These are some notes from my Algebra I class. We use the textbook *Abstract Algebra* by Dummit and Foote, and will cover rings, groups, and modules.

PIDs, UFDs and All That

We always assume here that R is commutative and unital.

Preliminaries

Definition: If $a_1, \dots, a_n \in R$, then the *ideal generated by* $a_1, \dots, a_n$ is given by

$$(a_1, \dots, a_n) := \bigcap \{I \mid a_1, \dots, a_n \in I, I \text{ is an ideal in } R\}.$$

An ideal is called *principal* if $I = (a)$ for some $a \in I$. We may write $I = a \cdot R$ in this case. A ring where every ideal is principal is called a *principal ideal domain*.

Definition: If I and J are ideals in R, then IJ is given by

$$IJ = \left\{ \sum_{i=1}^{n} x_i y_i \,\middle|\, x_i \in I, y_i \in J, n \in \mathbb{N} \right\}.$$

Theorem (Isomorphism Theorems)**:**

First Isomorphism Theorem: Let $\varphi \colon R \to S$ be a ring homomorphism. Then, $\overline{\varphi} \colon R/\ker(\varphi) \to \operatorname{im}(\varphi)$ is an isomorphism given by $\overline{\varphi}(a + \ker(\varphi)) = \varphi(a)$.

Second Isomorphism Theorem: Let R be a ring, $S \subseteq R$ a subring, and let $I \subseteq R$ be an ideal. Then,

(i) $I + S$ is a subring of R;
(ii) I is an ideal of $I + S$;
(iii) $I \cap S$ is an ideal of S;
(iv) $S/I \cap S \cong I + S/I$.

Third Isomorphism Theorem: Let R be a ring, I, J ideals of R with $I \subseteq J$. Then, J/I is an ideal of R/I, and we have $(R/I)/(J/I) \cong R/J$.

Fourth Isomorphism Theorem: If R is a ring and I is an ideal, then there is a one-to-one correspondence between subrings of R/I and subrings of R containing I.

Definition: Let M be an ideal in R.

(i) We say M is prime if $M \neq R$ and, for any $ab \in M$, we have either $a \in M$ or $b \in M$.

(ii) We say M is maximal if $M \neq R$ and if $M \subseteq I \subseteq R$ where I is an ideal, then either $I = M$ or $I = R$.

Theorem: Let M be an ideal in R.

(i) M is prime if and only if R/M is an integral domain.

(ii) M is maximal if and only if R/M is a field.

Proof.

(i) Let M be maximal, with $a + M \in R/M$, $a + M \neq 0 + M$. Then, $a \notin M$, so that the ideal $(a) + M$ strictly contains M. Therefore, $1 + M \in (a) + M$, meaning there is some $r + M$ such that $(r + M)(a + M) = 1 + M$. Thus, an inverse exists.

Now, if R/M is a field, and $M \subsetneq I \subseteq R$, then I/M is an ideal of R/M, and since $I \supsetneq M$, we have

$I/M \neq 0 + M$. Since R/M is a field, its only ideals are either $0 + M$ and R/M, so $I/M = R/M$, meaning $I = R$.

(ii) We have $P \subseteq R$ is prime if and only if $ab \in P$ implies $a \in P$ or $b \in P$. Yet, means that $ab + P = 0 + P$ if and only if $a = 0 + P$ or $b = 0 + P$.

□

Chinese Remainder Theorem

Definition: We say two ideals I and J are *coprime* if $I + J = R$, or that there exist $x \in I$ and $y \in J$ such that $x + y = 1$.

Theorem (Chinese Remainder Theorem)**:** Let $I_1, \dots, I_n$ be pairwise coprime ideals of R. Then, for any $a_1, \dots, a_n \in R$, there exists $x \in R$ with $x \equiv a_i$ modulo I_i for all i. In other words, there a solution to the system of congruences given by

$$\begin{aligned} x + I_1 &= a_1 + I_1 \\ x + I_2 &= a_2 + I_2 \\ &\vdots \\ x + I_n &= a_n + I_n. \end{aligned}$$

Proof. It suffices to construct elements $y_1, \dots, y_n$ such that $y_i \equiv 1$ modulo I_i and 0 otherwise. Then, we will be able to set $x = \sum_i a_i y_i$ as our desired solution.

