30. 5/1

30.1. Last time we began to discuss ideals. Recall that an ideal of R is a special kind of additive subgroup of R: It is a subgroup that is moreover contagious under multiplication.

Example 30.1. If R is any ring and $a \in R$ is any element, then

$$aR = \{a \cdot x \mid x \in R\},$$

the set of multiples of a, is an ideal of R. Indeed, it is an additive subgroup, and the associativity identity $(a \cdot x) \cdot y = a \cdot (x \cdot y)$ shows that aR is contagious under multiplication. We say that aR is the *principal ideal* generated by a. Stillwell writes (a) for aR.

Thus, $m\mathbf{Z}$ is an ideal of $\mathbf{Z}$ for any integer m, and $\mu\mathbf{Z}[i]$ is an ideal of $\mathbf{Z}[i]$ for any Gaussian integer μ, and so on.

Example 30.2. In particular, $R = 1R$ and $\{0\} = 0R$ are ideals in any ring R.

Example 30.3. $\mathbf{Z}$ is not an ideal of $\mathbf{Z}[i]$. Even though it is a subgroup under addition, it is not contagious under multiplication, because, for instance, $i = 1 \cdot i$ and $1 \in \mathbf{Z}$, but $i \notin \mathbf{Z}$.

Similar reasoning shows that $m\mathbf{Z}$ is not an ideal of $\mathbf{Z}[i]$, and that $\mathbf{Z}$ is not an ideal of $\mathbf{Z}[\omega]$ or $\mathbf{Q}$ or $\mathbf{R}$ or $\mathbf{C}$.

30.2. We claimed last time that we would show:

Theorem 30.4. *If $I \subseteq R$ is an ideal, then R/I forms a ring and the additive group homomorphism $R \to R/I$ is a ring homomorphism.*

The easy part is saying what the ring structure has to be. We already know that R/I forms a group under the addition law

$$(x + I) + (y + I) := (x + y) + I.$$

We want to define the multiplication law to be

$$(x + I) \cdot (y + I) := x \cdot y + I.$$

The whole point is to check that this definition is consistent, or "well-defined".

Proof. To show that the multiplication above is well-defined, we need to make sure its definition is independent of how we choose the coset representatives x and y. So suppose that $x' + I = x + I$ and $y' + I = y + I$. Then $x' \in x + I$ and $y' \in I$, so there must be elements $a, b \in I$ such that $x' = x + a$ and $y' = y + b$. Now

$$\begin{aligned}
(x' + I) \cdot (y' + I) &= x'y' + I \\
&= (x + a)(y + b) + I \\
&= xy + xb + ay + ab + I \\
&= xy + I && \text{by contagiousness of } I! \\
&= (x + I) \cdot (y + I),
\end{aligned}$$

so the multiplication is indeed independent of the choice of representatives.

Checking that the multiplication is associative, commutative, distributes over addition, and admits the identity element $1_R + I$ is routine. Checking that $R \to R/I$ given by $x \mapsto x + I$ is a ring homomorphism is also routine. □

Example 30.5. We saw earlier that the quotient group $\mathbf{Z}[i]/\mathbf{Z}$ cannot form a ring in which $1 + \mathbf{Z}$ is the multiplicative identity. Let's demonstrate this in another way, by showing that the multiplication law $(x + \mathbf{Z}) \cdot (y + \mathbf{Z}) = xy + \mathbf{Z}$ is not well-defined.

Observe that $i + \mathbf{Z} = (1 + i) + \mathbf{Z}$. Under the proposed multiplication, we would simultaneously have

$$\begin{aligned}(i + \mathbf{Z}) \cdot (i + \mathbf{Z}) &= -1 + \mathbf{Z} = \mathbf{Z},\\ (i + \mathbf{Z}) \cdot (1 + i + \mathbf{Z}) &= i - 1 + \mathbf{Z} = i + \mathbf{Z}.\end{aligned}$$

But since $i \notin \mathbf{Z}$, we know that $\mathbf{Z} \neq i + \mathbf{Z}$ as cosets, a contradiction.

