33. 5/8

33.1. *Unique factorization domains* We say that an integral domain R is a *unique factorization domain*, or *UFD*, iff every element has nonzero non-unit element has some irreducible factorization, and has uniqueness of the same.

Theorem 33.1. *Let R be an integral domain. Then the following are equivalent:*

(1) R is a UFD.
(2) Every chain of principal ideals in R has finite length, and every irreducible element of R has the prime divisor property.

Proof. The previous two theorems show that (2) implies (1). Now suppose R is a UFD.

Suppose $a_1R \subseteq a_2R \subseteq \ldots$ is a chain of principal ideals in R. We must show that it has finite length. It is enough to assume that none of the ideals are $\{0\}$ or R. Since a_{i+1} must divide a_i, the existence and uniqueness of irreducible factorizations for nonzero non-unit elements implies that some irreducible factorization of a_{i+1} occurs as a sub-product of some irreducible factorization of a_i. But there are finitely terms in any irreducible factorization of a_1. Therefore only finitely many of the ideals a_iR can differ from their successors $a_{i+1}R$.

Suppose $a \in R$ is irreducible, and suppose a divides bc. We must show that a either divides b or divides c.

If $bc = 0$, then either $b = 0$ or $c = 0$ because R is an integral domain, and certainly a divides 0. So suppose $bc \neq 0$. We can write $bc = ax$ for some $x \in R$. Therefore, a times any irreducible factorization of x gives an irreducible factorization of bc. At the same time, so does the product of any irreducible factorizations of b and of c. So by uniqueness, a must occur up to units in at least one of the latter two factorizations, hence divides either b or c. □

Corollary 33.2. $\mathbf{Z}$ *and* $\mathbf{Z}[i]$ *and* $\mathbf{Z}[\sqrt{-2}]$ *and* $\mathbf{Z}[\omega]$ *are UFDs.*

Proof. Each of these rings is an integral domain with a size function given by the corresponding norm $\mathbf{N}$, so they are Euclidean domains. So by Theorem 31.5, their irreducible elements have the prime divisor property. At the same time, the norm $\mathbf{N}$ satisfies

$$\beta \text{ divides } \alpha \implies \mathbf{N}(\beta) \text{ divides } \mathbf{N}(\alpha) \implies \mathbf{N}(\beta) \leq \mathbf{N}(\alpha),$$

so Example 32.3 shows that in these rings, chains of principal ideals have finite length. □

Corollary 33.3. *For any field F, the polynomial ring $F[x]$ is a UFD.*

Proof. In place of the norm $\mathbf{N}$, we use the degree function, observing that

$$g(x) \text{ divides } f(x) \implies \deg g(x) \leq \deg f(x).$$

The rest is the same as the previous proof. □

Remark 33.4. As it turns out, $F[x, y]$ is a UFD for any field F. However, since it is neither a Euclidean domain nor a PID, one has to check directly that every irreducible element of $F[x, y]$ has the prime divisor property, which is harder.

33.2. *Numbers versus polynomials* We have seen that the polynomial rings $F[x]$ are very similar to the rings $\mathbf{Z}$, $\mathbf{Z}[i]$, *etc.*, even though their elements are not numbers per se. There is a kind of dictionary or Rosetta stone comparing algebraic integers and polynomials:

numbers	polynomials
$\mathbf{Z} \ni n$	$F[x] \ni f$
$\mathbf{Q} = \{\text{rational numbers}\}$	$F(x) = \{\text{rational functions of } x\}$
$\log \lvert n \rvert$	$\deg(f)$
$\{\pm 1\}$	$F^\times$
prime numbers	irreducible polynomials
long division of integers	long divison of polynomials
$\mathbf{Z}[\sqrt{d}]$	$F[x^{1/2}]$
$\mathbf{Z}[\alpha]$	$F[x, y]/(g(x, y))$

This Rosetta stone was pointed out in the early 20th century by the mathematician André Weil. It is the beginning of a subfield called arithmetic geometry, of which I will try to give some glimpse on Friday.

33.3. *Bonus material to the lecture* It turns out that $\mathbf{Z}[i]$ and $\mathbf{Z}[\sqrt{-2}]$ and $\mathbf{Z}[\omega]$ are all quotient rings of the polynomial ring $\mathbf{Z}[x]$.