We construct y_1 as follows. From our assumption, $I_1 + I_j = R$ for all $j \geqslant 2$, so for each $j \geqslant 2$, there exists $u_j \in I_1$ and $v_j \in I_j$ such that $u_j + v_j = 1$. Taking the product, we find that

$$\begin{aligned} \prod_{j=2}^{n} (u_j + v_j) &= 1 \\ &= \underbrace{v_2 \cdots v_n}_{=:y_1} \underbrace{+ \cdots + u_2 \cdots u_n}_{=:x_1}. \end{aligned}$$

We verify that y_1 does the job, which we can see by the fact that $y_1 \equiv 0$ modulo I_j for $j \neq 1$, as $v_2 \cdots v_j \in I_2 \cdots I_j \subseteq I_j$ for each $j \geqslant 2$. Similarly, each summand in x_1 contains at least one u_j, so $x_1 \equiv 0$ modulo I_1.

The rest of the y_i follow analogously. □

We can restate the Chinese Remainder Theorem in a variety of ways.

Theorem (Chinese Remainder Theorem, Alternative Versions)**:** Let $I_1, \dots, I_n$ be pairwise coprime ideals.

(i) There exists a surjective homomorphism

$$\begin{aligned} \varphi \colon R &\longrightarrow R/I_1 \times \cdots \times R/I_n \\ r &\longmapsto (r + I_1, \dots, r + I_n). \end{aligned}$$

This homomorphism induces an isomorphism

$$\overline{\varphi} \colon R/(I_1 \cap \cdots \cap I_n) \longrightarrow R/I_1 \times \cdots \times R/I_n.$$

(ii) If $I_1, \dots, I_n$ are pairwise coprime, then

$$R/I_1 \cdots I_n \cong R/I_1 \times \cdots \times R/I_n$$

are isomorphic.

Example: We observe that if $R = \mathbb{Z}$, and $p_1, \dots, p_r$ are distinct primes with $\ell_1, \dots, \ell_r$ positive integers, then

$$\mathbb{Z}/p_1^{\ell_1} \cdots p_r^{\ell_r}\mathbb{Z} \cong \mathbb{Z}/p_1^{\ell_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{\ell_r}\mathbb{Z}.$$

Example (Polynomial Interpolation)**:** If we let

$$p_i(x) = x - \alpha_i,$$

where $\alpha_i \in \mathbb{F}$, we observe that there is a surjective evaluation homomorphism

$$\text{ev}\colon \frac{\mathbb{F}[x]}{(p_i(x))} \to \mathbb{F},$$

given by $f(x) \mapsto f(\alpha_i)$. In particular, if $\alpha_1, \dots, \alpha_r$ are distinct, then

$$\frac{\mathbb{F}[x]}{(p_1(x), \dots, p_r(x))} \cong \mathbb{F} \times \cdots \times \mathbb{F},$$

so that, for all $\beta_1, \dots, \beta_r \in \mathbb{F}$, there is some $f(x) \in \mathbb{F}[x]$ such that $f(\alpha_i) = \beta_i$ for $i = 1, \dots, r$.

Field of Fractions and Localization

Given a ring R, how can we find maximal ideals in R? More specifically, given a commutative ring R with 1, and prime ideal $P \subseteq R$, we want to construct a new ring R_p with unique maximal ideal P.

Toward this end, we start by reviewing a useful construction known as the field of fractions.

Definition: Let R be an integral domain. We define the field $K = \text{frac}(R)$ to be the unique field with an injection

$$\begin{aligned} \iota\colon R &\hookrightarrow K \\ 1_R &\mapsto 1_K, \end{aligned}$$

satisfying the following universal property.

Given any embedding into a field, $\sigma\colon R \hookrightarrow L$, such that $1_R \mapsto 1_L$, there is a unique extension $\widetilde{\sigma}\colon K \to L$ such that the following diagram commutes.

$$\begin{tikzcd} R \arrow[r, hook, "\iota"] \arrow[dr, "\sigma"'] & K \arrow[d, "\widetilde{\sigma}"] \\ & L \end{tikzcd}$$

In order to construct K, we let $S \subseteq R \times R$ be defined by

$$S = \{(a, b) \mid b \neq 0\}.$$

We impose an equivalence relation on S by saying $(a, b) \sim (c, d)$ if and only if $ad - bc = 0$. Clearly, this relation is reflexive and symmetric. To see that it is transitive, we let $(a, b) \sim (c, d)$, and $(c, d) \sim (e, f)$, meaning $ad - bc = 0$ and $cf - de = 0$. Multiplying the first equation by f and the second equation by b, then subtracting, we get $adf - bde = 0$, meaning $d(af - be) = 0$. Since R admits no zero divisors, this means that $af - be = 0$, so the relation is transitive.

We write $[(a, b)] = \frac{a}{b}$ for K, with operations

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

These operations are well-defined and do satisfy the universal property. Verifying this is a pain, but it can be done.

