Commutative Algebra

Alec Zabel-Mena

June 20, 2023

Contents

Chapter 1

Rings and Ideals

1.1 Definitions and Examples.

Definition. A **commutative ring** R is a set together with two binary operations $+ : (a, b) \to a + b$ and $\cdot : (a, b) \to ab$ called **additon** and **multiplication** such that:

(1) R is an Abelian group over $+$, where we denote the identity element as 0 and the inverse of each $a \in R$ as $-a$.

(2) For any $a, b \in R$, $ab \in R$ and $a(bc) = (ab)c$. That is, R is closed under multiplication, and multiplication is associative.

(3) $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

(4) $ab = ba$ for all $a, b \in R$.

If there exists an element $1 \in R$ such that $a1 = 1a = R$, then we call R a ring with **identity**. If $1 = 0$, we call R the **zero ring** and write $R = 0$.

Definition. A commutative ring k with identity $1 \neq 0$ is called a **field** if for all $a \in k$, where $a \neq 0$, there exists a $b \in R$ such that $ab = 1$.

Lemma 1.1.1. *Let R be a commutative ring with identity. Then the following are true for all $a, b \in R$.*

(1) $0a = a0 = 0$.

(2) $(-a)b = a(-b) = -(ab)$.

(3) $(-a)(-b) = ab$

(4) $1 \neq 0$, *then* 1 *is unique and* $-a = (-1)a$.

Proof. (1) Notice $0a = (0 + 0)a = 0a + 0a$, so that $0a = 0$. Likewise, $a0 = 0$ by the same reasoning.

(2) Notice that $b - b = 0$, so $a(b - b) = ab + a(-b) = 0$, so that $a(-b) = -(ab)$. The same argument with $(a - a)b$ gives $(-a)b = -(ab)$.

(3) By the inverse laws of addition in R, we have $-(a(-b)) = -(-(ab))$, so that $(-a)(-b) = ab$.

(4) Suppose R has identity $1 \neq 0$, and suppose there is an element $2 \in R$ for which $2a = a2 = a$ for all $a \in R$. Then we have that $1 \cdot 2 = 1$ and $1 \cdot 2 = 2$, making $1 = 2$; so 1 is unique. Now, we have that $a + (-a) = 0$, so that $1(a + (-a)) = 1a + 1(-a) = 1a + (-a) = 0$ So $(-a) = -(1a) = (-1)a$ by (2).

■

Definition. Let R be a ring. We call an element $a \in R$ a **zero divisor** if $a \neq 0$ and there exists an element $b \neq 0$ such that $ab = 0$. Similarly, we call $a \in R$ a **unit** if there is a $b \in R$ for which $ab = ba = 1$. We call an element a **nilpotent** if there exists some $n \in \mathbb{Z}^+$ for which $x^n = 0$.

Definition. Let R be a ring. We call the set of all units in R the **group of units** and denote it $\mathcal{U}(R)$, or R^*.

Lemma 1.1.2. *Let R be a commutative ring with identity $1 \neq 0$. Then the group of units $\mathcal{U}(R)$ forms an Abelian group under multiplication.*

Proof. Let $a, b \in R$ be units in R. Then there are $c, d \in R$ for which $ac = ca = 1$ and $bd = db = 1$. Consider then ab. Then $ab(dc) = a(bd)c = ac = 1$ and $(dc)ab = d(ca)b = db = 1$ so that ab is also a unit in R. Moreover R^* inherits the associativity of $\cdot$ and 1 serves as the identity element of R^*. Lastly, if $a \in R^*$ is a unit there is a $b \in R$ for which $ab = ba = 1$. This also makes b a unit in R, and the inverse of a. Now, since R is a commutative ring, the multiplication in $\mathcal{U}(R)$ is commutative, making $\mathcal{U}(R)$ Abelian. ■

