Math250a

Trustin Nguyen

September 11, 2023

Contents

Chapter 1

Rings

1.1 Rings and Homomorphisms

Definition 1.1.1

Rings

Rings are sets that satisfy the properties:

- With respect to addition, R is a commutative group.
- Multiplication is associative and has a unit element.
- For all x, y, z,

$$(x + y)z = xz + yz \qquad \text{and} \qquad z(x + y) = zx + zy$$

We have that 0 is the unit element for addition and 1 is the unit element for multiplication. We also assume that $1 \neq 0$ and notice that $0x = 0$ for all $x \in R$, since we have $0x$ as the identity element for addition:

$$0x + x = (0 + 1)x = x$$

We can look at other properties such as $(-x)y = -(xy)$ which indicates additive inverses:

$$(-x)y + xy = (0)y = 0 \qquad \text{and} \qquad -(xy) + xy = 0$$

We can also look at multiplicative inverses now. Let U be the set of elements of A which have right and left inverses. We note that U is a multiplicative group. This is because if b is a left-sided inverse and c is a right-sided inverse, then we have cab for any a with both inverses to be: $cab = b$ and therefore, $c = b$. This is a multiplicative group where both c, b are two-sided inverses and c has a two-sided inverse which is a. This is called the group of units of A or A^*. If $1 \neq 0$, and $a \in A$ is invertible, we have the division ring.

Elements of a ring that are only left-invertible might not form a group.

Example 1.1.1: (The Shift Operator). Let E be the set of all sequences

$$a = (a_1, a_2, a_3, \ldots)$$

We define addition component wise. If R is the set of all mappings $f : E \to E$, where $f(a + b) = f(a) + f(b)$, and the composition is the composition of mappings, then R is a ring.

Proof. We should verify the properties of a ring using the fact that $f(a + b) = f(a) + f(b)$. □

Definition 1.1.2 **Field**

A ring is commutative if $xy = yx$ for all $x, y \in A$. A division ring is a ring where all elements that are non-zero are invertible. So we will call a commutative division ring a field.

Definition 1.1.3 **Subring**

A subring is an additive subgroup of our ring that contains a multiplicative unit, closed under multiplication, addition, and is a ring. The properties of the operations is inherited from the parent ring.

Definition 1.1.4 **Center**

The center of a ring A is the set of $a \in A$ that commute with all other elements in A. In short this is:

$$ar = ra \qquad \forall r \in A$$

We can try and check that this is a subring. Notice that it is closed under addition. If $a, b \in C$ where C is the center of A:

$$(a + b)r = ar + br = ra + rb = r(a + b)$$

So $a + b \in C$. Now for multiplication:

$$ab(r) = a(br) = a(rb) = (ar)b = rab = r(ab)$$

So it is closed under multiplication. Now we just check that the units for multiplication and addition are in the center. Clearly this is true as:

$$1r = r1 \qquad \text{and} \qquad 0r = r0$$

Two important methods in proving that a set is a subring is to show that it is associative and distributive in a general sense. We can use induction for distributivity:

Proof. Base case: We have that $x(y_1 + y_2) = xy_1 + xy_2$.

Inductive case: Suppose that this holds for $y_1, \ldots, y_n$. We will show that this holds for y_{n+1}. Note that:

$$x(y_1 + \ldots + y_n) = xy_1 + \ldots + xy_n$$

Now observe that by the distributive property:

$$x((y_1 + \ldots + y_n) + (y_{n+1})) = x(y_1 + \ldots + y_n) + xy_{n+1}$$

But we have that the first part is already calculated. Therefore:

$$x(y_1 + \ldots + y_n + y_{n+1}) = xy_1 + \ldots + xy_{n+1}$$

□

The other thing to prove is that if $x_i (i = 1, \ldots, n)$ and $y_j (j = 1, \ldots, m)$ are elements of A, then:

$$\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j$$

Proof. By the distributive property shown above, we have:

$$\sum_{i=1}^{n} x_i(y_1 + \ldots y_n) = \sum_{i=1}^{n} x_i y_1 + \ldots + x_i y_m$$

Now we recollapse the summation to get what is desired:

$$\sum_{i=1}^{n} x_i y_1 + \ldots + x_i y_m = \sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j$$

□

We also note that distributivity holds for subtraction:

$$x(y_1 - y_2) = xy_1 - xy_2$$

Example 1.1.2: Let S be a set and A a ring. Let $\mathrm{Map}(S, A)$ be the set of mappings of S into A. Then $\mathrm{Map}(S, A)$ is a ring if for $f, g \in \mathrm{Map}(S, A)$ we define

$$(fg)(x) = f(x)g(x) \qquad \text{and} \qquad (f + g)(x) = f(x) + g(x)$$

for all $x \in S$.

Proof. Observe that by the second property:

$$(f + g)(x) = f(x) + g(x)$$

we have that the sum of two mappings takes an input $x \in A$ and gives us an output $f(x) + g(x)$ where $f(x), g(x) \in A$. Since A is closed under addition, this output is also in A, therefore, $f + g \in A$. The same can be said for the product closure. The additive identity would be the zero map because if $f(x) = 0$ then for all $g(x) \in \mathrm{Map}(S, A)$, we have:

$$(f + g)(x) = f(x) + g(x) = 0 + g(x) = g(x) = (g)(x)$$

similarly, we see that the product identity is just the mapping to the constant 1 or whatever the multiplicative identity is in A. This is because:

$$(fg)(x) = f(x)g(x) = 1g(x) = g(x)$$

Associativity, like closure under multiplication, addition is inherited from A. Distributivity is trivial. □

Example 1.1.3: Let M be an additive abelian group, and let A be the set $\mathrm{End}(M)$ of group-homomorphisms of M into itself. If addition in A is the addition of mappings and multiplication is the composition of mappings, then we have that A is a ring. This can also be verified like the last exercise.