Now, we may extend this to all unital commutative rings, not just integral domains.

Definition: Let R be a unital commutative ring, and let $S \subseteq R$. We say S is *multiplicative* if

- $1 \in S$;
- $0 \notin S$;
- for any $x, y \in S$, $xy \in S$.

Example:

(i) If R is an integral domain, then $R \setminus \{0\}$ is multiplicative.

(ii) If $z \in R$ is such that z is not nilpotent, then $S = \{z^n \mid n \geqslant 0\}$ is multiplicative.

(iii) If P is a prime ideal, then $S = R \setminus P$ is multiplicative.

We will use (iii) to construct a ring with a unique maximal ideal. First, though, we construct a ring of fractions using multiplicative sets.

Definition: Let R be a unital commutative ring, and let $S \subseteq R$ be multiplicative. We construct a ring $S^{-1}R$ by taking an equivalence relation on $R \times S$ as follows:

$$(a, s) \sim (b, t) \Leftrightarrow \exists s' \in S \text{ such that } s'(at - bs) = 0.$$

We write

$$S^{-1}R = \{[(a, s)] \mid a \in R, s \in S\},$$

and denote

$$[(a, s)] = \frac{a}{s}.$$

This becomes a ring under the operations

$$\frac{a}{s} + \frac{b}{t} = \frac{at + bs}{st}$$
$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}.$$

We call $S^{-1}R$ the *localization of* R *with respect to* S.

We can see some basic properties of the localization.

Proposition: Let R be a unital commutative ring, $S \subseteq R$ multiplicative, and let $S^{-1}R$ be the corresponding localization.

- The additive identity in $S^{-1}R$ is $\frac{0}{1}$.
- The additive inverse of $\frac{a}{s}$ in $S^{-1}R$ is $\frac{-a}{s}$.
- For all $a \in R$ and all $s, s' \in S$, we have $\frac{as'}{ss'} = \frac{a}{s}$.
- Every element of the form $\frac{s}{t}$ where both $s, t \in S$ is invertible, with corresponding inverse $\frac{t}{s}$.
- The map $\iota_S \colon R \to S^{-1}R$ given by $r \mapsto \frac{r}{1}$ is an injective ring homomorphism such that $\iota_S(S) \subseteq (S^{-1}R)^{\times}$, where $(S^{-1}R)^{\times}$ denotes the group of invertible elements in $S^{-1}R$.

Unique Factorization Domains

Definition: A ring R is called *Noetherian* if, for any ascending chain of ideals $I_1 \subseteq I_2 \subseteq \cdots$, there is some index N such that for all $m \geqslant N$, $I_m = I_N$.

Proposition: The following are equivalent:

- R is Noetherian;
- every ideal in R is finitely generated.

Proof. Let R be Noetherian. Suppose toward contradiction that there exists I that is not finitely generated. Then, I is nonzero, so there is $\alpha_1 \in I$ such that $I_1 = (\alpha_1)$ is nonzero. Since I is not finitely generated, $I \neq I_1$, so there is $\alpha_2 \in I \setminus I_1$, so that $I_2 = (\alpha_1, \alpha_2)$ is such that $I_1 \subsetneq I_2$. Inductively, we generate $I_n = (\alpha_1, \dots, \alpha_n)$ such that $I_{n-1} \subsetneq I_n$, implying that we have a strictly ascending chain of ideals, which is a contradiction.

Suppose every ideal in R is finitely generated. Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals, and set $I = \bigcup I_n$ be their union. By assumption, I is finitely generated, so we have $I = (\alpha_1, \dots, \alpha_N)$ for some $\alpha_1, \dots, \alpha_N \in R$. Yet, since I is the union of all these ideals, there is some M such that $\alpha_1, \dots, \alpha_N \in I_M$, meaning the chain stabilizes. □

Corollary: If R is a principal ideal domain, then R is Noetherian.

Definition: Let R be an integral domain.

(i) Two elements $a, b \in R$ are called *associated* if $a = bu$ for some unit (invertible) element $u \in R$. Equivalently, a and b are associated if $(a) = (b)$

(ii) An element $a \in R$ is called *irreducible* if

- a is not a unit element;
- whenever $a = bc$ for some $b, c \in R$, then one of b or c is a unit.

(iii) An element a is called *prime* if $a \neq 0$, $a \notin R^\times$, and (a) is prime. Equivalently, a is prime if, whenever $a|bc$, it follows that $a|b$ or $a|c$, where divisibility in R is defined traditionally (i.e., there exists $z \in R$ such that $az = b$).

Note: Prime elements are irreducible, but not necessarily vice versa.

