# MATH RI: ADVANCED ALGEBRA I (RINGS AND IDEALS)

HEESUNG YANG

Abstract. This notes covers ring theory of the first half of Dalhousie's algebra comprehensive exam syllabus which is not covered in Advanced Algebra I (MATH 5045). This notes will cover Chapters VII.1–VII.6 (Basic ring theory), and the first half of Chapter VIII.2 (Principal ideal domains) of Dummit & Foote. Some propositions and lemmas are from the past comprehensive exams; the proofs of those lemmas and propositions are included in this notes as well.

## 1. Chapter VII.1: Introduction to Rings

**Definition 1.1.** A *ring* $R$ is a set with two binary operations called addition $(+)$ and multiplication $(\cdot)$ such that

(1) $\langle R, + \rangle$ is an abelian group
(2) $\cdot$ is associative (i.e., $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$)
(3) $\cdot$ and $+$ are distributive over one another (i.e., $a(b+c) = ab+ac$ and $(a+b)c = ac+bc$).

**Definition 1.2.** A ring $R$ is *commutative* if $ab = ba$ for all $a, b \in R$. Otherwise a ring $R$ is *non-commutative*. A ring $R$ *has a unity* (or *has an identity*) if $\cdot$ has an identity, which we call it 1 (i.e., $1 \in R$ and $1 \cdot a = a$ for all $a \in R$). An element $a \in R$ is a *unit* if there exist a left multiplicative inverse $a'$ and a right multiplicative inverse $a''$ such that $a'a = aa'' = 1$.

*Example.* $\mathbb{Z}, \mathbb{R}$, and $\mathbb{Z}[x]$ are examples of (commutative) rings. $M_2(\mathbb{Z})$, the $2 \times 2$-matrix ring over $\mathbb{Z}$ is a (non-commutative) ring.

**Proposition 1.1.** *$a' = a''$. In other words, a left multiplicative inverse of $a$ and a right multiplicative inverse of $a$ are the same.*

*Proof.* $a'a = 1$, so $a'aa'' = a''$. Thus $a' = a''$. □

**Definition 1.3.** A ring $R$ with unity $1 \neq 0$ is a *division ring* if every non-zero element $a \in R$ has a multiplicative inverse, i.e., for any $a \in R$ there is $b \in \mathbb{R}$ such that $ab = ba = 1$. Therefore, a *field* is a commutative division ring.

**Proposition 1.2** (Additional properties of a ring)**.** *Let $R$ be a ring.*

*(1) $0a = a0 = 0$ for all $a \in R$.*
*(2) $(-a)b = a(-b) = -(ab)$ for all $a, b \in R$, where $-a$ is the additive inverse of $a$.*
*(3) $(-a)(-b) = ab$ for all $a, b \in R$.*
*(4) If $R$ has unity 1, then the unity is unique and $-a = (-1)a$.*

**Definition 1.4.** A non-zero element $a \in R$ is a *zero-divisor* if there exists $b \neq 0 \in R$ such that $ab = 0$ or $ba = 0$. If $R$ is commutative, has unity 1, and has no zero-divisors, then $R$ is an *integral domain* (or *domain* in short). A *field* is an integral domain in which every non-zero element is a unit.

*Date*: 7 April 2019.

*Example.* $\mathbb{Z}$ is a commutative ring with unity 1 and units $\pm 1$. $\mathbb{Z}$ has no zero divisors. Thus $\mathbb{Z}$ is an integral domain. On the other hand, $\mathbb{Z}/6\mathbb{Z}$ has unity 1 and the units are $1, 5$. However, $\mathbb{Z}/6\mathbb{Z}$ has three zero divisors, namely $2, 3, 4$. Notice that $2 \cdot 3 = 4 \cdot 3 = 0$. Therefore $\mathbb{Z}/6\mathbb{Z}$ is not an integral domain.

*Example.* $\mathbb{Z}/p\mathbb{Z}$ for $p$ prime, $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{C}(x)$ are examples of fields.

**Proposition 1.3.** *Units cannot be zero divisors.*

*Proof.* Let $a$ be a unit, and suppose that there exists a non-zero $b$ such that $ab = 0$. Since $a$ is a unit, there exists $c$ such that $ca = 1$. Thus we have $b = 1b = (ca)b = c(ab) = c0 = 0$, but this contradicts the fact that $b$ is non-zero. Thus $a$ cannot be a left zero-divisor. Now suppose that there is $b'$ such that $b'a = 0$. Since $a$ is a unit, we have $ac = 1$. (We use the same $c$ thanks to Proposition 1.1.) Then $b' = b'1 = b'(ac) = (b'a)c = 0c = 0$, which again contradicts the fact that $b'$ is non-zero. Therefore no unit can be a zero divisor as required. □

**Proposition 1.4** (Cancellation property of integral domains)**.** *Let $R$ be a ring, and let $a, b, c \in R$ such that $a$ is not a zero divisor in $R$. If $ab = ac$, then either $a = 0$ or $b = c$. Therefore, if $R$ is an integral domain, and $ab = ac$, then we have $a = 0$ or $b = c$.*

*Proof.* If $ab = ac$, then $ab - ac = a(b - c) = 0$ per the distributive law. However, since $a$ is not a zero divisor, we have $a = 0$ or $b - c = 0$, as required. The second statement follows upon noting that integral domains cannot have zero divisors. □

**Corollary 1.1.** *Any finite integral domain is a field.*

*Proof.* Let $R$ be a finite integral domain, and let $a \in R \setminus \{0\}$. Clearly the map $x \mapsto ax$ is an injection due to the cancellation property. The map is also surjective as $R$ is finite. Thus $x \mapsto ax$ is a bijection, so there must exist an inverse map – thus there exists $b \in R$ so that $ba = 1$. Therefore $R$ is a field. □

**Theorem 1.1** (Wedderburn's little theorem)**.** *Any finite division ring is a field.*

**Definition 1.5.** A *subring* $S$ of the ring $R$ is a subgroup of $R$ that is closed under multiplication.

*Example.* $\mathbb{Z}$ is a subring of $\mathbb{Q}$; $\mathbb{Q}$ is a subring of $\mathbb{R}$.

*Example.* $n\mathbb{Z}$ for any $n \in \mathbb{Z}$ is a subring of $\mathbb{Z}$. However, $\mathbb{Z}/n\mathbb{Z}$ is *not* a subring of $\mathbb{Z}$ for any $n \geq 2$.

*Example.* The ring of all differentiable functions from $\mathbb{R}$ to $\mathbb{R}$ is a subring of the ring all continuous functions from $\mathbb{R}$ to itself. Both of these rings are subrings of the ring of all functions from $\mathbb{R}$ to itself.

*Example.* Let $K$ be a number field (i.e., any finite-dimensional field extension over $\mathbb{Q}$), and let $\mathcal{O}_K$ be the set of elements in $K$ whose minimal polynomial is monic. Then $\mathcal{O}_K$ is a subring of $K$; more specifically, $\mathcal{O}_K$ is called the ring of integers of $K$. (To see where this name comes from, consider the rational integer counterpart: note that $x - a = 0$ is the minimal polynomial of $a$ for any $a \in \mathbb{Z}$; for any $b = p/q \in \mathbb{Q} \setminus \mathbb{Z}$ where $\gcd(p, q) = 1$, the minimal polynomial is $qx - p = 0$ and cannot be monic.) For more information, please refer to the PMATH 641 (Algebraic number theory) course notes and the MATH 5055 (Galois theory) course notes.

**Proposition 1.5** (Subring test)**.** *Suppose $R$ is a ring, and that $S$ is a* non-empty *subset of $R$. If $a - b, ab \in S$ for any $a, b \in S$, then $S$ is a subring of $R$.*

## 2. Chapter VII.2: Some examples of rings

### 2.1. Polynomial rings

**Definition 2.1.** Let

$$R[x] := \{a_n x^n + \cdots + a_1 x + a_0 : n \geq 0, a_n \neq 0, a_i \in R\},$$

where $R$ is a commutative ring with unity $1 \neq 0$. Then $a_n x^n + \cdots + a_1 x + a_0$ is said to be a *polynomial in $x$ with coefficients in $R$.* Then $R[x]$ is the *ring of polynomials (or polynomial ring) in the variable $x$ with coefficients in $R$*, where addition and multiplication are the same as the standard addition and multiplication.

*Remark.* Clearly $R$ is a subring of $R[x]$, and any element in $R$ is a constant polynomial. Since we assume that $R$ is a commutative ring with unity $1 \neq 0$, the polynomial ring $R[x]$ is also a commutative ring with unity 1, where the unity is the same 1 from $R$.

**Proposition 2.1.** *Let $R$ be an integral domain, and let $p(x), q(x)$ be non-zero elements of $R[x]$. Then*

*(1) $R[x]$ is an integral domain;*
*(2) $\deg pq = \deg p + \deg q$; and*
*(3) the units of $R[x]$ are precisely the units of $R$.*

*Proof.* Let $\deg p = n$ and $\deg q = m$. Thus the leading term of $p(x)$ is $a_n x^n$; the leading term of $q(x)$ is $b_m x^m$. Thus the leading term of $p(x)q(x)$ is $a_n b_m x^{n+m}$. Since $R$ is an integral domain, $a_n b_m \neq 0$. (Note that $R$ has no zero divisors, and neither $a_n$ nor $b_m$ can be zero.) This proves both the first part and the second part. For the third part, suppose that $p(x)q(x) = 1$. By the second part we see $\deg pq = \deg p + \deg q = 0$; since $\deg p \geq 0$ for any polynomial $p(x) \in R[x]$, it follows that $\deg p(x) = \deg q(x) = 0$. Therefore $p(x), q(x) \in R$ as required. □

*Remark.* If $R$ has zero divisors (e.g., $\mathbb{Z}/6\mathbb{Z}$), then $R[x]$ also has zero divisors.