30.3. Earlier we introduced principal ideals. An easy generalization: For any finite list of elements $a_1, a_2, \ldots, a_k \in R$, the set of linear combinations

$$a_1R + a_2R + \cdots + a_kR = \{a_1x_1 + a_2x_2 + \cdots + a_kx_k \mid x_1, x_2, \ldots, x_k \in R\}$$

is an ideal of R. Sometimes it is convenient to abbreviate by writing

$$(a_1, a_2, \ldots, a_k) := a_1R + a_2R + \cdots + a_kR,$$

as Stillwell does, provided that we make clear that this is an ideal, not a vector of elements of R. If $I = (a_1, a_2, \ldots, a_k)$, then we say that $a_1, a_2, \ldots, a_k$ is a *generating set* for I.

We can now restate one of the very first theorems we proved, on Feb 10, in the language of ideals:

Theorem 30.6. *For any $a, b \in \mathbf{Z}$, not both zero, we have*

$$a\mathbf{Z} + b\mathbf{Z} = \gcd(a, b)\mathbf{Z}$$

as ideals of $\mathbf{Z}$. More generally, if $a_1, a_2, \ldots, a_k \in \mathbf{Z}$ are not all zero, then

$$a_1\mathbf{Z} + a_2\mathbf{Z} + \cdots + a_k\mathbf{Z} = \gcd(a_1, a_2, \ldots, a_k)\mathbf{Z}$$

as ideals of $\mathbf{Z}$.

Proof. This combines Theorem 3.1 and Theorem 3.2. □

This theorem can be restated as follows: If an ideal $I \subseteq \mathbf{Z}$ admits a finite generating set, then I is actually a principal ideal. In fact, every ideal of $\mathbf{Z}$ is a principal ideal, but there's a cleaner, more general way to show this namely, by showing that this is a consequence of long division.

30.4. *Principal ideals as lattices* Stillwell points out in §11.6:

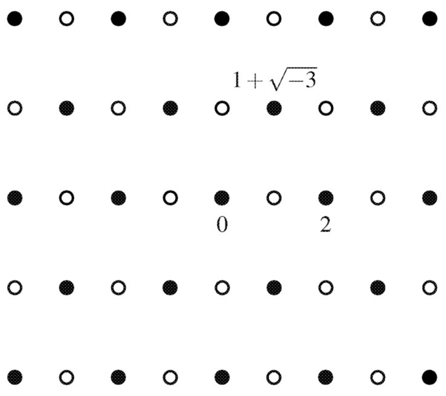
In a ring of complex quadratic integers like $\mathbf{Z}[i]$ or $\mathbf{Z}[\sqrt{-2}]$ or $\mathbf{Z}[\omega]$, the nonzero principal ideals look like rescaled and rotated versions of the ring itself, when they are drawn in the complex plane. For instance, if $\alpha \in \mathbf{Z}[\omega]$ is an Eisenstein integer, then $\alpha\mathbf{Z}[\omega]$ is a rescaled and rotated copy of the triangular/rhombic lattice $\mathbf{Z}[\omega]$.

30.5. *Non-principal ideals* Ideals that aren't principal may still look like lattices, but will have the wrong "shape".

Example 30.7. We claim that in $\mathbf{Z}[\sqrt{-3}]$, the ideal

$$(2, 1+\sqrt{-3}) = \{2\alpha + (1+\sqrt{-3})\beta \mid \alpha, \beta \in \mathbf{Z}[\sqrt{-3}]\}$$

is not principal. It looks like:



We notice that while $\mathbf{Z}[\sqrt{-3}]$ is a rectilinear lattice, the ideal $(2, 1+\sqrt{-3})$ is a triangular/rhombic lattice. So this is an informal visual proof that $(2, 1+\sqrt{-3})$ isn't principal.

To make the proof rigorous, we can use the picture to guess, and then calculate, a simplified expression for the ideal. Namely, it turns out that

$$(2, 1+\sqrt{-3}) = \{2m + (1+\sqrt{-3})n \mid m, n \in \mathbf{Z}\}.$$

If this were principal, say $(2, 1+\sqrt{-3}) = (\gamma)$, then γ would be a common divisor of 2 and $1+\sqrt{-3}$. Using norms and casework, one can check that this forces $\gamma = \pm 1$. But the work above shows $\pm 1 \notin (2, 1+\sqrt{-3})$.