Example 1.1.4: Another example of a ring is the polynomial ring over a field with one variable.

Example 1.1.5: We also have the set of $n \times n$ matrices with components that are in a field. The units are the invertible matrices.

Example 1.1.6: If S is a set and R is a set of real-valued functions on S, then R is a commutative ring. The units are functions that are nowhere 0.

Definition 1.1.5

Convolution Product

There are rings which are given by convolution. If G is a group and K is a field, then suppose that $K[G]$ is the set of formal linear combinations:

$$\alpha = \sum a_x x$$

with $x \in G$ and $a_x \in K$, where all but a finite number of a_x are equal to 0. If we have a similar one:

$$\beta = \sum b_x x \in K[G]$$

then our product is :

$$\alpha\beta = \sum_{a \in G} \sum_{y \in G} a_x b_y xy = \sum_{z \in G} \left(\sum_{xy=z} a_x b_y \right) z$$

This makes $Z[G]$ into a group ring which is a ring. Note that $K[G]$ is commutative if and only if G is commutative. In the context of functions, we have the convolution $f * g$ to be:

$$(f * g)(z) = \sum_{xy=z} f(x)g(y)$$

Definition 1.1.6

Ideals

A left ideal α of a ring A is a subset that is an additive subgroup of A where $A\alpha \subseteq \alpha$ or $A\alpha = \alpha$. A right ideal is defined similarly. A two-sided ideal is one that is both left and right. Consider the fact that all ideals in a commutative rings are two sided. Since we are working with commutative rings, we will just call all ideals as ideals.

Definition 1.1.7

Principal Ideals

A principal ideal is one that is generated by exactly one element.

If $a_1, \ldots, a_n \in A$, then we can denote an ideal to be $(a_1, \ldots, a_n)$ which by definition is:

$$\{x_1 a_1 + \cdots + x_n a_n\} \qquad \text{with} \qquad x_i \in A$$

If $\{a_i\}_{i \in I}$ is a family of ideals, then the intersection is also an ideal:

$$\bigcap_{i \in I} a_i$$

Proof. This will be proved by induction. For base case, we say that the intersection of two ideals is an ideal:

We will first prove additive closure as a subgroup. Suppose that $r_1, r_2 \in I_1 \cap I_2$, where I_1, I_2 are ideals. This means that:

$$r_1 + r_2 \in I_1 \qquad \text{and} \qquad r_1 + r_2 \in I_2$$

Therefore, the sum is in the ideal $I_1 \cap I_2$. As for the product, we have:

$$r_1 r_2 \in I_1 \qquad \text{and} \qquad r_1 r_2 \in I_2$$

So is is multiplicativily closed also. This is all from the property of ideals. Now suppose that we have an arbitrary $r \in R$, the parent ring. If $r_1 \in I_1 \cap I_2$, we can say that $r_1 r \in I_1 \cap I_2$ by the property of ideals. So we have finished.

Inductive Case: Suppose we have n unions of ideals. We will show that the union of $n+1$ ideals is an ideal also. But the union of two ideals is an ideal. So by the associativity of the union operator, we are done. □

Another thing to verify is that if $\alpha = (a_1, \ldots, a_n)$, then α is the intersection of all ideals containing the elements $a_1, \ldots, a_n$.

Definition 1.1.8 **Principle Ring**

A principal ring is a ring where every ideal is principal.

Example 1.1.7: Let $\mathbb{Z}$ be the ring we are working with and α be a proper ideal. Let d be the smallest positive integer in α. If $n \in \alpha$, then there are integers:

$$n = dq + r$$

which gives us the division algorithm. Since r is in α, we must have that $r = 0$. So all ideals of $\mathbb{Z}$ are multiples of some integer.

Definition 1.1.9 **Product of Ideals**

Let α, β be ideals of A, then the product $\alpha\beta$ is:

$$x_1 y_1 + \cdots + x_n y_n$$

the set of all sums where $x_i \in \alpha$ and $y_i \in \beta$.

Another idea: Let α, β be ideals of A. We will say that $\alpha\beta$ is the set of all sums

$$x_1 y_1 + \cdots + x_n y_n$$

for $x_i \in \alpha$ and $y_i \in \beta$. We see that $\alpha\beta$ is an ideal, because it is just the intersection of $\alpha\beta$. Clearly, all elements of that form lie in both α and β. Now what about the converse? Suppose $r_1 \in \alpha, \beta$. This actually does not seem true. Perhaps only when both α and β are prime ideals. Anyway, the set of these ideals is the entire ring with its unit element as the ideal (1). We define the product as above if both are left ideals and associativity as the standard: $(\alpha\beta)\psi = \alpha(\beta\psi)$

For the sum, we have $\alpha + \beta$ is a left ideal if both fare left ideals. Distributivity is held. Let α be a left ideal. Then αA is the set of sums $a_1 x_1 + \cdots + a_n x_n$. Furthermore, if A is commutative, let α, β be ideals. Then:

$$\alpha\beta \subseteq \alpha \cap \beta,$$

But not necessarily equality. We showed this above. But now try and prove that if $\alpha+\beta = A$, then $\alpha\beta = \alpha \cap \beta$.