Corollary. *a is a zero divisor if, and only if it is not a unit.*

Proof. Suppose that $a \neq 0$ is a zero divisor. Then there is a $b \in R$ such that $b \neq 0$ and $ab = 0$. Then for any $v \in R$, $v(ab) = (va)b = 0$ so that a cannot be a unit. On the other hand let a be a unit, and $ab = 0$ for some $b \neq 0$. Then there is a $v \in R$ for which $v(ab) = (va)b = 1b = b = 0$. Then $b = 0$ which is a contradiction. ■

Corollary. *If k is a field, then it has no zero divisors.*

Proof. Notice by definition of a field, every element is a unit, except for 0. ■

Definition. A commutative ring with identity $1 \neq 0$ is called an **integral domain** if it has no zero divisors.

Lemma 1.1.3. *Any finite integral domain is a field.*

Proof. Let R be a finite integral domain and consider the map on R, by $x \to ax$. By above, this map is 1–1, moreover since R is finite, it is also onto. So there is a $b \in R$ for which $ab = 1$, making a a unit. Since a is abitrarily chosen, this makes R a field. ■

Corollary. *If k is a field it is a (not necessarily finite) integral domain.*

Definition. A **subring** of a ring R is a subgroup of R closed under multiplication.

1.2 Polynomail Rings

Theorem 1.2.1. *Let R be a commutative ring with identity, and define $R[x] = \{f(x) = a_0 + a_1x + \cdots + a_nx^n : a_0, \ldots a_n \in R\}$. Define the operations $+$ and $\cdot$ on $R[x]$ for $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and $g(x) = b_0 + b_1x + \cdots + b_nx^n$ by:*

$$f + g = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n$$

$$fg = c_0 + c_1x + \cdots + c_kx^k \text{ where } c_j = \sum_{i=0}^{j} a_ib_{j-i} \text{ and } k = n + m$$

Then $R[x]$ is a commutative ring with identity.

Definition. Let R be a commutative ring with identity. We call the ring $R[x]$ the **ring of polynomials** in x with **coefficients** in R whose elements of the form

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

where $n \geq 0$ are called **polynomails**. If $a_n \neq 0$, then the **degree** of f is denoted $\deg f = n$, and f is called **monic** if $a_n = 1$. We call $+$ and $\cdot$ the **addition** and **multiplication** of polynomials.

Example 1.1. (1) Take R any commutative ring with identity and form $R[x]$. One can verify that the polynomial $0(x) = 0 + 0x + \cdots + 0x^n + \cdots = 0$, in this case we call 0 the **zero polynomial**. Similarly, the additive inverse of $f(x) = a_0 + a_1x^1 + \cdots + a_nx^n$ is the polynomial $-f(x) = -a_0 - a_1x^1 - \cdots - a_nx^n$. Now, since $R[x]$ has identity, the **identity** polynomial is $1(x) = 1 + 0x + \cdots = 1$, that is, it is the identity in R. Lastly, we call a polynomial f with $\deg f = 0$ a **constant polynomial**. Notice that 0 and 1 are constant polynomials.

(2) $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ and $\mathbb{C}[x]$ are the polynomial rings in x with coeffiients in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ respectively.

(3) Notice that the rings $\mathbb{Z}[\omega]$ and $\mathbb{Z}[i]$ are polynomial rings in ω and i, respectively, with coefficients in $\mathbb{Z}$, and where $\omega = \sqrt{D}$ if $D \not\equiv 1 \mod 4$ or $\omega = \frac{1+\sqrt{D}}{2}$ otherwise, and $i^2 = -1$. Notice that the highest degree a polynomial in $\mathbb{Z}[i]$ can achieve is $\deg = 1$; however, one may be able to form polynomial rings in other variables with coefficients in $\mathbb{Z}[i]$, i.e. take $Z[x]$, where $Z = \mathbb{Z}[i]$.

(4) $\mathbb{Z}/3\mathbb{Z}[x]$ is the polynomial ring with coefficients in $\mathbb{Z}/3\mathbb{Z}$.

Theorem 1.2.2. *Let R be an integral domain, and let $p, q \neq 0$ be polynomials in $R[x]$. Then the following are true:*

(1) $\deg pq = \deg p + \deg q$.