The question then arises: when are irreducibles prime?

Definition: We say $a \in R$ with $a \neq 0$, $a \notin R^\times$ has a *unique factorization* into irreducibles if

(i) we may write $a = up_1 \cdots p_r$, where u is a unit and $p_1, \dots, p_r$ are irreducible;

(ii) for any other such factorization

$$\begin{aligned} a &= u\prod_{i=1}^{r} p_i \\ &= v\prod_{j=1}^{s} q_j, \end{aligned}$$

where p_i, q_j are irreducible and u, v are units, we have

- $r = s$;
- upon permutation of factors, p_i and q_i are associated.

We call R a *unique factorization domain* if, for any $a \in R$ with $a \neq 0$, $a \notin R^\times$, a has unique factorization into irreducibles.

Proposition: If R a Noetherian ring, then every $a \in R$ with $a \neq 0$ and $a \notin R^{\times}$ admits a factorization into irreducibles.

Proof. First, we show that every such a has an irreducible factor or divisor. If a is itself irreducible, then we are done. Else, there are $b, c \in R$ with $a = bc$ and neither a nor b a unit. In particular, this means that $(a) \subsetneq (b)$. Inductively, if b is not irreducible, then we may find b_2, c_2 such that $b = b_2c_2$, meaning that $(b) \subsetneq (b_2)$, and so on and so forth.

This gives a chain of ideals

$$(a) \subsetneq (b) \subsetneq (b_2) \subsetneq \cdots$$

that eventually stabilizes, meaning that there is some b_N such that b_N is irreducible.

Now, we may show that a admits a factorization. If $a = bc$ with b irreducible (as we showed previously), then if c is not irreducible, we may take $c = b_1c_1$ and create this same chain of ideals

$$(c) \subsetneq (c_1) \subsetneq (c_2) \subsetneq \cdots$$

using the Noetherian condition to end up at an irreducible or a unit. □

The main issue facing general Noetherian rings is that the uniqueness of the factorization may go awry.

Example: For instance, in the ring $R = \mathbb{Z}\left[\sqrt{-5}\right]$, there is not unique factorization. For instance, we may write

$$\begin{aligned} 6 &= (2)(3) \\ &= \left(1 + \sqrt{-5}\right)\left(1 + \sqrt{-5}\right), \end{aligned}$$

where we may see that all of these are irreducible as follows. Define a norm on $\mathbb{Z}\left[\sqrt{-5}\right] \subseteq \mathbb{C}$ by $N\left(a + b\sqrt{-5}\right) = a^2 + 5b^2$, where this norm is multiplicative as it is inherited from $\mathbb{C}$.

Lemma: If N is a norm on the ring $R = \mathbb{Z}\left[\sqrt{-D}\right]$, where D is a square-free positive integer, then $u \in R$ is an invertible (or unit) element if and only if $N(u) = 1$.

Proof of Lemma. If $v \in R$ is such that $uv = 1$, then $N(uv) = N(u)N(v) = 1$, meaning that both $N(u)$ and $N(v)$ are 1.

Meanwhile, if $N(u) = 1$, then $1 = u\overline{u}$, meaning that $\overline{u} = u^{-1}$. □

We may show that 2 is irreducible relatively quickly. Observe that if there were a factorization of $2 = ab$ into irreducibles, then $4 = N(a)N(b)$ would hold, with neither $N(a)$ nor $N(b)$ being equal to 1. This would mean that $N(a) = 2$ for some $a = x + y\sqrt{-5}$, or that $x^2 + 5y^2 = 2$. Yet, reducing modulo 5, this implies that $x^2 \equiv 2$ modulo 5, yet the only squares in $\mathbb{Z}/5\mathbb{Z}$ are 1 and 4.

Given a factorization, there is a simple way to classify the uniqueness of the factorization.

Proposition: Let $a \in R$ be such that $a \neq 0$ and $a \notin R^{\times}$. If a admits a factorization

$$a = up_1 \cdots p_r,$$

with $p_1, \dots, p_n$ *prime*, then this factorization is unique (up to associates).