**Proposition 2.2.** *Let $R$ be a commutative ring with unity $1 \neq 0$, and $R[x]$ the polynomial ring of $R$. Let $p(x) = a_n x^n + \cdots + a_1 x + a_0$. Then the following are equivalent:*

*(i) $p(x)$ is a zero divisor in $R[x]$.*
*(ii) there exists a non-zero $c \in R$ such that $cp(x) = 0$.*

*Proof.* ((i) ⇒ (ii)) Suppose that $q(x) = b_m x^m + \cdots + b_1 x + b_0$ is a non-zero polynomial of the least degree such that $p(x)q(x) = 0$. Then we have $a_n b_m = 0$. Clearly $b_m \neq 0$ since $q(x)$ is of the least degree satisfying the desired property. Hence $\deg a_n q(x) < m$, and $(a_n q(x))p(x) = a_n q(x)p(x) = 0$. This forces $a_n q(x) \equiv 0$, and hence $a_n b_{m-1} = 0$. Note that the coefficient of $x^{m+n-1}$ of $p(x)q(x)$ is $a_{n-1}b_m + a_n b_{m-1}$ which is equal to 0. But then $a_n b_{m-1} = 0$ so $a_{n-1}b_m = 0$. Hence $\deg a_{n-1}q(x) < m$, so $a_{n-1}q(x) \equiv 0$. This implies $a_{n-1}b_{m-1} = 0$; and the coefficient of $x^{n+m-2}$ of $pq$ is $a_{n-1}b_{m-1} + a_{n-2}b_m + a_n b_{m-2}$, which must equal 0. Thus $a_{n-2}b_m + a_n b_{m-2} = 0$. But then $a_n q(x) \equiv 0$, so $a_n b_{m-2} = 0$. Hence $a_{n-2}b_m = 0$. Repeating this argument, we see that $a_i b_m = 0$ for all $0 \leq i \leq n$, so $b_m p(x) = 0$ as desired.

((ii) ⇒ (i)) This direction is immediate. □

*Remark.* Suppose that $S$ is a subring of $R$. Then the polynomial ring $S[x]$ is also a subring of the polynomial ring $R[x]$.

### 2.2. **Matrix rings**

For any ring $R$ and a positive integer $n$, we can define $M_n(R)$, the set of all $n \times n$ matrices with entries from $R$. With the usual matrix addition and multiplication operation, $M_n(R)$ has a ring structure. Such ring is called a *matrix ring*. For any non-trivial ring $R$, the matrix ring $M_n(R)$ is non-commutative for any $n \geq 2$ (whether $R$ is commutative or not) because the matrix multiplication itself is not commutative. Also, $M_n(R)$ cannot be an integral domain either as it is possible to construct two non-zero square matrices with 1 or 0 for each entry whose product is the zero matrix.

We examine some subrings of $M_n(R)$. It is straightforward to verify that the set of scalar matrices ($a \in R$ on all diagonal entries, 0 everywhere else) is a subring of $M_n(R)$. Particularly, if $a = 1$, then that matrix serves as the unity of $M_n(R)$. Thus $M_n(R)$ has a unity if and only if $R$ has unity as well. Notice that the subring of scalar matrices is a subset (and also a subring) of the set of upper triangular matrices, which is again not that hard to verify that this is a subring of $M_n(R)$. This example serves to demonstrate that the "the subring of" relation is transitive. The ring of scalar matrices is a subring of the ring of upper triangular matrices; the ring of upper triangular matrices is a subring of $M_n(R)$; and the ring of scalar matrices is a subring of $M_n(R)$.

Note that as long as $\det(A) \neq 0$, $A$ is invertible. Thus, the group of units of $M_n(R)$ is $\mathrm{GL}_n(R) = \{A \in M_n(R) : \det(A) \neq 0\}$, also known as the general linear group of degree $n$ over $R$.

Finally, if $S$ is a subring of $R$, $M_n(S)$ is always a subring of $M_n(R)$.

### 2.3. **Group rings**

**Definition 2.2.** Let $R$ be a commutative ring with unity $1 \neq 0$, and suppose that $G$ is a finite group, say $G = \{g_1, g_2, \ldots, g_n\}$ whose operation is written multiplicatively. Then the *group ring* $R[G]$ of $G$ with coefficients in $R$ is

$$R[G] := \{a_1 g_1 + \cdots + a_n g_n : a_i \in R\},$$

with the addition and multiplication defined as follows:

$$(a_1 g_1 + \cdots + a_n g_n) + (b_1 g_1 + \cdots + b_n g_n) = (a_1 + b_1) g_1 + \cdots + (a_n + b_n) g_n$$

$$(a_1 g_1 + \cdots + a_n g_n)(b_1 g_1 + \cdots + b_n g_n) = \sum_{k=1}^{n} \left( \sum_{g_i g_j = g_k} a_i b_j \right) g_k.$$

We shall write $a_1 g_1 = a_1$ if $g_1$ is the identity in $G$; similarly, we write $1 g_i = g_i$ for any $g_i \in G$ where 1 is the unity in $R$. Therefore, the 1 in $R$ is the unity in $R[G]$ also.

*Remark.* It is a routine exercise to check that these operations indeed form a ring. Also note that the associativity of multiplication follows from the associativity of the group operation in $G$.

*Example.* Suppose that $G = D_8 = \langle r, s : r^4 = s^2 = 1, rs = sr^{-1} \rangle$, and let $R = \mathbb{Z}$. Then the elements $\alpha = r^2 + r - 2s$ and $\beta = -3r^2 + rs$ are in the group ring $\mathbb{Z}[D_8]$. Then we have

$$\alpha + \beta = r - 2x^2 - 2s + rs$$

$$\begin{aligned}\alpha\beta &= (r + r^2 - 2s)(-3r^2 + rs)\\ &= -3r^3 + r^2s - 3 + r^3s + 6r^2s - 2r^3\\ &= -3 - 5r^3 + 7r^2s + r^3s,\end{aligned}$$

so indeed $\alpha + \beta, \alpha\beta \in \mathbb{Z}[D_8]$.

Now we explore some properties of group rings.

**Proposition 2.3.** *Let $R$ be a commutative ring with unity $1 \neq 0$, and let $G$ be a finite group. Then the group ring $R[G]$ is commutative if and only if $G$ is an abelian group.*

*Proof.* □

**Proposition 2.4.** *$G$ is a subgroup of the group of units of $R[G]$.*

*Proof.* Note that, for any $g \in G$ we have $1_R g = g$. Thus the multiplication operation of $R[G]$ restricted to $G$ is just the usual group operation defined in $G$. But then since $G$ itself is a group, every $g$ has an inverse, which is a multiplicative inverse in $R[G]$ as well. Thus $g$ is in the group of units of $R[G]$, as required. □

**Proposition 2.5.** *If $\#G > 1$, then $R[G]$ is not an integral domain.*

*Proof.* We will prove that $R[G]$ must have a zero-divisor if $\#G =: m > 1$. Let $g \in G$. Then note that $1 - g \in R[G]$ and $1 + g + g^2 + \cdots + g^{m-1} \in R[G]$, and that

$$(1 - g)(1 + g + g^2 + \cdots + g^{m-1}) = 1 - g^m.$$

But then $g^m = 1$ since $\#G = m$, so actually $(1-g)(1+g+\cdots+g^{m-1}) = 0$. Since $1-g \in R[G]$ is a zero-divisor, $R[G]$ cannot be an integral domain. □

**Proposition 2.6.** *Suppose that $R$ is a commutative ring with unity $1 \neq 0$, and that $S$ is a subring of $R$. If $G$ is a finite group, then $S[G]$ is a subring of $R[G]$. If $H$ is a subgroup of $G$, then $R[H]$ is a subring of $R[G]$.*

## 3. Chapter VII.3: Ring homomorphisms and quotient rings

**Definition 3.1.** Let $R$ and $S$ be rings. Then $\varphi : R \to S$ is a *ring homomorphism* if the following axioms are satisfied for all $a, b \in R$:

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$
(ii) $\varphi(ab) = \varphi(a)\varphi(b)$

Additionally, if $\varphi$ is:

(1) surjective, then $\varphi$ is a *ring epimorphism.*
(2) injective, then $\varphi$ is a *ring monomorphism.*
(3) a ring homomorphism to itself (i.e., $R = S$), then $\varphi$ is a *ring endomorphism.*
(4) bijective, then $\varphi$ is a *ring isomorphism.*
(5) both a ring isomorphism and a ring endomorphism, then $\varphi$ is a *ring automorphism.*

*Remark.* Some textbooks stipulate that a ring homomorphism must preserve unity (i.e., $\varphi(1_R) = 1_S$ where each of $1_R$ and $1_S$ denotes the multiplicative identity of $R$ and $S$, respectively). Since Dummit & Foote does not have this stipulation, we shall assume that a unity may not be preserved.

*Example.* Suppose $\varphi : \mathbb{Z}[x] \to \mathbb{Z}$ is defined as $\varphi(p(x)) = p(0)$. This is a ring homomorphism. Suppose that $p(x)$ has constant term $a$ and $q(x)$ has constant term $b$ (i.e., $p(0) = a, q(0) = b$). Then $(p+q)(0) = a + b = p(0) + q(0)$ and $(pq)(0) = ab = p(0)q(0)$, preserving the ring structure. Particularly, $\ker \varphi$ consists of all the polynomials whose constant term is 0. Note that $\operatorname{im} \varphi = \varphi(\mathbb{Z}[x]) = \mathbb{Z}$ (i.e., $\varphi$ is surjective), since for any $a \in \mathbb{Z}$ you can let $p(x) = x + a$. Therefore $\varphi$ is an example of a ring epimorphism.

