Commutative Algebra

Alec Zabel-Mena

June 21, 2023

Contents

Chapter 1

Rings and Ideals

1.1 Definitions and Examples

Definition. A **commutative ring** A 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) A is an Abelian group over $+$, where we denote the identity element as 0 and the inverse of each $a \in A$ as $-a$.

(2) For any $a, b \in A$, $ab \in A$ and $a(bc) = (ab)c$. That is, A 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 $a, b \in A$.

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

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 $b \in A$ such that $ab = 1$.

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

(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 A, we have $-(a(-b)) = -(-(ab))$, so that $(-a)(-b) = ab$.

(4) Suppose A has identity $1 \neq 0$, and suppose there is an element $2 \in A$ for which $2a = a2 = a$ for all $a \in A$. 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 A be a ring. We call an element $a \in A$ a **zero divisor** if $a \neq 0$ and there exists an element $b \neq 0$ such that $ab = 0$. Similarly, we call $a \in A$ a **unit** if there is a $b \in A$ 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 A be a ring. We call the set of all units in A the **group of units** and denote it $\mathcal{U}(A)$, or A^*.

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

Proof. Let $a, b \in A$ be units in A. Then there are $c, d \in A$ 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 A. Moreover $\mathcal{U}(A)$ inherits the associativity of $\cdot$ and 1 serves as the identity element of A^*. Lastly, if $a \in A^*$ is a unit there is a $b \in A$ for which $ab = ba = 1$. This also makes b a unit in A, and the inverse of a. Now, since A is a commutative ring, the multiplication in $\mathcal{U}(A)$ is commutative, making $\mathcal{U}(A)$ 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 $b \in A$ such that $b \neq 0$ and $ab = 0$. Then for any $v \in A$, $v(ab) = (va)b = 0$ 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 $v \in A$ 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 A be a finite integral domain and consider the map on A, by $x \to ax$. By above, this map is 1–1, moreover since A is finite, it is also onto. So there is a $b \in A$ for which $ab = 1$, making a a unit. Since a is abitrarily chosen, this makes A a field. ■

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

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

1.2 Polynomail Rings

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

Definition. Let A be a commutative ring with identity. We call the ring $A[x]$ the **ring of polynomials** in x with **coefficients** in A 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 A any commutative ring with identity and form $A[x]$. 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 $A[x]$ has identity, the **identity** polynomial is $1(x) = 1 + 0x + \cdots = 1$, that is, it is the identity in A. Lastly, we call a polynomial f with $\deg f = 0$ a **constant polynomial**. Notice that 0 and 1 are constant polynomials.

(2) $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{A}[x]$ and $\mathbb{C}[x]$ are the polynomial rings in x with coeffiients in $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{A}$, 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 A be an integral domain, and let $p, q \neq 0$ be polynomials in $A[x]$. Then the following are true:*

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

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

(3) $A[x]$ *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 A; 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 $A[x]$. 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 A, then p and q are units. ■

1.3 Ring Homomorphisms and Factor Rings

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

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

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

(3) $\phi(1_A) = 1_B$.

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

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

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

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

(1) $\phi(A)$ *is a subring of* B*.*

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

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

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

Theorem 1.3.2. *Let A be a commutative ring with identity, and $I\mathfrak{a}$ an ideal in A. Let $A/\mathfrak{a}$ be the set of all $a + \mathfrak{a}$ with $a \in A$. 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 $A/\mathfrak{a}$ 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, $A/\mathfrak{a}$ inherits associativity in $+$ from addition in A. 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 A. Moreover, $A/\mathfrak{a}$ also inherits associativity and commutativity in $\cdot$ from multiplication in A. 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 A, then $1+\mathfrak{a}$ is the identity of $A/\mathfrak{a}$ 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 A as a group under addition. So that $+$ and $\cdot$ are coset addition and multiplication, which are well defined. ■