Proof. Suppose a admits another factorization,

$$a = vq_1 \cdots q_s,$$

where $q_1, \dots, q_s$ are irreducible and v is a unit. Then, we have

$$up_1 \cdots p_r = vq_1 \cdots q_s,$$

meaning that p_1 divides $vq_1 \cdots q_s$. Since p_1 is prime, $p_1 | q_j$ for some j, meaning that $q_j = v_1 p_1$ for some $v_1 \in R$. Yet, since q_j is irreducible, it follows that v_1 is a unit. By permuting elements, we may say that p_1 and q_1 are associated, so we have

$$up_1 \cdots p_r = vv_1 p_1 q_2 \cdots q_s.$$

Now, since R is a domain, it admits the cancellation property, so we may then write

$$up_2 \cdots p_r = vv_1 q_2 \cdots q_s.$$

Proceeding in this fashion, we observe first that $r \leqslant s$, as else, we would have p_i dividing a unit for R, which is not allowed. Thus, we find

$$u = vv_1 \cdots v_r q_{r+1} \cdots q_s.$$

Similarly, this means there cannot be any more q_j, or else the q_j would be a unit. Thus, these are the same factorizations (up to associates). □

Theorem: If a domain R is a principal ideal domain, then R is a unique factorization domain.

Proof. First, we show that if $a \in R$ is irreducible, then a is prime.

Observe that (a) is then contained in a maximal ideal M, where $M = (p)$ for some $p \in R$ with p not a unit. Since M is maximal, M is prime, so that p is prime, and $(a) \subseteq (p)$. Observe then that $a = pu$ for some $u \in R$; since a is irreducible and p is not a unit, it must be the case that u is a unit. Thus, $(a) = (p)$, so that a is prime.

Now, since R is a principal ideal domain, every element in R admits a factorization into irreducibles, and all irreducibles are prime. Therefore, the factorization is unique by the above lemma. □

Euclidean Domains

Definition: An integral domain R is called a *Euclidean Domain* if there exists $N \colon R \setminus \{0\} \to \mathbb{Z}_{\geqslant 0}$ such that for all $a, b \in R$, with $b \neq 0$, there exist $q, r \in R$ such that

- $a = qb + r$;
- either $r = 0$ or $N(r) < N(b)$.

Example:

- Any field admits the vacuous norm, $N(k) = 0$ for all $k \in F \setminus \{0\}$.
- The ring $R = \mathbb{Z}$ is Euclidean with the norm $N(n) = |n|$.
- The ring $R = \mathbb{F}[x]$, where $\mathbb{F}$ is a field, is Euclidean with norm $N \colon \mathbb{F}[x] \setminus \{0\} \to \mathbb{N}$ given by $N(f) = \deg(f)$.

Theorem: If R is Euclidean, then R is a principal ideal domain.

Proof. Let $I \subseteq R$ be an ideal. If $I = \{0\}$, then I is principal and we are done.

Else, suppose $I \neq 0$. There exists $\alpha \in I$ with $\alpha \neq 0$, so that $N(\alpha)$ is well-defined. Let $b \in I$ be such that $N(b)$ is minimal for all possible elements of I.

We claim that $I = (b)$. Let $a \in I$ be arbitrary, and perform Euclidean division on a by b, yielding

$$a = qb + r,$$

where $r = 0$ or $N(r) < N(b)$.

If $r \neq 0$, then $N(r) < N(b)$, but $r = a - bq \in I$, which would contradict minimality of $N(b)$, so that $r = 0$, and thus $a = bq \in (b)$. $\square$

Theorem: The Gaussian integers, $\mathbb{Z}[i]$, are Euclidean with norm

$$N(a + bi) = a^2 + b^2.$$

Proof. Observe that N is multiplicative. If we let $\alpha = a + bi$ and $\beta = c + di$ with $\alpha, \beta \neq 0$, we want to show that there exist γ and δ such that $\alpha = \beta\gamma + \delta$ and $\delta = 0$ or $N(\delta) < N(\beta)$.

Consider $\frac{\alpha}{\beta} \in \mathbb{C}$, so that

$$\begin{aligned} \frac{\alpha}{\beta} &= \frac{(a + bi)(c - di)}{c^2 + d^2} \\ &= \frac{(a + bi)(c - di)}{N(\beta)} \\ &=: x + yi, \end{aligned}$$

so that $\frac{\alpha}{\beta} \in \mathbb{Q}[i]$.

Now, we can find $x_0, y_0 \in \mathbb{Z}$ such that $|x - x_0| \leqslant \frac{1}{2}$ and $|y - y_0| \leqslant \frac{1}{2}$. Setting $\delta = x_0 + y_0 i$, we have that $\delta = \alpha - \beta\gamma \in \mathbb{Z}[i]$. We claim that if $\delta \neq 0$, then $N(\delta) < N(\beta)$.