31. 5/3

31.1. Warm-up: Determine all ideals of the following rings.

(1) $\mathbf{Z}$.
(2) $\mathbf{Z}/6\mathbf{Z}$.
(3) $\mathbf{C}$.
(4) $\mathbf{R} \times \mathbf{R}$, under coordinatewise addition and multiplication.

Note that there is an isomorphism of additive groups from $\mathbf{C}$ onto $\mathbf{R} \times \mathbf{R}$, given by $x + yi \mapsto (x, y)$, but this is definitely not an homomorphism of rings.

31.2. *Primes and irreducibility* Today, we'll use ideals to study primes.

Stillwell page 183 has a slight omission, but meant to define prime elements of general rings as follows: An element $a \in R$ is *prime*, or *irreducible*, iff it is not a unit and

$$a = xy \text{ in } R \implies \text{either } x \in R^\times \text{ or } y \in R^\times \text{ (or both).}$$

The reason that other authors prefer the term *irreducible* is to avoid confusion with the prime divisor property. To wit: We say that a satisfies the *prime divisor property* iff

$$a \text{ divides } bc \text{ in } R \implies \text{either } a \text{ divides } b \text{ or } a \text{ divides } c \text{ (or both).}$$

In general rings, both irreducibility and the prime divisor property can behave in pathological ways. Neither necessarily implies the other.

We might ask: In which rings does irreducibility imply the prime divisor property? In which rings does the converse hold? The answers will lead us to be interested only in the primes of rings "like" $\mathbf{Z}$.

31.3. *Integral domains* We say that a ring R is an *integral domain* iff $R \neq \{0\}$ and, for any elements $x, y \in R$ such that $xy = 0$, we must have either $x = 0$ or $y = 0$.

Example 31.1. $\mathbf{Z}$ is an integral domain. Fields, like $\mathbf{C}$, are integral domains. By contrast, $\mathbf{Z}/6\mathbf{Z}$ is not an integral domain because $2 \cdot 3 \equiv 0 \pmod 6$, and $\mathbf{R} \times \mathbf{R}$ is not an integral domain because $(1, 0) \cdot (0, 1) = (0, 0)$.

A nice thing about integral domains: Even when a nonzero element lacks an inverse, you can still cancel it from both sides of an equation.

Lemma 31.2 (Cancellation)**.** *Let R be an integral domain. If $a \in R$ is nonzero, then $ax = ay$ implies $x = y$ for all $x, y \in R$.*

Proof. Rearranging, $ax = ay$ implies $a(x - y) = 0$. Since a is nonzero, we require $x - y = 0$. □

Proposition 31.3. *Let R be an integral domain. If $a \in R$ is neither zero nor a unit, and satisfies the prime divisor property, then a is irreducible.*

Proof. We must show that if $a = xy$, then either $x \in R^\times$ or $y \in R^\times$. Tautologically, a divides xy, so by the prime divisor property, either a divides x or a divides y. Without loss of generality, suppose a divides x. Then $x = az$ for some $z \in R$. Then $a = xy = azy$. By cancellation, $1 = zy$, which proves that $y \in R^\times$. □

Example 31.4. The ring $\mathbf{Z}[\sqrt{-3}]$ is an integral domain, so every element of $\mathbf{Z}[\sqrt{-3}]$ that has the prime divisor property is irreducible.

By contrast, 2 is irreducible in $\mathbf{Z}[\sqrt{-3}]$, but does not satisfy the prime divisor property. Indeed: 2 divides $4 = (1+\sqrt{-3})(1-\sqrt{-3})$, but does not divide either $1+\sqrt{-3}$ or $1-\sqrt{-3}$.

31.4. *Euclidean and principal ideal domains* We follow Artin's *Algebra*, then explain later how the terminology relates to Stillwell's. A *size function* on a ring R is a function

$$\sigma : R - \{0\} \to \mathbf{N}_0 \qquad \text{(where } \mathbf{N}_0 = \mathbf{N} \cup \{0\}\text{)}$$

such that for all $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that

$$a = qb + r \quad \text{and} \quad \text{either } r = 0 \text{ or } \sigma(r) < \sigma(b).$$

We say that an integral domain R is *Euclidean* iff a size function on R exists. We say that R is a *principal ideal domain*, or *PID*, iff every ideal of R is principal.