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

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

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

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

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

Proof. The map $\pi : A \to A/\mathfrak{a}$ 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 $\mathfrak{a} \subseteq A$ a subring of A, and let $\mathfrak{b}$ an ideal in A. Define $\mathfrak{a}+\mathfrak{b} = \{a+b : a \in \mathfrak{a} \text{ and } b \in \mathfrak{b}\}$. Then $\mathfrak{a}+\mathfrak{b}A$ is a subring and $\mathfrak{a}\cap\mathfrak{b}$ is an ideal in A. Then*

$$\mathfrak{ab}\big/\mathfrak{b} \simeq \mathfrak{a}\big/\mathfrak{a}\cap\mathfrak{b}$$

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

$$A\big/\mathfrak{b} = (A/\mathfrak{a})\big/(\mathfrak{b}/\mathfrak{a})$$

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

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

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

1.4 Properties of Ideals

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

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

(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) Let $m, n \in \mathbb{Z}$. Then the least common multiple of m, n, $[m, n]$ is $[m, n]\mathbb{Z} = m\mathbb{Z} \cap n\mathbb{Z}$. Indeed, if $c = [m, n]$ is the least common multiple of m, n, then we have that $m|c$ and $n|c$, making $c \in m\mathbb{Z} \cap n\mathbb{Z}$; similarly, for any $c' \in m\mathbb{Z} \cap n\mathbb{Z}$, $c|c'$, by definition which puts $c' \in c\mathbb{Z}$. In general, for $n_1, \ldots, n_m \in \mathbb{Z}$, we define the **least common multiple** of $n_1, \ldots, n_m$ to be the largest such integer c generating the ideal $c\mathbb{Z} = n_1\mathbb{Z} \cap \cdots \cap n_m\mathbb{Z}$. And we write $c = [n_1, \ldots, n_m]$.

(4) Let $m, n \in \mathbb{Z}^+$ be coprime, i.e. $(m, n) = 1$. Then we can obtain $mn = [m, n]$ by observing the ideals generated by mn, (m, n), and $[m, n]$.

(5) 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 A with identity. Then*

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

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

Proof. Recall that $A = (1)$. 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 A is a field, then it is a commutative ring, moreover every $r \neq 0$ is a unit in A, 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 A, then every $r \neq 0 \in (1)$, which makes themn units. Hence all nonzero r is a unit in A. This makes A 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 $\ker \phi \neq A$, we must have $\ker \phi = (0)$. ■

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

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

Proof. Let $\mathfrak{a}$ a proper ideal of A. 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

$$J = \bigcup_{\mathfrak{a} \in \mathcal{C}} \mathfrak{a}$$

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 $\mathfrak{a} \in \mathcal{C}$ 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 $\mathfrak{a} = (1)$ by definition of J. This is a contradiction as $\mathfrak{a}$ 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 A be a commutative ring with identity. An ideal $\mathfrak{m}$ is maximal if, and only if $A/\mathfrak{m}$ is a field.*

Proof. If $\mathfrak{m}$ is maximal, then ther is no ideal $I \neq (1)$ for which $\mathfrak{m} \subseteq \mathfrak{a} \subseteq A$ By the fourth isomorphism theorem, the ideals of A containing $\mathfrak{a}$ are in 1–1 correspondence with the those of $A/\mathfrak{m}$. Therefore $\mathfrak{m}$ is maximal if, and only if the only ideals of $A/\mathfrak{m}$ 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 A 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, A, is prime if, and only if $A/\mathfrak{p}$ 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 ${}^{A}\!/\!_{\mathfrak{p}}$. Conversly, if ${}^{A}\!/\!_{\mathfrak{p}}$ 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 $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$.

Definition. Let A be a commutative ring with identity. We call A a **local ring** if it has one, and only one maximal ideal. We define the **residue field** of A to be the field $k = {}^{A}\!/\!_{\mathfrak{m}}$. We call a commutative ring with identity a **semi-local ring** if it has only finitely many maximal ideals.

Example 1.6. The tring $\mathbb{Z}$ is not a local ring, it is not even semi-local, since every prime ideal (p) of $\mathbb{Z}$, where $p \in \mathbb{Z}^+$ is prime, is also maximal.

Lemma 1.4.5. *Let A be a commutative ring with identity. Then the following are true.*

(1) If $\mathfrak{m} \neq (1)$ is an ideal of A such that every element of $A \backslash \mathfrak{m}$ is a unit, then A is a local ring having $\mathfrak{m}$ as its maximal ideal.