Definition 1.1.10 **Ring Homomorphisms**

A ring homomorphism must satisfy two properties for multiplication and addition:

$$f(a + a') = f(a) + f(a') \qquad f(aa') = f(a)f(a')$$

This means that $f(0) = 0$ and $f(1) = 1$.

Definition 1.1.11 **Kernel**

The kernel of the ring homomorphism is from an additive standpoint. The kernel is an ideal.

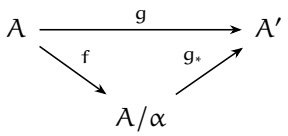
Definition 1.1.12 **Factor Ring**

The factor ring is A/α where α is an ideal. With A, α as additive rings, we have that A/α as the factor group. The multiplicative law for composition on A/α where if $x + \alpha$ and $y + \alpha$ are two cosets, then $(x + \alpha)(y + \alpha)$ would be $(xy + \alpha)$. This is well defined. To check, suppose that x_1, y_1 are in the same coset as x, y. Then we must show that x_1y_1 is in the same coset as xy. The $1 + \alpha$ is the identity coset. So we have the canonical map.

$$f : A \to A/\alpha$$

is a ring-homomorphism.

If $g : A \to A'$ is a ring-homomorphism whose kernel contains α, then there exists a unique ring-homomorphism $g_* : A/\alpha \to A'$ making the following diagram commutative:



Here is the proof

Proof. If $x \in A$, then $g(x) = g_*f(x)$. Hence for $x, y \in A$,

$$\begin{aligned} g_*(f(x)f(y)) = g_*(f(xy)) = g(xy) = g(x)g(y) \\ = g_*f(x)g_*f(y) \end{aligned}$$

Given $\mathcal{E}, \nu \in A/\alpha$, there is an $x, y \in A$ such that $\mathcal{E} = f(x)$ and $\nu = f(y)$. Since $f(1) = 1$, we have $g_*f(1) = g(1) = 1$, and so it is a multiplicative monoid-homomorphism.

So we have that $f : A \to A/\alpha$ is universal in the category of homomorphisms that has the kernel as α. □

If A is a ring and e is the identity element, then:

$$\lambda : \mathbb{Z} \to A$$

where $\lambda(n) = ne$ is a ring homomorphism, with the kernel as the ideal (n) generated by n. There is the injective homomorphism $\mathbb{Z}/n\mathbb{Z} \to A$, which is an isomorphism between the

ring $\mathbb{Z}/n\mathbb{Z}$ and a subring of A. If $n\mathbb{Z}$ is a prime ideal, then $n = 0$ or $n = p$. For the first case, A contains a subring isomorphic to $\mathbb{Z}$ where this subring has characteristic 0. Otherwise, we say that it has characteristic p. We say that $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

If K is a field, then it has characteristic 0 or $p > 0$. In the first case, it has a subfield that is isomorphic to the rational numbers and for the second case, it has an isomorphic image to $\mathbb{F}_p$. This subfield will be called a prime field. Prime fields are the smallest subfield of K containing 1 with no automorphism except for the identity. We can identify it with $\mathbb{Q}$ or $\mathbb{F}_p$. What we mean by prime ring is the integers $\mathbb{Z}$ if K has characteristic 0 or $\mathbb{F}_p$ if K has characteristic p.

If A is a subring of R and S is a subset of B that commutes with A, $as = sa$ for all $a \in A$ and $s \in S$, then consider $A[S]$ as the set of elements:

$$\sum a_{i_1 \cdots i_n} s_1^{i_1} \cdots s_n^{i_n}$$

The sum ranges over a finite number of tuples: $(i_1, \ldots, i_n)$ of integers, and $a_{i_1 \ldots} \in A$, $s_1, \ldots, s_n \in S$. If $B = A[S]$, we say that S is the set of generators or ring generators for B over A. If S is finite, then B is finitely generated as a ring over A. We also have that $A[S]$ consists of not necessarily commutative polynomials in elements of S with coefficients in A. Elements of S may not commute with each other.

Example 1.1.8: The ring of matrices is finitely generated over a field but matrices don't commute.

With all homomorphisms, they are determined by their action on the generators. So if $f : A \to A'$ is a ring homomorphism and $B = A[S]$, then there is an extension of f to a ring homomorphism of B by the values of S.

Let A be a ring, α be an ideal, and S be a subset of A. Then:

$$S \equiv 0 \pmod{\alpha}$$

if $S \subseteq \alpha$. If $x, y \in A$, then:

$$x \equiv y \pmod{\alpha}$$

if $x - y \in \alpha$. If α is principal, equal to (α), then:

$$x \equiv y \pmod{\alpha}$$

If $f : A \to A/\alpha$ is the canonical homomorphism, then $x \equiv y \pmod{\alpha}$ or $f(x) = f(y)$. The factor ring A/α is called the residue class ring. Cosets of α are called residue classes modulo α and if $x \in A$, then $x + \alpha$ is called the residue class of x modulo α.