Observe that since N is multiplicative, this condition is equivalent to $N\left(\frac{\delta}{\beta}\right) < 1$. We observe that

$$\begin{aligned} N\left(\frac{\delta}{\beta}\right) &= N\left(\frac{\alpha - \beta\gamma}{\beta}\right) \\ &= N\left(\frac{\alpha}{\beta} - \gamma\right) \\ &= (x - x_0)^2 + (y - y_0)^2 \\ &\leqslant \frac{1}{2} \\ &< 1. \end{aligned}$$

$\square$

Remark: While the remainder in Euclidean division for $\mathbb{Z}$ and $\mathbb{F}[x]$ *is* unique, this is not the case for general Euclidean domains. For instance, if we want to divide $a = 1 + i$ by $b = 2$ in $\mathbb{Z}[i]$ with our previously specified norm, we find that

$$\begin{aligned} 1 + i &= 2 \cdot 0 + (1 + i) \\ &= 2 \cdot 1 + (-1 + i), \end{aligned}$$

both of which satisfy the conditions for Euclidean division.

Now, in any PID (really, any UFD), we can talk about a greatest common divisor. In a principal ideal domain, the GCD for $a, b \in R$ is given by the unique (up to associates) element d such that

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

Meanwhile, greatest common divisors in a UFD are slightly more complicated. If we have two elements $a, b \in R$ with prime factorizations

$$\begin{aligned} a &= u p_1^{v_1} p_2^{v_2} \cdots p_n^{v_n} \\ b &= v p_1^{w_1} p_2^{w_2} \cdots p_n^{w_n}, \end{aligned}$$

then the greatest common divisor is given by

$$\gcd(a, b) = \prod_{i=1}^{n} p_i^{\min(v_i, w_i)}.$$

This is defined up to associates, similar to how the factorization of any element is defined up to associates.

Unique Factorization in Polynomial Rings

Our goal is to prove that if R is a UFD, then $R[x]$ is a UFD.

We do this by first discussing irreducibility in $R[x]$, including a full characterization of irreducible elements.

Definition: Assume R is a unique factorization domain, and let $0 \neq f(x) \in R[x]$. Writing

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

we define the *content* of f, written $c(f)$, to be

$$c(f) = \gcd(a_0, a_1, \ldots, a_n).$$

Proposition (Gauss's Lemma)**:** Let R be a UFD, and let $f(x), g(x) \in R[x]$ be nonzero polynomials. Then,

$$c(fg) = c(f)\,c(g).$$

Proof. For any nonzero polynomial $h \in R[x]$, we may write

$$h(x) = c(h)z(x),$$

where $c(z) = 1$, simply by factoring. Thus, writing

$$\begin{aligned} f(x) &= c(f)u(x) \\ g(x) &= c(g)v(x), \end{aligned}$$

where $c(u) = c(v) = 1$, hence

$$\begin{aligned} c(fg) &= c(c(f)\,c(g)uv) \\ &= c(f)\,c(g)\,c(uv). \end{aligned}$$

We want to show that $c(u(x)v(x)) = 1$ (up to associates).

Suppose not. Since $c(uv)$ is nonzero and (assumed to be) not a unit, we may find a prime p such that $p |\, c(uv)$. That is, we may find p such that p divides all coefficients of $u(x)v(x)$.

Consider now the reduction homomorphism

$$\pi \colon R[x] \to (R/(p))[x],$$

where we reduce all coefficients modulo (p). Since p is prime, (p) is prime, so that $R/(p)$ is an integral domain, meaning that $(R/(p))[x]$ is an integral domain.

Since $c(u) = c(v) = 1$, it follows that $\pi(u(x)) \neq 0$ and $\pi(v(x)) \neq 0$, as at least one coefficient in $u(x)$ or $v(x)$ is not divisible by p. Thus, in $(R/(p))[x]$ is a domain, it follows that $\pi(u(x))\pi(v(x)) \neq 0$. Yet, since π is a homomorphism, it follows that $0 = \pi(u(x)v(x)) = \pi(u(x))\pi(v(x))$, since we assumed that p divides all the coefficients of $u(x)v(x)$. $\square$

Corollary (Gauss's Lemma, Redux)**:** Let R be a UFD, and let $F = \text{frac}(R)$. Let $f(x) \in R[x]$, and assume $f(x)$ is reducible in $F[x]$. Then, $f(x)$ is reducible in $R[x]$.

Proof. Let $f(x)$ be reducible in $F[x]$, so that $f(x) = g(x)h(x)$, where $g(x)$ and $h(x)$ are nonconstant polynomials in $F[x]$.

By factoring, we have

$$\begin{aligned} g(x) &= \frac{a}{b}u(x) \\ h(x) &= \frac{c}{d}v(x), \end{aligned}$$

where $a, b, c, d \in R \setminus \{0\}$, $u(x), v(x) \in R[x]$, and $c(u) = c(v) = 1$.