Recall that for any ring R, there is always a unique ring homomorphism $\mathbf{Z} \to R$. It must send $1_{\mathbf{Z}} \mapsto 1_R$, and that determines where every other integer goes. By comparison, a ring homomorphism $\mathbf{Z}[x] \to R$ is determined by where it sends x, and this choice can be made freely.

In particular, there is a ring homomorphism $\Phi : \mathbf{Z}[x] \to \mathbf{Z}[i]$ that sends $n \mapsto n$ for every integer n, and sends $x \mapsto i$. In other words,

$$\Phi(f(x)) = f(i).$$

What is the kernel of Φ? It is precisely the set of polynomials $f(x) \in \mathbf{Z}[i]$ that have i as a root, when we allow f to take imaginary arguments. This set is the principal ideal formed by the multiples of $x^2 + 1$. Altogether,

$$\begin{aligned}
x \mapsto i : \mathbf{Z}[x] \to \mathbf{Z}[i] \quad & \text{is surjective with kernel } (x^2 + 1), \\
x \mapsto \sqrt{d} : \mathbf{Z}[x] \to \mathbf{Z}[\sqrt{d}] \quad & \text{is surjective with kernel } (x^2 - d) \qquad (d \text{ squarefree}), \\
x \mapsto \omega : \mathbf{Z}[x] \to \mathbf{Z}[\omega] \quad & \text{is surjective with kernel } (x^2 + x^2 + 1).
\end{aligned}$$

We can rewrite, *e.g.*, the first statement as the existence of a ring *isomorphism*

$$\mathbf{Z}[i]/(x^2 + 1) \to \mathbf{Z}[i].$$

This game can be also be played starting from a field instead of $\mathbf{Z}$. For instance, there is a ring isomorphism

$$\mathbf{R}[i]/(x^2 + 1) \to \mathbf{C}.$$

And we also get interesting results if we use quotients by non-principal ideals: There are ring isomorphisms

$$(\mathbf{Z}/3\mathbf{Z})[x]/(x^2+1) \quad \leftarrow \quad \mathbf{Z}[x]/(3, x^2+1) \quad \rightarrow \quad \mathbf{Z}[i]/3\mathbf{Z}[i].$$

In summary, we can build up all of the rings interesting to number theory by starting from familiar rings like $\mathbf{Z}$, $\mathbf{Q}$, or $\mathbf{Z}/m\mathbf{Z}$, then adjoining indeterminate variables, then quotienting by ideals to assign values to those variables. This is called giving *presentations* of the rings by *generators and relations*.

34. 5/10

34.1. Our goal today is to sum up our study of ring theory by explaining an analogue of unique prime factorization for ideals.

34.2. *Algebraic numbers and algebraic integers* The *leading term* of a nonzero polynomial in one variable is its term of highest degree. Such a polynomial is *monic* iff the coefficient of its leading term is 1.

A number $\alpha \in \mathbf{C}$ is *algebraic* iff it is a root of a nonzero polynomial with integer coefficients, or equivalently, of a monic nonzero polynomial with rational coefficients.

More strongly, α is an *algebraic integer* iff it is a root of a monic polynomial with integer coefficients. This means that some positive power of α can be expressed as an integer linear combination of smaller powers of α.

Example 34.1. Any rational number is an algebraic number. A rational number α is an algebraic integer if and only if α is an integer in the usual sense. To see the "only if" direction, note that if α has a denominator greater than 1, then there's no way for a positive power of α to be an integer.

Example 34.2. Consider the ring

$$\mathbf{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbf{Q}\}.$$

The use of parentheses in place of brackets is a conventional notation to indicate that $\mathbf{Q}(\sqrt{d})$ is actually a field. Indeed, if $x + y\sqrt{d} \neq 0$, then

$$\begin{aligned}\frac{1}{x + y\sqrt{d}} &= \frac{x - y\sqrt{d}}{x^2 - dy^2} \\ &= \frac{x}{x^2 - dy^2} + \left(-\frac{y}{x^2 - dy^2}\right)\sqrt{d} \in \mathbf{Q}(\sqrt{d}).\end{aligned}$$

The fields $\mathbf{Q}(\sqrt{d})$ are called the *quadratic number fields*. They are classified as real or imaginary based on whether d is positive or negative.