We have that a ring homomorphism which is bijective is a ring-isomorphism. So there is an inverse which would be verified to be a homomorphism.

Let $f : A \to B$ be a ring homomorphism. Then the image $f(A)$ of f is a subring of B

An injective ring-homomorphism $f : A \to B$ establishes an isomorphism between A and its image. This homomorphism will be called an embedding.

Let $f : A \to A'$ be a ring-homomorphism, and a' be an ideal of A'. Then $f^{-1}(a')$ is an ideal α in A, and there is the injective homomorphism:

$$A/\alpha \to A'/\alpha'$$

Proposition 1.1: Products exist in the category of rings.

Definition 1.1.13 **Zero divisors**

Elements are zero divisors if $x, y \neq 0$ but $xy = 0$. A ring is an integral domain if it does not have zero divisors and is commutative.

Example 1.1.9: The ring of integers $\mathbb{Z}$ does not have zero divisors and will be an integral domain. Also, if a set S has at least two elements and A is a ring with $1 \neq 0$, then the ring of mappings $\mathrm{Map}(S, A)$ has zero divisors. (Proof?)

Proof. We have that all fields are integral domains. This is because if $ab = 0$, we can divide on both sides to get that $b = 0$ (possible only in fields where every element is a unit). We know that $\mathbb{Q}$ is a field. Since $\mathbb{Z}$ is a subring of it, it is an integral domain. If a ring has no zero divisors, then its subset has no zero divisors. For the second one, just take one map to map an element s_1 to 0 and $s_{i>0}$ to any other non-zero elements in the ring. Then we take s_0 and map it to any non-zero element and $s_{i>0}$ to zeros. This works. □

Example 1.1.10: Let m be a positive integer $\neq 1$. The ring $\mathbb{Z}/m\mathbb{Z}$ has zero divisors if and only if m is not a prime number. The ring of $n \times n$ matrices over a field has zero divisors if $n \geqslant 2$.

Proof. We know that if m is a prime number, then $\mathbb{Z}/m\mathbb{Z}$ is a field. This means that it has no zero divisors. Now we need to show that if m is not prime, then $\mathbb{Z}/m\mathbb{Z}$ has zero divisors. We know that $m = ab$ for two non-zero elements neither are multiples of m: a, b. But $ab \mod m = 0$ So $ab = 0$ in $\mathbb{Z}/m\mathbb{Z}$. We are done. □

An idea to consider: If R is an integral domain, then if a, b generate the same ideal, then there is a unit u such that $au = b$. The converse also holds.

Proof. If we have that unit, then $(b) \subseteq (a)$. But we also have $a = bu^{-1}$ which means that $(a) \subseteq (b)$. Therefore, $(a) = (b)$. Suppose that $(a) = (b)$. By the definition of ideals as the set of linear combinations of generators with coefficients as elements in the ring, we have that $a = bc$, $b = ad$. But $a = adc$ so $a(1 - dc) = 0$. Since we are in an ID, we have that $1 - dc = 0$ and $1 = dc$. □

1.2 Commutative Rings

Definition 1.2.1 **Prime Ideal**

A prime ideal is an ideal $p \neq A$ such that A/p is an integral domain. This means that if $a_1 + p$ and $a_2 + p$ are two cosets of p and $a_1a_2 + p = p$, since A/p is an integral domain, and $a_1a_2 = 0$, then either a_1 or a_2 are in p. In other words, the alternate definition is that whenever $xy \in p$, then either $x \in p$ or $y \in p$.

Definition 1.2.2 **Maximal Ideal**

Let $\mathfrak{m}$ be an ideal. We say that $\mathfrak{m}$ is a maximal ideal if $\mathfrak{m} \neq A$ and if there is no ideal $\alpha \neq A$ containing $\mathfrak{m}$ and $\neq \mathfrak{m}j$.

We claim that every maximal ideal is prime.

Proof. We first suppose that $xy = 0$ and $x \notin \mathfrak{m}$ for $\mathfrak{m}$ maximal ideal in A. Then we notice that since $\mathfrak{m}$ is maximal, then appending x to our ideal gives the whole ring. In other words, we have that $\mathfrak{m} + Ax = A$. So we actually can write the identity of A as a useful sum:

$$1 = u + \alpha x$$

for $u \in \mathfrak{m}$. Then we multiply both sides by y:

$$y = uy + \alpha xy$$

to show that $y \in \mathfrak{m}$ since $uy \in \mathfrak{m}$ and $\alpha xy \in \mathfrak{m}$. This proves that all maximal ideals are prime. □

Let α be an ideal $\neq A$. Then α is contained in some maximal ideal $\mathfrak{m}$.

Proof. Observe that if $\alpha \subseteq \beta$, for all ideals β, then either $\alpha = \beta$for all, in which case α is maximal, or α is a proper subset of one of the β. We realize that this chain of inclusions can be continued. We have that $1 \notin \alpha_i$ so the union is a maximal ideal. □

The ideal $\{0\}$ is a prime ideal of A if an d only if A is an ID. Verified by definition.

Definition 1.2.3 **field**

We say that a field K is a commutative ring where $1 \neq 0$ and the multiplicative monoid of non-zero elements of K is a group. Essentially, every element has an inverse. The only ideals of K are the field K and the ideal $\{0\}$.