(2) If $\mathfrak{m}$ is a maximal ideal of A such that every element of $1+\mathfrak{m}$ is a unit, then A is a local ring.

Proof. Suppose that $\mathfrak{m} \neq (1)$. We have by lemma 1.4.2 that $\mathfrak{m}$ is contained in a maximal ideal. Moreover, $\mathfrak{m}$ contains no units by lemma 1.4.1. Since $x \in A \backslash \mathfrak{m}$ is a unit, we get $(x) = (1)$, which makes $\mathfrak{m}$ the only maximal ideal of A and A is a local ring.

Now, suppose that $\mathfrak{m}$ is maximal, and take $x \in A \backslash \mathfrak{m}$. Then the ideal $(x, \mathfrak{m}) = (1)$, so that there exists a $y \in A$, and $t \in \mathfrak{m}$ for which $xy - t = 1$; i.e. $xy = 1 - t$, which makes x a unit. By above, this makes A a local ring. ■

1.5 Eculidian Domains.

Definition. Let A be a commutative ring identity. We call a map $N : A \to \mathbb{N}$, with $N(0) = 0$ a **norm**, or, **degree**. If $N(a) \geq 0$, for all $a \in A$, then we call N **nonnegative** If $N(a) > 0$ for all $a \in A$ then we call N **positive**.

Definition. Let A be a commutative ring with identity, and $N : A \to \mathbb{N}$ a norm. We say thay A is a **Euclidean domain** if for all $a, b \in A$, with $b \neq 0$, there exist elements $q, r \in A$ such that

$$a = qb + r \text{ where } r = 0 \text{ or } N(r) < N(b)$$

We call q the **quotient** and r the **remainder** of a when **divided** by b.

Example 1.7. (1) Let k be any field, and $N : k \to \mathbb{N}$ defined by $N(a) = 0$ for all $a \in k$. Then N makes k into a Euclidean domain. Take $a, b \in k$, with $b \neq 0$, and $q = ab^{-1}$. Then $a = qb + r$ where $r = 0$.

(2) The integers $\mathbb{Z}$ is a Euclidean domain with norm $N(a) = |a|$, the absolute value of a. In fact, the motivation for Euclidean rings comes from the division theorem, or Euclid's theorem for integers.

(3) Let k be a field, and consider $k[x]$. Let $N : k[x] \to \mathbb{N}$ be defined by $N : f \to \deg f$. Then $fisaEuclideandomain.Ifkisnotafield,thenitisnotnecesarilytruethat\mathrm{k[x]}beaEuclideandomain.$

(4) Let $D \in \mathbb{Z}^+$ be squarefree, and consider $\mathbb{Z}[\sqrt{D}]$. Define $N : \mathbb{Z}[\sqrt{D}] = \mathbb{N}$ to be the absolute value of the field norm, that is $N(a + b\sqrt{D}) = \|a + b\sqrt{D}\|^2 = a^2 + Db^2$. We notice that $\mathbb{Z}[\sqrt{D}]$ is an integral domain, but it is not a Euclidean domain. This depends on our choice of D. Let $D = -1$ so tha t $\sqrt{D} = i$, and $i^2 = -1$. Then the Gaussian integers, $\mathbb{Z}[i]$, is a Euclidean domeain. Let $x = a + ib$, $y = c + id$ with $y \neq 0$. In $\mathbb{Q}[i]$, the field of fractions, we have that $\frac{x}{y} = r + is$, where

$$r = \frac{ac + bd}{\|y\|^2} \text{ and } s = \frac{bc - ad}{\|y\|^2}$$

Now, let p and q be the integers closest to r and s, respectively so that

$$|r - p| \leq \frac{1}{2} \text{ and } |s - q| \leq \frac{1}{2}$$

Let $w = (r - p) + i(s - q)$, and take $z = wy$. Then we have $z = x - (p + iq)y$, so that $x = (p + iq)y + z$, moreover, we have $N(w) = (r - p)^2 + (q - s)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. Since $\| \cdot \|$ is multiplicative, we have

$$N(w)N(y) \leq \frac{1}{2}N(y)$$

which makes $\mathbb{Z}[i]$ into a Euclidean domain.

