Math 453: Ring Theory Fact Sheet

March 7, 2019

Contents

1 Basic Concepts

Consider the set of continuous functions $C(\mathbf{R})$ from $f\colon \mathbf{R} \to \mathbf{R}$. The set $C(\mathbf{R})$ can be given two binary operations:

$$(f+g)(x) = f(x)+g(x), \quad (fg)(x) = f(x)g(x)$$

where the right hand sides are defined via regular addition and multiplication. This is a consequence of the basic analytic/topological facts that the sum and product of continuous functions is a continuous function. We see that under the addition operation, $C(\mathbf{R})$ is a commutative group with additive identity $\mathbf{0}$ where $\mathbf{0}(x) = 0$ for all $x \in \mathbf{R}$. Given a function $f\colon \mathbf{R} \to \mathbf{R}$, the additive inverse is given by the function $g\colon \mathbf{R} \to \mathbf{R}$ satisfying

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

for all $x \in \mathbf{R}$. Solving for $g(x)$, we see that

$$g(x) = -f(x).$$

The function g is continuous since f is continuous.

Under multiplication, $C(\mathbf{R})$ is a monoid with identity $\mathbf{1}\colon \mathbf{R} \to \mathbf{R}$ defined by $\mathbf{1}(x) = 1$ for all $x \in \mathbf{R}$. If $f\colon \mathbf{R} \to \mathbf{R}$ has a multiplicative inverse, then there would exist a continuous function $g\colon \mathbf{R} \to \mathbf{R}$ such that

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

for all $x \in \mathbf{R}$. Provided $f(x) \neq 0$, we can solve for $g(x)$:

$$g(x) = \frac{1}{f(x)}.$$

In particular, if $f(x) = 0$ for any $x \in \mathbf{R}$, then f cannot have a multiplicative inverse, and so $C(\mathbf{R})$ does not have inverses under multiplication for all functions. Finally, we have a distributive law:

$$(f(g+h))(x) = f(x)(g(x)+h(x)) = f(x)g(x)+f(x)h(x) = (fg)(x)+(fh)(x).$$

The set $C(\mathbf{R})$ with these two operations is an example of a commutative ring.

This ring can be connected back to $\mathbf{R}$ as well. Given $x_0 \in \mathbf{R}$, we define

$$\mathfrak{m}_{x_0} = \{f \in C(\mathbf{R}) \ : \ f(x_0) = 0\}.$$

Notice that $\mathfrak{m}_{x_0}$ is closed under addition and additive inverses. Even more, given $f \in \mathfrak{m}_{x_0}$ and $g \in C(\mathbf{R})$, we have $fg \in \mathfrak{m}_{x_0}$, and so $\mathfrak{m}_{x_0}$ is closed under an even stronger condition with regard to multiplication. The subset $\mathfrak{m}_{x_0}$ is an ideal in the ring $C(\mathbf{R})$.

1.1 Basic Definitions

Definition 1 (Rng)**.** A **rng** is a set R with a pair of binary operations

$$+\colon R \times R \to R, \quad \cdot\colon R \times R \to R$$

such that $(R,+)$ is a commutative group with identity 0, $(R,\cdot)$ is a semigroup, and for each $r,s,t \in R$, we have

$$r(s+t) = rs+rt, \quad (s+t)r = sr+tr.$$

We refer to $r(s+t) = rs+rt$ as **left distribution of multiplication** and we refer to $(s+t)r = sr+tr$ as **right distributions of multiplication**.

Definition 2 (Ring)**.** A **ring** is a set with a pair of binary operations

$$+ : R \times R \to R, \quad \cdot : R \times R \to R$$

such that $(R,+)$ is a commutative group with identity 0, $(R,\cdot)$ is a monoid with identity 1, and

$$a(b+c) = ab+ac, \quad (b+c)a = ba+ca.$$

A basic example of a ring is $\mathrm{M}(n,\mathbf{R})$, the set of n by n matrices with real coefficients. Matrix addition and matrix multiplication are the ring operations, and the identity for addition is the zero matrix and the identity for multiplication is I_n, the identity matrix.

Definition 3 (Commutative Ring)**.** A **commutative ring** is a set with a pair of binary operations

$$+ : R \times R \to R, \quad \cdot : R \times R \to R$$

such that $(R,+)$ is a commutative group with identity 0, $(R,\cdot)$ is a commutative monoid with identity 1, and

$$a(b+c) = ab+ac.$$

The integers $\mathbf{Z}$ with addition and multiplication is an example of a commutative ring. Note that $\mathrm{M}(n,\mathbf{R})$ is a commutative ring precisely when $n = 1$.

Definition 4 (Field)**.** A **field** is a set with a pair of binary operations

$$+ : R \times R \to R, \quad \cdot : R \times R \to R$$

such that $(R,+)$ is a commutative group with identity 0, $(R-\{0\},\cdot)$ is a commutative group with identity 1, and

$$a(b+c) = ab+ac.$$

The rational numbers $\mathbf{Q}$, the real numbers $\mathbf{R}$, and the complex number $\mathbf{C}$ are all examples of fields.

Definition 5 (Division Ring)**.** A **division ring** is a set with a pair of binary operations

$$+ : R \times R \to R, \quad \cdot : R \times R \to R$$

such that $(R,+)$ is a commutative group with identity 0, $(R-\{0\},\cdot)$ is a group with identity 1, and

$$a(b+c) = ab+ac, \quad (b+c)a = ba+ca.$$

Let $R = \mathbf{R}[1,x,y,z]$ be a 4–dimensional vector space with basis $\{1,x,y,z\}$. We define multiplication by

$$x^2 = -1, y^2 = -1, \quad z = xy = -yx.$$

We also declare that scalar multiples of 1 commute with everything in R. Note that

$$z^2 = (xy)(xy) = -xxyy = -1, \quad xz = xxy = -y, \quad zx = xyx = y, \quad yz = yxy = x, \quad zy = xyy = -x.$$

Any element $r \in R$ can be written uniquely as

$$r = \alpha_1 + \alpha_x x + \alpha_y y + \alpha_z z.$$

Given

$$s = \beta_1 + \beta_x x + \beta_y y + \beta_z z$$

we have

$$\begin{aligned} rs &= (\alpha_1 + \alpha_x x + \alpha_y y + \alpha_z z)(\beta_1 + \beta_x x + \beta_y y + \beta_z z) \\ &= \alpha_1\beta_1 + \alpha_1\beta_x x + \alpha_1\beta_y y + \alpha_1\beta_z z + \alpha_x\beta_1 x + \alpha_x\beta_x x^2 + \alpha_x\beta_y xy + \alpha_x\beta_z xz \\ &\quad + \alpha_y\beta_1 y + \alpha_y\beta_x yx + \alpha_y\beta_y y^2 + \alpha_y\beta_z yz + \alpha_z\beta_1 z + \alpha_z\beta_x zx + \alpha_z\beta_y zy + \alpha_z\beta_z z^2 \\ &= (\alpha_1\beta_1 - \alpha_x\beta_x - \alpha_y\beta_y - \alpha_z\beta_z) + (\alpha_1\beta_x + \alpha_x\beta_1 + \alpha_y\beta_z - \alpha_z\beta_y)x \\ &\quad + (\alpha_1\beta_y + \alpha_y\beta_1 + \alpha_z\beta_x - \alpha_x\beta_z)y + (\alpha_1\beta_z + \alpha_z\beta_1 + \alpha_x\beta_y - \alpha_y\beta_x)z. \end{aligned}$$