*Example.* The following example shows that we must take caution to verify that *both addition and multiplication* are preserved. Suppose that $\varphi_n : \mathbb{Z} \to \mathbb{Z}$ is defined as $\varphi_n(x) = nx$. $\varphi_n(x)$ is an *additive group homomorphism* since $\varphi_n(x+y) = n(x+y) = nx + ny = \varphi_n(x) + \varphi_n(y)$, for any $n$. However, $\varphi_n$ does not preserve multiplication unless $n = 0$ or $n = 1$. We have $\varphi_n(xy) = nxy$ whereas $\varphi_n(x)\varphi_n(y) = (nx)(ny) = n^2xy$. If $n = 0$ or $n = 1$, then $\varphi_n$ is either the zero map (if $n = 0$) or the identity map (if $n = 1$) – so in these two cases, $\varphi_n$ is a ring homomorphism. Otherwise, $n^2 \neq n$ so $\varphi_n$ does not preserve multiplication. Therefore $\varphi_n$ is *not a ring homomorphism* if $n \neq 0, 1$.

*Example.* $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic as rings. Suppose that $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$ is an isomorphism, and let $\varphi(2) =: a$. Then $\varphi(4) = \varphi(2+2) = 2a$ whereas $\varphi(4) = \varphi(2 \cdot 2) = \varphi(2)^2 = a^2$. Hence we must have $a^2 = 2a$, and this is possible only when $a = 0$ or $a = 2$. Clearly $2 \notin 3\mathbb{Z}$, so $a = 0$. But then $2\mathbb{Z}$ is generated by 2, and $\varphi(2) = 0$, so $\varphi$ must be the zero map. But this is impossible since neither $2\mathbb{Z}$ nor $3\mathbb{Z}$ are the zero sets. Hence $2\mathbb{Z}$ and $3\mathbb{Z}$ cannot be isomorphic as rings.

*Example.* We want to find all the ring homomorphisms from $\mathbb{Z}$ to $\mathbb{Z}/20\mathbb{Z}$. Suppose that $f : \mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}$. Since $\mathbb{Z} = (1)$, the behaviour of $f$ is completely determined by how $f$ affects 1. First and foremost, any ring homomorphism must be an additive group homomorphism, so $\langle f(1) \rangle \subseteq \mathbb{Z}/20\mathbb{Z}$ must be an additive subgroup. Also, note that $f(1) = f(1 \cdot 1) = f(1)^2$, so we must have $f(1)^2 = f(1)$ also. $\mathbb{Z}/20\mathbb{Z}$ is cyclic, so any of its subgroups is also cyclic. In particular, $\langle 0 \rangle, \langle 1 \rangle, \langle 2 \rangle, \langle 4 \rangle, \langle 5 \rangle, \langle 10 \rangle$ are the subgroups of $\mathbb{Z}/20\mathbb{Z}$.

(1) $\langle f(1) \rangle = \{0\}$

In this case, $f(1) = 0$, so the ring homomorphism obtained from this case is necessarily the zero map.

(2) $\langle f(1) \rangle = \langle 1 \rangle = \mathbb{Z}/20\mathbb{Z}$.

In this case $f(1) = 1$, so we have $f(k) = f(1 + 1 + \cdots + 1) = k$; similarly, $0 = f(0) = f(k + (-k)) = f(k) + f(-k) = k + f(-k)$, so $f(-k) = -k$. Hence in this case, $f(z) = z \pmod{20}$. Thus, if we are to take the convention that any ring homomorphism must preserve the unity, this is the only ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}/20\mathbb{Z}$.

(3) $\langle f(1) \rangle = \langle 2 \rangle$.

First we need $f(1)$ such that $f(1)^2 = f(1)$. We need $f(1)^2$ and $f(1)$ to share the same unit digit, so the only possible options are $6, 10$ and $16$. However $6^2 \not\equiv 6, 10^2 \not\equiv 10$ but $16^2 \equiv 16 \pmod{20}$. $f(1) = 16$, so $f(k) = 16k$. Hence $f(k) = f(1 \cdot k) = f(1)f(k) = 16f(k) = 256k \equiv 16k \pmod{20}$, so 16 is the multiplicative identity.

(4) $\langle f(1) \rangle = \langle 4 \rangle$.

First we need $f(1)$ such that $f(1)^2 = f(1)$. We need $f(1)^2$ and $f(1)$ to share the same unit digit, so the only possible option is 16. So this case yields the same isomorphism as the $\langle 2 \rangle$ case.

(5) $\langle f(1)\rangle = \langle 5\rangle$

In this case, only 5 and 15 have $5^2 \equiv 5, 15^2 \equiv 15$, so $f(1)$ may be either 5 or 15. Note that $f(1)$ must be the multiplicative identity of $\langle 5\rangle$ since $f(m) = f(1\cdot m) = f(1)f(m)$ for any $m \in \mathbb{Z}$. But note that $15\cdot 5 = 75 \equiv 15 \neq 5$, so 15 cannot be the multiplicative identity. Hence $f(1) = 5$. Indeed we see that $f(m) = 5m$, from which we have $f(m) = f(1 \cdot m) = f(1)f(m) = 5f(m) = 25f(m) \equiv 5f(m) \pmod{20}$ as required.

(6) $\langle f(1)\rangle = \langle 10\rangle = \{0, 10\}$.

Since $f(1) \neq 10$ (because we already know $f(1)^2 = 100 \equiv 0 \not\equiv 10 \pmod{20}$), $f(1) = 0$. Thus the zero map is the only possible choice, meaning that no ring homomorphism can have $\langle 10\rangle$ as its image.

So if $f_a : \mathbb{Z} \to \mathbb{Z}/20\mathbb{Z}$ is defined by $f_a(1) = a$, then the following list gives the complete list of ring homomorphisms: $f_0, f_1, f_5, f_{16}$.

Recall that from group theory that if $\varphi : G \to H$ is a group homomorphism, then $\ker\varphi$ is a normal subgroup of $G$, and $\operatorname{im}\varphi = \varphi(G)$ is a subgroup of $H$ (but not necessarily a normal subgroup of $H$). Thus it is natural to wonder if an analogous result holds for rings. The answer to this question is yes. Clearly, the ring counterpart of subgroups is subrings. What about the ring counterpart of normal subgroups? This prompts us to introduce the following definition.

**Definition 3.2.** Let $R$ be a ring, let $I \subset R$, and let $r \in \mathbb{R}$.

(1) $rI := \{ra : a \in I\}$ and $Ir := \{ar : a \in I\}$.

(2) Suppose that $I$ is not just a subset of $R$, but a subring of $R$. Then $I$ is a *left (resp. right) ideal* of $R$ if $I$ is closed under left (resp. right) multiplication by elements from $R$. In other words, $I$ is a left (resp. right) ideal if $rI \subseteq I$ (resp. $Ir \subseteq I$) for all $r \in R$.

(3) If $I$ is both a left ideal and a right ideal, then $I$ is said to be an *ideal* (or a *two-sided ideal*) of $R$.

*Remark.* A corollary to the above definition is that if $R$ is a commutative ring, then every ideal is an ideal (i.e. two-sided) since left ideals and right ideals coincide.

**Proposition 3.1** (Ideal test)**.** *Let $R$ be a ring, and let $I \subset R$. Then $I$ is an ideal if all of the following conditions are satisfied:*

*(i)* $I \neq \emptyset$

*(ii)* $a - b \in I$ *for all* $a, b \in I$

*(iii)* $ra \in I$ *for all* $a \in I$ *and* $r \in R$ *(closed under multiplication* by all the element of $R$, not just by the elements of $I$*).*

*If $R$ has unity* 1*, then (ii) may be replaced with*

*(ii')* $a + b \in I$ *for all* $a, b \in I$*.*

We shall introduce the following definition for the sake of giving an example of an ideal.

**Definition 3.3.** Let $R$ be a commutative ring with unity. If $x \in R$ such that $x^n = 0$ for some $n \in \mathbb{Z}$, then $x$ is said to be *nilpotent*. The *nilradical of $R$* $\eta(R)$ is the set of nilpotent elements of $R$, i.e., $\eta(R) = \{x \in R \mid x^n = 0 \text{ for some } n \in \mathbb{Z}\}$.

**Proposition 3.2.** *If $R$ is a commutative ring with unity, then $\eta(R)$ is an ideal of $R$.*

*Proof.* Let $a, b \in \eta(R)$ and $r \in R$. Suppose that $n \in \mathbb{Z}$ satisfies $a^n = 0$. Then $r^n a^n = (ra)^n = 0$, so $ra \in \eta(R)$ as well. Therefore, it follows that any element of the form $a^k b^l \in \eta(R)$. If

$m \in \mathbb{Z}$ is chosen such that $b^m = 0$ (which also implies that $(-b)^m = 0$), then we have

$$(a-b)^{m+n} = \sum_{k=0}^{m+n} \binom{m+n}{k} a^{m+n-k}(-b)^k.$$

But for any $0 \leq k \leq m$, we have $n \leq m+n-k \leq m+n$, so the first $m$ monomials of the RHS above is 0. But the remaining monomials all have $k > m$, which implies that $(-b)^k = 0$. Hence $(a-b)^{m+n} = 0$, so $a - b \in \eta(R)$. □

Now we are ready to discuss the kernel and the image of a ring homomorphism.

**Proposition 3.3.** *Let $R$ and $S$ be rings, and suppose that $\varphi : R \to S$ is a ring homomorphism.*

*(1) $\varphi(R) = \operatorname{im}\varphi$ is a subring of $S$ (but not necessarily an ideal of $S$).*
*(2) $\ker\varphi$ is an ideal of $R$.*
*(3) If $I$ is an ideal of $S$, then $\varphi^{-1}(I)$ is an ideal of $R$.*

*Proof.* (i) and (ii) are straightforward verification of axioms, so we shall prove (iii) only.

