Lecture notes for PM 441/641

David McKinnon
Department of Pure Mathematics
University of Waterloo

Spring 2020

1 What is an algebraic integer?

What is an algebraic integer?

That's the motivating question for this course. I mean, we will *define* an algebraic integer pretty early in the course, but you don't learn who your friend *is* just by learning their name.

So. We know what an algebraic *number* is: it's a complex number that is the root of a polynomial with integer coefficients. Which of these should we call "integers"?

It's tempting to say something about denominators here. But the problem is, say α is the root of the following polynomial:

$$x^{17} - 4x + 13$$

So ... what's the denominator of α? Tough to say, really. All we really know about α is that when you raise it to the power seventeen, you get the same thing as if you multiplied it by four and subtracted thirteen.

In fact, the minimal polynomial is really the only thing we ever know about an algebraic number, most of the time. So our definition of algebraic integer probably should relate to that.

The one place where we are really confident that we know what all the algebraic integers are is $\mathbb{Q}$, the field of rational numbers. Every rational number can be written uniquely as a/b, where a and b are (*gulp*) integers – *rational* integers, if you like – satisfying $b > 0$ and $\gcd(a, b) = 1$. The integers are just the ones where $b = 1$.

So what's the monic minimal polynomial of a/b? Silly question, but it still has an answer: it's $x - a/b$. So – and I'm aware of how silly this sounds – we can say that a/b is an integer if and only if its monic minimal polynomial has coefficients in $\mathbb{Z}$.

That is so lame. But it's the only thing we've got, so we define:

Definition 1.1. *Let α be an algebraic number. Then α is an algebraic integer if and only if it is the root of a monic polynomial $p(x) \in \mathbb{Z}[x]$ with coefficients in $\mathbb{Z}$.*

In fact, it will be helpful to make a slightly more general definition.

Definition 1.2. *Let A be a domain, and let T be a domain containing A. Let $\alpha \in T$ be any element. Then α is integral over A if and only if it is the root of a monic polynomial $p(x) \in A[x]$ with coefficients in A.*

Notice that I sneakily got rid of the "minimal" in "monic minimal polynomial". That's because it doesn't really matter, and often gets in the way. Like your irritating little brother. (Or like all of your irritating little brothers, if you don't have any.)

So the algebraic integers are just the elements of $\mathbb{C}$ that are integral over $\mathbb{Z}$. (If α is not algebraic over K, then we say that it is not integral over A.)

Let's do some examples. We've already seen that the algebraic integers in $\mathbb{Q}$ are just the rational integers $\mathbb{Z}$. Notice that i – the square root of -1 – is an algebraic integer, because it's a root of its monic minimal polynomial $x^2 + 1$, which has coefficients in $\mathbb{Z}$.

More examples. The cube root of unity, $w = e^{2\pi i/3}$, is an algebraic integer, because it's a root of $x^2 + x + 1$. Notice a curious feature here, though. We often write

$$w = \frac{1 - \sqrt{-3}}{2}$$

which has a denominator. I mean, it blatantly does. And yet, w is still an integer because of that monic polynomial thing. This doesn't mean we've got the wrong definition of algebraic integer – as if! – but it does mean that there's something subtle going on here. We'll come back to this later.

Just to show that not everything is an algebraic integer, notice that $w/2 = \frac{1-\sqrt{-3}}{4}$ is *not* an algebraic integer, because its monic minimal polynomial is $m(x) = x^2 + (1/2)x + (1/4)$, which doesn't have integer coefficients. And if $p(x)$ is any other monic polynomial with integer coefficients and $p(w/2) = 0$, then it has $m(x)$ as a factor, which is impossible by Gauss' Lemma.

In fact, we have the following general and useful result.

Theorem 1.3. *Let $\alpha \in \overline{\mathbb{Q}}$ be an algebraic number that is the* *root of a monic polynomial with integer coefficients. Then the monic minimal polynomial of α has integer coefficients.*

Proof: Say $f(\alpha) = 0$, where $f(x) \in \mathbb{Z}[x]$ is monic, and let $m(x) \in \mathbb{Q}[x]$ be the monic minimal polynomial of α over $\mathbb{Q}$. Then $f(x) = m(x)q(x)$ for some polynomial $q(x) \in \mathbb{Q}[x]$. Pulling out a least common denominator d from the coefficients of $m(x)$ and $q(x)$, we get $df(x) = M(x)Q(x)$, where $M(x)$ and $Q(x)$ have integer coefficients. Moreover, we can ensure that the coefficients of $M(x)$ have no common factor, and similarly for $Q(x)$. In other words, we can ensure that $M(x)$ and $Q(x)$ are primitive polynomials.

By Gauss' Lemma, this means that the polynomial $M(x)Q(x)$ is also primitive. But it equals $df(x)$ ... so $d = 1$, and $m(x)$ had integer coefficients all along. ♣

Let's do an example. What are the algebraic integers in $\mathbb{Q}(\sqrt{2})$?

Well, any element of $\mathbb{Q}(\sqrt{2})$ is of the form $a + b\sqrt{2}$. The monic minimal polynomial for $a + b\sqrt{2}$ is

$$(x - a - b\sqrt{2})(x - a + b\sqrt{2}) = x^2 - 2ax + a^2 - 2b^2$$

So if a and b are integers, this polynomial has integer coefficients, and therefore $a + b\sqrt{2}$ is an algebraic integer.

Conversely, if this polynomial has integer coefficients, then $2a$ is an integer (as in, $2a \in \mathbb{Z}$) and so is $a^2 - 2b^2$. If $a = n/2$ and $b = \ell/k$, then

$$a^2 - 2b^2 = n^2/4 - 2\ell^2/k^2$$

Since this is an integer, we deduce that we can take $k^2 = 4$, or $k = 2$. This means that $n^2 - 2\ell^2$ is a multiple of 4, and a quick check of the possibilities shows that this means that n and ℓ are both even. So a and b are actually both integers.

Putting all this together, we see that $a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ is an algebraic integer if and only if a and b are both integers. In other words, the set of algebraic integers in $\mathbb{Q}(\sqrt{2})$ is the ring $\mathbb{Z}[\sqrt{2}]$.

It's a ring. Hmm. I wonder if that's an accident.

2 Algebraic integers form a ring

Now that we know what algebraic integers are, we'd like to be able to add and subtract and multiply them, just like we can with kindergarten-style integers. To do this, we need to take a little digression, and talk about modules. If you already know what a module is, you can skip that section. Otherwise, take a few moments to go to the module section and read up on them. We'll wait for ya.

OK, nice to have you back. Or maybe you never left, which is also cool. You do you. Let's get with the subtraction and stuff.

The reason we need the module stuff is to give a slightly different definition of integral over A. Which is to say, we need to prove a theorem.

Theorem 2.1. *Let T be a domain containing a domain A, and let $\alpha \in T$. Then α is integral over A if and only if the ring $A[\alpha] \subset T$ is a finitely generated A-module.*

Proof: Let K be the fraction field of A.

First, assume that α is integral over A. Then in particular it is algebraic over K, and so it has a monic minimal polynomial $p(x)$ with coefficients in K. Since α is integral over A, those coefficients actually lie in A, so we have:

$$\alpha^d = a_{d-1}\alpha^{d-1} + \ldots + a_0$$

where $a_i \in A$ are the (negatives of) the coefficients of the minimal polynomial $p(x)$. But this equation makes clear that α^d is in the A-module M generated by $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$. And multiplying that equation by α makes it clear that α^{d+1} is in the A-module generated by $\{\alpha, \ldots, \alpha^d\}$ ... which is just M!

Continuing in this way, we find that every power of α is contained in M. So all of $A[\alpha] = M$, and is therefore finitely generated.

To go the other way, assume that $A[\alpha]$ is a finitely generated A-module. Then there is a finite set of generators for $A[\alpha]$. Call them $p_1(\alpha), \ldots, p_n(\alpha)$, where the p_i are polynomials. Pick a positive integer d that is larger than the degree of any of the $p_i(x)$, and write α^d as an A-linear combination of the $p_i(\alpha)$:

$$\alpha^d = a_1 p_1(\alpha) + \ldots + a_n p_n(\alpha)$$

Because d is greater than the degree of any of the $p_i(x)$, this equality means that α is the root of a *monic* polynomial of degree d – namely, $q(x) = x^d - a_1 p_1(x) - \ldots - a_n p_n(x)$. So α is integral over A. ♣

This, surprisingly, allows us to prove that the ring of integers in a number field is a ring.

Theorem 2.2. *Let K be a number field, and let A be the set of algebraic integers in K. Then A is a ring.*

Proof: Certainly 0 and 1 are in A, so we just have to check that A is closed under addition, subtraction, and multiplication.

Let α and β be any elements of K. If $\{1, \alpha, \alpha^2, \ldots, \alpha^a\}$ generate $\mathbb{Z}[\alpha]$ over $\mathbb{Z}$, and if $\{1, \beta, \beta^2, \ldots, \beta^b\}$ generate $\mathbb{Z}[\beta]$ over $\mathbb{Z}$, then certainly $\{\alpha^i \beta^j \mid 0 \le i \le a, 0 \le b \le b\}$ generate $\mathbb{Z}[\alpha, \beta]$ over $\mathbb{Z}$. So $\mathbb{Z}[\alpha, \beta]$ is finitely generated.

But $\mathbb{Z}[\alpha \pm \beta]$ and $\mathbb{Z}[\alpha\beta]$ are contained in $\mathbb{Z}[\alpha, \beta]$, and $\mathbb{Z}$ is noetherian. So they are submodules of a finitely generated $\mathbb{Z}$-module for noetherian $\mathbb{Z}$, and we can deduce that $\alpha \pm \beta$ and $\alpha\beta$ are integral over $\mathbb{Z}$ too. We triumphantly conclude, with a flourish, that A is a ring, as desired. ♣

3 The ring of integers is just $\mathbb{Z}^n$ with a fancy multiplication

Think about $\mathbb{Z}$. It's isomorphic to $\mathbb{Z}^1$, as a ring. (Hey. I've got a *PhD.*) It's the ring of integers in the number field $\mathbb{Q}$, which has degree 1 over $\mathbb{Q}$.

Think about $\mathbb{Z}[i]$. It's the ring of integers in the number field $\mathbb{Q}(i)$, which has degree 2 over $\mathbb{Q}$. And $\mathbb{Z}[i]$ is isomorphic to $\mathbb{Z}^2$ as an additive group, although the multiplication is different.

This pattern holds in general. If K is a number field of degree d over $\mathbb{Q}$, then the ring of integers in K (which is usually denoted $\mathcal{O}_K$) is isomorphic to $\mathbb{Z}^d$ as an additive group.

We need a tiny bit of new technology to prove this properly. Here it is.

Definition 3.1. *Let K be a field, and let L be a finite-dimensional*

K-vector space that is also a ring. Define two functions $Tr_{L/K}\colon L \to K$ and $N_{L/K}\colon L \to K$, called the trace and the norm, respectively, by

$$Tr(\alpha) = Tr(T_\alpha) \text{ and } N(\alpha) = \det(T_\alpha)$$

where $T_\alpha\colon L \to L$ is the linear transformation

$$T_\alpha(x) = \alpha x$$

Note that if L is a field, then the roots of the characteristic polynomial for T_α are the same as the roots of the minimal polynomial for α over K. So we have

$$\mathrm{Tr}(\alpha) = \alpha_1 + \ldots + \alpha_d$$

and

$$N(\alpha) = \alpha_1 \ldots \alpha_d$$

where $d = [L : K]$ and $\alpha_1 \ldots, \alpha_d$ are the roots (counted multiple times maybe) of the minimal polynomial of α, including α. If L and K are number fields, then these are just the Galois conjugates of α. Notice that some of the α_i might not lie in L!

Now, the characteristic polynomial of T_α is degree $[L : K]$, but the minimal polynomial $m(x)$ of α over K is degree $[K(\alpha) : K]$, which might be smaller. Since the roots are the same and both polynomials have coefficients in K, this means that the characteristic polynomial of T_α is $m(x)^r$, where $r = [L : K]/[K(\alpha) : K] = [L : K(\alpha)]$.

So we can calculate as follows. Write the minimal polynomial for α over K as

$$m(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

Then we get

$$m(x)^r = x^{rn} + ra_{n-1}x^{rn-1} + \ldots + a_0^r$$

But $a_{n-1} = -\alpha_1 - \ldots - \alpha_d$, and $a_0 = \alpha_1 \ldots \alpha_d$. So we deduce:

$$\mathrm{Tr}_{L/K}(\alpha) = -ra_{d-1}$$

and

$$N_{L/K}(\alpha) = (-1)^{dr} a_0^r$$

which is the general formula for the trace and norm in the case that L is a field.

So, for example, let $M = Q(\sqrt{2}, \sqrt{3})$, $L = \mathbb{Q}(\sqrt{2})$. Then

$$\mathrm{Tr}_{L/\mathbb{Q}}(1 + \sqrt{2}) = (1 + \sqrt{2}) + (1 - \sqrt{2}) = 2$$

but

$$\mathrm{Tr}_{M/\mathbb{Q}}(1+\sqrt{2}) = (1+\sqrt{2}) + (1+\sqrt{2}) + (1-\sqrt{2}) + (1-\sqrt{2}) = 4$$

because there are four elements of the Galois group of $M/\mathbb{Q}$, and they move $1 + \sqrt{2}$ to two different places twice each.

The reason we've done all this, is that the trace $\mathrm{Tr}_{L/K}$ allows us to define a pairing on L.

Definition 3.2. *Let K be a field, L a finite-dimensional K-vector space that is also a ring. Define a pairing on L by $\langle \alpha, \beta \rangle = Tr_{L/K}(\alpha\beta)$.*

It's easy to check that this is a symmetric, K-bilinear pairing on L. If L is a field, then it's also easy to see that it is non-degenerate, by which I mean the following:

Theorem 3.3. *Let L/K be a finite extension of fields of characteristic zero. For every $x \in L$, there is some $y \in L$ such that $Tr(xy) \neq 0$, unless $x = 0$.*

The proof of this is easy: set $y = 1/x$. (For a proof of the corresponding result for finite fields, see the finite rings section.) But it enables the following theorem:

Theorem 3.4. *Let A be the ring of integers in a number field K with $[K : \mathbb{Q}] = d$. Then A is isomorphic to $\mathbb{Z}^d$ as an additive group.*

Proof: First, we prove the following lemmas:

Lemma 3.5. *For every element $\alpha \in K$, there is an integer $N \in \mathbb{Z}$ satisfying $N\alpha \in \mathcal{O}_K$. In particular, the fraction field of $\mathcal{O}_K$ is K.*

Proof of lemma: Let $p(x)$ be the monic minimal polynomial for α over $\mathbb{Q}$. There is some large integer $N \in \mathbb{Z}$ such that $Np(x)$ has integer coefficients. The monic minimal polynomial for $N\alpha$ is just $N^r p(x/N)$, where r is the degree of p. This has integer coefficients, so $N\alpha$ is integral, as desired. ♣

Lemma 3.6. *Let L/K be a finite extension of number fields, and let $\alpha \in L$ be an algebraic integer. Then $Tr(\alpha)$ and $N(\alpha)$ are also algebraic integers.*

Proof: The trace of α is the sum of its conjugates and the norm is the product of its conjugates. The conjugates of α are all integers (they have the same monic minimal polynomial!), so their sum and product is also an algebraic integer. ♣

Now for the proof of the theorem. Choose a basis $\{x_1, \ldots, x_d\}$ for K as a $\mathbb{Q}$-vector space. After multiplying the x_i by a big integer, we can assume that the x_i all lie in $\mathcal{O}_K$.

Define a $\mathbb{Q}$-linear transformation $\phi\colon K \to \mathbb{Q}^d$ by

$$\phi(\alpha) = (\mathrm{Tr}_{K/\mathbb{Q}}(x_1\alpha), \ldots, \mathrm{Tr}_{K/\mathbb{Q}}(x_d\alpha))$$

It's easy to check that this is a K-linear transformation. And if $\alpha \in K$ is in the kernel of ϕ, then we must have $\mathrm{Tr}_{K/\mathbb{Q}}(x_i\alpha) = 0$ for all i, and therefore $\mathrm{Tr}_{K/\mathbb{Q}}(x\alpha)$ for all $x \in K$! This is impossible by the nondegeneracy of the trace (Theorem 3.3), and so ϕ is injective.