Given $r = \alpha_1 + \alpha_x x + \alpha_y y + \alpha_z z$, we define

$$\overline{r} = \alpha_1 - \alpha_x x - \alpha_y y - \alpha_z z.$$

The reader can verify that

$$r\overline{r} = \alpha_1^2 + \alpha_x^2 + \alpha_y^2 + \alpha_z^2$$

and if $r \neq 0$, then

$$r^{-1} = \frac{\overline{r}}{\alpha_1^2 + \alpha_x^2 + \alpha_y^2 + \alpha_z^2}.$$

In particular, this ring is a division ring since every non-zero element has an inverse under multiplication.

Definition 6 (Zero Divisor)**.** Given a ring R, we say $r \in R$ is a **zero divisor** if there exists $s \in R$ with $s \neq 0$ such that $rs = 0$. If $r \neq 0$ and is a zero divisor, we call r a **non-zero zero divisor**.

Let $R = \mathbf{Z}/4\mathbf{Z}$. Then $\overline{2} \cdot \overline{2} = \overline{0}$ and so $\overline{2}$ is a non-zero zero divisor.

Definition 7 (Unit)**.** Given a ring R, we say that $r \in R$ is a **unit** if there exists $s \in R$ such that $rs = sr = 1$. We denote the subset of R of units by $R^\times$.

If $R = \mathbf{Z}$, then $R^\times = \{\pm 1\}$. If $R = \mathrm{M}(n, \mathbf{R})$, then $R^\times = \mathrm{GL}(n, \mathbf{R})$.

Definition 8 (Integral Domain)**.** We say that a commutative ring R is a **integral domain** if R has no non-zero zero divisors.

Definition 9 (Left/Right Cancellation)**.** We say that a commutative ring R has the **left cancellation property** if whenever $ab = ac$ for $a, b, c \in R$ with $a \neq 0$, then $b = c$. We say that a commutative ring R has the **right cancellation property** if whenever $ba = ca$ for $a, b, c \in R$ with $a \neq 0$, then $b = c$.

1.2 List of Properties for rngs, rings, fields, division fields, and integral domains

For the reader's sake, we list all of the properties of rngs, rings, commutative rings, fields, division fields and integral domains.

1.2.1 Properties of a Rng

(Additive Identity) There exists $0 \in R$ such that $0_R + r = r + 0_R = r$ for all $r \in R$. Often we write 0 instead of 0_R and we call 0_R the additive identity.

(Additive Inverses) For each $r \in R$, there exists $s \in R$ such that $r + s = s + r = 0_R$. We write $s = -r$ for this unique element and we call $-r$ the additive inverse of r.

(Additive Associativity) For each $r, s, t \in R$, we have $r + (s + t) = (r + s) + t$.

(Additive Commutativity) For each $r, s \in R$, we have $r + s = s + r$.

(Multiplicative Associativity) For each $r, s, t \in R$, we have $r(st) = (rs)t$.

(Left/Right Distribution) For each $r, s, t \in R$, we have $r(s + t) = rs + rt$ and $(s + t)r = sr + tr$.

1.2.2 Properties of a Ring

(Additive Identity) There exists $0 \in R$ such that $0_R + r = r + 0_R = r$ for all $r \in R$. Often we write 0 instead of 0_R and we call 0_R the additive identity.

(Additive Inverses) For each $r \in R$, there exists $s \in R$ such that $r + s = s + r = 0_R$. We write $s = -r$ for this unique element and we call $-r$ the additive inverse of r.

(Additive Associativity) For each $r, s, t \in R$, we have $r + (s + t) = (r + s) + t$.

(Additive Commutativity) For each $r, s \in R$, we have $r + s = s + r$.

(Multiplicative Identity) There exists $1_R \in R$ such that $1_R r = r 1_R = r$ for all $r \in R$.

(Multiplicative Associativity) For each $r, s, t \in R$, we have $r(st) = (rs)t$.

(Left/Right Distribution) For each $r, s, t \in R$, we have $r(s + t) = rs + rt$ and $(s + t)r = sr + tr$.

1.2.3 Properties of a Commutative Ring

(Additive Identity) There exists $0 \in R$ such that $0_R + r = r + 0_R = r$ for all $r \in R$. Often we write 0 instead of 0_R and we call 0_R the additive identity.

(Additive Inverses) For each $r \in R$, there exists $s \in R$ such that $r + s = s + r = 0_R$. We write $s = -r$ for this unique element and we call $-r$ the additive inverse of r.

(Additive Associativity) For each $r, s, t \in R$, we have $r + (s + t) = (r + s) + t$.

(Additive Commutativity) For each $r, s \in R$, we have $r + s = s + r$.

(Multiplicative Identity) There exists $1_R \in R$ such that $1_R r = r 1_R = r$ for all $r \in R$.

(Multiplicative Associativity) For each $r, s, t \in R$, we have $r(st) = (rs)t$.

(Multiplicative Commutativity) For each $r, s \in R$, we have $rs = sr$.

(Distribution) For each $r, s, t \in R$, we have $r(s + t) = rs + rt$.

1.2.4 Properties of an Integral Domain

(Additive Identity) There exists $0 \in R$ such that $0_R + r = r + 0_R = r$ for all $r \in R$. Often we write 0 instead of 0_R and we call 0_R the additive identity.

(Additive Inverses) For each $r \in R$, there exists $s \in R$ such that $r + s = s + r = 0_R$. We write $s = -r$ for this unique element and we call $-r$ the additive inverse of r.

(Additive Associativity) For each $r, s, t \in R$, we have $r + (s + t) = (r + s) + t$.

(Additive Commutativity) For each $r, s \in R$, we have $r + s = s + r$.

(Multiplicative Identity) There exists $1_R \in R$ such that $1_R r = r 1_R = r$ for all $r \in R$.

(Multiplicative Associativity) For each $r, s, t \in R$, we have $r(st) = (rs)t$.

(Multiplicative Commutativity) For each $r, s \in R$, we have $rs = sr$.

(Multiplicative Cancellation) Given $r, s, t \in R$ with $r \neq 0$ such that $rs = rt$, then $s = t$.