Since $0_S \in I$ and $f(0_R) = 0_S$, $0_R \in \varphi^{-1}(I)$, thereby showing that $f^{-1}(I)$ is non-empty. That $0_S \in I$ implies that $f^{-1}(I)$ must contain $\ker\varphi$ also. Suppose that $r_1, r_2 \in \varphi^{-1}(I)$. Then $\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2) \in I$ as $I$ is an ideal such that $\varphi(r_1), \varphi(r_2) \in I$. Hence $r_1 - r_2 \in \varphi^{-1}(I)$, so $\varphi^{-1}(I)$ is closed under subtraction. Let $r$ be any element in $R$. Then $\varphi(rr_1) = \varphi(r)\varphi(r_1) \in I$ since $\varphi(r_1) \in I$, whence it follows $rr_1 \in \varphi^{-1}(I)$. One can use the similar argument (just replace $rr_1$ with $r_1 r$) to show that $\varphi^{-1}(I)$ is closed under both left multiplication and right multiplication. Thus $\varphi^{-1}(I)$ is an ideal in $R$ containing $\ker\varphi$. □

If $G$ is a group and $H$ a normal subgroup of $G$, then $G/H$ is a quotient group, where its group operation is induced by the group operation for $G$. Recall that $H$ being a normal subgroup of $G$ is crucial in making the group operation well-defined. This is also a crucial fact in deriving the first isomorphism theorem for groups. Furthermore, in group theory, we learnt that $H$ is a normal subgroup if and only if $H$ is the kernel of some group homomorphism. Does the similar claim hold for ideals? First, we shall introduce the notion of quotient rings, and then proceed to verify whether the operations are well-defined. Also, since any ideal is a subring, any ideal is automatically an additive normal subgroup. Thus $R/I$ is always an additive quotient group.

**Definition 3.4.** Let $R$ be a ring, and $I$ an ideal of $R$. Then the additive quotient group $R/I$ is called the *quotient ring of $R$ by $I$* where the addition and the multiplication are defined as follows:

(1) $(r+I)+(s+I) = (r+s)+I$ for all $r, s \in R$, and
(2) $(r+I)\cdot(s+I) = rs+I$ for all $r, s \in R$.

We have yet to verify that the multiplication as defined above is well-defined and that such multiplication satisfies all the necessary properties (such as distributive properties). However, since the remaining properties such as distributive properties follow from the corresponding axioms satisfied by $R$, it in fact suffices to prove that the multiplication is well-defined.

Suppose that $\alpha, \beta \in I$. Then $(r+\alpha)+I = r+I$ and $(s+\beta)+I = s+I$. So we have

$$((r+\alpha)+I)((s+\beta)+I) = (r+\alpha)(s+\beta)+I = (rs+r\beta+\alpha s+\alpha\beta)+I.$$

Since $I$ is an ideal of $R$, for any $r, s \in R$ we have $r\beta, \alpha s \in I$. Therefore

$$(r + \alpha)(s + \beta) + I = (rs + \alpha\beta) + I = rs + I,$$

since evidently $\alpha\beta \in I$. Hence the multiplication is well-defined.

**Definition 3.5.** Let $R$ be a ring, and let $I$ be an ideal of $R$. Then $\pi : R \to R/I$ defined by $r \mapsto r + I$ is the *natural projection of $R$ onto $R/I$*.

**Theorem 3.1.** *Let $R$ be a ring, and $I$ an ideal of $R$. Then $\pi$ is a ring epimorphism with kernel $I$. Thus every ideal is the kernel of a ring homomorphism. Therefore, the set of ideals and the set of kernels of ring homomorphisms coincide.*

*Proof.* Since $I$ is an ideal, $R/I$ is a ring (hence an additive abelian group *a fortiori*). Hence $\pi$ is a group homomorphism with kernel $I$. So it remains to verify that $\pi$ preserves multiplication, which follows from the fact that

$$\pi(rs) = rs + I = (r + I)(s + I) = \pi(r)\pi(s).$$

That $\pi$ is surjective follows from the definition of $\pi$. Finally, the last statement follows since we previously proved that the kernel of a ring homomorphism is an ideal. □

We shall conclude this section with the isomorphism theorems for rings. Each isomorphism theorem for rings has its counterpart for groups, as we shall see.

**Theorem 3.2** (First isomorphism theorem for rings)**.** *If $\varphi : R \to S$ is a ring homomorphism, then the kernel of $\varphi$ is an ideal of $R$, the image of $\varphi$ is a subring of $S$, and*

$$R/\ker\varphi \cong \varphi(R) = \operatorname{im}\varphi.$$

*Proof.* The first two statements are already proved in Proposition 3.3, so it suffices to prove the last statement only. Let $I = \ker\varphi$, and let $\overline{\varphi} : R/I \to \varphi(R)$ be the homomorphism induced by $\varphi$ (i.e., $\overline{\varphi} : r + I \mapsto \varphi(r)$). Then $\overline{\varphi}^{-1}(\operatorname{im}\varphi)$ is precisely the cosets of $I$. We previously verified that $\overline{\varphi}$ is a well-defined group epimorphism, so it suffices to verify that $\overline{\varphi}$ preserves multiplication and is injective. Indeed, we have

$$\overline{\varphi}((r + I)(s + I)) = \overline{\varphi}(rs + I) = \varphi(rs) = \varphi(r)\varphi(s) = \overline{\varphi}(r + I)\overline{\varphi}(s + I).$$

Suppose that $\varphi(r) = 0$. Then $r \in \ker\varphi$ so $\overline{\varphi}(r + I) = \varphi(r) = 0$ if and only if $r \in \ker\varphi = I$. Therefore the kernel of $\overline{\varphi}$ is trivial. Hence $R/\ker\varphi \cong \varphi(R)$ as rings, as desired. □

The proofs of the remaining three theorems are straightforward. First, use the corresponding theorems for groups to get an *additive group isomorphism* or *correspondence*. Second, verify that the same group isomorphism is a multiplicative map, thereby showing that it is a *ring isomorphism* as well. Again, this is straightforward from the way multiplication is defined in quotient rings.

**Theorem 3.3** (Second isomorphism theorem for rings)**.** *Let $A$ be a subring of $R$, and $B$ an ideal of $R$. Then*

*(i)* $A + B := \{a + b : a \in A, b \in B\}$ *is a subring of $R$.*
*(ii)* $A \cap B$ *is an ideal of $A$.*
*(iii)* $(A + B)/B \cong A/(A \cap B)$.

**Theorem 3.4** (Third isomorphism theorem for rings)**.** *Let $I$ and $J$ be ideals of $R$ with $I \subseteq J$. Then $J/I$ is an ideal of $R/I$ and $(R/I)/(J/I) \cong R/J$.*

The fourth isomorphism theorem for rings is called the lattice isomorphism theorem for rings in some literature. The theorem, however, is more commonly known as the correspondence theorem for rings, which is the name we will go by in the notes.

**Theorem 3.5** (Correspondence theorem for rings)**.** *Let $I$ be an ideal of $R$. Then there is an inclusion-preserving bijection between the set of subrings $A$ of $R$ containing $I$ and the set of subrings of $R/I$. Furthermore, $A$ is an ideal of $R$ containing $I$ if and only if $A/I$ is an ideal of $R/I$.*

*Example.* We conclude with an application of the correspondence theorem. Suppose we want to find all the ideals of $\mathbb{Z}[x]/(2, x^2+1)$. First note that

$$\mathbb{Z}[x]/(2, x^2+1) \cong \mathbb{F}_2[x]/(x^2+1),$$

and that $(x^2+1) = (x+1)^2$ over $\mathbb{F}_2$. So by the correspondence theorem, there is a bijection between the set of ideals of $\mathbb{F}_2[x]$ containing $(x^2+1)$ corresponds and the set of ideals of $\mathbb{F}_2[x]/(x^2+1)$. $\mathbb{F}_2[x]$ is a PID, so every ideal can be written in the form $(f(x))$. Since $x^2+1 = (x+1)^2$, it follows that $f(x)$ must be one of $1, x+1$, and $(x+1)^2 = (x^2+1)$. Hence the ideals of $\mathbb{F}_2[x]/(x^2+1)$ are $(0), (1)$, and $(x+1)$, so the ideals of $\mathbb{Z}[x]/(2, x^2+1)$ are the zero ideal, the entire ring, and $(2, x+1)$.

## 4. Chapter VII.4: Properties of ideals

**Definition 4.1.** Let $I$ and $J$ be ideals of $R$.

(1) $I + J := \{a + b \mid a \in I, b \in J\}$ (the *sum of $I$ and $J$*)
(2) $IJ := \{a_1b_1 + \cdots + a_nb_n \mid a_i \in I, b_i \in J, n \in \mathbb{N}\}$ (the *product of $I$ and $J$*)
(3) $I^n$, called the *$n$th power of $I$*, is the set consisting of all finite sums of elements of the form $a_1a_2 \cdots a_n$ where $a_i \in I$ for all $i$.

*Remark.* Clearly, $I, J \subseteq I + J$. In fact, $I + J$ is the smallest ideal of $R$ containing both $I$ and $J$. From the definition, it is also clear that $IJ \subset (I \cap J)$; $IJ$ may be strictly smaller than $I \cap J$. It should be noted that $IJ$ must consist of all *finite sums of the elements of the form $ab$* where $a \in I, b \in J$; note that the set $\{ab : a \in I, b \in J\}$ need not be closed under addition, so cannot be an ideal in general.

From now on, we shall assume that $R$ is a ring with unity $1 \neq 0$.