(2) The units of $R[x]$ are precisely the units of R

(3) $R[x]$ *is an integral domain.*

Proof. Consider the leading terms $a_n x^n$ and $b_m x^m$ of p and q respectively. Then $a_n b_m x^{m+n}$ is the leading term of pq; moreover we require $a_n b_m \neq 0$. Now, if $\deg pq < m+n$, then $ab = 0$, making a and b zero divisors of R; impossoble. Therefore $ab \neq 0$. It also follows that since no term of p is a zero divisor, then p cannot be a zero divisor of $R[x]$. Lastly, if $pq = 1$, then $\deg p + \deg q = 0$, so that pq is a constant polynomial. Noticing that constant polynomials are simply just elements of R, then p and q are units. ∎

1.3 Ring Homomorphisms and Factor Rings.

Definition. Let R and S be commutative rings with identity. We call a map $\phi : R \to S$ a **ring homomorphism** if

(1) ϕ is a group homomorphism with respect to addition.

(2) $\phi(ab) = \phi(a)\phi(b)$ for any $a, b \in R$.

(3) $\phi(1_R) = 1_S$.

We denote the **kernel** of ϕ to be the kernel of ϕ as a group homomorphism. That is

$$\ker \phi = \{r \in R : \phi(r) = 0\}$$

Moreover, if ϕ is 1–1 and onto, we call ϕ an **isomorphism** and say that R and S are **isomorphic**, and write $R \simeq S$.

Lemma 1.3.1. *Let R and S be commutative rings with identity, and $\phi : R \to S$ a ring homomorphism. Then*

(1) $\phi(R)$ *is a subring of* S*.*

(2) $\ker \phi$ *is a subring of* R*.*

Proof. Let $s_1, s_2 \in \phi(R)$. Then $s_1 = \phi(r_1)$ and $s_2 = \phi(r_2)$ for some $r_1, r_2 \in R$. Then $s_1 s_2 = \phi(r_1)\phi(r_2) = \phi(r_1 r_2) \in \phi(S)$. Additionally, $s^{-1} = \phi^{-1}(r) = \phi(r^{-1})$ for some $s \in S$, $r \in R$. This is sufficient to make S a subring of S.

By similar reasoning, if $r_1, r_2 \in \ker \phi$, then $\phi(r_1)\phi(r_2) = \phi(r_1 r_2) = 0$ so that $r_1 r_2 \in \ker \phi$, and $\phi(r^{-1}) = \phi^{-1}(r) = 0$ so $\phi^{-1} \in \ker \phi$. ∎

Corollary. *For any $r \in R$ and $a \in \ker \phi$, then $ar \in \ker \phi$ and $ra \in \ker \phi$.*

Proof. We have $\phi(ar) = \phi(a)\phi(r) = \phi(a)0 = 0$ so $ar \in \ker \phi$. The same happens for ra. ∎

Definition. Let R be a comutative ring with identity. We call a subset $\mathfrak{a}$ of R an **ideal** of R if it is a subgroup under $+$, and for any $r \in R$, and $a \in \mathfrak{a}$, $ra \in \mathfrak{a}$.

Theorem 1.3.2. *Let R be a commutative ring with identity, and I af an ideal in R. Let $R/\mathfrak{a}$ be the set of all $a+\mathfrak{a}$ with $a \in R$. Define operations $+$ and $\cdot$ by*

$$(a+\mathfrak{a})+(b+\mathfrak{a}) = (a+b)+\mathfrak{a}$$
$$(a+\mathfrak{a})(b+\mathfrak{a}) = ab+\mathfrak{a}$$

Then $R/\mathfrak{a}$ forms a commutative ring with identity under $+$ and $\cdot$.