(Distribution) For each $r, s, t \in R$, we have $r(s + t) = rs + rt$.

1.2.5 Properties of a Division Field

(Additive Identity) There exists $0 \in R$ such that $0_R + r = r + 0_R = r$ for all $r \in R$. Often we write 0 instead of 0_R and we call 0_R the additive identity.

(Additive Inverses) For each $r \in R$, there exists $s \in R$ such that $r + s = s + r = 0_R$. We write $s = -r$ for this unique element and we call $-r$ the additive inverse of r.

(Additive Associativity) For each $r, s, t \in R$, we have $r + (s + t) = (r + s) + t$.

(Additive Commutativity) For each $r, s \in R$, we have $r + s = s + r$.

(Multiplicative Identity) There exists $1_R \in R$ such that $1_R r = r 1_R = r$ for all $r \in R$.

(Multiplicative Inverses) For each $r \in R$ with $r \neq 0_R$, there exists $s \in R$ such that $rs = sr = 1_R$. We write $s = r^{-1}$ for this unique element and we call r^{-1} the multiplicative inverse of r.

(Multiplicative Associativity) For each $r, s, t \in R$, we have $r(st) = (rs)t$.

(Distribution) For each $r, s, t \in R$, we have $r(s + t) = rs + rt$ and $(s + t)r = sr + tr$.

1.2.6 Properties of a Field

(Additive Identity) There exists $0 \in R$ such that $0_R + r = r + 0_R = r$ for all $r \in R$. Often we write 0 instead of 0_R and we call 0_R the additive identity.

(Additive Inverses) For each $r \in R$, there exists $s \in R$ such that $r + s = s + r = 0_R$. We write $s = -r$ for this unique element and we call $-r$ the additive inverse of r.

(Additive Associativity) For each $r, s, t \in R$, we have $r + (s + t) = (r + s) + t$.

(Additive Commutativity) For each $r, s \in R$, we have $r + s = s + r$.

(Multiplicative Identity) There exists $1_R \in R$ such that $1_R r = r 1_R = r$ for all $r \in R$.

(Multiplicative Inverses) For each $r \in R$ with $r \neq 0_R$, there exists $s \in R$ such that $rs = sr = 1_R$. We write $s = r^{-1}$ for this unique element and we call r^{-1} the multiplicative inverse of r.

(Multiplicative Associativity) For each $r, s, t \in R$, we have $r(st) = (rs)t$.

(Multiplicative Commutativity) For each $r, s \in R$, we have $rs = sr$.

(Distribution) For each $r, s, t \in R$, we have $r(s + t) = rs + rt$.

1.3 Homomorphism and Subrings

Definition 10 (Homomorphism)**.** Let R, S be commutative rings. We say that a function $\varphi : R \to S$ is a **ring homomorphism** if

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2), \quad \varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2), \quad \varphi(1) = 1$$

holds for all $r_1, r_2 \in R$.

Definition 11 (Kernel)**.** For commutative rings R, S and a homomorphism $\varphi : R \to S$, we define the **kernel of φ**

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

Definition 12 (Subring)**.** Given a commutative ring R and a subset $S \subset R$, we say that S is a **subring** if S satisfies the following:

(1) $0, 1 \in S$.

(2) If $s, t \in S$, then $s + t \in S$.

(3) If $s, t \in S$, then $st \in S$.

(4) If $s \in S$, then $-s \in S$.

When S is a subring of R, we write $S \leq R$.

Definition 13 (Subfield)**.** Given a field E, we say a subset $F \subset E$ is a **subfield** if F satisfies the following:

(1) $0, 1 \in F$.

(2) If $\alpha, \beta \in F$, then $\alpha + \beta \in F$.

(3) If $\alpha, \beta \in F$, then $\alpha\beta \in F$.

(4) If $\alpha \in F$, then $-\alpha \in F$.

(5) If $\alpha \in F$, then $\alpha^{-1} \in F$

When F is a subfield of E, we write $F \leq E$. We also refer to E as an **extension** of F and write E/F to denote that E is an extension of F.

Remark. It turns out that there are no non-trivial quotients of fields and so we will never use the quotient notation when working with fields. In particular, the reader should not confuse our notation for extensions of fields E/F with that of a quotient E/F.

Lemma 1.1. *Let R be a commutative ring and let $S \subset R$. Then S is a subring of R if and only if the following conditions are satisfied:*

(1) $1 \in S$.

(2) $r - s \in S$ *for all* $r, s \in S$.

(3) $rs \in S$ *for all* $r, s \in S$.

We will prove this lemma and leave the proof of the forthcoming lemma as an exercise for the reader.

Proof. Clearly, if S is a subring, then S satisfies the above reduced class of conditions. For the converse, by (1) and (2), we see that $1 - 1 = 0 \in S$. To see that S is closed under multiplication, given $r, s \in S$, we use r and $-s$ in (2) and get $r + s \in S$. To see that S is closed under inverses, we use that $0 \in S$ and take $r = 0$ and $-s$ in (2) to get $-s \in S$ for all $s \in S$. By (3), we know that S is closed under multiplication. This verifies all of what is needed in the definition of a subring. □

Lemma 1.2. *Let E be a field and let $F \subset E$. Then F is a subfield of E if and only if the following conditions are satisfied:*

(1) $F \neq \emptyset$.

(2) $\alpha - \beta \in F$ *for all* $\alpha, \beta \in F$.

(3) $\alpha\beta^{-1} \in F$ *for all* $\alpha, \beta \in F$.

1.4 Examples

1.4.1 Products

Given commutative rings R, S, we define the product ring to be the set $R \times S$ with the addition and multiplication given coordinate-wise. Specifically,

$$(r_1, s_1) + (r_2, s_2) \stackrel{\text{def}}{=} (r_1 + r_2, s_1 + s_2), \quad (r_1, s_1)(r_2, s_2) \stackrel{\text{def}}{=} (r_1 r_2, s_1 s_2).$$

1.4.2 Polynomial Rings

1.4.3 Other functional rings

2 Ideals

2.1 Basics

Definition 14 (Closed Under Multiplication)**.** Given a commutative ring R and a subset $\mathfrak{a} \subset R$, we say $\mathfrak{a}$ is **closed under multiplication** if $a_1 a_2 \in \mathfrak{a}$ for all $a_1, a_2 \in \mathfrak{a}$.

Definition 15 (Closed Under External Multiplication)**.** Given a commutative ring R and a subset $\mathfrak{a} \subset R$, we say $\mathfrak{a}$ is **closed under external multiplication** if $ra \in \mathfrak{a}$ for all $r \in R$ and $a \in \mathfrak{a}$.

Definition 16 (Ideal)**.** Let R be a commutative ring. We say a non-empty subset $\mathfrak{a} \subset R$ is an **ideal** if $\mathfrak{a}$ is a subgroup of R under addition, additive inverses, and closed under external multiplication. When $\mathfrak{a}$ is an ideal in R, we will write $\mathfrak{a} \lhd R$.