But that means that, by the First Isomorphism Theorem, $A = \mathcal{O}_K$ is isomorphic to a submodule of $\mathbb{Q}^d$. Better yet, by Lemma 3.6, it's isomorphic to a submodule of $\mathbb{Z}^d$! Since A contains d $\mathbb{Q}$-linearly independent elements (namely $\{x_1, \ldots, x_d\}$, we see that it must be isomorphic to $\mathbb{Z}^d$, as desired. ♣

This has all sorts of fun consequences.

Corollary 3.7. *Let I be a nonzero ideal in the ring of integers $\mathcal{O}_K$ of a number field K with $[K : \mathbb{Q}] = d$. Then I is isomorphic to $\mathbb{Z}^d$ as an additive group.*

Proof: Let $a \in I$ be any nonzero element, and let $\{x_1, \ldots, x_d\}$ be a basis for $\mathcal{O}_K$ as a $\mathbb{Z}$-module. Since I is an additive subgroup of $\mathcal{O}_K \cong \mathbb{Z}^d$, it must be a free abelian group of rank at most d. And $\{ax_1, \ldots, ax_d\}$ is a linearly independent set with d elements sitting inside I, so the rank of I is also at least d. ♣

Corollary 3.8. *Let K be a number field with ring of integers $A = \mathcal{O}_K$, I a nonzero ideal of A. Then A/I is a finite ring. If $I = (\alpha)$ is a principal ideal, then A/I has $\left|N_{K/\mathbb{Q}}(\alpha)\right|$ elements.*

Proof: Clearly A/I is a ring, so we just need to show that it's finite. We also know that A/I is finitely generated as an additive group – because A is – and so as additive groups, we get $A/I \cong \mathbb{Z}^r \times T$ for some finite abelian group T. All we need to do is show that $r = 0$.

But if $r \geq 1$, then A/I would have an element $\overline{x}$ of infinite order, that is the image of some element $x \in A$. If $\{x_1, \ldots, x_d\}$ is a linearly independent subset of I (which exists by Corollary 3.7), then $\{x, x_1, \ldots, x_d\}$ would also be linearly independent. To see this, notice that any linear relation

$$ax + a_1x_1 + \ldots + a_dx_d = 0$$

either has $a = 0$ (which would imply $a_i = 0$ for all i by the independence of the $\{x_i\}$), or else would reduce to $ax \equiv 0 \pmod{I}$, which is a contradiction. So $r = 0$ and A/I is finite.

For the last sentence of the theorem, assume $I = (\alpha)$ is principal. Then generators for I as a $\mathbb{Z}$-module are just $\{\alpha a_1, \ldots, \alpha a_d\}$, where $\{a_1, \ldots, a_d\}$ are generators for A as a $\mathbb{Z}$-module. In other words, I is the image of $\mathcal{O}_K$ under the linear transformation $L(x) = \alpha x$.

The determinant of L is $N_{L/K}(\alpha)$. But the absolute value of the determinant of L is also the volume of the image of the unit hypercube under L, which in turn is the cardinality of the quotient $\mathbb{Z}^d/L(\mathbb{Z}^d) = \mathcal{O}_K/I$. ♣

Corollary 3.9. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then every nonzero prime ideal of $\mathcal{O}_K$ is maximal.*

Proof: Let P be a nonzero prime ideal of $\mathcal{O}_K$. Then $\mathcal{O}_K/P$ is a domain. But it's also finite, so it must be a field. ♣

[If you haven't seen the proof that a finite commutative domain is a field, go find it. It is awesome. And in the algebra section.]

Corollary 3.10. *Let K be a number field with ring of integers $\mathcal{O}_K$. Any subring A of $\mathcal{O}_K$ is a noetherian ring. In particular, $\mathcal{O}_K$ is noetherian.*

Proof: Let I be an ideal of A. We want to show that I is finitely generated as an A-module. But I is an additive subgroup of $\mathcal{O}_K$, which is isomorphic to $\mathbb{Z}^d$ as an additive group, so in particular, I is a finitely generated $\mathbb{Z}$-module. Since A contains $\mathbb{Z}$ (it contains 1 and is closed under ±), this means *a fortiori* that I is a finitely generated A-module too. ♣

We end with some definitions that are handy for describing rings of integers.

Definition 3.11. *Let A be a domain, T a domain containing A. Then T is integral over A if and only if every element of T is integral over A.*

Definition 3.12. *Let A be a domain, T a domain containing A. The integral closure of A in T is the set of elements of T that are integral over A.*

Definition 3.13. *A domain T is integrally closed if and only if the integral closure of T in its fraction field K is just T.*

This enables us to prove a few more useful results.

Theorem 3.14. *Let A be a domain, and let T be a domain containing A. Let U be a domain containing T, and let $\alpha \in U$. If α is integral over T and T is integral over A, then α is integral over A.*

Proof: Let $m(x)$ be the monic minimal polynomial for α over the fraction field of T. Then the coefficients $m_1, \ldots, m_r$ of $m(x)$ lie in T, and α is integral over $A[m_1, \ldots, m_r]$.

But each of the m_i is integral over A, so the ring $D = A[m_1, \ldots, m_r]$ is a finitely generated A-module. Since α is integral over D, the ring $D[\alpha]$ is a finitely generated D-module, generated by $d_1, \ldots, d_n$. But then $D[\alpha]$ is generated as an A-module by the finite set $\{m_i d_j\}$, so α is integral over A, as desired. ♣

Corollary 3.15. *Let A be a domain, K a field containing A. The integral closure T of A in K is integrally closed.*

Proof: Say that $t \in K$ is integral over T. Then since T is integral over A, we deduce from Theorem 3.14 that t is integral over A, and therefore an element of T. ♣

We can now make the following definition:

Definition 3.16. *A Dedekind domain is an integrally closed commutative domain such that every nonzero prime ideal is maximal.*

In particular, the ring of integers $\mathcal{O}_K$ in a number field K is a Dedekind domain. There are many other examples of Dedekind domains, but these will do for now.

4 Geometry of Numbers

So we know that $\mathcal{O}_K$ is isomorphic to $\mathbb{Z}^d$ as an additive group. The natural question is: what's the multiplication like?

We're not really going to answer that question, because it's very complicated. So we'll answer a different question.

Is there a *geometric* way to view the ring $\mathcal{O}_K$?

That might seem a bit dumb. I mean, we're doing *number theory* here, not geometry. But it turns out that the geometric angle is extremely useful in number theory, and not just because it pays my rent. Let's elaborate.

The ring $\mathbb{Z}$ is this nice, orderly, one-dimensional lattice in $\mathbb{R}^1$. Cool. And $\mathbb{Z}[i]$ (the ring of integers in $\mathbb{Q}(i)$) is a nice, orderly, two-dimensional lattice in $\mathbb{C}$. Which is cool.

But ... $\mathbb{Z}[\sqrt{2}]$ is isomorphic to $\mathbb{Z}^2$ just like $\mathbb{Z}[i]$ is. (*As additive groups!* They are very different rings!) And yet, $\mathbb{Z}[\sqrt{2}]$ is all scrunched up inside $\mathbb{R}^1$, instead of respectfully spread out over $\mathbb{R}^2$. Something ain't right.

The purpose of this section is to explain how you can view $\mathcal{O}_K \cong \mathbb{Z}^d$ as a nice, respectable lattice in $\mathbb{R}^d$, if you just look at it the right way.

To start with, we make a definition. I mean, because of course.

Definition 4.1. *A lattice in $\mathbb{R}^d$ is an additive subgroup that is isomorphic to $\mathbb{Z}^d$ and spans $\mathbb{R}^d$.*

In particular, notice that if Λ is a lattice in $\mathbb{R}^d$, then a basis for Λ is a basis for $\mathbb{R}^d$, and the elements of Λ are just the linear combinations of that basis, with integer coefficients.

So, let's say that K is a number field of degree d over $\mathbb{Q}$. Then there are exactly d homomorphisms $\phi_1, \ldots, \phi_d$ from K to $\mathbb{C}$. For some of them, the image of ϕ_j is contained in $\mathbb{R}$ – we'll call those real embeddings, and rearrange the ϕ_j so that the real embeddings are $\phi_1, \ldots, \phi_r$. (Recall that a homomorphism from a field to any other ring is injective.)

The rest of the ϕ_j – called complex embeddings – are homomorphisms from K to $\mathbb{C}$ whose image is not contained in $\mathbb{R}$. That means that ϕ_j and its complex conjugate (namely, the homomorphism you get by composing ϕ_j with complex conjugation) are different homomorphisms, and so the conjugate $\overline{\phi_j}$ must be somewhere else in the list of ϕ_j. Let's pair those up, so that each embedding ϕ_j for $j > r$ is either right before or right after its complex conjugate.

By stringing together all these homomorphisms into one big vector, we get an embedding of K into $\mathbb{C}^d$.

Definition 4.2. *Let K be a number field of degree d over $\mathbb{Q}$, and let $\phi_1, \ldots, \phi_r$ be its real embeddings and $\phi_{r+1}, \ldots, \phi_d$ its complex embeddings. The Minkowski map of K is the embedding*

$$\Phi_K(x) = (\phi_1(x), \ldots, \phi_r(x), \phi_{r+1}(x), \ldots, \phi_d(x))$$

of K into $\mathbb{C}^d$.

But ... we wanted an embedding of K into $\mathbb{R}^d$, not $\mathbb{C}^d$. Luckily, there is a nifty way around this.

For $\phi_1. \ldots, \phi_r$, the fix is easy: those embeddings are to $\mathbb{R}$ anyway, so we can just forget about the rest of $\mathbb{C}$.

For $\phi_{r+1}, \ldots, \phi_d$, we know that they're paired up by complex conjugates. So if $x = (x_1, \ldots, x_r, x_{r+1}, \ldots, x_d)$ is a point in the image of Φ_K, we know that, for example, $x_{r+1} = \overline{x_{r+2}}$. This is two real linear relations between the coordinates of x for each pair of complex embeddings.

So, to sum up, we have just realised that the image of Φ_K is contained in the following real linear subspace of $\mathbb{C}^d$:

$$\mathrm{Im}(x_1) = 0, \ldots, \mathrm{Im}(x_r) = 0$$

$$\mathrm{Re}(x_{r+1}) = \mathrm{Re}(x_{r+2}), \ldots, \mathrm{Re}(x_{d-1}) = \mathrm{Re}(x_d)$$
$$\mathrm{Im}(x_{r+1}) = -\mathrm{Im}(x_{r+2}), \ldots, \mathrm{Im}(x_{d-1}) = -\mathrm{Im}(x_d)$$

That's d real linear relations on our vector space of $2d$ real dimensions. We have just successfully embedded K into a d-dimensional real vector space, namely, the one described by those equations above. This space is called Minkowski space, and we'll call it V_K. Just to warn you, though, there are other people out there who define Minkowski space slightly differently (or completely differently, if they're talking about the Minkowski space in differential geometry). We will ignore such people, but I figured I'd warn you about them in case any of them asks you for money.

The most important next step is to prove that the image $\Phi_K(\mathcal{O}_K)$ of $\mathcal{O}_K$ is a lattice in V_K.

The next step is to figure out the image of $\mathcal{O}_K$ under Φ_K, and prove that it's a lattice.

Theorem 4.3. *The image $\Phi_K(\mathcal{O}_K)$ of $\mathcal{O}_K$ under the Minkowski map Φ_K is a lattice in V_K.*

Proof: Let $\{x_1, \ldots, x_d\}$ be a basis of $\mathcal{O}_K$ over $\mathbb{Z}$. All we need to do is show that $\{\Phi_K(x_1), \ldots, \Phi_K(x_d)\}$ is a basis of V_K over $\mathbb{R}$.

To do *that*, all we need to do is show that $\{\Phi_K(x_1), \ldots, \Phi_K(x_d)\}$ is linearly independent over $\mathbb{C}$. You all remember first year linear algebra – let's make a matrix!

$$B = \begin{pmatrix} \phi_1(x_1) & \dots & \phi_1(x_d) \\ \vdots & & \vdots \\ \phi_d(x_1) & \dots & \phi_d(x_d) \end{pmatrix}$$

The columns of the matrix B are exactly the vectors $\Phi_K(x_i)$.

So, assume that there was some linear dependence relation between the rows of B. Then there would be complex numbers $a_1, \dots, a_d$ such that for each i, we have

$$a_1\phi_1(x_i) + \ldots + a_d\phi_d(x_i) = 0$$

If $\alpha = b_1x_1 + \ldots + b_dx_d$ is any element of K, then we must also have

$$a_1\phi_1(\alpha) + \ldots + a_d\phi_d(\alpha) = 0$$

by the linearity of the ϕ_i. This means that the functions $\phi_1, \dots, \phi_d$ are linearly dependent, as homomorphisms from K to $\mathbb{C}$.

This turns out to be famously impossible, by a theorem of Dirichlet:

Theorem 4.4. *Let $f_1, \dots, f_n$ be distinct homomorphisms from an abelian group G to the multiplicative group F^* of a field F. Then $f_1, \dots, f_n$ are linearly independent over F.*

For the proof of this theorem, see the algebra section.

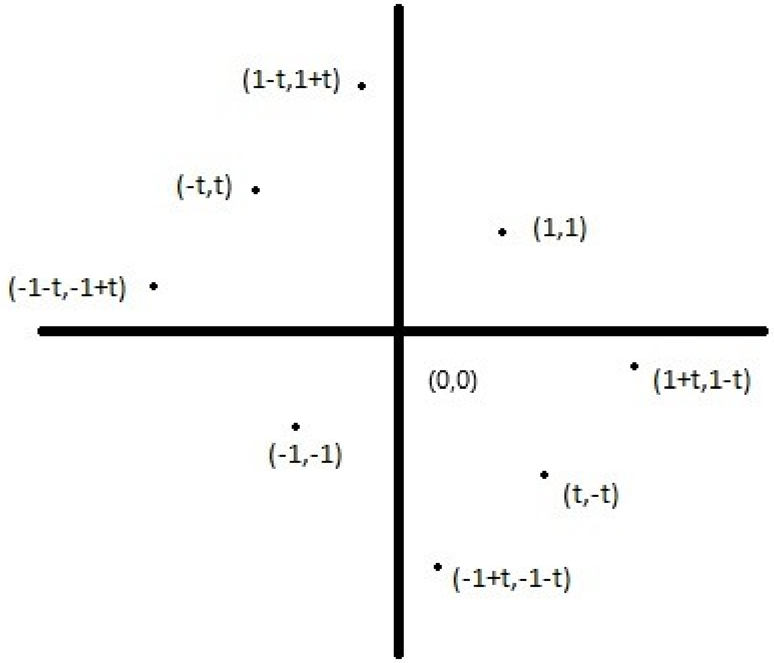
But if the vectors $\Phi_K(x_i)$ are linearly independent over $\mathbb{C}$, then they are certainly linearly independent over $\mathbb{R}$. ♣

Let's look at an example of this. In the case of $\mathbb{Q}$, Minkowski space is just the real line, and $\mathbb{Z}$ is a beautiful one-dimensional lattice there.

For an imaginary quadratic extension like $\mathbb{Q}(i)$, Minkowski space is just $\mathbb{C}$, and the ring of integers $\mathbb{Z}[i]$ is a beautiful two-dimensional lattice, just like we want. Except ... not quite. In fact, $\mathbb{Q}(i)$ embeds in a slightly weird two-dimensional real subspace of $\mathbb{C}^2$, namely $x_1 = \overline{x_2}$. This matters almost not at all, except that the basis vectors 1 and i for $\mathbb{Z}[i]$ over $\mathbb{Z}$ map to $(1, 1)$ and $(i, -i)$, which have lengths $\sqrt{2}$ (instead of 1, as you would expect). This turns out to be really important later. But for now, don't worry about it too much.

More interesting is the case of a real quadratic extension, like $\mathbb{Q}(\sqrt{2})$. Its ring of integers is $\mathbb{Z}[\sqrt{2}]$, as we saw in the section defining algebraic integer in the first place.