Proof. Notice that $(a+\mathfrak{a})+(b+\mathfrak{a}) = (a+b)+(\mathfrak{a}+\mathfrak{a}) = (a+b)+2\mathfrak{a} = (a+b)+\mathfrak{a}$. Moreover, $R/\mathfrak{a}$ inherits associativity in $+$ from addition in R. Now, take $0+\mathfrak{a} = \mathfrak{a}$ as the additive identity and $-a+I$ as the inverse of $a+\mathfrak{a}$ for each $\mathfrak{a}$.

Now, notice, that $(a+\mathfrak{a})(b+\mathfrak{a}) = ab + a\mathfrak{a} + b\mathfrak{a} + \mathfrak{a}^2 = ab + (\mathfrak{a}+\mathfrak{a}+\mathfrak{a}) = ab+\mathfrak{a}$ by distribution of multiplication over addition in R. Moreover, $R/\mathfrak{a}$ also inherits associativity and commutativity in $\cdot$ from multiplication in R. Now, notice then

$$(a+\mathfrak{a})((b+\mathfrak{a})+c+\mathfrak{a}) = (a+\mathfrak{a})((b+c)+\mathfrak{a}) = a(b+c)+\mathfrak{a} = (ab+ac)+\mathfrak{a} = (ac+\mathfrak{a})+(bc+a)$$

Observe also that if 1 is the identity of R, then $1+\mathfrak{a}$ is the identity of $R/\mathfrak{a}$ as $a+$. Since $(a+\mathfrak{a})(1+\mathfrak{a}) = a+\mathfrak{a}$.

Lastly, notice that $a+\mathfrak{a}$ is just the left coset of a by $\mathfrak{a}$ in R as a group under addition. So that $+$ and $\cdot$ are coset addition and multiplication, which are well defined. ■

Definition. Let R be a commutative ring with idenity and $\mathfrak{a}$ an ideal in R. We call the ring $R/\mathfrak{a}$ under addition and muiltplication of cosets the **factor ring** (or **quotient ring**) of R over $\mathfrak{a}$.

Theorem 1.3.3 (The First Isomorphism Theorem)**.** *If $\phi : R \to S$ is a ring homomorphism from rings R into S, then $\ker\phi$ is an ideal of R and*

$$\phi(R) \simeq R/\ker\phi$$

$$\begin{tikzcd}
R \arrow[r, "\phi"] \arrow[d, "\pi"'] & S \\
R/\ker\phi \arrow[ur, "\overline{\phi}"'] &
\end{tikzcd}$$

Proof. By the first isomorphism theorem for groups, ϕ is a group isomorphism. Now, let $K = \ker\phi$ and consider the map $\pi : R \to R/\mathfrak{a}$ by $a \xrightarrow{\pi} a+K$. Define the map $\overline{\phi} : R/K \to \phi(R)$ such that $\overline{\phi} \circ \pi = \phi$, then $\overline{\phi}$ defines the ring isomorphism. ■

Proof. The map $\pi : R \to R/\mathfrak{a}$ defined by $a \to a+\mathfrak{a}$, for any ideal $\mathfrak{a}$, is onto, with $\ker\pi = \mathfrak{a}$. ■

Theorem 1.3.4 (The Second Isomorphism Theorem). *Let $A \subseteq R$ a subring of R, and let B an ideal in R. Define $A + B = \{a + b : a \in A \text{ and } b \in B\}$. Then $A + BR$ is a subring and $A \cap B$ is an ideal in A. Then*

$$^{A+B}\!\big/_{B} \simeq {}^{A}\!\big/_{A \cap B}$$

Theorem 1.3.5 (The Third Isomorphism Theorem). *Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals in a ring R, with $\mathfrak{a} \subseteq \mathfrak{b}$. Then ${}^{\mathfrak{b}}\!/_{\mathfrak{a}}$ is an ideal of ${}^{R}\!/_{\mathfrak{a}}$ and*

$$^{R}\!\big/_{J} = {}^{({}^{R}\!/_{\mathfrak{a}})}\!\big/_{({}^{\mathfrak{b}}\!/_{\mathfrak{a}})}$$