For the readers' sake, we also restate the definition of an ideal in terms of properties: A subset $\mathfrak{a}$ is an ideal in R if the following properties are satisfied:

(1) $0 \in \mathfrak{a}$.

(2) For each $a_1, a_2 \in \mathfrak{a}$, we have $a_1 + a_2 \in \mathfrak{a}$.

(3) For each $a \in \mathfrak{a}$, we have $-a \in \mathfrak{a}$.

(4) For each $a \in \mathfrak{a}$ and each $r \in R$, we have $ra \in \mathfrak{a}$.

The reader can verify that the following properties are equivalent to (1)-(4):

(1') $\mathfrak{a} \neq \emptyset$.

(2') For each $a_1, a_2 \in \mathfrak{a}$, we have $a_1 - a_2 \in \mathfrak{a}$.

(3') For each $a \in \mathfrak{a}$ and each $r \in R$, we have $ra \in \mathfrak{a}$.

Given a commutative ring R, the **zero ideal** is defined to be $\{0\}$. The reader can verify that $\{0\}$ is an ideal in R. The ring R is also an ideal in R. We say that an ideal $\mathfrak{a}$ is **non-zero** if $\mathfrak{a} \neq \{0\}$ and **proper** if $\mathfrak{a} \neq \mathbf{R}$.

Lemma 2.1. *If R is a commutative ring and $\mathfrak{a} \lhd R$ is an ideal with $r_0 \in \mathfrak{a}$ such that r_0 is a unit, then $\mathfrak{a} = R$.*

Proof. Since $\mathfrak{a}$ is closed under external multiplication and r_0 is a unit, we know that $r_0^{-1} \in R$ exists and that $r_0^{-1} r_0 \in \mathfrak{a}$. In particular, $1 \in \mathfrak{a}$. Given $r \in R$, since $\mathfrak{a}$ is closed under external multiplication and $1 \in \mathfrak{a}$, we see that $r \cdot 1 = r \in \mathfrak{a}$. Hence, $R \subset \mathfrak{a}$. By definition, $\mathfrak{a} \subset R$ and so $R = \mathfrak{a}$. □

Corollary 2.2. *Let R be a commutative ring with and let $\mathfrak{a}$ be an ideal in R. Then the following are equivalent:*

(1) $\mathfrak{a} = R$.

(2) $\mathfrak{a}$ *contains a unit.*

(3) $1 \in \mathfrak{a}$.

Remark. The above corollary follows easily from the previous lemma and the same type of arguments used in the proof of the lemma. One consequence of this corollary is that subrings cannot be ideals unless the subring is the whole ring R. Indeed, a subring must contain 1. Likewise, an ideal cannot be a subring unless it is the whole ring R.

Definition 17 (Prime Ideal)**.** Given a commutative ring and an ideal $\mathfrak{p} \lhd R$, we say that $\mathfrak{p}$ is a **prime ideal** if given $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$.

Definition 18 (Primary Ideal)**.** Given a commutative ring and an ideal $\mathfrak{p} \lhd R$, we say that $\mathfrak{p}$ is a **primary ideal** if given $ab \in \mathfrak{p}$, then either $a \in \mathfrak{p}$ or $b^n \in \mathfrak{p}$ for some $n \in \mathbf{N}$.

Definition 19 (Maximal Ideal)**.** Given a commutative ring and an ideal $\mathfrak{p} \lhd R$, we say that $\mathfrak{m}$ is a **maximal ideal** if whenever $\mathfrak{m} \subset \mathfrak{a}$ for some ideal $\mathfrak{a}$, then either $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = R$.

Definition 20 (Generators)**.** Given a ring R, an ideal $\mathfrak{a} \lhd R$, and a subset $S \subset \mathfrak{a}$, we say that S generates $\mathfrak{a}$ if every $a \in \mathfrak{a}$ can be written as

$$a = \sum_{j=1}^{n} r_j s_j$$

where $r_j \in R$ and $s_j \in S$. When S generates $\mathfrak{a}$, we write $\mathfrak{a} = \langle S \rangle$.

Definition 21 (Principle Ideal)**.** Given a ring R, we say an ideal $\mathfrak{a} \lhd R$ is **principle** if $\mathfrak{a}$ is generated by $\{a\}$ for some $a \in \mathfrak{a}$.

If an ideal $\mathfrak{a}$ is principle and generated by $a \in \mathfrak{a}$, we typically write $\langle a \rangle$.

Lemma 2.3. *Let R be a commutative ring such that R has no non-zero, proper ideals. Then R is a field.*

Proof. Let $\mathfrak{a}$ be an ideal of F that is not the trivial ideal. Then $\alpha \in \mathfrak{a}$ with $\alpha \neq 0$. Since F is a field, α is a unit and so $\mathfrak{a} = F$. □

Theorem 2.4 (Krull's Theorem)**.** *Let R be a commutative ring. Then R has a proper, maximal ideal $\mathfrak{m}$.*

Definition 22 (Local Ring)**.** We say that a commutative ring R is a **local ring** if R has a unique proper, maximal ideal.

Definition 23 (Principle Ideal Domain)**.** We say that an integral domain R is a **principle ideal domain** if every ideal in R is a principle ideal.

2.2 Products and Sum Sets

Given a commutative ring R and subsets $S,T \subset R$, we define the **sum of** S,T to be the subset

$$S+T = \{s+t \ : \ s \in S,\ t \in T\}$$

and we define the **product of** S,T to be the subset

$$ST = \{st \ : \ s \in S,\ t \in T\}.$$

We also define the nth power set of S to be

$$S^n = \{s_1 \dots s_n \ : \ s_1, \dots, s_n \in S\}.$$

Lemma 2.5. *If R is a commutative ring and $\mathfrak{a}, \mathfrak{b}$ are ideals in R, then $\mathfrak{a}+\mathfrak{b}$ is an ideal in R.*

The product set of ideals is not an ideal in general. When $\mathfrak{a}, \mathfrak{b}$ are ideals in R, we define the **product ideal**

$$\mathfrak{ab} = \left\{ \sum_{j=1}^{n} a_j b_j \ : \ a_1 \dots, a_n \in \mathfrak{a},\ b_1, \dots, b_n \in \mathfrak{b} \right\}.$$

The product ideal is generated by the product set of $\mathfrak{a}, \mathfrak{b}$ defined above.