Substituting this information into the expression for $f(x)$, we have

$$\begin{aligned} f(x) &= \frac{ac}{bd}u(x)v(x) \\ bdf(x) &= acu(x)v(x), \end{aligned}$$

so that

$$bd\,c(f) = ac\,c(u)\,c(v).$$

meaning

$$bd\,c(f) = ac.$$

In particular, this means that $\frac{ac}{bd}$ is a valid representative for $c(f)$, so that $\frac{ac}{bd} \in R$. Therefore,

$$f(x) = \left(\frac{ac}{bd}u(x)\right)v(x),$$

both nonconstant and in $R[x]$, meaning $f(x)$ has a nontrivial factorization in $R[x]$, and thus f is reducible. □

Corollary (Classification of Irreducibles)**:** Let R be a UFD, let $F = \text{frac}(R)$, and let $f(x) \neq 0 \in R[x]$.

(i) If $f(x)$ is constant, then f is irreducible in $R[x]$ if and only if $f(x)$ is irreducible in R.

(ii) If $f(x)$ is not constant, then f is irreducible in $R[x]$ if and only if $c(f) = 1$ and $f(x)$ is irreducible in $F[x]$.

Proof.

(i) Observe that $R[x]$ and R have the same units (since R is an integral domain, and so admits no nilpotent elements), meaning that the product of two nonzero polynomials is a constant if and only if the polynomials themselves are constant.

(ii) Let f be nonconstant. If f is irreducible in $R[x]$, then we may write

$$f(x) = c(f)u(x),$$

where $u(x)$ is nonconstant and has $c(u) = 1$. Yet, since f is irreducible, it also follows that $c(f) = 1$. Additionally, f is irreducible in $F[x]$ by the contrapositive of Gauss's Lemma.

If f is irreducible in $F[x]$, and has content 1, then for any factorization

$$f(x) = g(x)h(x),$$

where $g(x), h(x) \in F[x]$, either g or h must be a constant. Now, since f is contained in $R[x]$, we may take a common denominator to yield

$$f(x) = a u(x),$$

where $u(x)$ is nonconstant and has content 1, with $a \in R$. Since f has content 1, it follows that a is a unit element, meaning that any factorization of f must contain a unit, so that f is irreducible in $R[x]$.

□

Theorem: If R is a UFD, then $R[x]$ is a UFD.

Proof. Let $F = \text{frac}(R)$, and let $f(x) \in R[x]$ be a nonzero, non-unit element. If $f(x) \in R$, then f is a product of irreducibles in R by part (i) of the classification, meaning the product is automatically unique up to permutation and associates as R is a UFD.

Now, if f is nonconstant, then $f(x) \in F[x]$ is nonzero and non-unit, as the units in $F[x]$ are the elements of F. Since $F[x]$ is a principal ideal domain (as $F[x]$ is a Euclidean domain, following from the division algorithm), $F[x]$ is a UFD, so we may write

$$f(x) = \prod_{i=1}^{n} g_i(x),$$

where the $g_i(x)$ are irreducible in $F[x]$. Writing

$$g_i(x) = \frac{a_i}{b_i} u_i(x),$$

where the $u_i(x) \in R[x]$ with $c(u_i) = 1$ for each i, we have

$$\prod_{i=1}^{n} \frac{a_i}{b_i} \in R,$$

as $f(x) \in R[x]$, so we may write

$$f(x) = \prod_{i=1}^{n} \frac{a_i}{b_i} \prod_{i=1}^{n} u_i(x).$$

Each of the $u_i(x)$ are irreducible in $R[x]$ by the classification, and the product $\prod_{i=1}^{n} \frac{a_i}{b_i} \in R$ is either a unit or a product of irreducibles. This gives the existence of such a factorization for f.

To see uniqueness, if

$$\begin{aligned} f(x) &= \left(\prod_{i=1}^{k} a_i\right)\left(\prod_{i=1}^{m} p_i(x)\right) \\ &= \left(\prod_{j=1}^{\ell} b_j\right)\left(\prod_{j=1}^{m} q_j(x)\right) \end{aligned}$$

are factorizations where a_i, b_j are irreducible in R, and p_i, q_j are nonconstant and irreducible with content 1, then we may take the content of both sides, yielding

$$c\left(\left(\prod_{i=1}^{k} a_i\right)\left(\prod_{i=1}^{k} p_i(x)\right)\right) = \prod_{i=1}^{k} a_i$$

$$c\left(\left(\prod_{j=1}^{\ell} b_j\right)\left(\prod_{j=1}^{\ell} q_j(x)\right)\right) = \prod_{j=1}^{\ell} b_j.$$