If $\mathfrak{m}$ is a maximal ideal of A, then $A/\mathfrak{m}$ is a field.

Proof. If $x \in A$ and $\overline{x}$ is its residue class mod $\mathfrak{m}$, then suppose that $x \notin \mathfrak{m}$. Then by the previous idea, we say that:

$$1 = u + yx$$

for some $y \in A$ and $u \in \mathfrak{m}$. This means that the residue class of yx mod $\mathfrak{m}$ is the multiplicative identity. Therefore, we have that y is the inverse of x. □

The converse is also true: If $\mathfrak{m}$ is an ideal of A such that $A/\mathfrak{m}$ is a field, then $\mathfrak{m}$ is maximal.

Proof. Suppose that $x + \mathfrak{m}$ is some element of $A/\mathfrak{m}$, the field. Then it must have an inverse $y + \mathfrak{m}$ such that $xy + \mathfrak{m} = 1 + \mathfrak{m}$. This means that $xy + u_1 = 1 + u_2$. But this means that $xy + u' = 1$. For $u' \in \mathfrak{m}$. Therefore, adding an arbitrary element $x \notin \mathfrak{m}$ would make the ideal into the entire ring. So $\mathfrak{m}$ is maximal. □

Let $f : A \to A'$ be a homomorphism of commutative rings. Let p' be a prime ideal of A', and let $p = f^{-1}(p')$. Then p is prime.

Proof. Suppose that $x, y \in A$, and that $x \notin p$, Then we see that $f(x) \notin p'$. This means that $f(x)f(y) = f(xy) \in p'$ therefore, $f(y) \in p'$ so $f^{-1}(f(y)) = y \in p$, so p is prime. □

(Revisit) An exercise would be to prove that if f is surjective and if $\mathfrak{m}'$ is maximal in A', then $f^{-1}(\mathfrak{m}')$ is maximal in A.

Example 1.2.1: Let $\mathbb{Z}$ be the ring of integers. Since an idela is also an additive subgroup of $\mathbb{Z}$, every ideal $\neq \{0\}$ is principal. Let p be a prime ideal $\neq \{0\}$ $p = n\mathbb{Z}$. Then n is a prime number, by the definition of prime ideal. As for the converse, if p is a prime number, then $p\mathbb{Z}$ is a prime ideal. Furthermore, $p\mathbb{Z}$. is a maximal ideal. If $p\mathbb{Z}$ is contained in an ideal $n\mathbb{Z}$, then $p = nm$ for some m. This means that either $n = 1$ or $n = p$. So $p\mathbb{Z}$ is maximal.

If n is an integer, the factor ring $\mathbb{Z}/n\mathbb{Z}$ is the ring of integers modulo n which is shown as:

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}(n)$$

and if n is prime, then this is a field which is $\mathbb{F}_p$. Due to the property of groups, we have that if $x \not\equiv 0 \pmod{p}$, then $x^{p-1} \equiv 1 \pmod{p}$. We usually write $\pmod{p}$ instead of $\pmod{p\mathbb{Z}}$. The units of the ring are the elements that are relatively prime to n. The order of this group of elements in $\mathbb{Z}/n\mathbb{Z}$ is called $\varphi(n)$ which is the Euler phi-function. So we say that if x is relatively prime to n, then $x^{\varphi(n)} \equiv 1 \pmod{n}$.

Theorem 1.2.1 **Chinese Remainder Theorem**

Let $\alpha_1, \ldots, \alpha_n$ be ideals of A such that $\alpha_i + \alpha_j = A$ for all $i \neq j$. Give elements $x_1, \ldots, x_n \in A$, there exists $x \in A$ such that $x \equiv x_i \pmod{\alpha_i}$ for all i.

Proof. If $n = 2$, then we have:

$$1 = a_1 + a_2$$

for two elements $a_i \in \alpha_i$. Then we have that:

$$x = x_2 a_1 + x_1 a_2$$

Now if $i > 2$, we have elements $a_i \in \alpha_1$ and $b_i \in \alpha_i$ such that:

$$a_i + b_i = 1$$

We say that the product $\prod_{i=2}^{n}(a_i + b_i) = 1$ and lies in

$$\alpha_1 + \prod_{i=2}^{n} \alpha_i$$

Now we have:

$$\alpha_1 + \prod_{i=2}^{n} \alpha_i = A$$

So by $n = 2$ case, we have an element $y_1 \in A$ where:

$$y_1 \equiv \pmod{\alpha_1}$$
$$y_1 = 0 \pmod{\prod_{i=2}^{n} \alpha_i}$$

We repeat this process to get other elements $y_2, \ldots, y_n$. Then we say that: $x = x_1 y_1 + \ldots + x_n y_n$. □