Lemma 2.6. *Let R be a commutative ring with ideals $\mathfrak{a}, \mathfrak{b}$. Then $\mathfrak{a} \cap \mathfrak{b}$ is an ideal in R. Additionally, we have*

$$\mathfrak{ab} \subset \mathfrak{a} \cap \mathfrak{b} \subset \mathfrak{a} + \mathfrak{b}.$$

For an ideal $\mathfrak{a}$, we define the nth power of $\mathfrak{a}$ inductively: For $n = 2$, we have

$$\mathfrak{a}^2 = \mathfrak{aa}$$

where the right hand side is the product ideal of $\mathfrak{a}$ with itself. For $n > 2$, we define

$$\mathfrak{a}^n = \mathfrak{a}^{n-1}\mathfrak{a}.$$

2.3 Quotient Rings

Given a subring $S \subseteq R$, we can define a quotient space R/S as in the case of groups. We define an equivalence relation $\sim_S$ on R by $r_1 \sim_S r_2$ if and only if $r_1 - r_2 \in S$. The quotient space R/S is the set of equivalence classes $[r]_S$ under this equivalence relation $\sim_S$. Note that since R is a commutative group under addition and S is a subgroup of R (as a group under addition), the quotient space R/S is a commutative group. For clarity, we describe the additive operation on the quotient space. Given $r \in R$, we denote the equivalence class $[r]_S$ by $r+S$. Note that this notation is not randomly chosen. Specifically, given $r' \in [r]_S$, by definition of $\sim_S$, we know that $r' - r \in S$ and so there exists $s_0 \in S$ such that $r' = r + s_0$. In particular, every element in $[r]_S$ is of the form $r + s_0$ for some $s_0 \in S$. Consequently,

$$[r]_S = \{r + s_0 \ : \ s_0 \in S\} = r + S.$$

Given two equivalence classes $r_1 + S, r_2 + S \in R/S$, we have the binary operation

$$+ \colon R/S \times R/S \to R/S$$

given by

$$+(r_1 + S, r_2 + S) = (r_1 + r_2) + S.$$

One must check that this binary operation is well defined (i.e. independent of the choice of representatives r_1, r_2). Given $r_3 \in r_1 + S$ and $r_4 \in r_2 + S$, we must show that $(r_3 + r_4) \sim_S (r_1 + r_2)$. By definition of $\sim_S$, there exists $s_1, s_2 \in S$ such that $r_3 = r_1 + s_1$ and $r_4 = r_2 + s_2$. In particular,

$$(r_3 + r_4) - (r_1 + r_2) = r_1 + s_1 + r_2 + s_2 - r_1 - r_2 = s_1 + s_2 \in S.$$

For a general subring, we cannot endow the quotient space with a commutative ring structure. Specifically, we would like to define a multiplicative operation on R/S via

$$(r_1 + S) \cdot (r_2 + S) \stackrel{\text{def}}{=} (r_1 r_2) + S.$$

In order for this operation to be well defined, we need to prove that it is independent of our choices of r_1, r_2. Given $r_3 \in r_1 + S$ and $r_4 \in r_2 + S$, we need $r_3 r_4 \sim_S r_1 r_2$. By definition of $\sim_S$, there exist $s_1, s_2 \in S$ such that $r_3 = r_1 + s_1$ and $r_4 = r_2 + s_2$. In particular, we have

$$r_3 r_4 = (r_1 + s_1)(r_2 + s_2) = r_1 r_2 + s_1 r_2 + s_2 r_1 + s_1 s_2.$$

If $r_3 r_4 \sim_S r_1 r_2$, we see that

$$s_1 r_2 + s_2 r_1 + s_1 s_2 \in S.$$

This need not be the case for a general subring. However, if S is an ideal, we know that $s_1 r_2, s_2 r_1, s_1 s_2 \in S$ and so $r_1 r_2 \sim_S r_3 r_4$.

Definition 24 (Quotient Ring)**.** Let R be a commutative ring with identity and $\mathfrak{a} \lhd R$. Then $R/\mathfrak{a}$ is a commutative ring and is called the **quotient ring** associated to $\mathfrak{a}$.

As before, we define the index of a subring $S \subseteq R$ to be $||S|| \stackrel{\text{def}}{=} |R/S|$. Note that we have chosen different notation for the index in the setting of rings than we used in the setting of groups. We have done this for future notational reasons. Specifically, when we begin our study of fields, we will use the notation $[L : K]$ to denote the degree of the field extension. Our use of $||\cdot||$ is somewhat common, especially when one is working with ideals in rings of integers of number fields.

Given a ring R and $\mathfrak{a} \lhd R$, we have the associated quotient ring $R/\mathfrak{a}$. There is a **canonical ring homomorphism** $\psi_{\mathfrak{a}} : R \to R/\mathfrak{a}$ given by $\psi_{\mathfrak{a}}(r) = r + \mathfrak{a}$. Note that this homomorphism is surjective.

2.4 Isomorphism Theorem: Rings

The proofs of these results are similar enough to the setting of groups that we omit the proofs; the reader can easily find proofs of these results online or any any reasonable textbook in abstract algebra.

Theorem 2.7 (First Isomorphism Theorem)**.** *Let R, R' be commutative rings and $\psi : R \to R'$ be a ring homomorphism. Then $\psi(R)$ is isomorphic to $R/\ker\psi$. In particular, if ψ is surjective, R' is isomorphic to $R/\ker\psi$.*

Theorem 2.8 (Second Isomorphism Theorem)**.** *Let R be a commutative ring, $S \leq R$ a subring, and $\mathfrak{a} \lhd R$. Then*

(a) The subset

$$S + \mathfrak{a} \stackrel{def}{=} \{s + a \ : \ s \in S, \ a \in \mathfrak{a}\}$$

is a subring of R.

(b) $S \cap \mathfrak{a}$ is an ideal in S.

(c) The rings $(S + \mathfrak{a})/\mathfrak{a}$ and $S/(S \cap \mathfrak{a})$ are isomorphic.

Theorem 2.9 (Third Isomorphism Theorem)**.** *Let R be a commutative ring and $\mathfrak{a} \lhd R$. Then*

(a) If $S \leq R$ and $\mathfrak{a} \subseteq S \subseteq R$, then $S/\mathfrak{a}$ is a subring of $R/\mathfrak{a}$.

(b) Every subring of $R/\mathfrak{a}$ is of the form $S/\mathfrak{a}$, for some $S \leq R$ such that $\mathfrak{a} \subseteq S \subseteq R$.

(c) If $\mathfrak{b} \lhd R$ and $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R$, then $\mathfrak{b}/\mathfrak{a}$ is an ideal of $R/\mathfrak{a}$.

(d) Every ideal of $R/\mathfrak{a}$ is of the form $\mathfrak{b}/\mathfrak{a}$, for some $\mathfrak{b} \lhd R$ such that $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R$.

(e) If $\mathfrak{b} \lhd R$ and $\mathfrak{a} \subseteq \mathfrak{b} \subseteq R$, then the rings $(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a})$ and $R/\mathfrak{b}$ are isomorphic.