How does $\mathbb{Z}[\sqrt{2}]$ embed in Minkowski space $V_K \cong \mathbb{R}^2$? The two embeddings of $\mathbb{Q}(\sqrt{2})$ in $\mathbb{R}$ are $\phi_1(a + b\sqrt{2}) = a + b\sqrt{2}$, and $\phi_2(a + b\sqrt{2}) = a - b\sqrt{2}$. So we have the following picture ($t = \sqrt{2}$):



So $\mathbb{Z}[\sqrt{2}]$ becomes a rectangular lattice in Minkowski space, tilted at an angle of 45° with respect to the coordinate axes, and side lengths $\sqrt{2}$ and 2.

5 Discriminants

This section delves a little deeper into the geometry of Minkowski space. Why, for example, is $\mathbb{Z}[i]$ a weird lattice with squares of side length $\sqrt{2}$, instead of a perfectly simple lattice with unit squares?

Definition 5.1. *Let $\{v_1, \ldots, v_n\}$ be a subset of a complex inner product space V. Define the matrix A whose columns are the coordinate vectors of $\{v_1, \ldots, v_n\}$ with respect to some unitary basis of V. The discriminant of $\{v_1, \ldots, v_n\}$ is defined to be the square of the determinant of A:*

$$\operatorname{disc}(v_1, \ldots, v_n) = (\det(A))^2$$

If this matrix is not square, then the discriminant of $\{v_1, \ldots, v_n\}$ is defined to be zero.

Definition 5.2. *The discriminant of a lattice Λ in Minkowski space V_K is defined to be the discriminant of any basis of Λ over $\mathbb{Z}$. In particular, the discriminant of the ring of integers of a number field K is the discriminant of a basis $\{x_1, \ldots, x_d\}$ for $\mathcal{O}_K$ over $\mathbb{Z}$, considered as a subset of Minkowski space $V_K \subset \mathbb{C}^d$. The discriminant of a number field is defined to be the discriminant of its ring of integers.*

It looks like this depends on the choice of unitary basis of $\mathcal{O}_K$ that you choose there, but it really doesn't. If you pick a different unitary basis, then you change the discriminant by multiplying the determinant of A by the determinant of the change of basis matrix between the two unitary bases. But that matrix is unitary *with integer entries*, and so its determinant is ±1. Specifically:

Theorem 5.3. *Let K be a number field, and let $\{x_1, \ldots, x_d\}$ and $\{y_1, \ldots, y_d\}$ be bases for the same lattice $\Lambda \subset V_K$ over $\mathbb{Z}$. Then*

$$\operatorname{disc}(x_1, \ldots, x_d) = \operatorname{disc}(y_1, \ldots, y_d)$$

Proof: The two discriminants differ by multiplication by the square of the determinant of the linear transformation T satisfying $T(x_i) = y_i$. Since the x_i are a $\mathbb{Z}$-basis for $\mathcal{O}_K$, each y_i is a $\mathbb{Z}$-linear combination of the x_i, so the linear transformation T has coefficients in $\mathbb{Z}$, and its determinant is also in $\mathbb{Z}$. Similarly, the inverse of T also has a determinant in $\mathbb{Z}$. Thus, the determinant of T must be a unit in $\mathbb{Z}$ – namely, ± 1 – so its square is 1, and the two discriminants are equal. ♣

Notice, by the way, that despite that squaring thing, the discriminant of a number field can still be negative! This is because complex numbers can get involved. Take $\mathbb{Q}(i)$, for example. Its discriminant is computed as follows, using the basis $\{1, i\}$ for $\mathbb{Z}[i]$ over $\mathbb{Z}$:

$$\operatorname{disc}(\mathbb{Q}(i)) = \left(\det \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}\right)^2 = -4$$

(The unitary basis we chose for $\mathbb{C}^2$ was the basis $\{(1,0),(0,1)\}$.)

Whenever you see a new definition in mathematics, the first question you should ask is “Why would you define that?” And because you are all responsible mathematicians, I will presume that you have just asked this question, and so I should answer it.

The discriminant is an isomorphism invariant of the number field. That is, if two number fields are isomorphic, then they must have the same discriminant, because they’ll have isomorphic rings of integers, which will have identical discriminants. (Any isomorphism of number fields must fix $\mathbb{Q}$ pointwise, and so will fix $\mathbb{Z}$. The isomorphism will therefore restrict to an isomorphism of the rings of integers, and thus will map a basis of one to a basis of the other. The discriminants will therefore be the same.)

In other words, the discriminant "discriminates" between number fields. (See? Those old-timers in the nineteenth century did a few things right, turns out.)

For example, how would you show that $\mathbb{Q}(\sqrt{3})$ is not isomorphic to $\mathbb{Q}(\sqrt{5})$? You can do this with elementary techniques, but it's kind of annoying. But the discriminant of $\mathbb{Q}(\sqrt{3})$ is 12, and the discriminant of $\mathbb{Q}(\sqrt{5})$ is 5, so they can't be isomorphic. Boom.

This brings up the question of how to compute the discriminant of a number field? I mean, that mysterious unitary basis thing sounds a little scary. Luckily, there's a shortcut.

Theorem 5.4. *Let K be a number field, and let $\{v_1, \ldots, v_n\}$ be a subset of K. Then the discriminant of $\{v_1, \ldots, v_n\}$ is given by the following determinant:*

$$\det \begin{pmatrix} Tr_{K/\mathbb{Q}}(v_1^2) & Tr_{K/\mathbb{Q}}(v_1 v_2) & \ldots & Tr_{K/\mathbb{Q}}(v_1 v_d) \\ \vdots & \vdots & & \vdots \\ Tr_{K/\mathbb{Q}}(v_d v_1) & Tr_{K/\mathbb{Q}}(v_d v_2) & \ldots & Tr_{K/\mathbb{Q}}(v_d^2) \end{pmatrix}$$

where the determinant is understood to be zero if the matrix is not square.

Proof: Once you realise that $\langle x, y\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$ is a nondegenerate symmetric bilinear pairing on M_K, this is just a standard fact from linear algebra. You can find the proof in the algebra section. ♣

There's a nice relationship between the discriminant of a lattice and the discriminant of a finite index sublattice.

Theorem 5.5. *Let K be a number field, and let Λ be a lattice in V_K. If $\Gamma \subset \Lambda$ is a sublattice of finite index n, then*

$$disc(\Gamma) = n^2 disc(\Lambda)$$

Proof: The proof is almost disappointingly easy. Let $T \colon V_K \to V_K$ be the linear transformation that takes a basis of Λ to a basis of Γ. Since the index of Γ in Λ is T, it immediately follows that

$$\det(\Gamma)^2 = \det(T)^2 \det(\Lambda)^2$$

where by det(lattice), I mean the determinant of some basis of that lattice. (The squares eliminate the indeterminacy of which basis you pick.)

But we know that $|\det(T)| = n$, so the desired result follows. (If you don't know this yet, check out the geometry section.) ♣

You may be wondering when you will see the explanation for that silly-looking $\sqrt{2}$ when we embed $\mathbb{Z}[i]$ in Minkowski space. Worry not – the answer is coming. Just, y'know, not yet.

Discriminants also let us define the norm of an ideal in $\mathcal{O}_K$.

Definition 5.6. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let $I = v_1\mathbb{Z} + \ldots + v_n\mathbb{Z}$ be a lattice in Minkowski space V_K. (A nonzero ideal of $\mathcal{O}_K$ is such a lattice.) We define*

$$\begin{aligned} N_{K/\mathbb{Q}}(I) &= \left(\frac{disc(v_1, \ldots, v_n)}{disc(K)}\right)^{1/2} \\ &= \left|\frac{\det(v_1|\ldots|v_n)}{\det(x_1|\ldots|x_n)}\right| \end{aligned}$$

where $\{x_1, \ldots, x_n\}$ is (the image in V_K of) a basis of $\mathcal{O}_K$ over $\mathbb{Z}$.

The notation suggests that there might be some more general norm, for a general extension L/K. There is. But I'm not going to tell you what it is right now. And in fact, I'm mostly going to write just $N(I)$, without the subscript. So there.

Theorem 5.7. *Let K be a number field, $\mathcal{O}_K$ its ring of integers. Let I be a lattice in V_K, and let $a \in K$ be nonzero. Then*

$$N(aI) = |N(a)|N(I)$$

Proof: Let $\{v_1, \ldots, v_n\}$ be a $\mathbb{Z}$-basis of I. Then $N(aI)$ is the absolute value of the determinant of the basis $\{av_1, \ldots, av_n\}$, which is the image of the basis $\{v_1, \ldots, v_n\}$ under the linear transformation $v \mapsto av$. The new basis therefore has determinant with absolute value $N(a)N(I)$. ♣

Corollary 5.8. *Let K be a number field, $\mathcal{O}_K$ its ring of integers. Let $a \in K$, $a \neq 0$, $I = a\mathcal{O}_K = ax_1\mathbb{Z} + \ldots + ax_n\mathbb{Z}$, where $\{x_1, \ldots, x_n\}$ is a basis of $\mathcal{O}_K$ over $\mathbb{Z}$. (This is called the fractional ideal of K generated by a.) Then*

$$|N(a)| = N(a\mathcal{O}_K)$$

Proof: Both $|N(a)|$ and $N(I)$ are the absolute value of the determinant of the linear transformation $T(v) = av$ from K to K as a $\mathbb{Q}$-vector space. ♣

Theorem 5.9. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let I be nonzero integral ideal of $\mathcal{O}_K$. Then $\mathcal{O}_K/I$ has $N(I)$ elements.*

Proof: We already know that $\mathcal{O}_K$ is isomorphic to $\mathbb{Z}^d$, and that I is a subgroup also isomorphic to $\mathbb{Z}^d$. The norm $N(I)$ is the absolute value of the determinant of the linear transformation mapping the lattice $\mathcal{O}_K$ to the lattice I. That means that the quotient $\mathcal{O}_K/I$ has $N(I)$ elements, as desired. (For a proof of that last step, see the geometry section.) ♣

But discriminants can do much more. For example, if you have a number field K, and you want to compute the ring of integers, how would you do it?

Well, quite often, you find an algebraic integer in K, adjoin it to $\mathbb{Z}$, and cross your fingers that you've found all of $\mathcal{O}_K$. Which, y'know, sometimes works. But not always.

But if you did make a guess that some ring A was the ring of integers of K, how would you check? Well, we know that

$$\text{disc}(A) = n^2\text{disc}(\mathcal{O}_K)$$

so if disc(A) is squarefree, then it must be equal to disc$(\mathcal{O}_K)$, and so $A = \mathcal{O}_K$. That's often not enough, so we will develop more tricks later.

There's a useful shortcut for computing the discriminant of the ring $\mathbb{Z}[\alpha]$, if α is an algebraic integer.

Theorem 5.10. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let $\alpha \in \mathcal{O}_K$. Let $m(x)$ be the monic minimal polynomial of α over $\mathbb{Q}$. Then*

$$disc(\mathbb{Z}[\alpha]) = disc(m(x))$$

At this point, it might be useful to know that the discriminant of a polynomial $m(x)$ is equal to

$$\text{disc}(m(x)) = \prod_{i<j}(r_i - r_j)^2$$

where $r_1, \ldots, r_n$ are the roots of $m(x)$, with multiplicity. So, in particular, the discriminant of a polynomial is zero if and only if it has repeated roots.

Proof: A nice basis for $\mathbb{Z}[\alpha]$ over $\mathbb{Z}$ is the set $\{1, \alpha, \ldots, \alpha^{d-1}\}$. Let's use this to compute the discriminant:

$$\operatorname{disc}(\mathbb{Z}[\alpha]) = \det \begin{pmatrix} 1 & \ldots & 1 \\ \sigma_1(\alpha) & \ldots & \sigma_n(\alpha) \\ \vdots & & \vdots \\ \sigma_1(\alpha)^{d-1} & \ldots & \sigma_n(\alpha)^{d-1} \end{pmatrix}^2$$

where $\sigma_1, \ldots, \sigma_n$ are the embeddings of K in $\mathbb{C}$. (This includes the real embeddings, by the way – a real embedding of K is still an embedding of K in $\mathbb{C}$. It's just not a complex embedding.)

This is a very famous determinant, named after the famous French person Alexandre-Théophile Vandermonde.

OK, fine. The French person is no longer famous. But his determinant is, and its square equals:

$$\operatorname{disc}(\mathbb{Z}[\alpha]) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

But this is exactly the discriminant of $m(x)$, because the $\sigma_i(\alpha)$ are exactly the roots of $m(x)$. ♣

Computing the discriminant of a polynomial looks yucky, because it looks like it involves computing the roots. But the discriminant is a symmetric function of the roots, so it's actually a function of the coefficients of the polynomial, which is much nicer.

Well. Somewhat nicer. The function of the coefficients is no picnic. There are some general formulas which enable one to compute the discriminant of a polynomial, but we'll stick to small degrees. Degree 0 and 1 polynomials have silly discriminants that you could calculate from scratch if you ever needed to. Here are some formulas in degrees 2 and 3:

$$\mathrm{disc}(x^2 + ax + b) = a^2 - 4b$$

$$\mathrm{disc}(x^3 + ax + b) = -4a^3 - 27b^2$$

You might be lamenting the absence of a quadratic term in that second formula there. Well, despair not: a simple change of variables converts any cubic into that form. Let $x = X - (a/3)$. Then:

$$\begin{aligned} x^3 + ax^2 + b + c &= (X - a/3)^3 + a(X - a/3)^2 + b(X - a/3) + c \\ &= X^3 + \left(b - \frac{a^2}{3}\right) X + \left(\frac{2a^3}{27} - \frac{ab}{3} + c\right) \end{aligned}$$

So if you have a cubic polynomial with a quadratic term in it, and you want to figure out its discriminant, make that substitution, compute the discriminant, and then undo the substitution.

Anyway. Let's do an example of computing the ring of integers. Let $K = \mathbb{Q}(\alpha)$, where α is a root of $x^3 + x + 1$.

We're going to guess that $\mathcal{O}_K = \mathbb{Z}[\alpha]$. The discriminant of $\mathbb{Z}[\alpha]$ is equal to the discriminant of x^3+x+1, which is $-4(1)^3 - 27(a)^2 = -31$. This is a squarefree integer, so our guess was right! We have $\mathcal{O}_K = \mathbb{Z}[\alpha]$.

But what happens if our guess is wrong? Or if it's right, but the discriminant isn't squarefree?

I'll tell you when you're older.

6 Ideals

Now we know what the ring of integers looks like as an additive group, and have a geometric picture of what that looks like. The next question is: what are the ideals of it like?

Let $A = \mathcal{O}_K$ be the ring of integers in a number field K, and let I be a nonzero ideal. (I think we all know what the zero ideal looks like.) We already know that A/I is a finite ring. So what are finite rings like?

Turns out there's a whole section devoted to that very question. Go check it out.

Now that you've read the finite rings section, you know that A/I is isomorphic to $A/P_1^{m_1} \times \ldots \times A/P_r^{m_r}$, where the P_i are the prime ideals of A that contain I.

This suggests that we should start by figuring out the prime ideals of A. The Chinese Remainder Theorem will then take us to the case of a general ideal.

So what are the prime ideals of $A = \mathcal{O}_K$? Let's pick one, call it P, and see what it looks like. It's easy to check that $P \cap \mathbb{Z}$ is a prime ideal of $\mathbb{Z}$. (In fact, $\mathbb{Z}/(P \cap \mathbb{Z})$ embeds naturally in the domain A/P.)

But we know what the prime ideals of $\mathbb{Z}$ are – they're the ideals generated by prime numbers! In particular, we see that our prime ideal P of A contains a prime number $p \in \mathbb{Z}$. In this case, we say that P *lies over* the ideal (p) of $\mathbb{Z}$.

We can also see that A/P is a module over $\mathbb{Z}/p\mathbb{Z}$. And it's a field, because P is a maximal ideal. So A/P is a finite field of characteristic p ... and we know what those fields look like! (If you don't, check out the section on finite fields.)

But which finite field is it? Well, it's hard to say, because it depends. We do know, at least, that A/P is a finite field of degree at most $[K : \mathbb{Q}]$ over $\mathbb{Z}/p\mathbb{Z}$, because generators for A as a $\mathbb{Z}$-module will still be generators for A/P as a $\mathbb{Z}/(P\cap\mathbb{Z})$-module. Let's do an example and see what it looks like.