We note that if $\alpha_1, \alpha_2, \ldots, \alpha_n$ are ideals of a ring A such that

$$\alpha_1 + \cdots + \alpha_n = A$$

then if $\nu_1, \ldots, \nu_n$ are positive integers, then

$$q\alpha_1^{\nu_1} + \cdots + \alpha_n^{\nu_n} = A$$

Corollary 2.2 Let $\alpha_1, \ldots, \alpha_n$l be ideals of A. Assume that $\alpha_i + \alpha_j = A$ where $i \neq j$. Let

$$f : A \to \prod_{i=1}^{n} A/\alpha_i = (A/\alpha_1) \times \cdots \times (A/\alpha_n)$$

be the map of A into the product induced by the canonical map of A onto A/α_i for each factor. Then the kernel of f is $\bigcap_{i=1}^{n} \alpha_i$, and f is surjective, which gives the isomorphism:

$$A/\bigcap \alpha_i \to \prod A/\alpha_i$$

Proof. We note that if $a \in A$ lies in all of the quotient sets, then it is in the kernel. So $a \in \bigcap_{i=1}^{n} \alpha_i$. By the Chinese Remainder Theorem, we have that we can always find an $x \in A$ such that it is equivalent to a chosen set of x_i's modulo α_i, which means that we can always choose what element in each component of the tuple that x is mapped to. □

The theorem and the corollary are used frequently on the integers $\mathbb{Z}$ and to distinct prime ideals $(p_1), \ldots, , (p_n)$. These work because they are maximal. You could also take integers $m_1, \ldots, m_n$ which are relatively prime in pairs and use the theorem on principal ideals $(m_1) = m_1\mathbb{Z}, \ldots, (m_n = m_n\mathbb{Z})$. This is the classical example of the Chinese Remainder Theorem: where you can choose an integer such that it is equivalent to $x_i \mod p_i$.'

In particular, let m be an integer > 1 and let

$$m = \prod_i p_i^{r_i}$$

be the factorization of m into primes, with exponents $r_i \geqslant 1$. Then there is the ring isomorphism:

$$\mathbb{Z}/m\mathbb{Z} \approx \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}$$

This is just saying that:

$$\mathbb{Z}/\bigcap_i p_i^{r_i} \approx \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}$$

If A is a ring, we have that A^* is the multiplicative group of invertible elements of A. The following assertions are exercises:

(Revisit) The ring-isomorphism of $\mathbb{Z}/m\mathbb{Z}$ onto the product induces a group isomorphism:

$$(\mathbb{Z}/m\mathbb{Z})^* \approx \prod_i (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^*$$

From our isomorphism, we have:

$$\varphi(m) = \prod_i \varphi(p_i^{r_i})$$

And finally, if p is a prime number and r is an integer $\geqslant 1$, then

$$\varphi(p^r) = (p-1)p^{r-1}$$

Proof. For the last formula, we go by induction. For $r = 1$, we have that $\mathbb{Z}/p\mathbb{Z}$ is a field and the group has order $p - 1$. Now let $r \geqslant 1$ and consider the homomorphism:

$$\mathbb{Z}/p^{r+1}\mathbb{Z} \to \mathbb{Z}/p^r\mathbb{Z}$$

which we get from the inclusion of ideas $(p^{r+1}) \subseteq (p^r)$. So now there is the group homomorphism:

$$\lambda : (\mathbb{Z}/p^{r+1}\mathbb{Z})^* \to (\mathbb{Z}/p^r\mathbb{Z})^*$$

which is surjective because any element of $\mathbb{Z}/p^r\mathbb{Z}$ is prime to p and will represent an element of $(\mathbb{Z}/p^{r+1}\mathbb{Z})^*$. Let a be an integer representing an element of $(\mathbb{Z}/p^{r+1}\mathbb{Z})^*$ where $\lambda(a) = 1$. Then we have:

$$a \equiv 1 \pmod{p^r\mathbb{Z}}$$

so we have

$$a \equiv 1 + xp^r \pmod{p^{r+1}\mathbb{Z}}$$

we see that letting $x = 0, 1, \ldots, p - 1$ gives vales that are distinct in $\mathbb{Z}/p^{r+1}\mathbb{Z}$ which are in the kernel of λ. We also have that the element x can be one of the p integers because every integer is congruent to one of the p integers mod (p). So the kernel has order p which proves the formula. The kernel of λ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. (Proof?) □

1.3 Polynomials and Group Rings

We define polynomials by considering the infinite cyclic group generated by X and with S as a subset with the powers of X. Then the set of polynomials $A[X]$ is defined by the set of mappings: $S \to A$ where all but a finite number of elements are sent to a non-zero element in a. So our polynomials look like:

$$f(X) = \sum_{i=0}^{n} a_i X^i$$

and by the convolution rule:

$$f(X)g(X) = \sum_{k=1}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) X^k$$

Notice that we have the unit element 1 and the embedding:

$$A \to A[X] \qquad \text{by} \qquad a \mapsto aX^0$$

Let A be a sub ring of a commutative ring B. Let $x \in B$. If $f \in A[X]$ is a polynomial, we have the polynomial function:

$$f_B : B \to B$$

by:

$$f_B(x) = f(x) = a_0 + a_1 x + \ldots + a_n x^n$$

We have:

$$ev_b : f \mapsto f(b)$$

as a ring homomorphism of $A[X]$ into B. This is called the evaluation homomorphism. Let $x \in B$. So the subring $A[x]$ of B generated by x over A is the ring of all polynomial values. If there is an isomorphism by evaluation from $A[X]$ to $A[x]$, then we have that x is transcendental over A or that x is a variable over A.

Example 1.3.1: Let $\alpha = \sqrt{2}$. Then the set of real numbers of the for $a + b\alpha$ where $a, b \in \mathbb{Z}$ is a subring of the real numbers generated by $\sqrt{2}$. But we have that α is not transcendental over $\mathbb{Z}$, because $x^2 - 2$ is in the kernel of the map $f \mapsto f(\sqrt{2})$. But we do have that $e = 2.718\ldots$ and π are transcendental over $\mathbb{Q}$. We require the kernel to be trivial, or that the value is not a root of any polynomial in the given ring.