Any element $\alpha \in \mathbf{Q}(\sqrt{d})$ is an algebraic number. By contrast, α is algebraic integer if and only if either of the following hold:

(1) $d \equiv 1 \pmod 4$ and $\alpha \in \mathbf{Z}[\frac{1+\sqrt{d}}{2}]$.
(2) $d \not\equiv 1 \pmod 4$ and $\alpha \in \mathbf{Z}[\sqrt{d}]$.

This is proved in Stillwell, §10.4.

34.3. *Number fields and their rings of integers* The set of all algebraic numbers forms a field, which we denote

$$\bar{\mathbf{Q}} \subseteq \mathbf{C}.$$

A *number field* is a field $K \subseteq \bar{\mathbf{Q}}$ such that, for some finite list of elements $\gamma_1, \ldots, \gamma_k \in K$, we can write

$$K = \{a_1\gamma_1 + \cdots + a_k\gamma_k \mid a_1, \ldots, a_k \in \mathbf{Q}\}.$$

In fancier language, this means the field K is finite-dimensional as an abstract vector space over the field $\mathbf{Q}$.

The set of all algebraic integers forms a subring

$$\bar{\mathbf{Z}} \subseteq \bar{\mathbf{Q}}.$$

The *ring of integers* of a number field K is

$$\mathcal{O}_K = K \cap \bar{\mathbf{Z}},$$

or in words, the subring of K formed by the elements that are algebraic integers.

Example 34.3. $\mathbf{Q}$ is a number field. Its ring of integers is $\mathcal{O}_{\mathbf{Q}} = \mathbf{Z}$.

Example 34.4. Any quadratic number field $\mathbf{Q}(\sqrt{d})$ is a number field, since we can take $\{\gamma_1, \gamma_2\} = \{1, \sqrt{d}\}$ above. Example 34.2 says that

$$\mathcal{O}_{\mathbf{Q}(\sqrt{d})} = \begin{cases} \mathbf{Z}[\frac{1+\sqrt{d}}{2}] & d \equiv 1 \pmod 4 \\ \mathbf{Z}[\sqrt{d}] & d \not\equiv 1 \pmod 4 \end{cases}$$

In particular, $\mathbf{Z}[\omega]$ is the ring of integers of $\mathbf{Q}(\sqrt{-3})$.

Example 34.5. Let $\zeta_n = e^{2\pi i/n}$. Then the field

$$\mathbf{Q}(\zeta_n) = \{a_0 + a_1\zeta_n + \cdots + a_{n-1}\zeta_n^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in \mathbf{Q}\}$$

that appeared on Problem Set 6 is a number field. With some work, one can show that $\mathcal{O}_{\mathbf{Q}(\zeta_n)} = \mathbf{Z}[\zeta_n]$.

Example 34.6. There is a number field

$$\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6} \mid a_0, a_1, a_2, a_3 \in \mathbf{Q}\}.$$

As a ring, it is isomorphic to $\mathbf{Q}[x, y]/(x^2 - 2, y^2 - 3)$. With some work, one can show that $\mathcal{O}_{\mathbf{Q}(\sqrt{2},\sqrt{3})} = \mathbf{Z}[\sqrt{2}, \sqrt{3}]$.

Remark 34.7. For any integral domain R, there is always a field $\mathrm{Frac}(R)$ called the *field of fractions of* R that captures the intuitive notion of the "smallest" field containing R as a subring. More precisely: There is an injective ring homomorphism $\iota : R \to \mathrm{Frac}(R)$, and any other injective ring homomorphism $R \to F$, where F is a field, can be factored as

$$R \xrightarrow{\iota} \mathrm{Frac}(R) \to F$$

in a unique way.

In particular, it turns out that $\mathrm{Frac}(\mathcal{O}_K)$ can be identified with K. For instance, $\mathrm{Frac}(\mathbf{Z}[\omega]) = \mathbf{Q}(\sqrt{-3})$. It is possible for subrings of a given R to have the same field of fractions as R: For instance, $\mathrm{Frac}(\mathbf{Z}[\sqrt{-3}]) = \mathbf{Q}(\sqrt{-3})$ as well.