Theorem 31.5. *Let R be an integral domain. Then*

$$R \text{ is Euclidean} \overset{(1)}{\Longrightarrow} R \text{ is a PID} \overset{(2)}{\Longrightarrow} \left(\begin{array}{c}\text{irreducibles in } R \text{ have the}\\ \text{prime divisor property}\end{array}\right).$$

Proof of (1). Suppose R is Euclidean with size function σ. We must show that if $I \subseteq R$ is an ideal, then $I = aR$ for some $a \in R$. If $I = \{0\}$, then we can take $a = 0$, so suppose $I \neq \{0\}$. Let

$$S = \{\sigma(x) \mid x \in I - \{0\}\} \subseteq \mathbf{N}_0.$$

Since I is not the zero ideal, S is nonempty. By well-ordering, we can choose $a \in I$ such that $\sigma(a)$ is minimal. We claim that every element of I is a multiple of a. Indeed, for any $x \in I$, we can write $x = qa + r$ where either $r = 0$ or $\sigma(r) < \sigma(a)$. But $\sigma(r) < \sigma(a)$ contradicts minimality of $\sigma(a)$, because $r = x - qa \in I$. Therefore $r = 0$, and a divides x. □

Proof of (2). Suppose that R is a PID. We must show that if $a \in R$ irreducible and divides bc, then a either divides b or divides c. Suppose a does not divide b. Since R is a PID, we can write

$$aR + bR = xR$$

for some $x \in R$. Note that $a, b \in xR$, meaning x divides both a and b. But a is irreducible, so either $x \in R^\times$ or $x = ua$ for some $u \in R^\times$. The latter would imply that a divides b, a contradiction, so we must have $x \in R^\times$.

Now $xR = 1R = R$. Therefore

$$aR + bR = R.$$

Rescaling both sides by c, we get

$$acR + bcR = cR.$$

But a divides bc, so the left-hand side is contained in aR. Therefore $c \in aR$, meaning a divides c. □

31.5. Our earlier theorems about long division imply that:

(1) $a \mapsto |a|$ is a Euclidean function on $\mathbf{Z}$.
(2) $\mathbf{N}(x + yi) = x^2 + y^2$ is a Euclidean function on $\mathbf{Z}[i]$.
(3) $\mathbf{N}(x + y\sqrt{-2}) = x^2 + 2y^2$ is a Euclidean function on $\mathbf{Z}[\sqrt{-2}]$.
(4) $\mathbf{N}(x + y\omega) = x^2 - xy + y^2$ is a Euclidean function on $\mathbf{Z}[\omega]$, where $\omega = e^{2\pi/3}$.

But note, for instance, that Theorem 2.3 is different from—in fact, strictly stronger than—the statement that $a \mapsto |a|$ is a size function.

Our notion of a size function is different from Stillwell's notion of a Euclidean function (which is not standard). However, a Euclidean function on R in the sense of Stillwell always restricts to a size function on $R - \{0\}$.

32. 5/5

32.1. *Polynomial rings* Last time we introduced size/Euclidean functions, and commented that Stillwell's definition was different. Why do most authors define them like we do, and not like Stillwell does? It's because they want to include the following example:

Example 32.1. Let R be any ring. The *polynomial ring* in x over R is

$$R[x] = \{\text{polynomials in } x \text{ with coefficients in } R\}.$$

The ring operations are the usual addition and multiplication of polynomials. You can check that if R is an integral domain, then $R[x]$ is an integral domain as well.

Suppose that F is a field, a fortiori an integral domain. Due to polynomial long division, the degree function $\deg : F[x] - \{0\} \to \mathbf{N}_0$ is a size function on $F[x]$. Thus $F[x]$ is a Euclidean domain.

By the preceding example and Theorem 31.5, $F[x]$ is a PID. Let

$$F[x, y] = F[x][y],$$

the ring of polynomials in two variables x and y. Do you think $F[x, y]$ is a PID?

32.2. Today we study how elements of general integral domains factor into irreducible elements. If R is an integal domain and $a \in R$, then an *irreducible factorization* of a is an expression

$$a = p_1 \cdots p_k,$$

where $p_1, \ldots, p_k \in R$ are irreducible and may include repetitions.