Example 1.3.2: Let p be a prime number and $K = \mathbb{Z}/p\mathbb{Z}$. Then K is a field. Let $f(X) = X^p - X \in K[X]$. Then f is not 0, but it is the 0 function. Since every element has order $p - 1$, we have that $x^{p-1} = 0$. So a non-zero polynomial gives us a 0 function.

We can look at other homomorphisms such as:

$$\varphi : A \to B$$

for two commutative rings and the homomorphism of polynomial rings $A[X] \to B[X]$ as

$$f(X) = \sum a_i X^i \mapsto \sum \varphi(a_i) X^i = (\varphi f)(X).$$

We call that $f \mapsto \varphi f$ is a reduction map.

Example 1.3.3: The map φ could be an isomorphism such as if $f(X)$ has complex coefficients. Then the complex conjugate is a reduction map on the coefficients.

Example 1.3.4: Let p be a prime ideal of A. Let $\varphi : A \to A'$ be the canonical homomorphism of A onto A/p. If $f(X)$ is a polynomial in $A[X]$, then φf wil be called the reduction of f modulo p. So we are taking all coefficients $\mod p$.

Example 1.3.5: If we have $A = \mathbb{Z}$ and $p = (p)$ where p is prime, we have that the polynomial $3X^4 - X + 2$ is a polynomial mod 5 where the coefficients $3, -1, 2$ are integers $\mod 5$ or elements in $\mathbb{Z}/5\mathbb{Z}$.

So now, we can look at evaluation maps and reduction maps together to generalize:

Let $\varphi : A \to B$ be a homomorphism of commutative rings. Let $x \in B$. Then there is a unique homomorphism extending φ:

$$A[X] \to B \qquad \text{such that} \qquad X \mapsto x$$

and this homomorphism is $\sum a_i X^i \mapsto \sum \varphi(a_i) x^i$. The statement says that we have a composition:

$$A[X] \longrightarrow B[X] \xrightarrow{ev_x} B$$

where the first map changes the coefficients of $A[X]$ and the second evaluates to an element of B.

Chapter 2

Modules

2.1 Basic Definitions

Let A be a ring. A left module over A or a left A-module M is an abelian group where for $a, b \in A$ and $x, y \in M$, we have:

$$(a + b)x = ax + bx \text{ and } a(x + y) = ax + ay$$

we leave it to the reader to show that $a(-x) = -(ax)$ and $0x = 0$. By definition of an operation, we have $1x = x$. We can also define a right $A-$ module. We will only look at left modules.

Definition 2.1.1 **Submodules**

Let M be an A-module. A submodule N of M is an additive subgroup such that $AN \subseteq N$. So N is a module with the operation same as A on M.

Example 2.1.1: We have that A is a module over itself, any commutative group is a $\mathbb{Z}$ module, an additive group consisting of 0 alone is a module over any ring, and any left ideal of A is a module over A.

Let J be a two-sided ideal of A. Then the factor ring A/J is actually a module over A. If $a \in A$ and $x + J$ is a coset of J in A, then there is the operation $a(x + J) = ax + j$. Furthermore, if M is a module and N is a submodule, we have the factor module. If L is a left ideal of A, then A/L is also a module.

Definition 2.1.2 **Vector Space**

A module over a field is a vector space. Let V is a vector space over the field k. Let R be the ring of all linear maps of V onto itself. Then V is a module over R. Similarly, if $V = K^n$ is the vector space of n tuples of elements of K, and R is the ring of $n \times n$ matrices with components in K, then V is a module over R.

Definition 2.1.3 **Torsion Submodules**

Let A be an integral domain and let M be an A-module. We say that the torsion submodule M_{tor} is the subset of elements $x \in M$ such that there is an $a \in A$, $a \neq 0$, such that $ax = 0$. We can see that M_{tor} is a submodule. This is because we only need to check closure of addition and multiplication. Notice that if r, s kill a, b respectively, then rs kills their sum and r kills their product.

Let α be a left ideal and M a module. We define αM as the set of all elements:

$$a_1x_1 + \ldots + a_nx_n$$

where $a_i \in \alpha$ and $x_i \in M$. This is a submodule of M. If α, β are left ideals, then there is associativity:

$$\alpha(\beta M) = (\alpha\beta)M$$

There are also other facts such as $(\alpha + \beta)M = \alpha M + \beta M$. If N, N' are submodules of M, then $\alpha(N + N') = \alpha N + \alpha N'$.

Let M be an A-module, and N a submodule. We have a module structure on the factor group M/N. Let $x + N$ be a coset of N in M and let $a \in A$. We define $a(x + N)$ to be the coset $ax + N$. We know that this is well-defined because if we also have a coset $y + N$ which is equal to $x + N$, we know that $ax \in ay + N$. So we have an operation of A on M/N which means that M/N is a module. We call this the factor module of M by N.

Definition 2.1.4 **Module-Homomorphism**

A module homomorphism is a map:

$$f : M \to M'$$

which sends stuff from one module to another. This is a group homomorphism:

$$f(ax) = af(x)$$

for all $a \in A$ and $x \in M$.