Theorem 1.3.6 (The Fourth Isomorphism Theorem). *Let $\mathfrak{a}$ an ideal in a ring R, then the correspondence between A and ${}^{A}\!/_{\mathfrak{a}}$, for any subring $A \subseteq R$ is an inclusion preserving bijection between subrings of A containing $\mathfrak{a}$ and ${}^{R}\!/_{\mathfrak{a}}$. Moreover, A is an ideal if, and only if ${}^{A}\!/_{\mathfrak{a}}$ is an ideal.*

Lemma 1.3.7. *Let R be a ring with ideals $\mathfrak{a}$ and $\mathfrak{b}$. Then $\mathfrak{a} + \mathfrak{b}$, $\mathfrak{a}\mathfrak{b}$ and $\mathfrak{a}^n$, for any $n \geq 0$ are ideals of R and we have the lattice*

$$\begin{tikzcd}
 & R \arrow[d, dash] & \\
 & \mathfrak{a}+\mathfrak{b} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathfrak{a} \arrow[dr, dash] & & \mathfrak{b} \arrow[dl, dash] \\
 & \mathfrak{a}\mathfrak{b} \arrow[d, dash] & \\
 & (0) &
\end{tikzcd}$$

1.4 Properties of Ideals

Definition. Let R be a commutative ring with identity. We call the smallest ideal containing a nonempty subset A in R the **ideal generated** by A, and we write (A). We call an ideal **principle** if it is generated by a single element of R, i.e. $\mathfrak{a} = (a)$ for some $a \in \mathfrak{a}$. We say that the ideal (A) is **finitely generated** if $|A|$ is finite, and if $A = \{a_1, \ldots, a_n\}$, then we denote $(A) = (a_1, \ldots, a_n)$.

Example 1.2. (1) In any commutative ring with identity, the trivial ideal and R are the ideals generated by 0 and 1, respectively, so we write them as (0) and $R = (1)$.

(2) In $\mathbb{Z}$, we can write the ideals $n\mathbb{Z} = (n) = (-n)$. Notice that every ideal in $\mathbb{Z}$ is a principle ideal. Moreover, for $m, n \in \mathbb{Z}$, $n|m$ if, and only if $n\mathbb{Z} \subseteq n\mathbb{Z}$. Notice that

$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ is the ideal generated by n and n, where $d = (m, n)$ is the greatest common divisor of m and n. Indeed, by definition, $d|m, n$ so that $d\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$, and if $c|m, n$, then $c|d$, making $m\mathbb{Z} + n\mathbb{Z} \subseteq d\mathbb{Z}$. Then $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$ is the ideal generated by the greatest common divisor (m, n) and consists of all diophantine equations of the form

$$mx + ny = (m, n)$$

In general, we can define the **greatest common divisor** for integers $n_1, n_2, \ldots, n_m$ to be the smallest such integer d generating the ideal $n_1\mathbb{Z} + \cdots + n_m\mathbb{Z} = d\mathbb{Z}$. We then write $d = (n_1, \ldots, n_m)$.

(3) Consider the ideal $(2, x)$ of $\mathbb{Z}[x]$. $(2, x)$ is not a principle ideal. We have that $(2, x) = \{2p_x q : p, q \in \mathbb{Z}[x]\}$, and that $(2, x) \neq \mathbb{Z}[x]$. Suppose that $(2, x) = (a)$ for some polynomial $a \in \mathbb{Z}[x]$, then $2 \in (a)$, so that $2 = p(x)a(x)$, of degree $\deg p + \deg a$. This makes p and a constant polynomials in $\mathbb{Z}[x]$. Now, since 2 is prime in $\mathbb{Z}$, then only values for p and q are $p = \pm 1$ and $a = \pm 2$. If $a(x) = \pm 1$, then every polynomial in $\mathbb{Z}[x]$ can be written as a polynomial in (a), so that $(a) = \mathbb{Z}[x]$, impossible. If $a(x) = \pm 2$, then since $x \in (a)$, we get $x = 2q(x)$ where $q \in \mathbb{Z}[x]$. This cannot happen, so that $(a) \neq (2, x)$.