**Definition 4.2.** Let $A$ be any subset of the ring $R$.

(1) Let $(A)$ be the smallest ideal of $R$ generated by $A$. Then $(A)$ is called the *ideal generated by $A$*.
(2) The *left ideal generated by $A$* is $RA := \{r_1a_1 + \cdots + r_na_n \mid r_i \in R, a_i \in A, n \in \mathbb{N}\}$. Similarly, we define the *right ideal generated by $A$* to be $AR := \{a_1r_1 + \cdots + a_nr_n \mid r_i \in R, a_i \in A, n \in \mathbb{N}\}$.
(3) The *two-sided ideal generated by $A$* is $RAR := \{r_1a_1r_1' + \cdots + r_na_nr_n' \mid r_i, r_i' \in R, a_i \in A, n \in \mathbb{N}\}$.
(4) If $\#A$ is finite, then $(A)$ is a *finitely generated ideal*. In this case, if $A = \{a_1, a_2, \ldots, a_n\}$, then we omit the set brackets, and write $(A) = (a_1, a_2, \ldots, a_n)$ instead.
(5) More specifically, if $\#A = 1$, then $(A)$ is a *principal ideal*. In this case, if $A = \{a\}$, then we omit the set brackets, and write $(A) = (a)$.

Recall that the subgroup of $G$ generated by a subset $B \subset G$ is

$$\langle B \rangle = \bigcap_{\substack{H \supseteq B \\ H \text{ subgroup}}} H$$

because the intersection of any non-empty collection of subgroups is a subgroup. We can do the same things for ideals. In other words,

$$(A) = \bigcap_{\substack{I \supseteq A \\ I \text{ ideal}}} I.$$

Now we will briefly explore why the uses of "the" are justified for (2) and (3) of Definition 4.2. Note that every left ideal generated by $A$ must contain $RA$ – since $R$ contains 1, $RA$ necessarily contains $A$. Conversely, any left ideal containing $A$ must contain all the elements of the form $r_1a_1 + \cdots + r_na_n$ for $r_i \in R, a_i \in A$ for all $i$. Therefore such ideal must contain $RA$. Hence, $RA$ is precisely the left ideal generated by $A$. The same line of reasoning can be used for $AR$ and $RAR$ as well.

*Remark.* If $R$ is commutative, then evidently $RA = AR = RAR = (A)$. If $R$ is a commutative ring and $I$ is a principal ideal (that is, $I = (a)$ for some $a \in R$), then $I = (a) = Ra = \{ra \mid r \in R\}$. If $R$ is not commutative, then $(a) = RaR = \{r_1ar_1' + \cdots + r_nar_n' \mid r_i, r_i' \in R, n \in \mathbb{N}\}$.

*Example.* If $R = \mathbb{Z}$, then $(n) = n\mathbb{Z}$ is an ideal. In fact every ideal of $\mathbb{Z}$ is of the form $(n)$ for some $n \in \mathbb{Z}$. Notice that if $(n, m)$ is an ideal, then $(d) = (n, m)$ where $\gcd(n, m) = d$. Thus $\mathbb{Z}$ is an example of a *principal ideal domain* (PID).

*Example.* Let $R = \mathbb{Z}[x]$ and $I = (2, x)$. We show that $I$ is an ideal but is not a principal ideal. Suppose instead then that there exists $p(x) \in R$ such that $(p(x)) = (2, x)$. Every element in $I$ is of the form $2f(x)+xg(x)$, so it necessarily has an even constant term. Therefore $2 \in (p(x))$, so there is $q(x)$ such that $p(x)q(x) = 2$. But then $\deg p(x)q(x) = 0 = \deg p(x) + \deg q(x)$, so the generator $p(x)$ must be of degree 0. Particularly, $p(x)$ can only be $\pm 1$ or $\pm 2$. If $p(x) = \pm 1$, then $(p(x)) = \mathbb{Z}[x](\pm 1) = \mathbb{Z}[x]$, but this contradicts the fact that polynomials with an odd constant term are not in $(p(x))$. Therefore $p(x)$ is 2 or $-2$. We also need $x \in (p(x)) = (2) = (-2)$. This means there is $r(x) \in \mathbb{Z}[x]$ so that $2r(x) = x$. However this is impossible since every coefficient of $2r(x)$ is even whereas $x$ has coefficient 1. Therefore $(2, x)$ is not a principal ideal.

On the other hand, if $\mathbb{Z}[x]$ were replaced with $\mathbb{Q}[x]$, then $(2, x)$ is in fact principal. Note that $\frac{1}{2} \cdot 2 = 1 \in (2, x)$, so in fact $(2, x) = (1) = \mathbb{Q}[x]$ – this is because $\mathbb{Q}$ is a field.

The last example illustrates an important relationship between units, ideals, and fields, which we shall state and prove below.

**Proposition 4.1.** *Let $I$ be an ideal of $R$.*

*(1) $I = R$ if and only if $I$ contains a unit.*
*(2) Assume that $R$ is commutative. Then $R$ is a field if and only if its only ideals are 0 and $R$.*

*Proof.* ((1), $\Rightarrow$) Suppose that $I = R$. Then $I = (1)$, and clearly 1 is a unit.

((1), $\Leftarrow$) Assume that $I$ contains a unit $u$. Then there is $v \in R$ such that $vu = 1$. Therefore $1 = vu \in I$, so $I = (1) = R$ as required.

((2), $\Rightarrow$) Suppose that $R$ is a field. Therefore every non-zero element of $R$ has a multiplicative inverse. Thus once a non-zero element is in an ideal $I$, 1 is necessarily in $I$ also. In other words, there cannot be any ideals between 0 and $R$.

((2), $\Leftarrow$) Suppose that $R$ only has 0 and $R$ as its only ideals. If $u$ is any non-zero element of $R$, then $R = (u)$. Therefore $1 \in (u)$. This means that $u$ has a multiplicative inverse. Our choice of non-zero $u$ is arbitrary, so it follows that every non-zero element of $R$ is a unit. This is precisely what it means for $R$ to be a field.pr $\square$

**Corollary 4.1.** *Let $F$ be a field. Then any ring homomorphism $\varphi : F \to R$ is either the zero map or an injection.*

*Proof.* Recall that $\ker \varphi$ is always an ideal of $F$. But since $F$ is a field, $\ker \varphi$ can only be the zero ideal or the entire field. If $\ker \varphi = (0)$, then $\varphi$ is an injection. If $\ker \varphi = F$, then $\varphi$ is the zero map. $\square$

Next, we introduce two important classes of ideals: prime ideals and maximal ideals. Prime ideals essentially generalizes the prime numbers from number theory. To illustrate this point, we take a quick detour to elementary number theory.

**Theorem 4.1.** *Suppose that $a, b \in \mathbb{N}$ and $p$ is a prime. If $p \mid ab$ then $p \mid a$ or $p \mid b$. In other words, at least one of $a$ and $b$ must be a multiple of $p$.*

*Proof.* We will prove the contrapositive instead. Suppose that $p \nmid a$ and $p \nmid b$. Then $p$ cannot show up in the prime factorization of $a$ and that of $b$; therefore $p$ cannot show up in the prime factorization of $ab$ either, so $p \nmid ab$ as required. $\square$

Recall that if $R = \mathbb{Z}$, then $(p) = p\mathbb{Z}$. Therefore $a \in (p)$ if and only if $p \mid a$. With this insight, we can reformulate the above number-theoretic statement in terms of ideals.

**Theorem 4.2.** *Let $R = \mathbb{Z}$, $p$ a prime, and $a, b \in \mathbb{Z}$. If $ab \in (p)$, then $a \in (p)$ or $b \in (p)$.*

Prime ideals is the generalization of this idea to any general commutative ring.

**Definition 4.3.** Let $R$ be a commutative ring. Then an ideal $P$ is a *prime ideal* if:

(1) $P$ is a proper ideal of $R$; and
(2) for any $a, b \in R$ such that $ab \in P$, at least one of $a$ and $b$ lies in $P$.

**Proposition 4.2.** *Let $R$ be a commutative ring. Then $R/P$ is an integral domain if and only if $P$ is a prime ideal.*

*Proof.* ($\Rightarrow$) Suppose that $R/P$ is an integral domain, and let $\bar{r} := r + P, \bar{s} := s + P \in R/P$ such that $rs \in P$. Then $\bar{r}\bar{s} = \overline{rs} = \bar{0}$ since $rs \in P$. But then $R/P$ is an integral domain, so at least one of $\bar{r} = \bar{0}$ and $\bar{s} = \bar{0}$ must hold. Therefore, at least one of $r$ and $s$ must lie in $P$, so $P$ is a prime ideal.

($\Leftarrow$) Suppose that $P$ is a prime ideal, and suppose that $rs \in P$. This gives us

$$(r + P)(s + P) = rs + P = 0 + P.$$

But then $P$ is a prime ideal, so at least one of $r$ and $s$ must be in $P$. Therefore at least one of $r + P$ and $s + P$ must be equal to $0 + P$, so $R/P$ cannot have any zero-divisor, as required. $\square$

**Corollary 4.2.** *Let $R$ be a commutative ring. Then $R$ is an integral domain if and only if $(0)$ is a prime ideal.*

*Proof.* ($\Rightarrow$) Suppose that $R$ is an integral domain, and let $ab = 0 \in (0)$. $R$ has no zero-divisor, so $a = 0$ or $b = 0$. Thus at least one of $a$ and $b$ is in $(0)$. Thus $(0)$ must be a prime ideal.

($\Leftarrow$) Suppose that $(0)$ is a prime ideal, and that $a, b \in R$ satisfy $ab = 0 \in (0)$. But since $(0)$ is a prime ideal, we have $a = 0$ or $b = 0$. Hence $R$ cannot have any zero divisor, so $R$ is an integral domain. □

We shall state two interesting results involving prime ideals before moving onto another class of ideals.