We already know that $\mathbb{Z}[\sqrt{2}]$ is the ring of integers in the field $\mathbb{Q}(\sqrt{2})$. We know that every prime integer $p \in \mathbb{Z}$ is a non-unit in $\mathbb{Z}[\sqrt{2}]$, because $1/p$ is not an algebraic integer, no matter how much you extend the base field. Let's pick $p = 5$, because I like 5. What are the prime ideals of $\mathbb{Z}[\sqrt{2}]$ that contain 5? They correspond to the prime ideals of the quotient ring $\mathbb{Z}[\sqrt{2}]/(5)$, so let's compute with that:

$$\begin{aligned} \mathbb{Z}[\sqrt{2}]/(5) = &\cong \big(\mathbb{Z}[x]/(x^2-2)\big)/(5) \\ &\cong \mathbb{Z}[x]/(x^2-2, 5) \\ &\cong (\mathbb{Z}[x]/(5))/(x^2-2) \\ &\cong \mathbb{F}_5[x]/(x^2-2) \end{aligned}$$

[If the preceding set of deductions freaks you out, let me set your mind at ease. The first isomorphism is clear, I hope. Then next one is the Third Isomorphism Theorem for rings. So is the next one. And the last one is, again, clear.

I mean, really, this is all the Universal Property of Quotients at work. The isomorphisms above are all pretty easy to guess, and you just check that they work. On homework assignments, feel free to be as glib as I just was with deductions like these.]

The polynomial $x^2 - 2$ is irreducible modulo 5. (It has no roots, for example.) So $\mathbb{Z}[\sqrt{2}]/(5)$ is a domain! A field, in fact – it's $\mathbb{F}_{25}$! In particular, the ideal (5) is prime in $\mathbb{Z}[\sqrt{2}]$, and it is, naturally, the only (proper) ideal of $\mathbb{Z}[\sqrt{2}]$ that contains 5.

Let's do $p = 7$ next. We compute similarly:

$$\begin{aligned}\mathbb{Z}[\sqrt{2}]/(7) = \ &\cong \big(\mathbb{Z}[x]/(x^2-2)\big)/(7)\\ &\cong \mathbb{Z}[x]/(x_2-2,7)\\ &\cong (\mathbb{Z}[x]/(7))/(x^2-2)\\ &\cong \mathbb{F}_7[x]/(x^2-2)\\ &\cong (\mathbb{F}_7[x]/(x-3)) \times (\mathbb{F}_7[x]/(x+3))\\ &\cong \mathbb{F}_7 \times \mathbb{F}_7\end{aligned}$$

This calculation is exactly the same as the previous one, except with 7 instead of 5 ... until step 5, where there is more work to do, because $x^2 - 2$ is reducible modulo 7. This factorisation induces an isomorphism from the Chinese Remainder Theorem, which then simplifies as above.

In particular, there are two prime ideals of $\mathbb{Z}[\sqrt{7}]$ that contain the element 7. They are the ideals $(\sqrt{2}-3, 7)$ and $(\sqrt{2}+3, 7)$.

How did I figure out that those were the two ideals? Well, the prime ideals of $\mathbb{Z}[\sqrt{2}]$ containing 7 correspond to the prime ideals of the ring $\mathbb{F}_7 \times \mathbb{F}_7$, by the string of isomorphisms on the previous page. The ring $\mathbb{F}_7 \times \mathbb{F}_7$ has exactly two prime ideals: the one generated by $(1, 0)$, and the one generated by $(0, 1)$. Let's follow those ideals back through the isomorphisms.

We get

$$((1,0)) \mapsto (1 \pmod{x-3}, 0 \pmod{x+3})$$

On the left side, we have the ideal of $\mathbb{F}_7 \times \mathbb{F}_7$ generated by the ordered pair $(1,0)$. On the right, we have the ideal of $(\mathbb{F}_7[x]/(x-3)) \times (\mathbb{F}_7[x]/(x+3))$ generated by, again, $(1,0)$.

Next up:

$$\mapsto (x+3) \pmod{x^2-2}$$

This step is the trickiest. We need an ideal that is the unit ideal modulo $(x-3)$, but the zero ideal modulo $(x+3)$. The two ideals are coprime (otherwise the Chinese Remainder Theorem wouldn't apply!), so the ideal $(x+3)$ must do the trick.

Then our ideal turns into:

$$\mapsto ((x+3) \pmod{7}) \pmod{x^2-2}$$

which is the ideal of $\mathbb{Z}[x]$ generated by $(x+3)$, reduced mod (7) and then mod (x^2-2).

Another step back:

$$\mapsto (x+3) \pmod{x^2-2, 7}$$

Same ideal, except now we're taking the quotient by (7) and (x^2-2) at the same time.

Next:

$$\mapsto \big((x+3) \pmod{x^2-2}\big) \pmod{7}$$

Which is the same ideal again, except we take the quotient by (x^2-2) first, then the quotient by (7).

Finally:

$$\mapsto (\sqrt{2}+3) \pmod{7}$$

because the first isomorphism maps $\sqrt{2}$ to x.

So the ideal corresponding to $(1,0)$ is just the ideal $(\sqrt{2}+3,7)$, as advertised. There is a very similar calculation for the other ideal, which I will leave to you.

Notice that in this case, we have

$$(7) = (\sqrt{2}-3,7) \cap (\sqrt{2}+3,7) = (\sqrt{2}-3,7)(\sqrt{2}+3,7)$$

In other words, we have "factored" the ideal (7) into a product of prime ideals. This is what literary types call *foreshadowing.*

One last example. What about $p = 2$? Seems like that might be special and weird ... and it is. Let's do it.

$$\begin{aligned}\mathbb{Z}[\sqrt{2}]/(2) = \ &\cong \left(\mathbb{Z}[x]/(x^2-2)\right)/(2) \\ &\cong \mathbb{Z}[x]/(x_2-2,2) \\ &\cong \left(\mathbb{Z}[x]/(2)\right)/(x^2-2) \\ &\cong \mathbb{F}_2[x]/(x^2-2) \\ &\cong \mathbb{F}_2[x]/(x^2)\end{aligned}$$

Yup, special and weird. The polynomial x^2 is not irreducible modulo 2, but the Chinese Remainder Theorem – for all its cleverness – cannot help us with it, because its roots are rudely not distinct. Nevertheless, we are stuck with the task of determining the prime ideals of this ring, so we must work harder.

The ring $\mathbb{F}_2[x]/(x^2)$ has four elements, because it's a two-dimensional vector space over $\mathbb{F}_2$. These elements are represented by 0, 1, x, and $x+1$. Let P be a prime ideal of $\mathbb{F}_2[x]/(x^2)$. Then P certainly contains 0, and certainly does not contain 1.

P must contain something more than just 0, though, because $\mathbb{F}_2[x]/(x^2)$ is not a domain. (To see this, notice that $x \neq 0$, but $x^2 = 0$.) If P contains $x+1$, then P must also contain

$(x+1)^2 = x^2 + 2x + 1 = 1$, which is bad. So P must be the set $\{0, x\}$, better known as the ideal (x).

[In real life, when the numbers are larger than 2, you use the fact that prime ideals of $F[x]/(g(x))$ are exactly the ideals $(q(x))$, where $q(x)$ is an irreducible factor of $g(x)$ in $F[x]$. This theorem is proven in the algebra module.]

So what are the prime ideals of $\mathbb{Z}[\sqrt{2}]$ that contain 2? They correspond to the prime ideals of $\mathbb{F}_2[x]/(x^2)$, which is to say that there is only one ideal of $\mathbb{Z}[\sqrt{2}]$ containing 2, and it is the ideal $(\sqrt{2})$. In this case, we again have a factorisation $(2) = (\sqrt{2})^2$ of the ideal (2) into a product of prime ideals.

It's not too hard to parlay these techniques into a general theorem.

Theorem 6.1. *Let K be a number field, and let $\alpha \in \mathcal{O}_K$. Let $m(x)$ be the monic minimal polynomial of α over $\mathbb{Q}$, and let $p \in \mathbb{Z}$ be prime. Then the prime ideals of $\mathbb{Z}[\alpha]$ containing p are exactly the ideals $(q(\alpha), p)$, where $q(x)$ is an irreducible factor of $m(x)$ modulo p.*

Moreover, if $f(x) = q_1(x)^{a_1} \dots q_r(x)^{a_r}$ is a factorisation of $f(x)$ modulo p into irreducible factors, then there is a corresponding ideal factorisation $(p) = (q_1(\alpha), p)^{a_1} \dots (q_r(\alpha), p)^{a_r}$.

Proof: First, we compute:

$$\begin{aligned}
\mathbb{Z}[\alpha]/(p) = \; &\cong \left(\mathbb{Z}[x]/(m(x))\right)/(p) \\
&\cong \mathbb{Z}[x]/(m(x), p) \\
&\cong \left(\mathbb{Z}[x]/(p)\right)/(m(x)) \\
&\cong \mathbb{F}_p[x]/(m(x))
\end{aligned}$$

This makes it plain that the prime ideals of $\mathbb{Z}[\alpha]$ that contain p correspond exactly to the prime ideals of $\mathbb{F}_p[x]/(m(x))$, which are the ideals generated by the irreducible factors of $m(x)$ modulo p. Tracing back these ideals through the chain of isomorphisms gives the desired result.

The factorisation of ideals follows immediately:

$$(p) = (q_1(\alpha))^{a_1} \cap \ldots \cap (q_r(\alpha))^{a_r} = (q_1(\alpha))^{a_1} \ldots (q_r(\alpha))^{a_r}$$

because the ideals are pairwise coprime. ♣

But the next question is: what happens if the ring of integers is *not* of the form $\mathbb{Z}[\alpha]$? Stay tuned.

7 Factorisation of algebraic integers

Back in the good old days, when integers were *real* integers, you could take an integer and factor it into primes. Well. Unless it was zero. Can we still do that now, with our modern notion of algebraic integers?

No.

Before I explain why not, though, let's pause a moment to answer the question "Why would you even want to factor an integer into primes?" And please don't say "so I can eavesdrop on my roommate's cell phone conversations".

For a pure mathematician – a number theorist – factorisation allows the simplification of multiplicative problems. Want to work modulo n, but n is big? Just factor n into primes $n = p_1^{a_1} \ldots p_r^{a_r}$, and then the Chinese Remainder Theorem lets you calculate modulo each $p_i^{a_i}$ separately, which is much easier for a variety of reasons.

There are other benefits of the factorisation, but most of them – yes, even the eavesdropping thing which you should *never do* – boil down to being able to use the Chinese Remainder Theorem to reduce a calculation modulo n to a calculation modulo the power of a prime.

As you can see from the general Chinese Remainder Theorem in the algebra section, it's really a theorem about *ideals*, not numbers. But it really does depend on the ideals being coprime. So what we really want to do is to factor n into a product of prime ideals.

In $\mathbb{Z}$, a prime ideal is the same thing as an ideal generated by a prime number. This is not always the same in $\mathcal{O}_K$.

For example, consider the ideal $P = (2, \sqrt{10})$ of $\mathbb{Z}[\sqrt{10}]$. The quotient $\mathbb{Z}[\sqrt{10}]/P$ has two elements, which means it's isomorphic to the field $\mathbb{F}_2$, so P is a prime ideal. But it's not principal, because if it were, there would be some element $a + b\sqrt{10} \in \mathbb{Z}[\sqrt{10}]$ of norm ± 2. But $N(a + b\sqrt{10}) = a^2 - 10b^2$. Since ± 2 are not squares modulo 5, the equations $a^2 - 10b^2 = \pm 2$ have no solutions modulo 5, and therefore no solutions in integers.

But as we were saying, we don't really care if we can factor algebraic integers into a product of prime algebraic integers. We care if we can factor algebraic integers into a product of prime ideals. And that we can do.

Here's the general idea. Back in the good old days, if we wanted to factor an integer n, we'd find a prime factor p, compute n/p, and start over with n/p. Since n/p is simpler than n, this process eventually stops, and we're left with a prime factorisation of n.

So now, we'll start with an ideal I of $\mathcal{O}_K$. (Hey, if we're factoring algebraic integers into products of ideals, we can factor the ideals too.) We'll find a prime ideal P that's a factor of I (never mind what that means for now), then divide I by P (again, suspend your disbelief for the moment), and start over with IP^{-1}. Since IP^{-1} is simpler than I (patience!), this process eventually stops, and we're left with a prime factorisation of I.

There are lots of murky steps in that plan. Let's elucidate them, starting with the "divide by an ideal" thing. In order to divide ideals, we need to be a bit broad-minded about what the answer might have to be, in the same way that when we started dividing integers back in the day, we needed to be broad-minded about allowing fractions as answers.

Definition 7.1. *Let K be a number field, $\mathcal{O}_K$ its ring of integers. A fractional ideal of K is a nonzero, finitely generated $\mathcal{O}_K$-submodule of K.*

A fractional ideal is designed to be the analogue of rational numbers, except for ideals. The idea is that, someday, a fractional ideal will just be a quotient of nonzero ideals of $\mathcal{O}_K$. We'll get there soon.

The following definition is sometimes useful to avoid confusion.

Definition 7.2. *Let K be a number field with ring of integers $\mathcal{O}_K$. An integral ideal of $\mathcal{O}_K$ is a fractional ideal of $\mathcal{O}_K$ that is* *contained in $\mathcal{O}_K$. In other words, an integral ideal of $\mathcal{O}_K$ is just an ideal of $\mathcal{O}_K$, in the traditional sense.*

Some examples are in order first, though. For starters, let $\alpha \in K$ be any nonzero element. Then $\alpha\mathcal{O}_K$ is called the principal fractional ideal generated by α, and it's just the integer multiples of α. So, for example, the fractional ideal $(1/2)$ of $\mathbb{Z}$ is the set of integers and half-integers: $\{0, \pm(1/2), \pm1, \pm(3/2), \ldots\}$.

In general, a finitely generated $\mathcal{O}_K$-module is just a module of the form $a_1\mathcal{O}_K + \ldots + a_r\mathcal{O}_K$. (Note that there might be relations amongst the a_i!) A fractional ideal is just one of those, except that the a_i are all in K. (And at least one of them isn't zero.)

So, for example, any (nonzero) ideal of $\mathcal{O}_K$ is also a fractional ideal of $\mathcal{O}_K$, because $\mathcal{O}_K$ is noetherian, meaning that all its ideals are finitely generated.

But there are lots more fractional ideals than that. For example, if $K = \mathbb{Q}(\sqrt{10})$, then the set $I = (1/2)\mathcal{O}_K + (\sqrt{10}/4)\mathcal{O}_K$ is also a fractional ideal of $\mathcal{O}_K$. This is not, in any sense, a "two-dimensional module", because $1/2$ and $\sqrt{10}/4$ are "linearly dependent over $\mathcal{O}_K$": $(2\sqrt{10})(1/2) + (-4)\sqrt{10} = 0$. But it's also not a "one-dimensional module" (except it secretly sort of is), because there is no single element of I that generates the entire module as an $\mathcal{O}_K$-module. (This is because the fractional ideal $4I$ is just the ideal $(2, \sqrt{10})$ of $\mathcal{O}_K$, which we already showed was not principal. If I were principal – generated by a single element – then we could multiply its generator by 4 and get a generator for $(2, \sqrt{10})$.)

Ok. Now that we have defined the things that can be the outcome of division by ideals, let's define the division.

Definition 7.3. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let I and J be two fractional ideals of $\mathcal{O}_K$. We define the quotient of I by J to be the set*

$$(I : J) = \{a \in K \mid aJ \subset I\}$$

The idea here is to mimic division of plain old integers from kindergarten. What's (6) divided by (3)? It's all the numbers n with the property that $n(3) \subset (6)$. (Remember that $(n) \subset (m)$ if and only if $m \mid n$. Big ideals go with small generators: there are way more multiples of 2 than multiples of 68.) If you start with a multiple of 3 and multiply it by 2, you always get a multiple of 6. And if $n(3k)$ is always a multiple of 6, no matter what k is, then n must surely be a multiple of 2.

Or, to put it more succinctly: $(n : m) = (n/m)$.

In general, it's useful to note that if $\alpha \in K$ is any nonzero element, then $(\mathcal{O}_K : \alpha\mathcal{O}_K)$ is generated as an $\mathcal{O}_K$-module by $1/\alpha$. In other words, $(\mathcal{O}_K : \alpha\mathcal{O}_K) = (1/\alpha)\mathcal{O}_K$.