Lemma 1.4.1. *Let $\mathfrak{a}$ an ideal in ring R with identity. Then*

(1) $\mathfrak{a} = (1)$ if, and only if $\mathfrak{a}$ contains a unit.

(2) If R is commutative, then R is a field if, and only if its only ideals are (0) and (1).

Proof. Recall that $R = (1)$. Now, if $\mathfrak{a} = (1)$, then $1 \in \mathfrak{a}$, and 1 is a unit. Conversly, suppose that $u \in \mathfrak{a}$ with u a unit. By definition, we have that $r = r \cdot 1 = r(uv) = r(vu) = (rv)u$, so that $1 \in \mathfrak{a}$. This makes $\mathfrak{a} = (1)$.

Now, if R is a field, then it is a commutative ring, moreover every $r \neq 0$ is a unit in R, which makes $r \in \mathfrak{a}$ for some ideal $\mathfrak{a} \neq (0)$. This makes every $\mathfrak{a} \neq (0)$ equal to (1). Conversly, if (0) and (1) are the only ideals of the commutative ring R, then every $r \neq 0 \in (1)$, which makes themn units. Hence all nonzero r is a unit in R. This makes R into a field. ■

Corollary. *If k is a field, then any nonzero ring homomorphism ϕ defined on k is 1–1.*

Proof. If k is a field, then either $\ker \phi = (0)$ or $\ker \phi = (1)$. Now, since $\ker \phi \neq R$, we must have $\ker \phi = (0)$. ■

Definition. For any ideal $\mathfrak{m}$ in a ring R, we call $\mathfrak{m}$ **maximal** if $\mathfrak{m} \neq R$, and if $\mathfrak{n}$ is an ideal with $\mathfrak{m} \subseteq N \subseteq R$, then either $\mathfrak{m} = \mathfrak{n}$ or $\mathfrak{n} = R$.

Lemma 1.4.2. *If R is a commutative ring with identity, every proper ideal is contained in a maximal ideal.*

Proof. Let $\mathfrak{a}$ a proper ideal of R. Let $\mathcal{S} = \{N : N \neq (1) \text{ is a proper ideal, and } \mathfrak{a} \subseteq N\}$. Then $\mathcal{S} \neq \emptyset$, as $\mathfrak{a} \in \mathcal{S}$, and the relation $\subseteq$ partially orders $\mathcal{S}$. Let $\mathcal{C}$ be a chain in $\mathcal{S}$ and define

$$J = \bigcup_{A \in \mathcal{C}} A$$

We have that $J \neq \emptyset$ since $(0) \in J$. Now, let $a, b \in J$, then we have that either $(a) \subseteq (b)$ or $(b) \subseteq (a)$, but not both. In either case, we have $a - b \in J$ so that J is closed under additive inverse. Moreover, since $A \in \mathcal{C}$ is an ideal, by definition, J is closed with respect to absorbption. This makes J an ideal.

Now, if $1 \in J$, then $J = (1)$ and J is not proper, and $A = (1)$ by definition of J. This is a contradiction as A must be proper. Thereofre J must also be a proper ideal. Therefore, $\mathcal{C}$ has an upperbound in $\mathcal{S}$, therefore, by Zorn's lemma, $\mathcal{S}$ has a maximal element $\mathfrak{m}$, i.e. it has a maximal ideal $\mathfrak{m}$ with $\mathfrak{a} \subseteq \mathfrak{m}$. ■

Lemma 1.4.3. *Let R be a commutative ring with identity. An ideal $\mathfrak{m}$ is maximal if, and only if ${}^{R}\!/_{\mathfrak{m}}$ is a field.*