**Proposition 4.3.** *Let $R$ be a commutative ring with unity. Suppose that $I$ and $J$ are ideals of $R$, and suppose that $P$ is a prime ideal of $R$. Then the following are true.*

*(i) If $P$ contains no zero divisors, then $R$ cannot contain any zero divisors either.*
*(ii) If $I \cap J \subseteq p$, then $I \subseteq p$ or $J \subseteq p$.*

*Proof.* (i) Suppose $a \in R$ is a zero divisors of $R$. Then there exists a non-zero $b \in R$ such that $ab = 0$. Since $p$ is an ideal, necessarily $0 \in p$. Hence $ab \in p$, so either $a \in p$ or $b \in p$. But since $a$ and $b$ are zero divisors of each other, it follows that $p$ contains a zero divisor, which is a contradiction. Hence $R$ cannot contain any zero divisor either.

(ii) Suppose that $I \not\subseteq p$ and $J \not\subseteq p$. Then there exist $r \in I$ and $s \in J$ such that $r, s \notin p$. Since $p$ is prime, it follows that $rs \notin p$. But then $rs \in I$ and $rs \in J$ since $I$ and $J$ are ideals. Hence $rs \in I \cap J$. Thus $rs$ is in $I \cap J$ but not in $p$. Therefore $I \cap J \not\subseteq p$ as required. □

**Proposition 4.4.** *Suppose that $R$ is a commutative ring with unity. Then $\eta(R)$ is contained in every prime ideal of $R$.*

*Proof.* Suppose that $N = \eta(R)$, and let $P$ be a prime ideal of $R$. If $x \in N$, then $x^m \in P$ for some $m \in \mathbb{Z}$ since $x$ is in the nilradical of $R$. Let $n$ be the smallest integer such that $x^n \in P$. Suppose that $n > 1$ so that $x \notin P$. Then $x^n = x \cdot x^{n-1} \in P$, so it follows that $x \in P$ or $x^{n-1} \in P$. But this contradicts the minimality of $n$, so it follows that $x \in P$. Since this works for every prime ideal, it follows that

$$N \subseteq \bigcap_{P \text{ prime}} P.$$

As for the reverse inclusion, we will show that if $x \notin N$, then one can find a prime ideal that does not contain $x$. Let $S = \{1, x, x^2, \dots\}$, and consider the set of ideals of $R$ that does not intersect with $S$. Clearly this set is non-empty since the zero ideal does not intersect with $S$. By Zorn's lemma, there is a maximal element $M$ in this set.

We want to show that $M$ is a prime ideal. Suppose that there are some elements such that $a \notin M$ and $B \notin M$ but $ab \in M$. If $A_a := \{z \in R : az \in M\}$, then $A_a$ (and similarly, $A_b$) is an ideal of $R$ such that $M \subsetneq A_a$. But recall that $M$ is a maximal element of the set of ideals not intersecting with $S$; therefore $A_a$ must intersect with $S$, so there is some $m$ such that $x^m \in A_a$. Similarly, there is some $m'$ such that $x^{m'} \in A_b$. Therefore we see that $x^{m+m'} = x^m x^{m'} \in A_{ab}$. But since $ab \in M$, it follows that $A_{ab} = M$, so $x^{m+m'} \in M$. This is a contradiction, so $M$ is a prime ideal that does not intersect with $S$. Thus we found a prime ideal that does not contain $x$, so $x \notin \bigcap P$, as required.

□

Another important class of ideals is the class of ideals that are not contained in any proper ideal.

**Definition 4.4.** An ideal $M$ of a ring $R$ is a *maximal ideal* if $M \neq R$, and the only ideals containing $M$ are $M$ and $R$.

**Proposition 4.5.** *In a ring with unity, every proper ideal is contained in a maximal ideal.*

**Proposition 4.6.** *Let $R$ be a commutative ring. Then $R/M$ is a field if and only if $M$ is a maximal ideal.*

*Proof.* ($\Leftarrow$) Thanks to the correspondence theorem for rings (Theorem 3.5), there is a bijection between the set of ideals containing $M$ and the set of ideals of $R/M$. But the only ideal of $R$ containing $M$ is $R$ since $M$ is maximal, so the only ideals of $R/M$ are $R/M$ and 0. Therefore, $R/M$ is a commutative ring that has no non-trivial ideals, so $R/M$ is a field.

($\Rightarrow$) Since $R/M$ is a field, the only ideals of $R/M$ are $R/M$ and 0. So by the correspondence theorem for rings, there is only one ideal containing $M$, and that ideal is $R$. Therefore $M$ is a maximal ideal of $R$. □

**Proposition 4.7.** *Let $R$ be a commutative ring with unity. An ideal $M$ of $R$ is maximal if and only if for every $r \in R \setminus M$ there exists $x \in R$ such that $1 - rx \in M$.*

*Proof.* ($\Leftarrow$) Suppose that $J$ is an ideal of $R$ such that $M \subsetneq J \subset R$, and let $r \in J \setminus M \subseteq R \setminus M$. $J$ is an ideal of $R$, so $rx \in J$ where $x$ satisfies the given assumption. But then $1_R - rx \in M \subsetneq J$, so $(rx) + (1_R - rx) = 1_R \in J$, which forces $J = R$. Therefore $M$ is maximal.

($\Rightarrow$) Suppose that $M$ is maximal. Since $r \in R \setminus M$, we have $M \subsetneq (r) + M \subset R$. Thus, $(r) + M = R$ by the maximality of $R$. $(r) + M$ is an ideal, so $1_R \in (r) + M$. Thus there exist $x \in R$ and $m \in M$ so that $rx + m = 1_R$. Now it follows that $1_R - rx = m \in M$ as desired. □

**Corollary 4.3.** *Every maximal ideal of a commutative ring is a prime ideal.*

*Proof.* Let $M$ be a maximal ideal of a commutative ring $R$. Then $R/M$ is a field, so $R/M$ is an integral domain as well. Hence $M$ is a prime ideal, as required. □

*Example.* The set of non-zero prime ideals of $\mathbb{Z}$ and the set of maximal ideals of $\mathbb{Z}$ coincide. In fact, the only non-zero prime ideals are of the form $(p) = p\mathbb{Z}$ for some prime $p$. We already observed that any ideals of $(p)$ for $p$ prime is a prime ideal. If $n$ is not a prime (without loss of generality, assume $n \in \mathbb{N}$), then there exist $1 < a, b < n$ such that $n = ab$. Thus $n \in (n)$ but $a, b \notin (n)$, so $(n)$ cannot be a prime ideal. Indeed, if $n$ is composite, then $\mathbb{Z}/(n) = \mathbb{Z}/n\mathbb{Z}$, and if $ab = n$ then $b$ is a zero-divisor of $a$. Recall that if $p$ is a prime, then $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$, and $\mathbb{Z}/p\mathbb{Z}$ forms the finite field of $p$ elements ($\mathbb{F}_p$). Thus $(p)$ is not just a prime ideal, but also a maximal ideal. $\mathbb{Z}$ is an integral domain (in fact, a principal ideal domain, so it is *a fortiori* an integral domain), so (0) is a prime ideal. But $(0) \subsetneq (p) \subsetneq \mathbb{Z}$ for any prime $p$, so (0) is not a maximal ideal. Indeed, $\mathbb{Z}$ is not a field.

*Example.* $(x)$ is maximal and prime in $\mathbb{Q}[x]$ since $\mathbb{Q}[x]/(x) \cong \mathbb{Q}$, and $\mathbb{Q}$ is a field. However, $(x)$ in $\mathbb{Z}[x]$ is prime but not maximal in $\mathbb{Z}[x]$, since $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$, which is an integral domain but is not a field.

*Example.* $(x^2+1)$ is both maximal and prime in $\mathbb{R}[x]$. Recall from field theory that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{R}(i) \cong \mathbb{C}$ (see the MATH 5055 notes for more information on this), the field of complex numbers.

## 5. Chapter VII.5: Rings of fractions

In this section, we aim to prove that every commutative ring $R$ (for convenience, we shall always assume that a ring has unity 1) is a subring of a larger ring $Q$ such that every non-zero element that is not a zero divisor is a unit. Our focus will be on constructing this larger ring containing $R$. Before doing this for general case, it always helps to consider a familiar specific example. So for the sake of a familiar example, let $R = \mathbb{Z}$. We will explore why this larger ring $Q$ is $\mathbb{Q}$ that we are familiar with.

Recall that $\mathbb{Q}$ consists of elements of the form $p/q$ where $p, q \in \mathbb{Z}$. Thus every rational number has multiple representations. Indeed, $a/b = c/d$ if and only if $ad = bc$ (clearly, $b, d \neq 0$); using the equivalence relation notion, we conclude that $(a, b) \sim (c, d)$ if and only if $ad = bc$. The addition and multiplications are the operations we are all familiar with. Proving that the addition and multiplication are well-defined is a routine exercise, so we shall skip the verification. For any non-zero $p/q \in \mathbb{Q}$, the multiplicative inverse is $q/p \in \mathbb{Q}$, so every non-zero element is a unit. Hence, $\mathbb{Q}$ has a field (and hence a ring) structure, and $\mathbb{Z}$ is a subring of $\mathbb{Q}$ since every element $b \in \mathbb{Z}$ can be written of the form $b/1 \in \mathbb{Q}$. Let $N := \mathbb{Z} \setminus \{0\}$. Then $\mathbb{Q} = N^{-1}\mathbb{Z}$. The "ring of fractions" is thus the generalization of this idea onto any commutative ring with unity 1.

**Definition 5.1.** We say that a set $S$ is *multiplicatively closed* if $S$ is a non-empty set such that $xy \in S$ whenever $x, y \in S$.