Theorem 7.4. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $\alpha \in K$ be any nonzero element. Then $(\mathcal{O}_K : \alpha\mathcal{O}_K) = (1/\alpha)\mathcal{O}_K$.*

Proof: Firstly, $((1/\alpha)\mathcal{O}_K)(\alpha\mathcal{O}_K) = \mathcal{O}_K$, so $(1/\alpha)\mathcal{O}_K \subset (\mathcal{O}_K : \alpha\mathcal{O}_K)$. And conversely, if $x \in (\mathcal{O}_K : \alpha\mathcal{O}_K)$, then in particular $x\alpha(1) \in \mathcal{O}_K$, and so $x \in (1/\alpha)\mathcal{O}_K$. ♣

It's also useful to note that fractional ideals have denominators, in the following sense.

Theorem 7.5. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let I be a fractional ideal of $\mathcal{O}_K$. Then there is some* *nonzero $\alpha \in \mathcal{O}_K$ such that $\alpha I \subset \mathcal{O}_K$ – in other words, αI is an integral ideal of $\mathcal{O}_K$. In other other words, $I = \frac{1}{\alpha}J$ for some integral ideal J of $\mathcal{O}_K$.*

Proof: Write $I = a_1\mathcal{O}_K + \ldots + a_n\mathcal{O}_K$ for $a_i \in K$. For each i, we can write $a_i = x_i/y_i$ for x_i and y_i in $\mathcal{O}_K$. But then if we define $y = y_1 \ldots y_n$, we see that $yI \subset \mathcal{O}_K$, because the product y clears all the denominators of the a_i. ♣

This means, by the way, that fractional ideals are all isomorphic to $\mathbb{Z}^n$ as additive groups, just like integral ideals. Nonzero integral ideals, I mean. Because the function $f(x) = ax$ is an isomorphism of $\mathbb{Z}$-modules (abelian groups!) from I to aI. If I is isomorphic to $\mathbb{Z}^d$ as an additive group, then so is aI. In particular, we have:

Theorem 7.6. *Let K be a number field with ring of integers $\mathcal{O}_K$. Every fractional ideal of $\mathcal{O}_K$ is a lattice in Minkowski space V_K.*

But there's a basic issue we haven't addressed yet: what if $(I : J)$ isn't a fractional ideal at all?

Never gonna happen.

Theorem 7.7. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let I and J be fractional ideals of $\mathcal{O}_K$. Then $(I : J)$ is a fractional ideal of $\mathcal{O}_K$.*

Proof: First, notice that if a and b are elements of $(I : J)$, then certainly $a \pm b$ are also elements of $(I : J)$, just from the definition. And if $r \in \mathcal{O}_K$ and $a \in (I : J)$, then $ra \in (I : J)$, because $rJ \subset J$. So $(I : J)$ is an $\mathcal{O}_K$-module.

All that's left to show is that $(I : J)$ is finitely generated. But Theorem 7.5 promises us a nonzero $a \in \mathcal{O}_K$ such that $aI \subset \mathcal{O}_K$, and a nonzero b such that $bJ \subset \mathcal{O}_K$. (This is good, because we know that integral ideals are finitely generated because $\mathcal{O}_K$ is noetherian.)

It's not hard to check that $(abI : abJ) = (I : J)$, and $(abI : abJ) \subset (\mathcal{O}_K : abJ)$ because $abI \subset \mathcal{O}_K$.

But now we can pick any nonzero $\alpha \in J$, so that $ab\alpha\mathcal{O}_K \subset abJ$, giving us $(I : J) = (abI : abJ) \subset (\mathcal{O}_K : abJ) \subset (\mathcal{O}_K : ab\alpha\mathcal{O}_K)$. That last fractional ideal is generated by $1/(ab\alpha)$ (by Theorem 7.4) – it's finitely generated! Since $\mathcal{O}_K$ is a noetherian ring, this means that the $\mathcal{O}_K$-submodule $(I : J)$ of $(\mathcal{O}_K : ab\alpha\mathcal{O}_K)$ is also finitely generated. So we're done. ♣

All looks good! But there is a snake in the garden.

Let I be the ideal $(2, 1+\sqrt{5})$ of $A = \mathbb{Z}[\sqrt{5}]$. Let's compute $(1 : I)$, where by "1" I mean the unit ideal.

The property $aI \subset A$ is the same as the property $a(2) \in A$ and $a(1+\sqrt{5}) \in A$. If we write $a = x + y\sqrt{5}$, this is the same as

$$\begin{aligned} x &= n/2 \\ y &= m/2 \\ x + 5y &\in \mathbb{Z} \\ x + y &\in \mathbb{Z} \end{aligned}$$

for regular old integers m and n in $\mathbb{Z}$. This, in turn, is the same as $m \equiv n \pmod 2$. So we get:

$$\begin{aligned} (1 : I) &= \left\{ \frac{n + m\sqrt{5}}{2} \mid n \equiv m \pmod 2 \right\} \\ &= \left\{ n\left(\frac{1+\sqrt{5}}{2}\right) + k\sqrt{5} \right\} \end{aligned}$$

where $k = (m-n)/2 \in \mathbb{Z}$. So, in summary

$$(1:I) = \left(\frac{1+\sqrt{5}}{2}\right)\mathbb{Z} + \sqrt{5}\mathbb{Z} = \left(\frac{1+\sqrt{5}}{2}\right)\mathcal{O}_K + \sqrt{5}\mathcal{O}_K$$

where this last equality is because $(A:I)$ is an $\mathcal{O}_K$-module, so it's closed under multiplication by $\mathcal{O}_K$.

So far, things seem all right. But wait:

$$\begin{aligned} I(1:I) &= \left(2\mathcal{O}_K + (1+\sqrt{5})\mathcal{O}_K\right)\left(\frac{1+\sqrt{5}}{2}\mathcal{O}_K + \sqrt{5}\mathcal{O}_K\right) \\ &= (1+\sqrt{5})\mathcal{O}_K + 2\sqrt{5}\mathcal{O}_K + (3+\sqrt{5})\mathcal{O}_K + (5+\sqrt{5})\mathcal{O}_K \\ &= I \end{aligned}$$

This last equality may not be obvious, but certainly each of the generators in the second-last line lie in I – which proves one inclusion – and each of 2 and $1+\sqrt{5}$ can be obtained by integer-linear combinations of $1+\sqrt{5}$ and $2\sqrt{5}$ and $3+\sqrt{5}$ – which proves the other inclusion.

So. I divided by I equals I. That's not the way division is supposed to work. Worse, it's a huge problem for our plan: if I divided by I isn't simpler than I, then our procedure to factor I might never end.

But the keen-eyed amongst you will have noticed that $\mathbb{Z}[\sqrt{5}]$ is not the ring of integers of $\mathbb{Q}(\sqrt{5})$! Which is, when it comes down to it, the whole problem.

Theorem 7.8. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then for every prime ideal P of $\mathcal{O}_K$, we have $P(\mathcal{O}_K : P) = \mathcal{O}_K$.*

Proof: First, notice that $P(\mathcal{O}_K : P)$ is a fractional ideal of $\mathcal{O}_K$

that is contained in $\mathcal{O}_K$. It also contains P, because $1 \in (\mathcal{O}_K : P)$. So it must either be P or $\mathcal{O}_K$.

If $P(O_K : P) = \mathcal{O}_K$, then we're done. So let's assume that $P(\mathcal{O}_K : P) = P$. Then we have $P(\mathcal{O}_K : P)(\mathcal{O}_K : P) = P(\mathcal{O}_K : P) = P \subset (\mathcal{O}_K : P)$. In particular, $(\mathcal{O}_K : P)$ is closed under multiplication! Since it's also closed under addition and subtraction, and contains 0 and 1, it's a ring! Weird!!

[WARNING: In real life, $(\mathcal{O}_K : P)$ is never actually a ring, because in real life, our assumption $P(\mathcal{O}_K : P) = P$ never actually happens. We are all Alice in Wonderland right now, and strange and marvelous things are happening.]

So $R = (\mathcal{O}_K : P)$ is a ring. And R contains $\mathcal{O}_K$, because P is an ideal. And R is a finitely generated $\mathcal{O}_K$-module, because it's a fractional ideal of $\mathcal{O}_K$. So R is integral over $\mathcal{O}_K$.

But $\mathcal{O}_K$ is integrally closed! Which means that $R = (\mathcal{O}_K : P) = \mathcal{O}_K$. Which is a problem, because:

Lemma 7.9. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let A be a subring of $\mathcal{O}_K$ with fraction field K, and let I be a nonzero ideal of A. Then $(A : I) \neq A$.*

Proof: Let P be a maximal ideal of A containing I. Then $(A : P) \subset (A : I)$, so if we prove the lemma for P, it will immediately follow for I. In other words, we can safely assume that $I = P$ is prime.

Choose any nonzero $x \in P$. Since A is a finitely generated $\mathbb{Z}$-module (it's a $\mathbb{Z}$-submodule of the finitely generated $\mathcal{O}_K$), it's a noetherian ring. (Every ideal of A is a finitely generated $\mathbb{Z}$-module, so *a fortiori* it's a finitely generated A-module.) So by the last theorem in the algebra section, we know that the principal ideal (x) contains a finite product of prime ideals of A. Let's choose the finite product with the fewest prime ideals in it, and write $P_1 \dots P_n \subset (x) \subset P$.

Now, P is a prime ideal, so if a product of ideals is a subset of P, one of the factors must also be a subset of P. (If none of them were contained in P, then we could pick from each P_i an element not in P ... but their product would be in P.) So let's say $P_1 \subset P$. But P_1 is a maximal ideal (the quotient A/P is a finite domain!), so we have $P = P_1$.

Let $J = P_2 \dots P_n$. (If $n = 1$ then $I = A$.) By the minimality of n, we know that $J \not\subset (x)$, so we can choose some $y \in J - (x)$. Then we have $yP \subset (x)$, but $y \notin (x)$, so we deduce that $(y/x)P \subset A$ but $y/x \notin A$. In other words, $y/x \in (A : P) - A$, as advertised. ♣

This is a big old contradiction, so our original assumption that $P(\mathcal{O}_K : P) = P$ must be wrong. That only leaves $P(\mathcal{O}_K : P) = \mathcal{O}_K$ as a possibility. And we're done. ♣

Theorem 7.8 motivates the following definition.

Definition 7.10. *Let A be a domain, I a fractional ideal of A. Then I is said to be invertible if there is a fractional ideal J of A with $IJ = A$. The ideal J is said to be the inverse of I, and is written I^{-1}.*

(Note that the ideal J, if it exists, is unique: if $IJ = IJ' = A$, then $J = JA = JIJ' = AJ' = J'$.)

So Theorem 7.8 can be rephrased as "prime ideals of $\mathcal{O}_K$ are invertible." In fact, all nonzero ideals of $\mathcal{O}_K$ are invertible, because they're all products of prime ideals. But we haven't proven that yet.

In any case, we're now ready to execute our plan.

Theorem 7.11. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then every nonzero ideal of $\mathcal{O}_K$ is the product of finitely many prime ideals. Moreover, this factorisation is unique up to reordering the factors.*

Proof: Let I be an ideal of the ring of integers $\mathcal{O}_K$ of a number field K. We want to write $I = P_1 \dots P_r$ for prime ideals $P_1, \dots, P_r$. (Those prime ideals might not all be different – we're modern, broad-minded people here.)

First off, I is contained in some nonzero prime ideal P. Consider the fractional ideal IP^{-1}. Since $\mathcal{O}_K \subset P^{-1} = (\mathcal{O}_K : P)$, we have $I \subset IP^{-1}$, and since $I \subset P$, we have $IP^{-1} \subset PP^{-1} = \mathcal{O}_K$. So IP^{-1} is an integral ideal of $\mathcal{O}_K$, and not just a fractional one.

If $IP^{-1} = \mathcal{O}_K$, then we're done: $I = P$! Otherwise, we can restart this whole process with $I_1 = IP^{-1}$, and end up with the integral ideal $I_2 = IP_1^{-1}P_2^{-1}$. And so on, and so on ... $I_{k+1} = I_k P_{k+1}^{-1} = IP_1^{-1} \dots P_{k+1}^{-1}$ for each k.

If at any point we have $I_k = \mathcal{O}_K$, then we're done, and $I = P_1 \dots P_k$. If we don't ...

... well, if we don't, then consider the ideal $J = \bigcup_{k=1}^{\infty} I_k$. The set J is an ideal, because for any a and b in J, there are I_k and I_ℓ such that $a \in I_k$ and $b \in I_\ell$. Picking the bigger of k and ℓ (and calling it k), this means that a and b are both in I_k. So their sum and difference are also in I_k, and therefore in J. Similarly, if $r \in \mathcal{O}_K$, then $ra \in J$. So J is an ideal of $\mathcal{O}_K$.

But $\mathcal{O}_K$ is noetherian, so J is finitely generated, by $a_1, \ldots, a_n$. For each a_i, there is some I_{k_i} that contains it. If m is the biggest of all the k_i, then all the a_i are contained in I_m. But then J is contained in I_m, so since $I_m \subset J$, we get $J = I_m$, and so, for example, $I_{m+1} = I_m$.

Think about what that means, though. We have $I_m = I_{m+1} = I_m P_{m+1}$, which contradicts Nakayama's Lemma. (See the algebra section for a proof of that.) So the sequence of I_k *does* eventually stop, and so $I = P_1 \ldots P_n$ is a product of prime ideals, as desired.

The uniqueness is easy: if $P_1 \ldots P_n = Q_1 \ldots Q_m$, then $P_1 \ldots P_n \subset Q_m$, and so since Q_m is prime, we get $P_i \subset Q_m$ for some i. This means $P_i = Q_m$, so we can divide both sides by Q_m (multiply both sides by Q_m^{-1}) to get a simpler equation. Keep going until you pair up all the P_i and Q_j. (There can't be any left over at the end because you'd have a nonempty product of prime ideals equal to the whole ring, which is manifestly impossible.) ♣

Incidentally, this means that every nonzero ideal of $\mathcal{O}_K$ is invertible, because a product of invertible ideals is invertible. Which is nice.

We saw a bunch of examples of this factorisation thing in the previous section, on ideals. Remember the cheesy "foreshadowing", in which we factored (7) into a product of prime ideals? This section is what that was foreshadowing!

This is what literary types call *careful plotting.*

8 Local rings: The ideal norm is multiplicative

Yes, Virginia, it's true that $N(IJ) = N(I)N(J)$. But it's surprisingly difficult and interesting to prove it, so we're devoting a whole section to it.

Let's write $I = P_1^{a_1} \dots P_r^{a_r}$ and $J = Q_1^{b_1} \dots Q_s^{a_s}$ as products of prime ideals. If none of the P_i and Q_j are the same, then the ideals are coprime, and the Chinese Remainder Theorem rides to our rescue:

$$N(IJ) = \#(\mathcal{O}_K/IJ) = \#(\mathcal{O}_K/I) \cdot \#(\mathcal{O}_K/J) = N(I)N(J)$$

Sadly, this falls down a bit if I and J are not coprime. But the Chinese Remainder Theorem can still help. Let's rewrite $I = P_1^{a_1} \dots P_n^{a_n}$, and $J = P_1^{b_1} \dots P_n^{b_n}$, where we allow the a_i and b_i to be zero if some P_i doesn't happen to turn up in the prime factorisation of one of I or J. Then we have:

$$\begin{aligned} N(I) &= \#(\mathcal{O}_K/I) = \#(\mathcal{O}_K/P_1^{a_1}) \dots \#(\mathcal{O}_K/P_n^{a_n}) \\ N(J) &= \#(\mathcal{O}_K/J) = \#(\mathcal{O}_K/P_1^{b_1}) \dots \#(\mathcal{O}_K/P_n^{b_n}) \\ N(IJ) &= \#(\mathcal{O}_K/IJ) = \#(\mathcal{O}_K/P_1^{a_1+b_1}) \dots \#(\mathcal{O}_K/P_n^{a_n+b_n}) \end{aligned}$$

So all we need to do is show that for any nonzero prime ideal P, we have

$$\#(\mathcal{O}_K/P^{a+b}) = \#(\mathcal{O}_K/P^a) \cdot \#(\mathcal{O}_K/P^b)$$

If $P = (\pi)$ were a principal ideal, we'd have a path to victory. Namely, we'd be able to define $f \colon \mathcal{O}_K/P^n \to \mathcal{O}_K/P^{n+1}$ by $f(x) = \pi x$. (This isn't a ring homomorphism – just a homomorphism of additive groups.) It's injective, and its image is P/P^{n+1}, so we can count the elements of $\mathcal{O}_K/P^{n+1}$ using $\mathcal{O}_K/P \cong (\mathcal{O}_K/P^{n+1})/(P/P^{n+1})$, so that $N(P) = N(P^{n+1})/N(P^n)$. A simple induction, and we're home and dry!