Lemma 1.5.1. *Every ideal in a Euclidean domain A, is a principle ideal.*

Proof. If $I = (0)$, we are done. Now, let $N : A \to \mathbb{N}$ be the norm of A, and consider the image $N(I) = \{N(a) : a \in I\}$. By the well ordering principle, $N(I)$ has a minimum element $N(d)$ for some $d \neq 0$ in I Notice that $(d) \subseteq I$. Now, let $a \in I$. Since A is a Euclidean domain, there exist $q, r \in A$ for which

$$a = qd + r \text{ where } r = 0 \text{ or } N(r) < N(d)$$

Then notice that

$$r = a - qd$$

putting $r \in I$ and $N(r) \in N(I)$. Since $N(d)$ is the minimum element, we must have $r = 0$ so that $a = qd$, which puts $a \in (d)$. Therefore $I = (d)$, making I principle. ∎

Example 1.8. (1) The polynomial ring $\mathbb{Z}[x]$ is not a Euclidean domain. The ideal $(2, x)$ is not principle.

(2) Consider $\mathbb{Z}[\sqrt{-5}]$, i.e. $D = -5$. Suppose the ideal $(3, 2 + \sqrt{-5})$ is a principle ideal, that is $(3, 2+\sqrt{5}) = (a+b\sqrt{-5})$ for some $a, b \in \mathbb{Z}$. Then we get that $3 = x(a+b\sqrt{-5})$ and $2 + \sqrt{-5} = y(a + b\sqrt{-5})$. Then notice that $N(x) = a^2 + 5b^2 = 9$, and since $a^2 + 5b^2 \in \mathbb{Z}^+$, we must have that $a^2 + 5b^2 = 1, 3, 9$.

(i) If $a^2+5b^2 = 9$, then $N(x) = 1$ making $x = \pm 1$ and $a+b\sqrt{-5} = \pm 3$, which cannot happen since $2 + \sqrt{-5}$ is not divisible by 3.

(ii) the equation $a^2 + 5b^2 = 3$ cannot happen since it has no integer solutions. This makes

(iii) $a^2 + b\sqrt{5} = 1$, which makes $(a + \sqrt{-5}) = \mathbb{Z}[\sqrt{-5}]$, moreover, we get the equation $3x + y(2 + \sqrt{-5}) = 1$ for any $x, y \in \mathbb{Z}[\sqrt{-5}]$. Multplying both sides by $2 - \sqrt{-5}$, we get that $3|(2 - \sqrt{-5})$ which is impossible.

In all three cases, we were led to an impossibility, hence $\mathbb{Z}[\sqrt{-5}]$ cannot be a Euclidean domain.

Definition. Let A be a commutative ring with identity, and $a, b \in A$ with $b \neq 0$. We say that b **divides** a if there is an $x \in A$ for which $a = bx$. We write $b|a$. We also say that a is a **multiple** of b.

Definition. Let A be a commutative ring with identity. We call a nonzero element $d \in A$ a **greatest common divisor** of elements $a, b \in A$ if

(1) $d|a$ and $d|b$.

(2) If $c \in A$ is nonzero such that $c|a$ and $c|b$, then $c|d$.

We write $d = (a, b)$.

Lemma 1.5.2. *Let A be a commutative ring with identity. For any $a, b \in A$ a nonzero element $d \in A$ is the greatest common divisor if*

(1) $(a, b) \subseteq (d)$.

(2) If $c \in A$ is nonzero with $(a, b) \subseteq (c)$, then $(d) \subseteq (c)$.

In particular, $d = (a, b)$.

Proof. The first two statements follow from definition, and the last follows lemma 1.5.1. ∎

Lemma 1.5.3. *If A is a commutative ring with identity, and $a, b \in A^*$, such that $(a, b) = (d)$ for some $d \in A^*$, then d is the greatest common divisor of a and b.*

Lemma 1.5.4. *Let A be an inetegral domain. If $c, d \in A$ generate the same principle ideal, i.e. $(d) = (c)$, then $d = uc$ for some unit $u \in A$.*

Proof. If $c = 0$ or $d = 0$, we are done. Suppose then that $c, d \neq 0$. Since $(d) = (c)$, we have that $d = xc$ and $c = yd$ for some $x, y \in A$. Then $d = (xy)d$, which makes $d(1 - xy) = 0$. Since $d \neq 0$, we get $xy = 1$, making x and y units of A. ∎

Definition. We call an integral domain in which every principle ideal is generated by two elements a **Bezout domain**.