34.4. We have seen that $\mathbf{Z}[\sqrt{d}]$ can fail to have unique prime factorization, but that this is sometimes fixed by enlarging it to $\mathcal{O}_{\mathbf{Q}(\sqrt{d})}$. For instance, $\mathbf{Z}[\sqrt{-3}]$ is not a UFD, but $\mathcal{O}_{\mathbf{Q}(\sqrt{-3})} = \mathbf{Z}[\omega]$ is a UFD.

But $\mathcal{O}_{\mathbf{Q}(\sqrt{d})}$ can still fail be a UFD. In $\mathcal{O}_{\mathbf{Q}(\sqrt{-5})} = \mathbf{Z}[\sqrt{-5}]$, we saw the example $6 = 2 \cdot 3 = (1 - \sqrt{-5})(1 + \sqrt{-5})$.

It turns out that even if $\mathcal{O}_K$ fails to have unique prime factorization for nonzero elements, it always retains a notion of unique prime factorization for nonzero ideals. This is actually the origin of the name "ideal": It stands for "ideal number", in the sense that ideals of $\mathcal{O}_K$ behave the way that the numbers in $\mathcal{O}_K$ would behave in an ideal world.

34.5. *Product ideals* In order to discuss factorization of ideals, we need notions of products and primality for ideals. If I and J are ideals of the same ring, then their *product* is defined as

$$I \cdot J = \{x_1 y_1 + \cdots + x_k y_k \mid x_i \in I,\ y_i \in J\}.$$

Note that this can be different from—more precisely, larger than—the set $\{xy \mid x \in I,\ y \in J\}$, which isn't always closed under addition.

34.6. *Prime ideals* To motivate the definition of primality for ideals, recall the prime divisor property for an element $a \in R$: It's the condition that

$$a \text{ divides } bc \implies \text{either } a \text{ divides } b \text{ or } a \text{ divides } c.$$

In general, we know that a divides x if and only if $x \in aR$. So the above condition is equivalent to:

$$bc \in aR \implies \text{either } b \in aR \text{ or } c \in aR.$$

In general, if $I \subseteq R$ is an arbitrary ideal, then we say that I is *prime* iff $I \neq R$ and $ab \in I$ implies that either $a \in I$ or $b \in I$ (or both). (Note that we do allow the zero ideal $\{0\}$ to be prime, if it satisfies the definition.)

This definition ensures that the principal ideal aR is prime if and only if a is a non-unit with the prime divisor property. For instance, $a\mathbf{Z}$ is a prime ideal of $\mathbf{Z}$ if and only if a is prime.

Remark 34.8. We see that

$$\begin{aligned} & R/I \text{ is an integeral domain} \\ \iff & ab + I = I \text{ implies } a + I = I \text{ or } b + I = I \text{ in } R \\ \iff & ab \in I \text{ implies } a \in I \text{ or } b \in I \text{ in } R. \end{aligned}$$

Thus I is prime if and only if R/I is an integral domain.

We can finally state the unique prime factorization theorem for ideals of rings of integers of number fields.

Theorem 34.9 (Dedekind)**.** *Let K be a number field. Then any nonzero ideal $I \subseteq \mathcal{O}_K$ admits a factorization*

$$I = P_1 \cdots P_2 \cdots P_k,$$

where the P_i are prime ideals of $\mathcal{O}_K$ that may repeat. Moreover, this factorization is unique up to reordering.

Example 34.10. In $R = \mathcal{O}_{\mathbf{Q}(\sqrt{-5})} = \mathbf{Z}[\sqrt{-5}]$, the element 2 is irreducible. Nonetheless, the principal ideal $2R$ can be factored further into non-principal ideals!: Explicitly,

$$\begin{aligned}
&(2, 1 - \sqrt{-5}) \cdot (2, 1 + \sqrt{-5}) \\
&= (2R + (1 - \sqrt{-5})R) \cdot (2R + (1 + \sqrt{-5})R) \\
&= (2 \cdot 2)R + (2 \cdot (1 - \sqrt{-5}))R + (2 \cdot (1 + \sqrt{-5}))R \\
&\qquad + ((1 - \sqrt{-5}) \cdot (1 + \sqrt{-5}))R \\
&= 4R + (2 - 2\sqrt{-5})R + (2 + 2\sqrt{-5})R + 6R \\
&= 2R.
\end{aligned}$$

This is why Dedekind's theorem does not contradict the failure of R to be a UFD.