But sadly, as we have seen, P need not be principal. So instead, we're going to embed $\mathcal{O}_K$ into a bigger ring in which P generates a principal ideal. Then the idea outlined in the previous paragraph will be a winner.

At this point, you should go read the section on local rings. Unless, of course, you already know all about local rings, in which case you should just forge ahead. If it turns out that you didn't know everything you thought about local rings, well, the local rings section will still be there for you.

So the good news is, it will turn out that the localisation $(\mathcal{O}_K)_P$ of $\mathcal{O}_K$ at the prime ideal P is always a DVR. And we can make our earlier optimistic idea into a reality, using the localisations.

Theorem 8.1. *Let P be an invertible prime ideal of a domain A. Then the local ring A_P is a DVR.*

Proof: The local rings section takes care of one part of the definition of a DVR: A_P is noetherian! And localisation takes care of the "local ring" part. All that's left is to show that the maximal ideal P_P of A_P is principal.

Well, we know that P is an invertible ideal of A, so we have $P^{-1}P = A$. That means that there are elements $a_1, \ldots, a_n \in P$ and $b_1, \ldots, b_n \in P^{-1} = (A : P)$ satisfying $a_1b_1 + \ldots + a_nb_n = 1$.

Each term $a_ib_i \in A$ by definition of $(A : P)$. If all those terms a_ib_i were elements of P, then we'd have $1 \in P$, which we don't.

So at least one of them, say a_1b_1, must be an element of $A - P$.

This means, however, that a_1b_1 is a unit in A_P! It will turn out that this means that P_P is generated by a_1.

To see this, let $x \in P_P$ be any element. Then $x = a_1b_1y$ for some $y \in P_P$, because a_1b_1 is a unit of A_P.

But $b_1 \in (A : P)$, and $y = u/v$ for some $u \in P$, so $b_1y = (b_1u)/v \in A_P$, because $b_1u \in A$. This means that $x = a_1(b_1y) \in a_1A_P$, so $P_P = a_1A_P$! ♣

Great! So if we pass to the localisation, our ideal P becomes principal. Next, we need to make sure that the quotients work out the same.

Theorem 8.2. *Let A be a domain, and let P be a nonzero prime ideal of A. Then for any positive integer $n \in \mathbb{Z}$, we have*

$$A/P^n \cong A_P/P_P^n$$

Proof: If you want to show that two things are isomorphic, write down an isomorphism.

Define $f\colon A/P^n \to A_P/P_P^n$ by $f(x + P^n) = x + P_P^n$. It's really easy to check that this is a well defined homomorphism. Ideally, we would write down an inverse homomorphism and gallop home, but unfortunately that turns out to be a bit of a pain in the neck. So we'll show that f is one-to-one and onto.

("Ideally". Sorry.)

To show that f is injective, assume that $f(x+P^n) = 0+P_P^{n+1}$. Then we would have $x \in P_P^n$, so $x = a/b$, where $b \notin P$ but $a \in P^n$. Then $bx \in P^n$ but $b \notin P$. Thus, b and P^n are coprime, so there exist α and β in A, and $y \in P^n$, such that

$$\alpha b + \beta y = 1$$

Notice that $\alpha \notin P$ because $y \in P^n \subset P$ and $1 \notin P$.

We can then compute:

$$\begin{aligned} x &= \frac{\alpha a}{\alpha b} \\ x(1 - \beta y) &= \alpha a \\ x &= \alpha a + \beta x y \end{aligned}$$

which is in P^n since $a \in P^n$ and $y \in P^n$. Thus, if $f(x) = 0$, then $x = 0$, so f is injective.

Now to show that f is surjective. Let $a/b \in A_P$, where $a, b \in A$ but $b \notin P$. We want to find some $x \in A$ such that $x + P_P^n = a/b + P_P^n$. In other words, we want to find $x \in A$ such that $x - a/b \in P_P^n$, or equivalently, $bx - a \in P^n$.

We know that the ideals (b) and P^n are coprime, so there are α and β in A, and $y \in P^n$, such that $\alpha b + \beta y = 1$.

Let $x = \alpha a$. Then

$$\begin{aligned} bx - a &= b\alpha a - a \\ &= (1 - \beta y)a - a \\ &= -ay\beta \end{aligned}$$

which is an element of P^n because $y \in P^n$. So f is surjective, and we're done. ♣

Finally, we need to show that the quotients work out *correctly*, and not just the same.

Theorem 8.3. *Let D be a DVR with maximal ideal P, and assume that D/P is finite. Then $\#(D/P^n) = (\#(D/P))^n$.*

Proof: We will show this by induction. The $n = 1$ case is, um. Straightforward.

So assume that $\#(D/P^n) = (\#(D/P))^n$. To win the day, it's enough to show that $\#(D/P^{n+1}) = \#(D/P^n) \cdot \#(D/P)$.

Let $q\colon D/P^{n+1} \to D/P^n$ be the reduction modulo P^n. Its kernel is P^n/P^{n+1}, and it's onto. If we can show that P^n/P^{n+1} has the same number of elements as D/P, then we'll be done!

Now, P^n/P^{n+1} is a (D/P)-module.

No, really! It's clearly an abelian group, and the (D/P) action is the easiest thing possible: $(a + P)(x + P^{n+1}) = ax + P^{n+1}$, which is well defined because $x \in P^n$.

But P is a maximal ideal, and so D/P is a field, making P^n/P^{n+1} into a vector space. If we can show that its dimension is 1, then it will have the same number of elements as D/P, and we'll be done.

I claim that π^n is a basis for P^n/P^{n+1} over D/P.

It's clearly linearly independent, because it's nonzero and there's only one of it. And if $x + P^{n+1} \in P^n/P^{n+1}$, then $x = a\pi^n + P^{n+1}$ for some $a \in D$, so x is in the (D/P)-span of π^n. Woo! ♣

Theorem 8.4. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then for any two nonzero ideals I and J of $\mathcal{O}_K$, we have $N(IJ) = N(I)N(J)$.*

Proof Write $I = P_1^{a_1} \dots P_n^{a_n}$ and $J = P_1^{b_1} \dots P_n^{b_n}$ for non-negative integers $a_1, \dots, a_n, b_1, \dots, b_n$. Then

$$IJ = P_1^{a_1+b_1} \dots P_n^{a_n+b_n}$$

and so

$$\begin{aligned} N(IJ) &= N(P_1^{a_1+b_1}) \dots N(P_n^{a_n+b_n}) \\ &= N(P_1)^{a_1+b_1} \dots N(P_n)^{a_n+b_n} \\ &= N(P_1^{a_1}) \dots N(P_n^{a_n}) N(P_1^{b_1}) \dots N(P_n^{b_n}) \\ &= N(I)N(J) \end{aligned}$$

by a combination of the Chinese Remainder Theorem and the magic of DVRs. ♣

Do you remember, back in the day, when we factored the ideal (p) in the ring $\mathbb{Z}[\alpha]$? Well, we can do that in $\mathcal{O}_K$ now, because of unique factorisation of ideals. And the multiplicativity of the norm of ideals lets us notice something else.

Definition 8.5. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $p \in \mathbb{Z}$ be prime. Then we can factor*

$$(p) = P_1^{e_1} \dots P_r^{e_r}$$

as a product of prime ideals. The number $e(P_i) = e_i$ is called the ramification index of P_i over p, and the number $f(P_i) = f_i = \log_p(N(P_i))$ is called the residue field degree (because it is the degree of the field extension $(\mathcal{O}_K/P_i)/(\mathbb{Z}/p)$).

The prime p is said to be ramified in K if $e_i \geq 2$ for some i. It is said to be unramified otherwise.

Notice that if $d = [K : \mathbb{Q}]$ is the degree of the number field K, then by taking the norm of both sides of the previous equation, we get

$$e_1 f_1 + \dots e_r f_r = d$$

because the norm is multiplicative, and $N(p) = p^d$. That's kind of cool.

Also, do you remember when you asked what you would do if you were trying to guess the ring of integers of a number field, and you guessed wrong? Remember I told you that I'd tell you when you were older?

Well, you're older now, and I think you're old enough to know the truth.

The local rings are the key. It turns out that just having DVRs for local rings is enough to make your guess the ring of integers. Now, that's a lot of checking – infinitely many primes at which to localise! – but you can narrow that down fast by proving that you just need to check the primes whose squares divide the discriminant of your guess.

Let's do this in detail now.

Theorem 8.6. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let A be a subring of $\mathcal{O}_K$ of finite index. Then $A = \mathcal{O}_K$ if and only if for every nonzero prime ideal P of A, the ring A_P is a DVR.*

Proof: One direction we've already done: if $A = \mathcal{O}_K$,then its localisations are all DVRs.

Thus, let's assume that A_P is a DVR for all nonzero prime ideals P of A, and let P be any nonzero prime ideal of A. Let $I = P\mathcal{O}_K$ be the ideal of $\mathcal{O}_K$ generated by P.

Unless I is the unit ideal of $\mathcal{O}_K$, I is contained in some nonzero prime ideal Q of $\mathcal{O}_K$. The ideal $Q \cap A$ is a prime ideal of A containing P ... but P is maximal, so $P = Q$, giving $A_P \subset (\mathcal{O}_K)_Q$. (This is straightforward to check.) We will prove first that $A_P = (\mathcal{O}_K)_Q$, by showing that there are no rings strictly between A_P and K.

Let $x \in K$ be any element. We're going to show that if $x \notin A_P$, then $A_P[x] = K$.

Since A has fraction field K, there is some element α of A such that $\alpha x \in A \subset A_P$. If π is a uniformizer for A_P, we can write $\alpha = u\pi^r$ for some unit $u \in A_P^*$ of A_P and some non-negative integer r.

Thus, we may write $x = \frac{b}{\pi^t}$ for some unit $b \in A_P^*$. In particular, every element of K may be written as $u\pi^n$ for some unit u of A_P and some integer n. The integer n is negative if and only if $x \notin A_P$.

If $x \notin A_P$, then consider the ring $A_P[x]$. It contains $x = u\pi^n$ for some negative integer n. It also contains $u^{-1}\pi^{1-n}$, because it's in A_P: $1 - n \geq 0$ and u is a unit in A_P. Therefore, $A_P[x]$ contains π^{-1}.

But then $A_P[x]$ must also contain $u(\pi^{-1})^n$ for all units u of A_P and all positive integers n. This means it contains all of K.

Great! So now, since $(\mathcal{O}_K)_Q$ is a ring that contains A_P and is contained in K, it must either equal A_P or equal K. Except it doesn't equal K. So $A_P = (\mathcal{O}_K)_Q$, as desired.

There is an unsettling possibility remaining, though. What if I generates the unit ideal of $\mathcal{O}_K$?

Well, in that case, there's some element of P whose inverse x (in K) is contained in $\mathcal{O}_K$ but not in A_P. This means that $A_P[x] = K$. But x is integral over $\mathbb{Z}$ (this is the definition of $\mathcal{O}_K$, after all), so *a fortiori* it's also integral over A_P. (Since $\mathbb{Z} \subset A_P$, the monic minimal polynomial for x over $\mathbb{Z}$ that has coefficients in $\mathbb{Z}$, also has coefficients in A_P.)

But if x is integral over A_P, then $K = A_P[x]$ is also integral over A_P! Which means that π^{-1} is integral over A_P. Which is blatantly isn't: any polynomial in $A_P[x]$ with π^{-1} as a root must have a factor of $\pi x - 1$, which since A_P is a PID means that it's not monic.

What a relief! We can dispense with that unsettling case, and rest easy that $A_P = (\mathcal{O}_K)_Q$ for all P and Q with $P \subset Q$.

This, sadly, is not the triumphant finish. We want to show that $A = \mathcal{O}_K$.

Well, not proving it isn't going to get this theorem proven. Let $x \in \mathcal{O}_K$ be any element. We want to show that $x \in A$. Well, write $x = a/b$ for $a, b \in A$. It would be cool if we could show that there's some way of writing x so that the denominator b was a unit of A, because then x would obviously be in A.

The set of possible denominators for x is obviously

$$D = \{b \in A \mid bx \in A\}$$

It's not hard to see that D is the intersection of the two fractional ideals $(A : xA)$ and A of A, so D is itself a fractional ideal of A. And since $D \subset A$, D is an *integral* ideal of A too.

If $D = A$, then we're done, because then 1 is a possible denominator for x.

If $D \neq A$, then there is some nonzero prime ideal P containing D. In particular, every way of writing x as a fraction of elements of A involves a denominator lying in P. This is *exactly* what it means to be *not an element of A_P*.

So $x \notin A_P$, and so $x \notin (\mathcal{O}_K)_Q$ for some prime ideal Q of $\mathcal{O}_K$.

But $x \in \mathcal{O}_K$, so this is impossible, and the happy case $D = A$ is the only one.

Which means we're done. ♣

And then the next step.

Theorem 8.7. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let A be a subring of $\mathcal{O}_K$ of finite index. Let $p \in \mathbb{Z}$ be a prime number such that p^2 does not divide the discriminant of A. Then for any prime ideal P of A containing p, the localisation A_P is a DVR.*

Proof: Let $n = [\mathcal{O}_K : A]$ be the index of A in $\mathcal{O}_K$. We know that p does not divide n, because otherwise p^2 would divide the discriminant of A.

Let P be any prime ideal of A containing p, and let Q be a prime ideal of $\mathcal{O}_K$ containing P.

We will show that $(\mathcal{O}_K)_Q = A_P$, and so of course A_P will be a DVR. Let $x \in (\mathcal{O}_K)_Q$. Then $x = a/b$ for $a, b \in \mathcal{O}_K$, $b \notin Q$. Since n is coprime to p, it is also coprime to Q, and so $nb \notin P \subset Q$. But $na, nb \in A$, so we have $x = na/nb \in A_P$. So $(\mathcal{O}_K)_Q = A_P$, as desired. ♣

So how does all this help us figure out whether a ring A is the ring of integers of K or not?

Watch and learn, baby.

Let $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial x^3+3x+3. We're going to guess that $\mathbb{Z}[\alpha]$ is the ring of integers of K.

First, the discriminant of $x^3 + 3x + 3$ is $-351 = -3^3 \cdot 13$. Which isn't squarefree, so we don't know if our guess is right or not yet. Darn.

However, the only prime whose square divides the discriminant of $\mathbb{Z}[\alpha]$ is 3, so the localisation of $\mathbb{Z}[\alpha]$ at any prime that doesn't contain 3 must be a DVR. The only thing left is to check 3.

The prime ideals of $\mathbb{Z}[\alpha]$ that contain 3 correspond to the irreducible factors of $x^3 + 3x + 3$ modulo 3. Those irreducible factors are all x, so the only prime ideal of $\mathbb{Z}[\alpha]$ that contains 3 is the ideal $P_3 = (3, \alpha)$.

But $3 = \alpha(-\alpha^2 - 3)$, because of the minimal polynomial for α! (Always remember: for most algebraic numbers, the minimal polynomial is the only useful thing you know about it!) In particular, $P_3 = (\alpha)$ is a principal ideal! So when you localise at P_3, you get a principal maximal ideal, and the resulting local ring is a DVR.

In short, our guess was correct, and the ring of integers of $\mathbb{Q}(\alpha)$ is $\mathbb{Z}[\alpha]$.

You may also remember that I would tell you how to deal with stuff if the ring of integers was not of the form $\mathbb{Z}[\alpha]$ for some element α. Well, it's time we had that rite of passage too.

The idea is that when you want to calculate in $\mathcal{O}_K$, there's actually probably only a finite set of prime ideals you care about.