Lemma 1.5.5. *Every Euclidean domain is a Bezout domain.*

Theorem 1.5.6 (The Extended Euclidean Algorithm)**.** *Let A be a Euclidean and $a, b \neq 0$ elements of A. Let $d = r_n$ be the least nonzero remainder obtained by dividing a from b recursively $n+1$ times. Then*

(1) $d = (a, b)$ is the greatest common divisor of a and b.

(3) There exist $x, y \in A$ for which $ax + by = d$.

Proof. By lemma 1.5.1, we get that the ideal (a, b) is principle, so there exists a greatest common divisor of a and b. Now, let $d = r_n$ be obtained by dividing a and b recursively $(n+1)$ times. Then the $(n+1)^{st}$ equation gives $r_{n-1} = q_{n+1}r_n$, so that $r_n | r_{n-1}$. Now, by induction on n if $r_n | r + k + 1$ and $r_n | r_k$ then the $(k+1)^{st}$ equation gives $r_{k-1} = q_{k+1}r_k + r_{k+1}$, which implies that $r_n | r_{k-1}$. Therefore we get in the 1^{st} equation that $r_n | b$, and in the 0^{th} that $r_n | a$. That is, $d | a$ and $d | b$.

Now, notice that $r_0 \in (a, b)$ and that $r_1 = b - qr_0 \in (b, r_0) \subseteq (a, b)$. By induction on r_n, if $r_{k-1}, r_n \in (a, b)$ then

$$r_{k+1} = r_{k-1} - q_{k+1}r_k \in (r_{k-1}, r_n) \subseteq (a, b)$$

which puts $r_n \in (a, b)$ making $d = (a, b)$ the greatest common divisor. ■

1.6 Principle Ideal Domains.

Definition. An integral domain A is called a **principle ideal domain (PID)** if every ideal in A is principle.

Example 1.9. (1) Every Euclidean domain is a PID, as dictated by lemma 1.5.1. Hence the rings $\mathbb{Z}$ and $\mathbb{Z}[i]$ are PIDs, however, the polynomial ring $\mathbb{Z}[x]$ is not principle, recall the ideal $(2, x)$.

(2) The ring $\mathbb{Z}[\sqrt{-5}]$ is not a PID, consider the ideal $(3, 2 + \sqrt{-5})$. However, notice that $(3, 1 + \sqrt{-5})(3, 1 - \sqrt{-5}) = (3)$ is principle, despite $(3, 1 + \sqrt{-5})$ and $(3, 1 - \sqrt{-5})$ are not principle.

(3) The ring $\mathbb{Z}[1 + \frac{\sqrt{-19}}{2}]$ is a PID, but not a Euclidean domain.

Lemma 1.6.1. *Let A be a principle ideal domain and let d be a generator for the ideal (a, b), for $a, b \in A$. Then the following are true.*

(1) $d = (a, b)$; i.e. d is the greatest common divisor of a and b.

(2) There exist $x, y \in A$ for which $ax + by = d$.

(3) d is unique up to unit.

Lemma 1.6.2. *Every nonzero prime ideal in a principle ideal domain A is maximal.*

Proof. Let $(p) \neq (0)$ be a prime ideal of A. Let (m) be an ideal of A containing (p). Then $p \in (m)$ so that $p = rm$ for some $r \in A$. Now, since p is prime, and $rm \in (p)$, then either $r \in (p)$ or $m \in (p)$. If $m \in (p)$, then $(p) = (m)$. Otherwise, if $r \in (p)$, then $r = ps$ for some $s \in A$. Then $p = rm = pms = p(ms)$ which makes $ms = 1$, hence m is a unit, which makes $(m) = (0)$. ∎

