}(\phi) = \{0\}$. If $a + N \in \mathrm{Ker}(\phi)$, then $\mu(a + N) = \phi(a) = 0$, so $a \in N$, so $a + N = 0 + N$.

Exercises.

Problem 1. Find all the ideals of $\mathbb{Z}$.

Problem 2. Let F be a field, prove that F has only two ideals $\{0\}$ and F itself.