Proof. If $\mathfrak{m}$ is maximal, then ther is no ideal $I \neq (1)$ for which $\mathfrak{m} \subseteq \mathfrak{a} \subseteq R$ By the fourth isomorphism theorem, the ideals of R containing $\mathfrak{a}$ are in 1–1 correspondence with the those of ${}^{R}\!/_{\mathfrak{m}}$. Therefore $\mathfrak{m}$ is maximal if, and only if the only ideals of ${}^{R}\!/_{\mathfrak{m}}$ are $(\mathfrak{m})$ and $(1+\mathfrak{m})$. ■

Example 1.3. (1) Let $n \geq 0$ an integer. The ideal $n\mathbb{Z}$ is maximal in $\mathbb{Z}$ if and only if ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$ is a field. Therefore $n\mathbb{Z}$ is maximal if, and only if $n = p$ a prime in $\mathbb{Z}$. So the maximal ideals of $\mathbb{Z}$ are those $p\mathbb{Z}$ where p is prime.

(2) $(2, x)$ is not principle in $\mathbb{Z}[x]$, but it is maximal in $\mathbb{Z}[x]$, as ${}^{\mathbb{Z}[x]}\!/_{(2,x)} \simeq {}^{\mathbb{Z}}\!/_{2\mathbb{Z}}$ which is a field.

(3) The ideal (x) is not maximal in ${}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, since ${}^{\mathbb{Z}}\!/_{(x)} \simeq \mathbb{Z}$, which is not a field. Moreover, $(x) \subseteq (2, x) \subseteq \mathbb{Z}[x]$. We construct this isomorphism by identifying $x = 0$, then all polynomials of ${}^{\mathbb{Z}[x]}\!/_{(x)}$ only have constant term in $\mathbb{Z}$.

Definition. We call an ideal $\mathfrak{p}$ in a commutative ring R with identity **prime** if $\mathfrak{p} \neq (1)$ and if $ab \in \mathfrak{p}$ then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Alternatively, if $(ab) \subseteq \mathfrak{p}$ then $(a) \subseteq \mathfrak{p}$ or $(b) \subseteq \mathfrak{p}$.

Example 1.4. The prime ideals of $\mathbb{Z}$ are $p\mathbb{Z}$ with p prime together with (0).

Lemma 1.4.4. *An ideal $\mathfrak{p}$ in a commutative ring with identity, R, is prime if, and only if ${}^{R}\!/_{pf}$ is an integral domain.*

Proof. Suppose that $\mathfrak{p}$ is prime, and let $(a+\mathfrak{p})(b+\mathfrak{p}) = ab+\mathfrak{p} = \mathfrak{p}$. This gives us that $ab \in \mathfrak{p}$ and hence $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. Then either $a + \mathfrak{p} = \mathfrak{p}$ or $b + \mathfrak{p} = \mathfrak{p}$ in ${}^{R}\!/_{\mathfrak{p}}$. Conversly, if ${}^{R}\!/_{\mathfrak{p}}$ is an integral domain, then for any $a + \mathfrak{p}, b + \mathfrak{p}$ $ab + \mathfrak{p} = \mathfrak{p}$ implies that either $a + \mathfrak{p} = \mathfrak{p}$ or $b + \mathfrak{p} = \mathfrak{p}$. Then $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, only when $ab \in \mathfrak{p}$. This makes $\mathfrak{p}$ prime. ■

Corollary. *Every maximal ideal is a prime ideal.*

Example 1.5. (1) The prime ideals of $\mathbb{Z}$ are $p\mathbb{Z}$, where p is prime, which are the maximal ideals of $\mathbb{Z}$.

(2) The ideal (x) in $\mathbb{Z}[x]$ is a prime ideal, but it is not maximal as $(x) \subseteq (2, x) \subseteq \mathbb{Z}[x]$.

Definition. We define a commutative ring with identity to be a **local ring** if it has only one maximal ideal. We define the **residue field** of R to be the field $k = {}^{R}\!/_{\mathfrak{a}}$.

Bibliography

[1] D. Dummit, *Abstract algebra.* Hoboken, NJ: John Wiley & Sons, Inc, 2004.

[2] I. N. Herstein, *Topics in algebra.* New York: Wiley, 1975.