2.5 Maximal ideals and fields

Recall that

Lemma 2.10. *If R is a ring and $\mathfrak{p}$ is an ideal in R, then $\mathfrak{p}$ is a prime ideal if and only if $R/\mathfrak{p}$ is an integral domain.*

A similar characterization of maximal ideals can also be established.

Lemma 2.11. *Let R be a commutative ring with identity and $\mathfrak{m} \lhd R$. Then $\mathfrak{m}$ is a maximal ideal if and only if $R/\mathfrak{m}$ is a field.*

Proof. We first assume that $\mathfrak{m}$ is maximal. Given $r \in R - \mathfrak{m}$, we know that the ideal generated by $\mathfrak{m}$ and r is all of R. In particular, for some $r' \in R$, we just have $r'r + r'm = 1_R$. Hence, $rr' + \mathfrak{m} = 1_R + \mathfrak{m}$, and so $r + \mathfrak{m}$ is a unit in $R/\mathfrak{m}$. Thus, $R/\mathfrak{m}$ is a field.

Next, we assume $R/\mathfrak{m}$ is a field. Since every non-zero element of $R/\mathfrak{m}$ is a unit, it follows that $R/\mathfrak{m}$ has no non-zero, proper ideals. Hence, by the Third Isomorphism Theorem, $\mathfrak{m}$ is maximal. □

Since fields are integral domains, we obtain an immediate corollary of Lemma 2.11.

Corollary 2.12. *Let R be a commutative ring with identity and $\mathfrak{a} \lhd R$. If $\mathfrak{a}$ is maximal, then $\mathfrak{a}$ is prime.*

We know that $p\mathbf{Z}$ is a maximal ideal in $\mathbf{Z}$ if and only if p is a prime. Consequently, by Lemma 2.11, $\mathbf{Z}/p\mathbf{Z}$ is a field if and only if p is a prime. The cardinality of $\mathbf{Z}/p\mathbf{Z}$ is p and hence when p is prime, yields a finite field of cardinality p. We denote this field by $\mathbf{F}_p$.

3 Polynomial Rings

This section addresses polynomial rings. Polynomials rings are sets of polynomials (e.g. $x^2 - 1$ or $x^2 + x + 1$) together with addition and multiplication operations. For instance

$$(x^2 - 1) + (x^2 + x + 1) = 2x^2 + x, \quad (x^2 - 1)(x^2 + x + 1) = x^4 + x^3 - x - 1.$$

We will work with polynomials with coefficients in a general field F though the reader can take $F = \mathbf{Q}$ in all that follows without worry. In more advanced part of this theory, the field F matters.

3.1 Basics

Given a field F and $\alpha_0, \ldots, \alpha_n \in F$, we can define a function $P\colon F \to F$ where

$$P(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \cdots + \alpha_1 x + \alpha_0.$$

We call P a **polynomial with coefficients in** F. Given two polynomials

$$P(x) = \sum_{j=0}^{n} \alpha_j x^j, \quad Q(x) = \sum_{j=0}^{m} \beta_j x^j$$

then

$$(P+Q)(x) = \sum_{j=0}^{\max\{m,n\}} (\alpha_j + \beta_j) x^j$$

and

$$(PQ)(x) = \sum_{j=0}^{m} \sum_{k=0}^{n} \alpha_k \beta_j x^{j+k}.$$

Under these two operations, the set of polynomials with coefficients in F is a commutative ring with additive inverse

$$\mathbf{0}\colon F \to F, \quad \mathbf{0}(x) = 0$$

and multiplicative identity given by

$$\mathbf{1}\colon F \to F, \quad \mathbf{1}(x) = 1.$$

We denote the ring of polynomials with coefficients in F by $F[x]$.

The remainder of this section will be on establish results for $F[x]$ that are analogous to $\mathbf{Z}$. Specifically, we will give a factorization theorem in terms of "primes" polynomials and we will also establish a concept of greatest common divisors. This all functions though the division algorithm for polynomials that you learned with you were little. We will first review this for $\mathbf{Z}$ in order to stress the connection.

Before proceeding forward, we remind the reader of a few basic concepts with regard to polynomials. Given $P \in F[x]$, we know that

$$P(x) = \sum_{j=0}^{n} \alpha_j x^j.$$

When we write this, it is assumed that $\alpha_n \neq 0$ and under this assumption, we say that P has **degree** n and write $\deg(P) = n$. We note that

$$\deg(P+Q) \leq \max\{\deg(P), \deg(Q)\}, \quad \deg(PQ) = \deg(P)\deg(Q).$$

We will use $\deg(P)$ as the analog of $|n|$ for $n \in \mathbf{Z}$; it is a measure of "complexity" in both cases. The algorithms we give below function on "complexity reduction", especially the Euclidean algorithm. The basic idea is that what you want to find should be a minimize of the complexity you define. You then find "operations" to perform that reduce (or at least do not increase) the complexity after applying the operation. You then prove that these moves do actually decrease the complexity (if not always like in our setting) and then stop once you find a minimal complexity object. This is an instance of a general strategy in problem solving when you want to find something. You introduce a notion of complexity and then find a minimizer of complexity. This method has been used extensively in mathematics and can be quite powerful; I have personally used it in research though others have used it to establish much more spectacular results than me.

3.2 Division Algorithm and Euclidean Algorithm

Given two elements $\alpha, \beta \in \mathbf{Z}$ with $\beta \neq 0$, there exist $q, r \in \mathbf{Z}$ such that $\alpha = q\beta + r$ where either $r = 0$ or $|r| < |\beta|$. For simplicity, we will assume that both $\alpha, \beta > 0$. To find q, r, we proceed as follows. There is a smallest integer q such that

$$q\beta \leq \alpha < (q+1)\beta.$$

In particular, $\alpha - q\beta = r \geq 0$ and $0 \leq r < \beta$.

Assuming still that $\alpha, \beta > 0$, the greatest common divisor of α, β is the largest positive integer d such that d divides a, b. It follows that any integer d' that divides α, β also divides d and that there exist $a, b \in \mathbf{Z}$ such that $a\alpha + b\beta = d$. Additionally, $\text{GCD}(\alpha, \beta) \leq \min\{\alpha, \beta\}$. To determine the greatest common divisor of α, β, we proceed as follows. We will assume that $\beta \leq \alpha$. Using the above, there exists $q_1, r_1 \in \mathbf{Z}$ such that $\alpha = q_1\beta + r_1$ with $0 \leq r < \beta$. If $r_1 = 0$, we define $\text{GCD}(\alpha, \beta) = \beta$. Note that $\beta + 0\alpha = \beta$ and that β divides both α, β. Otherwise, if $r_1 \neq 0$, we replace α with r_1. Using the division algorithm, there exist $q_1, r_2 \in \mathbf{Z}$ such that $\beta = q_2 r_1 + r_2$. If $r_2 = 0$, we set $\text{GCD}(\alpha, \beta) = r_1$. In this case, r_1 divides β and since $\alpha = q_1\beta + r_1$, we see that r_1 also divides β. Furthermore, we have $r_1 = \alpha - q_1\beta$. If $r_2 \neq 0$, we replace β with r_2. By the division algorithm, there exist q_3, r_2 such that $r_1 = q_3 r_2 + r_3$. If $r_3 = 0$, we set $\text{GCD}(\alpha, \beta) = r_2$. In this case, r_2 divides r_1 and since $\beta = q_2 r_1 + r_2$, we see that r_2 divides β. Similarly, since α equals $q_1\beta + r_1$, we see that r_2 divides β. Finally, we have

$$r_2 = \beta - q_2 r_1 = \beta + q_2(\alpha - q_1\beta) = (1 - q_1 q_2)\beta + q_2\alpha.$$