For any nonzero $\alpha \in \mathcal{O}_K$, the subring $A = \mathbb{Z}[\alpha]$ has finite index. So there are only finitely many primes that divide that index. For any prime ideal Q of $\mathcal{O}_K$ that doesn't contain any of those finitely many primes, we can let $P = Q \cap \mathbb{Z}[\alpha] = Q \cap A$, and then the local rings $(\mathcal{O}_K)_Q$ and A_P will be the same, and a lot of calculations involving Q will come out the same as if we just used $\mathbb{Z}[\alpha]$ and P instead.

For instance. Let's say we want to know which prime ideals of $\mathcal{O}_K$ contain a certain prime number $p \in \mathbb{Z}$. And let's say we can find an $\alpha \in \mathcal{O}_K$ whose minimal polynomial $m(x)$ has discriminant not divisible by p^2. So $[\mathcal{O}_K : \mathbb{Z}[\alpha]] = n$, which is not divisible by p. (In fact, all you need is for the index to be prime to p, which amounts to having the discriminant of $m(x)$ not being divisible by two more factors of p than $\mathrm{disc}(\mathcal{O}_K)$.)

We know how to factor the ideal (p) in $\mathbb{Z}[\alpha]$: the prime ideal factors correspond precisely to the irreducible factors of $m(x)$ modulo p:

$$(p) = P_1^{a_1} \dots P_n^{a_n}$$

Since p does not divide the index n of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$, we know that for each P_i, there is a prime ideal Q_i of $\mathcal{O}_K$ such that $P_i \subset Q_i$, and $(\mathcal{O}_K)_{Q_i} = A_{P_i}$. Moreover, the Q_i are exactly the prime ideals of $\mathcal{O}_K$ that contain p.

Therefore, we can factor $(p) = Q_1^{b_1} \dots Q_n^{b_n}$ for some positive integers b_i. If we can show that $a_i = b_i$ for all i, then we'll know that we can factor (p) in $A = \mathbb{Z}[\alpha]$ instead of in $\mathcal{O}_K$.

For each i, we know that A_{P_i} is a DVR. The element p lies in $P_i^{a_i}$, but not in $P_i^{a_i+1}$ (in A_{P_i}). But $A_{P_i} = (\mathcal{O}_K)_{Q_i}$, and so $P_i^r = Q_i^r$ for all r. Therefore, as an element of $(\mathcal{O}_K)_{Q_i}$, p lies in $Q_i^{a_i}$ but not in $Q_i^{a_i+1}$.

But by the magic of localisation, since p is an element of $\mathcal{O}_K$, this means that p lies in $Q_i^{a_i}$ but not in $Q_i^{a_i+1}$. The factorisation of (p) in $\mathcal{O}_K$ tells us that p lies in $Q_i^{b_i}$ but not in $Q_i^{b_i+1}$. So we must have $a_i = b_i$.

Let's do a concrete example. Let $K = \mathbb{Q}(\gamma)$, where γ is a root of $x^3 - x^2 - 2x - 8$. It's known – although not trivial to prove – that the ring of integers $\mathcal{O}_K$ is not of the form $\mathbb{Z}[\alpha]$ for any α. We don't need to take this for granted, because it's enough to know that we're not clever enough to find an α for which $\mathcal{O}_K = \mathbb{Z}[\alpha]$. The fact that *no one* is clever enough to find such an α is merely a salve to our egos.

We'll factor the ideal (5) in $\mathcal{O}_K$. First, we need to find an $\alpha \in \mathcal{O}_K$ such that 5 does not divide the discriminant of $\mathbb{Z}[\alpha]$. Let's try $\alpha = \gamma$.

The monic minimal polynomial for α over $\mathbb{Q}$ is x^3-x^2-2x-8. The discriminant of this polynomial is

$$2012 = 2^2 \cdot 503$$

Notice the lack of 5 as a prime factor. So we've found our α.

How does 5 factor in $\mathbb{Z}[\alpha]$? We use our handy theorem, which says that the factorisation corresponds to the factorisation of $x^3 - x^2 - 2x - 8$ modulo 5. Which is:

$$x^3 - x^2 - 2x - 8 = (x^2 + 3)(x - 1)$$

This means that (5) factors in $\mathbb{Z}[\alpha]$ as

$$(5) = (5, \alpha - 1), (5, \alpha^2 + 3)$$

And thanks to our argument above, since 5 does not divide the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$, we know that this factorisation works in $\mathcal{O}_K$ as well.

But can I always find such a useful $\alpha \in \mathcal{O}_K$? Sadly, no. But then, I'm pretty lazy – could a more energetic person find one? Sadly, still no. Examples of this are a bit abstruse, so I won't describe one here. But still, useful α are plentiful for many applications.

Anyway, we can now prove a cool fact about discriminants. First, a definition.

Definition 8.8. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let p be a prime number. We say that p is unramified in K if and only if the factorisation $(p) = P_1^{a_1} \dots P_n^{a_n}$ has distinct prime ideal factors – that is, $a_i = 1$ for all i. We say that p is ramified in K if it is not unramified.*

Theorem 8.9. *Let K be a number field with ring of integers $\mathcal{O}_K$. Let $p \in \mathbb{Z}$ be a prime number. Then p is ramified in K if and only if p divides the discriminant of K.*

Proof: This is a biconditional statement, so it's two theorems for the price of one. We start with forwards.

Assume that p is ramified in K. Then the prime factorization of the ideal (p) in $\mathcal{O}_K$ features a prime factor with exponent greater than one. Thus, $\mathcal{O}_K/(p)$ is a finite ring that is not a product of fields (because it contains nilpotent elements). Therefore, the trace pairing on $\mathcal{O}_K/(p)$ is degenerate, meaning that there is some $x \in \mathcal{O}_K/(p)$ such that $\mathrm{Tr}(xy) = 0$ for all $y \in \mathcal{O}_K/(p)$.

In other words, there is some $X \in \mathcal{O}_K$ such that for all $Y \in \mathcal{O}_K$, we have $\mathrm{Tr}(XY) \in (p)$. Without loss of generality, we may assume that X is not divisible by any integer greater than 1. (If X is divisible by n, replace it with X/n.) Extend X to a basis $\{x_1 = X, x_2, \dots, x_n\}$ of $\mathcal{O}_K$ over $\mathbb{Z}$, which because X is primitive is always possible. Then the discriminant of K is computed by the following matrix:

$$\det\begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(x_1^2) & \mathrm{Tr}_{K/\mathbb{Q}}(x_1x_2) & \dots & \mathrm{Tr}_{K/\mathbb{Q}}(x_1x_n) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(x_nx_1) & \mathrm{Tr}_{K/\mathbb{Q}}(x_nx_2) & \dots & \mathrm{Tr}_{K/\mathbb{Q}}(x_n^2) \end{pmatrix}$$

The entire first row of this matrix is divisible by p. So the determinant – and therefore the discriminant – is divisible by p.

Now for backwards. Assume that the discriminant is divisible by p. We want to show that p is ramified in K.

Well, the following determinant is divisible by p:

$$\det\begin{pmatrix} \mathrm{Tr}_{K/\mathbb{Q}}(x_1^2) & \mathrm{Tr}_{K/\mathbb{Q}}(x_1x_2) & \dots & \mathrm{Tr}_{K/\mathbb{Q}}(x_1x_n) \\ \vdots & \vdots & & \vdots \\ \mathrm{Tr}_{K/\mathbb{Q}}(x_nx_1) & \mathrm{Tr}_{K/\mathbb{Q}}(x_nx_2) & \dots & \mathrm{Tr}_{K/\mathbb{Q}}(x_n^2) \end{pmatrix}$$

which means that the columns of this matrix are linearly dependent. Thus, after reducing modulo p, there are not-all-zero elements $\{a_1, \dots, a_n\}$ of $\mathbb{F}_p$ satisfying, for all i:

$$a_1\mathrm{Tr}(x_ix_1) + \dots + a_n\mathrm{Tr}(x_ix_n) = 0$$

which by the linearity of trace implies, for each i:

$$\mathrm{Tr}((a_1x_1 + \dots a_nx_n)x_i) = 0$$

So, if we set $x = a_1x_1 + \dots a_nx_n$, we get $\mathrm{Tr}(xx_i) = 0$ for all i, and since the x_i are a basis of $\mathcal{O}_K/(p)$ over $\mathbb{F}_p$, this means $\mathrm{Tr}(xy) = 0$ for all $y \in \mathcal{O}_K/(p)$. This means that the trace form is degenerate, and therefore that $\mathcal{O}_K/(p)$ is not a product of fields, and so p ramifies in K. ♣

9 The class group: When is $\mathcal{O}_K$ a PID?

The question posed in the section title turns out to have an interesting answer. It turns out that you can sort ideals into equivalence classes, in such a way that one of the equivalence classes consists exactly of the principal ideals. Even better, it turns out that the set of equivalence classes can be made into a group under ideal multiplication. Let's make that idea come to life now.

Definition 9.1. *Let K be a number field with ring of integers $\mathcal{O}_K$. The ideal group I_K of K is the group of invertible fractional ideals of $\mathcal{O}_K$, with ideal multiplication as its operation.*

It's pretty easy to see that this is a group. The product of fractional ideals is again a fractional ideal, and invertible ideals all have an inverse by definition. (Duh.)

But this group is boring. It is, by unique factorisation of ideals, the free abelian group on the prime ideals of $\mathcal{O}_K$. And anyway, we're looking for equivalence classes where one of them consists of all the principal ideals. So we define a subgroup of I_K, which we'll call P_K, which consists of all the principal ideals. (It's pretty easy to see that P_K is a subgroup – the product of principal ideals is still principal, and the unit ideal is indeed principal.)

Now we're ready for the big definition of this section.

Definition 9.2. *Let K be a number field with ring of integers $\mathcal{O}_K$. The ideal class group of K (or class group, for short), denoted Cl(K), is the quotient group Cl$(K) = I_K/P_K$.*

So $\mathcal{O}_K$ is a PID if and only if $I_K = P_K$, which happens if and only if $\mathrm{Cl}(K) = 1$. Cool.

How do we figure out what $\mathrm{Cl}(K)$ is? Thereby hangs a tale.

The first and most important fact, is that $\mathrm{Cl}(K)$ is always finite. This will take some effort to prove. Here's the plan:

Step 1: Find a constant M_K such that every ideal class has a representative of norm at most M_K.

Step 2: Show that there are only finitely many ideals of $\mathcal{O}_K$ of norm at most B for any B.

Theorem 9.3. *Let K be a number field with ring of integers $\mathcal{O}_K$, with $[K : \mathbb{Q}] = n$, having r real embeddings and s pairs of complex embeddings. Then every ideal class in Cl(K) is represented by an integral ideal of norm at most*

$$M_K = \sqrt{|disc(K)|}\left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}$$

Proof: Pick any ideal class in $\mathrm{Cl}(K)$, and pick any integral representative I of it. (Note that every ideal class has an integral representative, because if I is a fractional ideal representing that class, there is some $a \in K$ such that $aI \subset \mathcal{O}_K$, and aI is in the same ideal class as I.) We will show that there is another representative, J, of the same class, such that $N(J) \leq M_K$.

Now, I and J represent the same ideal class if and only if $I = aJ$ for some nonzero $a \in K$. So what we'll actually do is find some $a \in K$ such that $J = aI$ has norm at most M_K.

We also need aI to be an integral ideal. But that means $aI \subset \mathcal{O}_K$, so $a \in I^{-1}$. Which will help narrow down the search.

OK. We want aI to have norm at most M, and we want $a \in I^{-1}$. We have

$$N(aI) = N(a)N(I)$$

so that means that we need

$$N(a) \leq M_K N(I)^{-1} = M_K N(I^{-1})$$

since the norm of ideals is multiplicative.

So let's look at the locus of vectors in Minkowski space V_K that have norm smaller than $M_K N(I^{-1})$, where by "norm" here I mean the product of the coordinates, since that's what norm means for elements of K. Specifically:

$$\Lambda = \{(v_1, \dots, v_n) \mid |v_1 \dots v_n| < M_K N(I^{-1})\}$$

We want to prove that there's an element of I^{-1} sitting inside Λ somewhere. The following lemma is famously useful in that regard.

Lemma 9.4 (Minkowski)**.** *Let L be a lattice in $\mathbb{R}^n$. Let S be a subset of $\mathbb{R}^n$ with the following properties:*

- *S is symmetric: if $v \in S$, then $-v \in S$*
- *S is convex: if v and w are in S, then the line segment joining v to w is entirely contained in S.*
- *S has volume strictly greater than $2^n |\det(L)|$.*

Then $S \cap L$ contains a nonzero vector.

We won't prove this here – we'll leave that to the geometry section. But it kind of makes sense that something like this should be true: if all your nonzero vectors are big, then they should combine to give you a big determinant.

But this lemma doesn't look useful at all for our situation. I mean, if you make one of the coordinates really small, you can make the other coordinates really big and still have a small norm. In particular, the locus Λ is not bounded, and its size is not easily measured, because the boundary is all curvy and infinite. Plus it's not convex ... in short, this lemma looks hopeless.

The good news is that we don't need to apply the lemma to Λ. We will apply it to a specially chosen *subset* $S \subset \Lambda$. The subset S will be awesome, and literally tailor-made for this application. And if we can find an element of $I^{-1} \cap S$, we will of course have found an element of $I^{-1} \cap \Lambda$.

So what is this marvelous set S? Wonder no more:

$$S = \{(v_1, \dots, v_n) \in V_K \mid \sum |v_i| \leq t\}$$

Well, ok, there is still a bit of wonderment left. What is t?

It's a secret. I'm not going to tell you what it is. So there.

Ok, fine. The number t is a variable, and we're going to apply the lemma to S for a complicated set of values of t, and not just one. So I don't really know what t is either. I may need to sulk briefly now.

At any rate, regardless of what t is, it's clear that the set S is convex and symmetric, so we just need to verify that it's big enough, and that it's contained in the locus of vectors of norm at most $M_K N(I^{-1})$.

So what is the volume of the set S? Why, it's $2^r \pi^s \left(\frac{t^n}{n!}\right)$, where

r and s are the number of real and complex embeddings of K, respectively. Honest.

OK, fine, you don't trust me any more, now that I've kept secrets from you. The calculation of the volume is in the geometry section.

So is the volume big enough? Let's check.

The lemma needs the volume of S to be at least $2^n|\det(I^{-1})|$.

We know that $|\det(I^{-1})| = N(I)^{-1}\sqrt{|\mathrm{disc}(K)|}$, because the determinant of $\mathcal{O}_K$ is the square root of the discriminant, and $N(I^{-1})$ is the determinant of the linear transformation taking a basis of $\mathcal{O}_K$ to a basis of I^{-1}. Combining the two determinants is multiplicative.

So we need $\mathrm{vol}(S) > 2^n N(I)^{-1}\sqrt{|\mathrm{disc}(K)|}$. This amounts to

$$2^r\pi^s\left(\frac{t^n}{n!}\right) > 2^n N(I)^{-1}\sqrt{|\mathrm{disc}(K)|}$$

After a bit of algebraic wrangling, this turns into the following:

$$t^n > \left(\frac{4}{\pi}\right)^s \frac{n!}{N(I)}\sqrt{|\mathrm{disc}(K)|}$$

(Remember that $n = r + 2s$.) So if t is big enough to satisfy that, there will be a vector in $S \cap I^{-1}$.

We also need to make sure that S is contained in Λ, the locus of vectors of norm at most $M_K N(I^{-1})$. That is, we need to make sure that when we find a vector in S, we have found a vector of norm at most $M_K N(I^{-1})$.

So let's say that $\sum |v_i| \leq t$. The trick to the next part is the arithmetic-geometric mean inequality. That inequality there looks an awful lot like an arithmetic mean statement:

$$\frac{1}{n}\sum |v_i| \leq \frac{t}{n}$$

But the geometric mean is never greater than the arithmetic mean, so we get

$$\left(\prod |v_i|\right)^{1/n} \leq \frac{t}{n}$$

Raising both sides to the power n reveals that the norm of any vector in S is at most $(t/n)^n$. In order to ensure that $S \subset \Lambda$, we therefore need:

$$\left(\frac{t}{n}\right)^n \leq M_K N(I^{-1})$$

We also need

$$t^n > \left(\frac{4}{\pi}\right)^s \frac{n!}{N(I)}\sqrt{|\mathrm{disc}(K)|}$$

We can divide both sides of the latter by n^n to get

$$\left(\frac{t}{n}\right)^n > \left(\frac{4}{\pi}\right)^s \frac{n!}{n^n}\sqrt{|\mathrm{disc}(K)|}N(I^{-1}) = M_K N(I^{-1})$$

(This is why M_K is the right bound – a different number makes these not match up as well.)