The collection of A-modules is a category with morphisms as the module homomorphisms. The identity map is a homomorphism such as for any module M', the map $\zeta : M \to M'$ where $\zeta(x) = 0$ for all $x \in M$ is the zero homomorphism.

Let M be a module and N a submodule. We have the group homomorphism:

$$f : M \to M/N$$

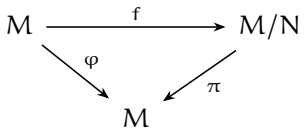
which is a module homomorphism. We have the mapping

$$f := m \in m + N$$

We see that this is a group homomorphism. Now we just check the other condition:

$$f(ax) = ax + N = a(x + N) = af(x)$$

We can say that f is universal in the category of homomorphisms of M whose kernel contains N. We have the following diagram:



(Revisit) Where π is injective, φ is a mapping from $M \to M$. We see that f is the unique mapping because

If $f : M \to M'$ is a module homomorphism, then the kernel and image are submodules of M and M' respectively. We prove the first by noting that if $k_1, k_2 \in \ker f$, then

$$f(k_1) = 0 \wedge f(k_2) = 0 \implies f(k_1 + k_2) = 0$$

and we have to show that if $a \in A$, then $ak \in \ker f$:

$$f(ak) = af(k) \text{Since we have a module homomorphism} \implies ak \in \ker f$$

Now to show that the image is a module, we have if $k_1, k_2 \in \Im f$:

$$f(g_1) = k_1, f(g_2) = k_2 \implies f(g_1 + g_2) = k_1 + k_2$$

which shows that $k_1 + k_2 \in \Im f$. For the added property of modules:

$$af(g_1) = ak_1 \implies f(ag_1) = ak_1$$

which means that $ak_1 \in \Im f$.

Definition 2.1.5 **Cokernel**

Let $f : M \to M'$ be a homomorphism. By the cokernel of f, we mean the factor module $M'/\Im f = M'/f(M)$. You can also mean the homomorphism $M' \to M'/f(M)$. Overall, the cokernel is the factor module of M'.

We have canonical homomorphisms applying to modules:

- Let N, N' be two submodules of a module M. Then $N + N'$ is a submodule and we have the isomorphism
$$N/(N \cap N') \approx (N + N')/N'$$
- If $M \supseteq M' \supseteq M''$are modules, then
$$(M/M'')/(M'/M'') \approx M/M'$$
- If $f : M \to M'$ is a module homomorphism, and N' is a submodule of M', then $f^{-1}(N')$ is a submodule of M and we have a canonical injective homomorphism
$$\overline{f} : M/f^{-1}(N') \to M'/N'$$
- If f is surjective, then $\overline{f}$ is a module-isomorphism.

The proofs are from confirming that all homomorphisms from abelian groups are A-homomorphisms of modules.

We see that a homomorphism which is bijective is a module isomorphism. The proof is the same for groups. We need to show that the inverse map is a module homomorphism.

We define a sequence of module homomorphisms:

$$M' \xrightarrow{f} M \xrightarrow{g} M''$$

If $\Im f = \ker g$. We have an exact sequence with the submodule N of a module M which is

$$0 \to N \to M \to M/N \to 0$$

If a homomorphism $u : N \to M$ satisfies:

$$0 \longrightarrow N \xrightarrow{u} M$$

is exact, then we say that u is a monomorphism/injective/ an embedding. And if

$$N \xrightarrow{u} M \longrightarrow 0$$

is exact, then it is an epimorphism/surjective.

2.2 Algebras

There are objects in math that satisfy the properties of rings except for the existence of a unit element. We can also see objects that don't satisfy associativity but do for distributivity. Let R be a ring and $x, y \in R$ with the bracket product as:

$$[x, y] = xy - yx$$

This is not associative but is distributive.

We can consider more general objects than a ring. Let A be a commutative ring. Let E, F be modules and consider a bilinear map:

$$g : E \times E \to F$$

where for $x \in E$, there is a map $y \mapsto g(x, y)$ that is A- linear and for a $y \in E$, the map $x \mapsto g(x, y)$ is also A-linear. An A-algebra is a module with a bilinear map $g : E \times E \to E$. This map is a law of composition on the module E. Assume that the algebras are associative and have a unit. One example of an algebra is $A[G]$ in which it is a module and we can look at the bilinear map:

$$f(x, y) = xy$$

We can view the group algebra as a special case of the situation below:

Let $f : A \to B$ be a ring-homomorphism such that $f(A)$ is contained in the center of B or $f(a)$ commutes with every element of B for every $a \in A$. Then we can see that B is an A-module with the operation of A on B by the map

$$(a, b) \mapsto f(a)b$$

for all $a \in A$ and $b \in B$. An algebra over A will be reference to the above ring homomorphism. The algebra is finitely generated if B is finitely generated as a ring over $f(A)$.

2.3 The Group of Homomorphisms

Let A be a ring and let X, X' be A-modules. We say that $\mathrm{Hom}_A(X', X)$ is the set of $A-$homomorphisms of X' into X. Then $\mathrm{Hom}_A(X', X)$ is an abelian group.

If A is commutative then we can make $\mathrm{Hom}_A(X', X)$ into an $A-$module by defining af for $a \in A$ and $f \in \mathrm{Hom}_A(X', X)$ with the map:

$$(af)(x) = af(x)$$