Continuing this process, we get a non-negative, strictly decreasing sequence of integers r_i such that

$$r_i = q_i r_{i-2} + r_{i-1}.$$

Eventually, there exists some $n \in \mathbf{N}$ such that $r_n = 0$ and we set $\text{GCD}(\alpha, \beta) = r_{n-1}$. One can check that r_{n-1} divides both α, β and that there exist $a, b \in \mathbf{Z}$ such that $r_{n-1} = a\alpha + b\beta$.

The division and Euclidean algorithms on $\mathbf{Z}$ will be our models for these algorithms on $F[t]$. Our measurement of complexity in $\mathbf{Z}$ is the absolute value of the number. On $F[t]$, our measurement of complexity is given by the degree of the polynomial. We now review the division algorithm for polynomials in $F[t]$.

Given polynomials $P_1, P_2 \in F[t]$ with $P_2 \neq 0_F$, we assert that there exist polynomials $Q, R \in F[t]$ such that $P_1 = QP_1 + R$ where either $R = 0_F$ or $\deg(R) < \deg(P_2)$. We outline the division algorithm in $F[t]$.

Division Algorithm.

To begin, if $\deg(P_1) < \deg(P_2)$, then we set $Q = 0_F$ and $R = P_1$. Assuming $\deg(P_1) \geq \deg(P_2)$, we write

$$P_1 = a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0, \quad P_2 = b_m t^m + b_{m-1}t^{m-1} + \cdots + b_1 t + b_0$$

where $a_n, b_m \neq 0_F$ and $n \geq m$. We define

$$Q_1(t) = \frac{a_n}{b_m} t^{n-m}$$

and note that

$$\begin{aligned} P_1 - Q_1 P_2 &= a_n t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 - a_n t^n - \frac{a_n}{b_m} b_{m-1} t^{n-1} - \cdots + \frac{a_n}{b_m} b_1 t^{n-m+1} - \frac{a_n}{b_m} b_0 t^{n-m} \\ &= \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1}\right) t^{n-1} + \cdots + \left(a_{n-m+1} - \frac{a_n}{b_m} b_1\right) t^{n-m+1} \\ &\quad + \left(a_{n-m} - \frac{a_n}{b_m} b_0\right) t^{n-m} + a_{n-m-1} t^{n-m-1} + \cdots + a_1 t + a_0 \end{aligned}$$

We replace P_1 with $P_{1,1} = P_1 - Q_1 P_2$, noting that $\deg(P_{1,1}) < \deg(P_1)$. If $\deg(P_{1,1}) < \deg(P_2)$, we define

$$Q = Q_1, \quad R - P_{1,1}.$$

Otherwise, for notational simplicity, write

$$P_{1,1} = a_{1,n_1} t^{n_1} + \cdots + a_{1,1} t + a_{1,0}$$

where $a_{1,n_1} \neq 0_F$ and $n_1 \geq m$. We define

$$Q_2 = \frac{a_{1,n_1}}{b_m} t^{n_1 - m}$$

and replace $P_{1,1}$ with $P_{2,1} = P_{1,1} - Q_2P_2$. As before, $\deg(P_{2,1}) < \deg(P_{1,1})$. If $\deg(P_{2,1}) < \deg(P_2)$, we define

$$Q = Q_1 + Q_2, \quad R = P_{2,1}.$$

Otherwise, we repeat this process, obtaining a sequence of polynomials Q_i and $P_{i,1}$ such that

$$P_{i+1,1} = P_{i,1} - Q_{i+1}P_2$$

and $\deg(P_{i+1,1}) < \deg(P_{i,1})$. Eventually $\deg(P_{i+1,1}) < \deg(P_2)$ and when this occurs, we set

$$Q = \sum_{j=1}^{i+1} Q_j, \quad R = P_{i+1,1}.$$

Theorem 3.1 (Division Algorithm: Polynomial Rings)**.** *Let F be a field and $P_1, P_2 \in F[t]$. Then there exist $Q, R \in F[t]$ such that $P_1(t) = Q(t)P_2(t) + R(t)$ with either $R(t) = 0_F$ or $\deg(R) < \deg(P_2)$. Moreover, Q, R are uniquely determined by this information*

Given $P_1, P_2 \in F[t]$, we say that P_2 **divides** P_1 if $P_1 = QP_2$ for some $Q \in F[t]$.

We next use Theorem 3.1 to produce a **Euclidean algorithm** for computing the **greatest common divisor** $\text{GCD}(P_1, P_2)$ of two polynomials $P_1, P_2 \in F[t]$. The greatest common divisor of P_1, P_2 should satisfy the following two conditions:

(a) $\text{GCD}(P_1, P_2)$ divides P_1 and P_2.

(b) There exists $H_1, H_2 \in F[t]$ such that $\text{GCD}(P_1, P_2) = H_1P_1 + H_2P_2$ and $\deg(H_1) < \deg(P_2)$ (provided $\deg(P_2) \neq 0$) and $\deg(H_2) < \deg(P_1)$ (provided $\deg(P_1) \neq 0$). In particular, if Q divides P_1, P_2, then Q divides $\text{GCD}(P_1, P_2)$.

Euclidean Algorithm.

Given $P_1, P_2 \in F[t]$, we will assume that $\deg(P_1) \geq \deg(P_2)$; if this is not the case, we can simply relabel P_1, P_2 so that it holds. By Theorem 3.1, there exist unique polynomials $Q_1, R_1 \in F[t]$ such that

$$P_1 = Q_1P_2 + R_1$$

where $\deg(R_1) < \deg(P_2)$ or $R_1 = 0_F$. If $R_1 = 0$, then we set $\text{GCD}(P_1, P_2) = P_2$. Since $R_1 = 0$, we see that P_2 divides P_1, P_2 and that

$$P_2 = 0_R P_1 + 1_R P_2.$$

In particular, $H_1 = 0_R$ and $H_2 = 1_R$. Since $\deg(H_1) = \deg(H_2) = 0$, we see that $\deg(H_1) < \deg(P_2)$ (provided $\deg(P_2) \neq 0$) and $\deg(H_2) < \deg(P_1)$ (provided $\deg(P_1) \neq 0$).