**Definition 5.2.** Suppose $R$ is a commutative ring with unity 1, and that $D$ is a non-empty multiplicatively closed subset of $R$ that contains 1 but does not contain 0 and any zero divisors. Then the *ring of fractions* of $D$ with respect to $R$ is $Q = D^{-1}R$.

**Theorem 5.1** (Existence and uniqueness of the ring of fractions)**.** *Let $R$ be a commutative ring with unity 1. Let $D$ be any non-empty multiplicatively closed subset of $R$ that contains 1 but not 0 and any of the zero divisors of $R$. Then there is a commutative ring $Q$ with 1 such that $R$ is a subring of $Q$, and every element in $D$ is a unit in $Q$. Additionally,*

1. *$Q = D^{-1}R$. That is, every element of $Q$ is of the form $r/d$ where $r \in R$ and $d \in D$. In particular if $D = R \setminus \{0\}$, then $Q$ is a field.*
2. *$Q$ is the* smallest *ring containing $R$ in which all elements of $D$ become units, in the following sense. Let $S$ be any commutative ring with unity, and let $\varphi : R \to S$ be any injective ring homomorphism such that $\varphi(d)$ is a unit in $S$ for every $d \in D$. Then there is an injective homomorphism $\Phi : Q \to S$ such that $\Phi|_R = \varphi$. Thus, any ring containing an isomorphic copy of $R$ in which all the elements of $D$ become units must also contain an isomorphic copy of $Q$.*

*Proof.* See p261-263 of Dummit & Foote. □

**Corollary 5.1.** *If $R$ is an integral domain and $D = R \setminus \{0\}$, then $Q$ is a field.*

If $R$ is an integral domain, there is a special term to refer to its ring of fractions $Q$.

**Definition 5.3.** Suppose that $R$ is an integral domain and $D = R \setminus \{0\}$, then $Q$ is called the *field of fractions* of $R$.

**Corollary 5.2.** *Let $R$ be an integral domain, and let $Q$ be the field of fractions of $R$. If a field $F$ contains a subring $r'$ isomorphic to $R$ then the subfield of $F$ generated by $R'$ is isomorphic to $Q$. Therefore, the smallest field containing an integral domain $R$ is its field of fractions.*

*Proof.* Suppose $\varphi : R \to R' \subseteq F$ be a ring isomorphism from $R$ to $R'$. In particular, $\varphi : R \to F$ is an injective homomorphism from $R$ into the field $F$. Let $\Phi : Q \to F$ be the extension of $\varphi$. Recall that $\Phi$ is injective, so $\Phi(Q)$ is an isomorphic copy of $Q$ in $F$; indeed, $\varphi(R) = R'$, so $\varphi(R) \subseteq \Phi(Q)$. For any $r_1, r_2 \in R$, we have $\varphi(r_1)\varphi(r_2)^{-1} = \varphi(r_1 r_2^{-1})$, so every subfield containing $\varphi(R) = R'$ has elements of this form. But then every element in $Q$ is precisely of the form $r_1 r_2^{-1}$ for some $r_1, r_2 \in R$. Therefore every subfield of $F$ containing $R'$ must contain $\Phi(Q)$. Therefore $\Phi(Q)$ is the subfield of $F$ generated by $R'$. □

We conclude with a universal property associated with rings of fractions.

**Proposition 5.1** (Universal property of localization)**.** *Let $S$ be a multiplicative subset of a commutative ring $R$. Then $\varphi_s : R \to S^{-1}R$ defined by $\varphi_s(r) = rs/s$ is well-defined. If $T$ is another commutative ring with identity, and $\psi : R \to T$ is a ring homomorphism such that $\psi(S)$ is a subset of the set of units in $T$, then there is a unique ring homomorphism $\overline{\psi} : S^{-1}R \to T$ such that $\overline{\psi}\varphi_s = \psi$.*

**Proposition 5.2.** *Suppose that $R$ is an integral domain, and $S$ a multiplicatively closed subset of $R$. Then $S^{-1}R$ is isomorphic to a subring of the quotient field of $R$.*

*Proof.* Consider the map $\varphi : R \to \mathrm{Frac}(R)$ defined by $\varphi(r) = r/1$, and $\psi_s : R \to S^{-1}R$ be $\psi_s(r) = rs/s$. We claim that $\varphi(S)$ consists of units of $\mathrm{Frac}(R)$. Suppose otherwise. If $\varphi(s) = s/1 = 0$, then $st = 0$ where $t \in R \setminus \{0\}$. But since $R$ is an integral domain, it follows $s = 0$, but this contradicts the fact that $0 \notin S$. Thus $\varphi(S)$ contains non-zero elements, so every element in $\varphi(S)$ is a unit in $\mathrm{Frac}(R)$. Thus by the universal property of localization there is a unique ring homomorphism $\eta : S^{-1}R \to \mathrm{Frac}(R)$ such that $\eta \circ \psi_s = \varphi$. To prove the claim, it suffices to show that $\eta$ must be injective. Suppose that $\eta(r/s) = 0$ where $r \in R$ and $s \in S$. Then $(r/s)/1 = r/s = 0$. Multiply by both sides by $st$ (where $s, t \in S$ hence $st \in S$; note that since both $s, t \neq 0$, it follows $st \neq 0$) to get $rt = 0$. But then $R$ is an integral domain, so it follows $r = 0$. Hence $\eta$ is injective. □

## 6. Chapter VII.6: The Chinese remainder theorem

Recall Bézout's identity from the number theory, which states that if $d = \gcd(n, m)$, then there exist infinitely many solutions $(x, y)$ to the equation $nx + my = k$ where $k$ is a multiple of $d$. Thus, if $n$ and $m$ are coprime, then there exist $x$ and $y$ so that $nx + my = 1$. Therefore, if we view $n\mathbb{Z}$ and $m\mathbb{Z}$ as ideals of $\mathbb{Z}$ we have $n\mathbb{Z} + m\mathbb{Z} = \gcd(m, n)\mathbb{Z}$. We can generalize this notion to other rings. We will restrict our attention to commutative rings with unity 1.

**Definition 6.1.** We say that ideals $A, B$ of a ring $R$ is *comaximal* if $A + B = R$.

**Theorem 6.1** (Chinese remainder theorem)**.** *Let $A_1, A_2, \ldots, A_k$ be pairwise comaximal ideals in $R$. Then the map*

$$\varphi : R \mapsto \prod_{i=1}^{k} R/A_i$$

*defined by*

$$\varphi(r) := (r + A_1, \ldots, r + A_k)$$

*is a ring epimorphism with kernel $A_1 \cap \cdots \cap A_k$, which is equal to $A_1A_2A_3 \cdots A_k$. Therefore, we have the isomorphism*

$$R/\prod_{i=1}^{k} A_i = R/\bigcap_{i=1}^{k} A_i \cong \prod_{i=1}^{k} R/A_i.$$

*Proof.* We will suppose that the base case ($k = 2$) holds, and suppose that the claim holds for $k - 1$ ideals. Now consider $A = A_1$ and $B = A_2A_3 \cdots A_k$. If we prove that $A_1$ and $A_2A_3 \cdots A_k$ are comaximal, then we can use the base case to finish the inductive step. Since $A_1, A_2, \ldots, A_k$ are mutually comaximal, for any $2 \leq i \leq k$ there exists $y_i \in A_i$ and $x_i \in A_1$ so that $x_i + y_i = 1$. Hence $(x_2 + y_2) \cdots (x_k + y_k) = 1$. Note that $(x_2 + y_2) \cdots (x_k + y_k)$ can be written in the form $X + y_2y_3 \ldots y_k$. Since each individual term in $X$ is a mutliple of $x_i$ for some $2 \leq i \leq k$ it follows that $X \in A_1$. Thus $1 \in A_1 + (A_2A_3 \cdots A_k)$, proving the comaximality of $A_1$ and $A_2A_3 \cdots A_k$. But then since we assume that the claim holds for $k = 2$, the inductive step is complete.

Now it remains to prove the base case. Suppose $k = 2$ and $\varphi(r) = (r + A_1, r + A_2)$. Since $A_1$ and $A_2$ are comaximal, there exist $a_1 \in A_1$ and $a_2 \in A_2$ so that $a_1 + a_2 = 1$. Hence for any $(p+A_1, q+A_2)$, we have $\varphi(pa_2+qa_1) = (pa_2+A_1, qa_1+A_2) = (pa_2+pa_1+A_1, qa_1+qa_2+A_2) = (p(a_2 + a_1) + A_1, q(a_1 + a_2) + A_2) = (p + A_1, q + A_2)$. Hence $\varphi$ is surjective. Clearly $\varphi$ is a homomorphism since $\varphi$ is a projection map. Finally, suppose $\varphi(r) = (0 + A_1, 0 + A_2)$. This implies that $r \in A_1$ and $r \in A_2$, so $\ker \varphi = A_1 \cap A_2$. So by the first isomorphism theorem for rings, we have

$$R/(A_1 \cap A_2) \cong R/A_1 \times R/A_2,$$

as desired. Thus it only remains to show that $A_1 \cap A_2 = A_1A_2$. Recall that $A_1A_2$ consists of finite sums of elements of the form $ab$ where $a \in A_1$ and $b \in A_2$. Therefore every element in $A_1A_2$ clearly belongs to both $A_1$ and $A_2$, per definition of ideals. Hence $A_1A_2 \subseteq A_1 \cap A_2$. Suppose that $a \in A_1 \cap A_2$, and suppose $a_1 + a_2 = 1$ where $a_1 \in A_1$ and $a_2 \in A_2$. Then $a = a1 = a(a_1 + a_2) = aa_1 + aa_2 = a_1a + aa_2 \in A_1A_2$, so the equality follows as required. □

## 7. Chapter VIII.2 (first half only): Principal ideal domains

**Definition 7.1.** Let $R$ be a commutative ring with unity 1 such that for every ideal $I$, there exists $a \in R$ such that $I = (a)$. Then $R$ is a *principal ideal domain (PID).*

**Definition 7.2.** Suppose that $R$ is an integral domain, and $a, b, d \in R$. We say that $d$ is a *divisor* of $a$ (written $d \,|\, a$) if there exists $x \in R$ such that $dx = a$. If $d \,|\, a$ and $d \,|\, b$, then $d$ is a *common divisor* of $a$ and $b$. If $D$ is a common divisor of $a$ and $b$ such that $d \,|\, D$ for any common divisor $d$ of $a$ and $b$, then $D$ is a *greatest common divisor* of $a$ and $b$.