Since contents are only well-defined up to associates, the most we can say is that

$$\prod_{i=1}^{k} a_i = u\prod_{j=1}^{\ell} b_j,$$

where $u \in R^{\times}$. Since there is at least one q_j, we may replace q_1 by uq_1, then divide, so that we find

$$\prod_{i=1}^{k} a_i = \prod_{j=1}^{\ell} b_j.$$

Since both of these are products of irreducibles in R, it follows that $k = \ell$ and, after permutation of factors, $b_i = u_i a_i$ for some $u_i \in R^{\times}$. Additionally, we also have the equality

$$\prod_{i=1}^{m} p_i = \prod_{j=1}^{n} q_j.$$

Since all of these factors are irreducible in $F[x]$, and $F[x]$ is a PID, we find that $n = m$ and, upon permutation of factors, we have $q_i(x) = \gamma_i p_i(x)$ for some $\gamma_i \in F \setminus \{0\}$. Write

$$\gamma_i = \frac{c_i}{d_i},$$

where $c_i, d_i \in R \setminus \{0\}$, so that

$$d_i q_i(x) = c_i p_i(x).$$

Taking the content of both sides, we then get that $\nu_i d_i = c_i$ for some $\nu_i \in R^{\times}$, so that $\gamma_i = \nu_i \in R^{\times}$, meaning that p_i and q_i are associates in $R[x]$. $\square$

Unique factorization in polynomial rings having the rigidity laid out in the classification theorem makes for very useful criteria to understand irreducibility.

Theorem (Eisenstein's Criterion)**:** Let R be a UFD, and let $p \in R$ be a prime element. If we write $f(x) \in R[x]$ as

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

then if

- $a_0 \neq 0$;
- $p \nmid a_n$;
- $p | a_i$ for $0 \leqslant i \leqslant n-1$;
- and $p^2 \nmid a_0$,

then $f(x)$ is irreducible in $F[x]$. If, in addition, $c(f) = 1$, then f is irreducible in $R[x]$.

Remark: This is the more general formulation of the case when $R = \mathbb{Z}$ and f is monic that we see in undergrad abstract algebra.

Proof. Suppose toward contradiction that f is reducible in $F[x]$, where we may write

$$f(x) = g(x)h(x)$$

with $g(x), h(x) \in R[x]$ nonconstant as in the proof of Gauss's Lemma. The reduction map $\pi\colon R[x] \to (R/(p))[x]$ is a homomorphism, so that

$$\overline{f}(x) = \overline{g}(x)\overline{h}(x).$$

Thus, by our assumptions, we have

$$\overline{f}(x) = \overline{a_n}x^n,$$

with $\overline{a_n} \neq \overline{0}$. Since the degree of $\overline{f}$ remains the same upon reduction, it follows that $\overline{g}$ and $\overline{h}$ have the same degrees as they had originally.

Observe that in a domain, the product of the highest-degree terms is the highest-degree term of the product, and similarly for the lowest-degree terms. Therefore, we must have $\overline{g}(x)$ and $\overline{h}(x)$ are monomials, as their product is a monomial. Writing

$$\begin{aligned}\overline{g}(x) &= \beta x^k\\ \overline{h}(x) &= \gamma x^\ell,\end{aligned}$$

with $\gamma, \beta \in R$ and $k = \deg(g)$, $\ell = \deg(h)$, we then get

$$\begin{aligned}g(x) &= bx^k + pu(x)\\ h(x) &= cx^\ell + pv(x),\end{aligned}$$

where $k, \ell > 0$ and $u(x), v(x) \in R[x]$. Then,

$$f(x) = \left(bx^k + pu(x)\right)\left(cx^\ell + pv(x)\right),$$

whence the constant term of this product is divisible by p^2. $\square$

Modules

For this section, a ring R may not be commutative nor unital.

Definition: Let R be a ring. A *left* R-*module* is a set M with operations

$$\begin{aligned}+\colon M \times M &\to M\\ (m, n) &\mapsto m + n\\ .\colon R \times M &\to M\\ (r, m) &\mapsto r.m,\end{aligned}$$

satisfying the following axioms:

(M0) $(M, +)$ is an abelian group;

(M1) $(r + s).m = r.m + s.m$ for all $r, s \in R$ and $m \in M$;

(M2) $(rs).m = r.(s.m)$ for all $r, s \in R$ and $m \in M$;

(M3) $r.(m + n) = r.m + r.n$ for all $r \in R$ and $m, n \in M$;

(M4) if R is unital, then $1.m = m$ for all $m \in M$.