If $R_1 \neq 0$, we replace P_1 with R_1. By Theorem 3.1, there exists $Q_2, R_2 \in F[t]$ such that

$$P_2 = Q_2R_1 + R_2$$

where either $R_2 = 0_F$ or $\deg(R_2) < \deg(R_1)$. If $R_2 = 0_F$, we set $\text{GCD}(P_1, P_2) = R_1$. Note that

$$R_1 = P_1 - Q_1P_2$$

and so we can take $H_1 = 1$ and $H_2 = Q_1$ in (b). It follows that $\deg(H_1) < \deg(P_2)$; note that if $\deg(P_2) = 0$, then $R_1 = 0$. We have $\deg(P_2) + \deg(Q_1) = \deg(P_1)$ and $\deg(P_2) > 0$, and so $\deg(H_2) < \deg(P_1)$. Finally, since $P_2 = Q_2R_1$, we see that

$$P_1 = R_1 + Q_2Q_1R_1 = R_1(1 + Q_2Q_1).$$

Hence R_1 divides both P_1, P_2 and so (a) holds.

If $R_2 \neq 0$, then we replace P_2 with R_2 and note that there exist $Q_3, R_3 \in F[t]$ such that

$$R_1 = Q_3 R_2 + R_3$$

where $R_3 = 0$ or $\deg(R_3) < \deg(R_2)$. If $R_3 = 0$, we set $\mathrm{GCD}(P_1, P_2) = R_2$. We have

$$P_1 = Q_1 P_2 + R_1, \quad P_2 = Q_2 R_1 + R_2, \quad R_1 = Q_3 R_2.$$

Substituting, we see that

$$R_2 = P_2 - Q_2 R_1 = P_2 - Q_2(P_1 - Q_1 P_2) = (1_F - Q_2)P_1 + Q_1 Q_2 P_2,$$

and $\deg(P_2) > \deg(Q_2) = \deg(1_F - Q_2)$. As $H_1 = 1_F - Q_2$, we see that $\deg(P_2) > \deg(H_1)$. Likewise,

$$\deg(P_1) = \deg(Q_1) + \deg(P_2) > \deg(Q_1) + \deg(Q_2) = \deg(Q_1 Q_2) = \deg(H_2).$$

Finally, since R_2 divides R_1 and $P_2 = Q_2 R_1 + R_2$, we see that R_2 divides P_2. Since $P_1 = Q_1 P_2 + R_1$, we see that R_2 also divides P_1.

We can continue this process, obtaining a sequence of polynomials $R_i \in F[t]$ with

$$R_i = Q_{i+2} R_{i+1} + R_{i+2}$$

and $\deg(R_{i+1}) < \deg(R_i)$. For some $n \in \mathbf{N}$, we will have $R_n = 0$ and $R_{n-1} \neq 0$. For such an n, we set $\mathrm{GCD}(P_1, P_2) = R_{n-1}$. We see that

$$R_i = R_{i-2} - Q_i R_{i-1} \tag{1}$$

for $i \geq 3$ and

$$R_1 = P_1 - Q_1 P_2, \quad R_2 = P_2 - Q_2 R_1. \tag{2}$$

Using (1) (many times) and (2), we obtain

$$\begin{aligned}
R_{n-1} &= R_{n-3} - Q_{n-1} R_{n-2} \\
&= R_{n-5} - Q_{n-3} R_{n-4} - Q_{n-1}(R_{n-4} - Q_{n-2} R_{n-3}) \\
&= R_{n-7} - Q_{n-5} Q_{n-6} - Q_{n-2}(R_{n-6} - Q_{n-4} R_{n-5}) - Q_{n-1}(R_{n-6} - Q_{n-4} R_{n-5}) - Q_{n-2}(R_{n-5} - Q_{n-3} R_{n-4}) \\
&\quad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \qquad\qquad \vdots \\
&= H_1 P_1 + H_2 P_2.
\end{aligned}$$

Since R_{n-1} divides R_{n-2} and $R_{n-3} = R_{n-1} + Q_{n-1} R_{n-2}$, we see that R_{n-1} divides R_{n-3}. Arguing via induction, we conclude that R_{n-1} divides R_i for all $i \geq 1$ and so R_{n-1} divides both P_1, P_2.

Finally, we prove that $\deg(H_1) < \deg(P_2)$ and $\deg(H_2) < \deg(P_1)$ unless $\deg(P_1) = \deg(P_2) = 0$. If $\deg(H_1) \geq \deg(P_2)$, then by Theorem 3.1, there exists $Q, R \in F[t]$ such that $H_1 = QP_2 + R$ with $\deg(R) < \deg(P_2)$ or $R = 0$. For this, we obtain

$$P_1(QP_2 + R) + H_2 P_2 = P_1 R + (P_1 Q + H_2) P_2 = \mathrm{GCD}(P_1, P_2).$$

If $R = 0$, we see that

$$\deg(\mathrm{GCD}(P_1, P_2)) \geq \deg(P_1) + \deg(P_2) + \deg(Q). \tag{3}$$

Since $\mathrm{GCD}(P_1, P_2)$ divides both P_1, P_2, we know that

$$\deg(\mathrm{GCD}(P_1, P_2)) \leq \min\{\deg(P_1), \deg(P_2)\}. \tag{4}$$

In particular, (3) contradicts (4) unless $\deg(P_1) = \deg(P_2) = \deg(Q) = \deg(H_1) = 0$. Hence, either $\deg(P_2) > \deg(H_1)$ or $\deg(P_1) = \deg(P_2) = 0$. If $R \neq 0$, since $\deg(R) < \deg(P_2)$, we again see that (3) holds. As before, (3) contradicts (4) unless $\deg(P_1) = \deg(P_2) = \deg(Q) = \deg(H_1) = 0$. In total, our assumption that $\deg(H_1) \geq \deg(P_2)$ leads to a contradiction unless $\deg(P_1) = \deg(P_2) = 0$. Thus, we conclude that $\deg(P_2) > \deg(H_1)$ or $\deg(P_1) = \deg(P_2) - 0$. The proof that $\deg(H_2) < \deg(P_1)$ or $\deg(P_1) = \deg(P_2) = 0$ is similar and left for the reader.

Remark. Given $P_1, P_2 \in F[t]$, the greatest common divisor $\mathrm{GCD}(P_1, P_2)$ is unique up to multiplication by a unit in $F[t]$. In a general commutative ring with identity R, we say that two elements $r_1, r_2 \in R$ are **associates** if there exists a unit $u \in R$ such that $ur_1 = r_2$. In particular, any two greatest common divisors of P_1, P_2 are associates. When we write $\mathrm{GCD}(P_1, P_2)$, we will assume that this is a monic polynomial and is unique under this additional condition.