Corollary. *If A is any commutative ring, such that the polynomial ring $A[x]$ is a principle ideal domain, then A is necessarily a field.*

Proof. If $A[x]$ is a PID, then $A \subseteq A[x]$, as a subring, must be an integral domain. Consider now, the ideal (x), then $A[x]/(x) \simeq A$ which makes (x) prime by lemma 1.4.4. Therefore (x) is maximal, which then makes A a field by lemma 1.4.3. ∎

Definition. Let A be a commutative ring, and $N : A \to \mathbb{N}$ a norm. We call N a **Dedekin-Hasse norm** if N is a positive norm suc that for all $a, b \in N$, either $a \in (b)$, or there exists an element $c \in (a, b)$ such that $N(c) < N(b)$.

Lemma 1.6.3 (The Dedekin-Hasse Criterion)**.** *An integral domain A is a PID if, and only if it has a Dedekin-Hasse norm.*

Proof. Let $\mathfrak{b} \neq (0)$ an ideal of A. Let $a \in \mathfrak{b}$ a nonzero element, so that $(a, b) \subseteq \mathfrak{b}$. Since N is Dedekin-Hasse, and by minimality of b, we get that $a \in (b)$ so that $\mathfrak{b} = (b)$ is principle. ∎

Example 1.10. Consider the ring $\mathbb{Z}[1 + \frac{\sqrt{-19}}{2}]$. With norm $N = \|\cdot\|^2$ the field norm. Let $x, y \in \mathbb{Z}[1 + \frac{\sqrt{-19}}{2}]$ be nonzero elements and that $\frac{x}{y} \notin \mathbb{Z}[1 + \frac{\sqrt{-19}}{2}]$. Write

$$\frac{x}{y} = \frac{a + b\sqrt{-19}}{c} \in \mathbb{Q}[1 + \frac{\sqrt{-19}}{2}]$$

where a, b, c are all coprime, with $c > 1$. Then there are integers u, v, w with $av + bu + cw = 1$, then $au - 19bv = cq + r$ for some quotient q and remainder r with $N(r) \leq \frac{c}{2}$ and let $s = u + v\sqrt{-19}$ and $t = q - w\sqrt{-19}$. Then we find that

$$0 < N(\frac{x}{y}s - t) \leq \frac{1}{4} + \frac{19}{c^2}$$

Then $s = 1, t = \frac{(a-1)+b\sqrt{-19}}{2} \in A$ satisfy $0 < N(\frac{x}{y}s - t)$

Now, suppose that $c = 3$, then $3 \nmid (a^2 + 19b^2)$. Then $a^2 + 19b^2 = 3q + r$ with $r = 1$ or $r = 2$. Then $s = a - b\sqrt{-19}, t = q$ statisfy $0 < N(\frac{x}{y}s - t)$. Finally, for $c = 4$, with a, b not both even, so that $a^2 + 19b^2$ is odd. Then $a^2 + 19b^2 = 4q + r$ so for $q, r \in \mathbb{Z}$ with $0 < r < 4$, then $s = a - b\sqrt{-19}, t = q$ satisfy $0 < N(\frac{x}{y}s - t)$. Now, if both a and b are odd, then $a^2 + 19b^2 \equiv 1 + 3 \mod 8$ so taht $a^2 + 19b^2 = 8q + 4$ for some $q \in \mathbb{Z}$, then

$$s = \frac{a - b\sqrt{-19}}{2} \text{ and } t = q$$

satisfy $0 < N(\frac{x}{y}s - t)$.

1.7 Unique Factorization Domains.

Definition. Let A be an integral domain. A nonzero element $r \in A$ that is not an associate is called **irreducible** if whenever $r = ab$, then either a or b are units in A; otherwise, we call r **reducible**.

Definition. Let A be an integral domain. An element $p \in A$ is called **prime** if the ideal (p) is a prime ideal. That is p is not a unit and whenever $p|ab$, then either $p|a$ or $p|b$. We call two elements $a, b \in A$ **associates** if $a = ub$ for some unit $u \in A$.