**Definition 7.3.** We say that $a, b \in R$ are *associates* if there exists a unit element $u \in R$ such that $a = ub$.

*Remark.* It should be remarked that there may be more than one GCDs of $a$ and $b$, *provided one exists*. A GCD is not always defined for any two or more arbitrary elements in an integral domain. For any two or more elements in a commutative ring with unity to have a GCD, we need the unique factorization condition. Thus, we can discuss GCD for any two or more elements if a ring is a *unique factorization domain (UFD). A fortiori* every PID is a UFD.

From the definition of a divisor, we see that $d \mid a$ if and only if $(a) \subseteq (d)$. Indeed, since there is $x \in R$ such that $dx = a$, we have $a = dx \in (d)$, so $(a) \subseteq (d)$. This gives us an alternative way of defining divisibility in the context of ring theory. Also, if $d$ is a common divisor of $a$ and $b$, and $D$ a greatest common divisor, then necessarily $d \mid D$, so we have $(D) \subseteq (d)$. Hence, $D$ is a greatest common divisor of $a$ and $b$ if and only if $(D)$ is the smallest principal ideal containing both $a$ and $b$. This gives rise to the following proposition.

**Proposition 7.1.** *Let $R$ be a commutative ring. If $a$ and $b$ are non-zero elements of $R$ such that $(a, b) = (d)$, then $d$ is a GCD of $a$ and $b$.*

Observe that the definition wrote *a* greatest common divisor rather than *the* greatest common divisor. It is known that the greatest common divisor is unique up to a sign for the integers (hence unique in $\mathbb{N}$), but we don't know if such uniqueness can be generalized in arbitrary principal ideal domains. The ensuing discussion will answer affirmatively to this question.

**Proposition 7.2.** *Let $R$ be an integral domain, and $d, d' \in R$ such that $(d) = (d')$. Then $d'$ and $d$ are associates, i.e., there exists a unit $u \in R$ such that $d' = ud$. Therefore, a greatest common divisor of any two elements is unique up to multiplication by a unit.*

*Proof.* If either $d$ or $d'$ is zero, then the claim follows trivially, so assume that both $d$ and $d'$ are non-zeros. Since $d \in (d')$ there is $x \in R$ such that $d = xd'$. Similarly, $d' \in (d)$ so $d' = yd$ for some $y \in R$. Putting them together, we have $d = xd' = xyd$, so $d(1 - xy) = 0$. But then $d$ is non-zero, and $R$ is an integral domain; thus, $xy = 1$, i.e., both $x$ and $y$ are units. The second part is immediate from the fact that any two greatest common divisors of $a$ and $b$ generate the same ideal, namely the smallest principal ideal containing both $a$ and $b$. □

**Proposition 7.3.** *Let $R$ be a PID, and let $a$ and $b$ be non-zero elements of $R$. Suppose that $d$ is a generator for the principal ideal generated by $a$ and $b$. Then the following are true.*

*(1) $d$ is a GCD of $a$ and $b$*
*(2) $d$ is unique up to multiplication by a unit of $R$. In other words, greatest common divisors of $a$ and $b$ are associates of each other.*
*(3) (Generalized Bézout's identity) $d$ can be written as a $R$-linear combination of $a$ and $b$: that is, there exist $x, y \in R$ such that $d = ax + by$.*

*Proof.* The first two claims follow immediately from Propositions 7.1 and 7.2. Since $(d) = (a, b)$, we have $d \in (a, b)$. Therefore there exist $x, y \in R$ such that $ax+by = d$, as required. □

A PID also satisfies a few other important conditions. Specifically, we will focus on two properties. First, every prime ideal is a maximal ideal in a PID. (Recall that in general, every maximal ideal is a prime ideal, whereas the converse is not true.) Second, every PID satisfies the ascending chain condition, whose definition we shall introduce now.

**Definition 7.4.** Suppose that $R$ is a commutative ring, and that

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

is an arbitrary ascending chain of ideals of $R$. If there exists $N$ such that $I_n = I_{n+1}$ for any $n \geq N$, then we say that $R$ *satisfies an ascending chain condition*. A ring satisfying the ascending chain condition is called a *Noetherian ring*.

**Proposition 7.4.** *Every PID is Noetherian.*

*Proof.* Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals of $R$, a PID. If $I := \bigcup I_n$, then $I$ is indeed an ideal. But $R$ is a PID, so there is $a \in R$ so that $I = (a)$. $a \in \bigcup I_n$, so there exists some $N$ such that $a \in I_N$, meaning $(a) \subseteq I_N \subseteq I$. Thus $I_N = I = (a)$, so $I_m = I$ for any $m \geq N$, as desired. □

*Remark.* In fact, a (commutative) ring $R$ is Noetherian if and only if every ideal of $R$ is finitely generated. So Proposition 7.4 can be derived as a corollary to this theorem. For the proof of this more general theorem and more information on Noetherian rings, refer to the PMATH 646 (Commutative algebra) notes.

**Proposition 7.5.** *Let $R$ be a principal ideal domain, and let $(p)$ be a non-zero prime ideal of $R$. Then $(p)$ is a maximal ideal. Thus, every non-zero prime ideal in a PID is also a maximal ideal.*

*Proof.* Suppose that $I = (m)$ is an ideal of $R$ containing $(p)$. $(p) \subseteq (m)$, so there exists $r \in R$ such that $p = rm$. Since $rm \in (p)$, at least one of $r$ and $m$ must lie in $(p)$. If $m \in (p)$ then $(m) \subseteq (p)$, so $(p) = (m) = I$. Suppose instead that $r \in (p)$. Then there is $s \in R$ such that $r = ps$. Hence $p = rm = psm$, or $p(1 - sm) = 0$. $(p)$ is a non-zero prime ideal, so $p \neq 0$, which forces $1 - sm = 0$. Therefore $sm = 1$, so $m$ is in fact a unit of $R$. Thus in this case, $I = (m) = R$, as required. □

**Corollary 7.1.** *Suppose that $R$ is a commutative ring such that the polynomial ring $R[x]$ is a PID. Then $R$ is a field.*

*Proof.* Suppose that $R[x]$ is a principal ideal domain. $R$ is a subring of $R[x]$, and $R[x]$ has unity 1 if and only if $R$ does. These facts lead us to conclude that $R$ must at least be an integral domain. Recall that $R[x]/(x) \cong R$; since $R$ is an integral domain, $(x)$ must be a prime ideal. But $R[x]$ is a PID, so $(x)$ is a maximal ideal also. $R[x]/(x)$ is thus in fact a field, so $R$ is also a field. □

The last proposition of this section provides the converse of Propositions 7.3 and 7.4.

**Proposition 7.6.** *Suppose that $R$ is an integral domain that satisfies the following two conditions.*

- *(i) (Generalized Bézout's identity) Any two non-zero elements $x, y \in R$ have a GCD which can be written in the form $rx + sy$ for some $r, s \in R$.*
- *(ii) (Ascending chain condition on principal ideals) If $x_1, x_2, x_3, \ldots$ are non-zero elements of $R$ such that $x_{i+1} \mid x_i$ for all $i \geq 1$, then there is a positive integer $N$ such that $x_n$ is a unit times $x_N$ for all $n \geq N$.*

*Then $R$ is a PID.*

*Proof.* Let $I$ be any finitely generated ideal of $R$, i.e., $I = (x_1, \ldots, x_n)$. By the first condition, we have $(x, y) = (d)$ where $d = \gcd(x, y)$. Indeed, $d = rx + sy \in (x, y)$, so $(d) \subseteq (x, y)$. Conversely, since $d \,|\, x$ and $d \,|\, y$, it follows that $x, y \in (d)$, or $(x, y) \subseteq (d)$. Hence $(d) = (x, y)$. Thus repeatedly applying this argument to $I$ (pick any of the two generators, apply this reasoning, and repeat this procedure) eventually gives us some $D \in R$ such that $I = (D)$.

Suppose that $J = (x_1, x_2, \ldots)$ is an ideal of $R$ that is infinitely generated. Then the chain of ideals $(x_1) \subsetneq (x_1, x_2) \subsetneq (x_1, x_2, x_3) \subsetneq \cdots$ is an ascending chain of ideals that does not stop. But from the first point, we know that there is $y_i$ such that $(x_1, x_2, \ldots, x_i) = (y_i)$, so our chain of ideals becomes in fact $(y_1) \subsetneq (y_2) \subsetneq (y_3) \subsetneq \cdots$. Therefore we have $y_{i+1} \,|\, y_i$ for any $i \geq 1$. But the second condition implies that for some sufficiently large $N$, we must have $y_n = u_n y_N$ for all $n \geq N$ (for some appropriate unit $u_n$), which implies that $(y_n) = (y_N)$ for all $n \geq N$. This contradicts the fact that the chain $(y_1) \subsetneq (y_2) \subsetneq \cdots$ does not stabilize. Hence every ideal of $R$ must be finitely generated, so every ideal is generated by a single element. Hence $R$ is a PID. $\square$

Department of Mathematics and Statistics, Dalhousie University, 6316 Coburg Rd, Halifax, NS, Canada B3H 4R2

*E-mail address*: hsyang@dal.ca