Define an *(ascending) chain* of ideals of R to be a sequence of inclusions $I_1 \subseteq I_2 \subseteq \ldots$, where $I_1, I_2, \ldots$ are all ideals of R. The *length* of a chain is the number of inclusions that are strict.

Theorem 32.2. *Let R be an integral domain. If every chain of principal ideals in R has finite length, then every nonzero, non-unit element of R has an irreducible factorization.*

Proof. We show the contrapositive. Let $a_0 \in R$. In general, suppose that $a_i \in R$ is neither zero nor a unit, yet fails to have an irreducible factorization. Since a_i cannot be irreducible itself, we must have $a_i = xy$, where $x, y \in R$ are not units. Moreover, since a_i is nonzero, x and y are nonzero. So at least one must fail to have an irreducible factorization: say, x.

We have $a_i R \subseteq xR$. The inclusion must be strict because if $xR \subseteq a_i R$, then a_i divides x, meaning $a_i = xy = a_i zy$ for some $z \in R$; after cancelling a_i, this forces y to be a unit, a contradiction. So taking $a_{i+1} = x$ gives a strict inclusion $a_i R \subsetneq a_{i+1} R$. By induction, we get a chain of principal ideals of infinite length. □

Example 32.3. The finiteness condition in Theorem 32.2 may seem strange, but it is something very closely related to the well-ordering property of $\mathbf{N}_0$.

As a demonstration of how this works, let's show that if R is a Euclidean domain with a size function σ for which

$$b \text{ divides } a \implies \sigma(b) \leq \sigma(a),$$

then every chain of principal ideals in R has finite length. Let σ be the size function satisfying the stated property. Then

$$aR \subseteq bR \implies \sigma(a) \geq \sigma(b),$$

which in turn implies

$$a_i R = a_{i+1} R \iff \sigma(a_i) = \sigma(a_{i+1}). \tag{32.1}$$

Now, if $a_1 R \subsetneq a_2 R \subsetneq \ldots$ is a chain of principal ideals, then the numbers $\sigma(a_i)$ form a decreasing sequence of elements of $\mathbf{N}_0$. By well-ordering, they must eventually stop at some minimal value $\sigma(a_\ell)$. By (32.1), this means the inclusions in the chain become equalities after the ℓth step.

Example 32.4. As it turns out, $F[x, y]$ is not a PID. For instance, (x, y) is not a principal ideal. However, every chain of principal ideals in $F[x, y]$ has finite length. The key in the proof is to show that if $(f) \subsetneq (g)$ is a strict inclusion of nonzero principal ideals in $F[x, y]$, then $\deg(f) > \deg(g)$. Note that deg is <u>not</u> a size function on $F[x, y]$, unlike the situation for $F[x]$.

32.3. We say that $a \in R$ has *uniqueness of irreducible factorization* iff, given any two irreducible factorizations

$$a = p_1 \cdots p_k = q_1 \cdots q_\ell,$$

we can reindex the q_i in such a way that $k = \ell$ and, for some units $u_i \in R^\times$, we have $u_i p_i = q_i$ for all i.

Theorem 32.5. *Let R be an integral domain. If every irreducible element of R satisfies the prime divisor property, then every element of R has uniqueness of irreducible factorization.*

Proof. Suppose $p_1 \cdots p_k = q_1 \cdots q_\ell$ are two irreducible factorizations of the same element of R. If $\max(k, \ell) = 1$, then we're done. Otherwise, by the prime divisor property and induction, we can show that p_k must divide at least one of the q_j.

Without loss of generality, say it is q_ℓ. Since q_ℓ is irreducible and p_k is not a unit, we must have $u_k p_k = q_\ell$. So after replacing p_{k-1} with $u_k^{-1} p_{k-1}$, we obtain an identity of irreducible factorizations $p_1 \cdots p_{k-1} = q_1 \cdots q_{\ell-1}$. Since $\max(k-1, \ell-1) < \max(k, \ell)$, we can use induction to conclude. □

Next time, we'll finish this whole discussion by studying Theorem 32.2, Example 32.3, and Theorem 32.5 in conjunction.