Lemma 1.7.1. *In an integral domain, a prime element is always irreducible.*

Proof. Let (p) be a nonzero prime ideal with $p = ab$, for some $a, b \in A$. Then $ab \in (p)$, so that either $a \in (p)$, or $b \in (p)$. Suppose that $a \in (p)$. Then $a = pr$ for some $r \in A$, so that $p = (pr)b = p(rb)$, so that $rb = 1$. This makes b a unit. Similarly, we see that a is a unit if $b \in (p)$. In either case, p is irreducible. ■

Example 1.11. (1) In the ring $\mathbb{Z}$ of integers, those elements which are irreducible are precisely those which are prime, since the ideals $2\mathbb{Z}, 3\mathbb{Z}, \dots, p\mathbb{Z}, \dots,$ for p a prime number are also the prime ideals of $\mathbb{Z}$

(2) Irreducible elements need not be prime. The element $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible, as was shown in example 1.8, however it is not prime. Notice that $3|9 = (2+\sqrt{-5})(2-\sqrt{-5})$, but $3 \nmid (2+\sqrt{-5})$ and $3 \nmid (2-\sqrt{-5})$.

Lemma 1.7.2. *In a principle ideal domain, a nonzero element is prime if, and only if it is irreducible.*

Proof. Let A be a PID, and suppose that p is irreducible. Let (m) be the principle ideal containing (p), then $p = rm$, and by irreducibility, either r or m are units, in either case, we get that either $(p) = (m)$ or $(m) = (1)$. This makes (p) a maximal ideal, and hence a prime ideal. ■

Example 1.12. (1) Since 3 is not prime in $\mathbb{Z}[\sqrt{-5}]$, then (3) is not a prime ideal in this ring. Therefore $\mathbb{Z}[\sqrt{-5}]$ cannot be a PID.

(2) Notice that since $\mathbb{Z}$ is a PID, then the fact that irreducible and prime elements coincide is guaranteed by lemma 1.7.2.

Definition. We call an integral domain A a **unique factorization domain (UFD)** if for every nonzero element $r \in A$ which is not a unit, the following are true.

(1) r can be written as the product of, not necessarily distinct, irreducible elements. We call this product the **factorization** of r.

(2) The factorization of r is unique up to associates.

Example 1.13. (1) All fields are unique factorization domains.

(2) Polynomial rings are unique factorization domains whenever the ground ring A is a unique factorization domain.

(3) The subring $\mathbb{Z}[2i]$ of $\mathbb{Z}[i]$ is an integral domain, but it is not a UFD. Notice that both 2 and $2i$ are irreducible in $\mathbb{Z}[2i]$, but that $4 = 2 \cdot 2 = (2i) \cdot (-2i)$.

(4) $\mathbb{Z}[\sqrt{-5}]$ is another example of an integral domain that is not a UFD.

Lemma 1.7.3. *In a unique factorization domain A, a nonzero element is prime if, and only if it is irreducible.*

Proof. Since prime elements are irreducible, it remains to show that irreducible elements are prime. Let p be irreducible and suppose that $p|ab$, for $a, b \in A$. Then $ab = pc$ for some $c \in A$. Writing ab as a product of irreducibles, since A is a UFD, p must be associate to one of the irreducibles in the factorization of a, or to one in the factorization of b. In either case, we get that $p|a$ or $p|b$, and hence p is prime. ■

Lemma 1.7.4. *Let $a, b \in A$ nonzero elements of a unique factorization domain A. If $a = up_1^{e_1} \dots p_n^{e_n}$ and $b = vp_1^{f_1} \dots p_n^{f_n}$, where $u, v \in A$ are units, then the element*

$$d = p_1^{\min\{e_1,f_1\}} \dots p_n^{\min\{e_n,f_n\}}$$

os the greatest common divisor of a and b.

Proof. Notice that by definition of d, that $d|a$ and $d|b$. Now, let c be a common divisor of a and b with the unique prime factorization $c = q_1^{g_1} \dots q_m^{g_m}$. Since $q_i|c$ for each $1 \leq i \leq m$, then $q_i|p_j$ for each prime factor in the factorizations of a and b. Since both q_i and p_j are irreducible, they are associates. That implies that the primes of c are the primes of a and b. Moreover notice that since each $g_i \leq e_i, f_i$, that $c|d$, and so $d = (a, b)$. ■

Definition. Let A be a principle ideal domain. Let $\{a_n\}$ a sequence of elements of A. We call the increasing sequence of ideals $\{(a_n)\}$ an **infinite ascending chain** of ideals in A and write

$$(a_1) \subseteq (a_2) \subseteq \cdots \subseteq (a_n) \subseteq \cdots \subseteq A$$

We say that the infinite ascending chain $\{(a_n)\}$ **stabalizes** if for some $k \geq n$, we have $(a_n) = (a_k)$.

Lemma 1.7.5. *In any principle ideal domian, infinite ascending chains of ideals stabalize.*

Proof. Let $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \cdots \subseteq A$ an infinite ascending chain of ideals and let $\mathfrak{a} = \bigcup \mathfrak{a}_k$. Then $\mathfrak{a}$ is an ideal in A, and since A is a PID, $\mathfrak{a} = (a)$ for some $a \in A$. This makes $a \in \mathfrak{a}_n$ for some n, and hence $\mathfrak{a}_n \subseteq \mathfrak{a}$. This makes $\mathfrak{a}_n = \mathfrak{a}$ for some $n \geq 1$, and hence this chain stabalizes. ■

Theorem 1.7.6. *Every principle ideal domain is a unique factorization domain.*

Proof. Let A be a PID, and $r \in A$ a nonzero element which is not a unit. If r is irreducible, we are done. Otherwise, we have $r = r_1 r_2$ fr some $r_1, r_2 \in A$. Now, if both r_1 and r_2 are irreducible, we are done. Suppose then, without loss of generality, thart r_1 is reducible. Then

$r_1 = r_{11}r_{12}$, and if both r_{11} and r_{12} are irreducible, we are done. Suppose then that r_{11} is reducible; continuing this process, we arrive at an infinite ascending chain of ideals

$$(r) \subseteq (r_1) \subseteq (r_{11}) \subseteq \cdots \subseteq A$$

and since A is a PID, this chain stabalizes. Thus r can be factored into irreducible elements; since this process terminates.

Now, by induction on n, for $n = 0$, we notice that r is a unit, and we are done. Suppose, then for $n \geq 1$, that $r = p_1 \dots p_n = q_1 \dots q_m$ for some $m \geq n$, and where each p_i and q_j are (not necessarily distinct) irreducibles for all $1 \leq i \leq n$ and $1 \leq j \leq m$. Notice that $p_1 | q_1 \dots q_m$, and so $p_1 | q_j$ for some j. This makes p_1 and q_j associates; i.e. $q_j = p_1 u$, with $u \in A$ a unit. Cancelling the p_1 from both sides of the equation, we get $p_2 \dots p_n = q_1 \dots q_{j-1} q_{j+1} \dots q_m$. Repeating this process, we get a 1–1 correspondence between associates, and hence the factorization of r is unique up to associates. Therefore A is a UFD. ■

Corollary. *Every Euclidean domain is a unique factorization domain.*

Proof. Notice that Euclidean domains are PIDs by lemma 1.5.1. ■

Corollary (The Fundamental Theorem of Arithmetic)**.** $\mathbb{Z}$ *is a unique factorization domain.*

Proof. Notce that $\mathbb{Z}$ is a Euclidean domain. ■

Corollary. *There exists a multiplicative Dedekind-Hasse norm on A.*

Proof. If A is a PID, then the theorem tells us it is a UFD. Define the norm $N : A \to \mathbb{N}$ by taking $0 \to 0$, $u \to 1$ if u is a unit, and $a \to 2^n$ where $a = p_1 \dots p_n$, where each p_i is irreducible. Notice that for every $a, b \in A$, $N(ab) = N(a)N(b)$. Now, suppose further that $a, b \neq 0$ and consider the ideal $(a, b) = (r)$, for some $r \in A$. UIf $a \notin (b)$, nether is r, and hence $b \nmid r$. Now, since $b = xr$, $x \in A$, then x cannot be a unit in A, so that $N(b) = N(xr) = N(x)N(r) > N(r)$. This completes the proof. ■

Bibliography

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

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