So we've deduced that if $\left(\frac{t}{n}\right)^n > M_K N(I^{-1})$, then there is a nonzero vector in $S \cap I^{-1}$. And if $\left(\frac{t}{n}\right)^n \leq M_K N(I^{-1})$, then $S \subset \Lambda$.

This looks bad. I mean, there are literally no values of t that satisfy both inequalities. But we're so close that we can sneak by. What we've actually shown is that for every $B > M_K N(I^{-1})$, there is a vector in I^{-1} of norm at most B. Equivalently, we've shown that for every $B > M_K N(I^{-1})$, there is an ideal J of norm at most B in the same ideal class as I.

But the norm of an ideal is an integer! As in, the kindergarten kind of integer. So there is an ideal J in the ideal class of I that has minimal norm (that is, there isn't an infinite sequence of ideals of ever-more-slightly decreasing norms), and that minimal norm must be smaller than every real number B that satisfies $B > M_K$. It immediately follows that the norm of J is at most M_K, as desired. ♣

That was Step 1, to show that every ideal class has a representative of norm at most M_K. Now for Step 2, to show that this means there are only finitely many ideal classes. Step 2 is much easier than Step 1.

Theorem 9.5. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let I be an ideal of $\mathcal{O}_K$. Then $N(I) \in I$.*

Proof: Well, we already know that $N(I)$ is the number of elements of $\mathcal{O}_K/I$. So $N(I)x \equiv 0 \pmod{I}$ for all $x \in \mathcal{O}_K$. In particular, $N(I) \cdot 1 \equiv N(I) \equiv 0 \pmod{I}$. So $N(I) \in I$, as desired. ♣

Theorem 9.6. *Let K be a number field with ring of integers $\mathcal{O}_K$, and let $B > 1$ be a real number. There are finitely many ideals of $\mathcal{O}_K$ of norm at most B.*

Proof: Let Λ be the gcd of all the integers in the interval $[1, B]$. For any ideal I of norm at most B, we have $\Lambda \in I$, because $N(I)$ divides Λ.

But then the ideal I must be a factor of the ideal (Λ). There are only finitely many of those. So we're done. ♣

Now we know that the class group is finite. The next question is: how do we calculate it?

10 How to compute the class group

To be honest, the techniques in this section aren't going to work all the time. In fact, if your number field has degree four or bigger, they're unlikely to work at all, or at best, with a lot of extra effort.

But there are a lot of cases where it does work. And it's a lot of fun to work through. So let's do it.

There are no big theorems in this section, although there are a couple of cute results. I'm just going to do an example, so that you can see how the process works.

There is one thing that's handy to know before we start, though.

Theorem 10.1. *Let $f(x)$ be a monic irreducible polynomial of degree d with coefficients in $\mathbb{Z}$, and let α be a root of f. For any integer n, if we let $K = \mathbb{Q}(\alpha)$, then*

$$N_{K/\mathbb{Q}}(\alpha - n) = (-1)^{\deg f} f(n)$$

Proof: We already know that the norm of α is equal to $(-1)^{\deg f} f(0)$, because $f(x)$ is the monic minimal polynomial for α over $\mathbb{Q}$. The monic minimal polynomial for $\alpha - n$ over $\mathbb{Q}$ is $f(x+n)$, so we conclude that the norm of $\alpha - n$ is $(-1)^{\deg f} f(0+n)$, as desired.

♣

OK, that's cute, but who cares? Patience.

Let's compute the class group of $K = \mathbb{Q}(\alpha)$, where α is a root of the cubic polynomial $x^3 - 3x + 3$.

First off, that polynomial is irreducible because of Eisenstein on the prime 3. So we're not sunk from the start.

Next, we have to check that the ring $\mathbb{Z}[\alpha]$ is, in fact, the ring of integers of K. We actually did this already, and it is the ring of integers. So that's nice.

The discriminant of $x^3 - 3x + 3$ is $-135 = -3^3 \cdot 5$, as noted before. Our next step is to compute the Minkowski bound for K, to find out how many ideals we need to look at before we know we've got all the members of the class group.

The polynomial $x^3 - 3x + 3$ has one real root (by calculus, or by seeing that the discriminant is negative – all real roots would make the discriminant the square of a real number). So $r = 1$ and $s = 1$. This enables us to compute the Minkowski bound:

$$M_K = \left(\frac{4}{\pi}\right)^1 \frac{3!}{3^3}\sqrt{135} < 4$$

So the class group is entirely represented by ideals of norm less than 4. Since prime ideals generate the class group (they generate the ideal group!), this means that the class group is generated by the prime ideals containing 2 or 3.

So what are those ideals? There's a systematic trick for this. The first step is going to look weird, but trust me. Plug each of $-1, 0, 1$ into $f(x)$ and factor the answers:

$$\begin{aligned} f(-1) &= 5 \\ f(0) &= 3 \\ f(1) &= 1 \end{aligned}$$

From this, we can immediately see that $f(x)$ is irreducible modulo 2 (no roots – it's a cubic!). It has one root modulo 3 (we knew that already), and we know that 3 divides the discriminant of K, so 3 is ramified in K. That means that the ideal (3) must factor as a product of three ideals, of which at least two are the same.

But if the third ideal were different, then the polynomial would have two roots modulo 3 – $f(x)$ modulo 3 would factor as a linear factor times the square of a different linear factor. So all three ideals are the same, and $f(x)$ is the cube of a linear polynomial modulo 3. (In this case, as we have already seen, $f(x) \equiv x^3 \pmod{3}$.

So the ideal (2) is a prime ideal of $\mathcal{O}_K$ – no further factoring possible. And the ideal (3) factors as $(3) = P_3^3$ for some ideal P_3 of $\mathcal{O}_K$. The class group of K is therefore generated by P_3 (since (2) is principal, and therefore represents the trivial element of the class group).

Now, we already know from before that P_3 is principal. But even if we didn't, we could learn it quickly from the fact the $f(0) = 3$. To wit: the norm of α is $f(0) = 3$. That means the ideal (α) has norm 3 and is therefore prime ($\mathcal{O}_K/(\alpha)$ has three elements, so it's the field $\mathbb{F}_3$). In other words, $(\alpha) = P_3$!

So all the prime ideals of norm less than 4 are principal. Since they generate the class group of K, we conclude that $\mathcal{O}_K$ is a PID, because the class group is trivial.

Let's do a slightly more complicated example.

Let $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial x^3+2x-7. We will compute the class group of K.

The discriminant of K is $-1355 = -5 \cdot 271$. It's squarefree, so we can be confident that $\mathbb{Z}[\alpha]$ is the ring of integers. The negative discriminant tells us that $r = s = 1$, as before.

The Minkowski bound is therefore:

$$M_K = \left(\frac{4}{\pi}\right)^1 \frac{3!}{3^3}\sqrt{1355} < 11$$

Thus, we only have to worry about prime ideals containing a prime that's less than 11. Namely, 2, 3, 5, and 7.

The number are bigger than in the last example. I want information modulo 7, so I'm going to plug -3 to 3 into f and factor the results:

$$\begin{aligned}
f(-3) &= -40 = -2^3 \cdot 5 \\
f(-2) &= -19 \\
f(-1) &= -10 = -2 \cdot 5 \\
f(0) &= -7 \\
f(1) &= -4 = -2^2 \\
f(2) &= 5 \\
f(3) &= 26 = 2 \cdot 13
\end{aligned}$$

We can read off this data that there is one root of f modulo 2, no roots modulo 3, two roots modulo 5, and one root modulo 7. Let's deal with these primes one at a time.

$p = 2$: The prime 2 is not ramified, so there are no multiple roots. So if there is only one root, the other factor must be an irreducible quadratic. Thus, the ideal (2) factor as:

$$(2) = P_2Q_2$$

where P_2 has norm 2 (corresponding to the linear factor $x+1 \pmod 2$), and Q_2 has norm 4 (corresponding to the quadratic factor).

$p = 3$: The prime 3 is also not ramified. And there are no roots. So f must be irreducible modulo 3, so (3) is a prime ideal of $\mathcal{O}_K$.

$p = 5$: The prime 5 *is* ramified, for a change, so there is at least one multiple root. And there are two roots in total, so it must be exactly one multiple root, and we can factor:

$$(5) = P_5^2 Q_5$$

where P_5 and Q_5 both have norm 5. If we actually factor $f(x)$ modulo 5, we get

$$f(x) = x^3 + 2x - 7 \equiv (x+1)^2(x-2) \pmod 5$$

which means that P_5 corresponds to the linear factor $x+1$ and Q_5 corresponds to the linear factor $x-2$.

$p = 7$: Back to the unramified case. There is exactly one root of f modulo 7, so it must be – like $p = 2$ – the product of a linear factor (namely x) and an irreducible quadratic factor. Thus, we factor

$$(7) = P_7 Q_7$$

where P_7 has norm 7 and Q_7 has norm $7^2 = 49$.

Ok. We now know that the class group is generated by the prime ideals $P_2, Q_2, (3), P_5, Q_5, P_7$, and Q_7. What are the relations?

Well, one easy one is (3) – it's already trivial in the class group, because it's principal. One fewer generator.

But (2) is also principal. And $P_2Q_2 = (2)$. So, in the class group $\mathrm{Cl}(K)$, we get $P_2 = Q_2^{-1}$. So we don't need Q_2 in our list of generators.

Similarly, $P_5^2Q_5 = 1$, and $P_7Q_7 = 1$, so we don't need Q_5 or Q_7 in our list of generators.

So our new list of generators is P_2, P_5, P_7.

We can also read some relations off our table of values up above. For example, we know that $f(-3) = -40 = -2^3 \cdot 5$. This means that the ideal $(\alpha + 3)$ factors as the product of an ideal of norm 8 and an ideal of norm 5. The ideal of norm 5 is Q_5, because Q_5 corresponds to the linear factor $x-2 \equiv x+3$ modulo 5. The ideal of norm 8 must be P_2^3, because P_2 corresponds to the linear factor $x + 1$ modulo 2.

Thus, $(\alpha + 3) = P_2^3Q_5$ is trivial in the class group! Which gives us the relation $P_2^3Q_5 = 1$. Combining this with $Q_5 = P_5^{-2}$ yields

$$P_2^3 = P_5^2$$

Going down the list of values of f gives us a few more relations. The $f(-2) = -19$ just tells us that some ideal of norm 19 is principal, which isn't useful. But $f(-1) = -10 = -2 \cdot 5$ means that $P_2P_5 = (\alpha + 1)$, so in $\mathrm{Cl}(K)$, we have:

$$P_2 = P_5^{-1}$$

Combined with the previous relation, we can eliminate P_2 from our list of generators, and note that $P_5^5 = 1$ (in $\mathrm{Cl}(K)$).

Next, $f(0) = -7$ means that $(\alpha) = P_7$. So P_7 is principal, and we don't need it as a generator of the class group.

As this point, I'm going to skip ahead to $f(2) = 5$. This says that $(\alpha - 2) = Q_5$ is principal. Since $Q_5 = P_5^{-2}$, we get $P_5^2 = 1$ in $\mathrm{Cl}(K)$. Combined with $P_5^5 = 1$, this means $P_5 = 1$ in the class group.

Our list of generators is now empty – the class group is trivial! So $\mathcal{O}_K$ is a PID.

There are some remaining questions here, but the one uppermost in my mind is: what happens if $\mathcal{O}_K$ is not a PID? How do you show that an ideal of $\mathcal{O}_K$ is not principal?

There is a way. A more or less foolproof way. (A pretty annoying and computation-intensive way, to be fair.) But it will have to wait for a little bit of extra technology, in the next section.

11 What are the units of $\mathcal{O}_K$?

It turns out that proving that an ideal is not principal can be boiled down to computing ... well, not necessarily *all* the units of K, but enough of them. We will prove a theorem about what all of the units are, and then we will do an example of how you can find enough of them to show that an ideal is not principal.

Here's the big theorem.

Theorem 11.1 (Dirichlet's Unit Theorem)**.** *Let K be a number field with ring of integers $\mathcal{O}_K$. The group of units $\mathcal{O}_K^*$ of $\mathcal{O}_K$ is generated by the roots of unity of K, together with a free abelian group of rank $r + s - 1$, where r is the number of real embeddings of K, and s is the number of (complex conjugate pairs of) complex embeddings of K.*

In particular, $\mathcal{O}_K^*$ is isomorphic to $T \times \mathbb{Z}^{r+s-1}$, where T is the finite group of roots of unity contained in K.

The proof has several steps to it, because of course it does. And believe it or not, the following proof is much easier than the one Dirichlet originally used.

The first step is to derive a simple way of testing to see if an element of $\mathcal{O}_K$ is a unit.

Theorem 11.2. *Let K be a number field with ring of integers $\mathcal{O}_K$. Then $\alpha \in \mathcal{O}_K$ is a unit if and only if $N(\alpha) = \pm 1$.*

Proof: If $N(\alpha) = \pm 1$, then the product of all the conjugates of α – all of which are algebraic integers! – is ± 1, which is a unit of $\mathcal{O}_K$. In particular, $1/\alpha$ is an algebraic integer that is contained in K, so it's contained in $\mathcal{O}_K$, so α is a unit of $\mathcal{O}_K$.

Conversely, if $\alpha\beta = 1$, then taking norms gives $N(\alpha)N(\beta) = 1$. Since those two norms are both integers, we easily deduce that $N(\alpha) = \pm 1$. ♣

Warning! There are plenty of elements of K that have norm ± 1 but are not units! They're just not algebraic integers – they're not elements of $\mathcal{O}_K$.

The way we're going to prove Dirichlet's Unit Theorem is to find a real vector space of dimension $r+s-1$ in which the group of units is a lattice. Which is obviously a lie, because a lattice is a free abelian group, and the unit group is obviously not free. (Hello, minus one!)

There is the additional problem that the group operation in any respectable lattice is addition, and the group operation for the group of units is multiplication.

But I know how to turn multiplication into addition – use logarithms! Here's how we do it. Let $V_K \subset \mathbb{C}^n$ be the Minkowski space of K, and let U_K be the subset of V_K where none of the coordinates are zero. Define a function $\psi\colon U_K \to \mathbb{R}^n$ by

$$\psi(z_1, \ldots, z_n) = (\log|z_1|, \ldots, \log|z_n|)$$

Now, it's important to notice that there's no need for any fancy complex logarithms here – we're taking absolute values of each coordinate before we take any logarithms. And because we've stripped out the zeroes, there's no trouble there either.

Notice, too, that the image of K in V_K passes through to $\mathbb{R}^n$ without trouble ... except for 0. But 0 is not a unit, so we won't miss it. Trust me. The point is, every nonzero element of K ends up in U_K after you stick it in V_K. (This is because if $\alpha \neq 0$, then none of the conjugates of α are zero either.)

Another neat fact about ψ: it's a homomorphism! I mean, in the sense that $\psi(uv) = \psi(u) + \psi(v)$. The multiplication in U_K is coordinatewise, which matches up with multiplication in K. I mean, in each coordinate, you take an absolute value – multiplicative homomorphism – and then you take a logarithm – homomorphism from multiplication to addition.

Next question: Is ψ injective?

No.

Theorem 11.3. *The kernel of ψ is the set*

$$\ker\psi = \{(u_1, \ldots, u_n) \mid |u_i| = 1 \, \textit{for all } i\}$$

The elements of $\ker\psi$ *that lie in K are exactly the roots of unity in K.*

Proof: The first claim is obvious from the definition of ψ. The second claim is more subtle. Certainly every root of unity w has $|\sigma_i(w)| = 1$ for all embeddings i. Conversely, the set of elements of $\mathcal{O}_K$ with $|\sigma(\alpha)| \leq 1$ is a finite set, because it's a closed and bounded subset of V_K, and $\mathcal{O}_K$ is a lattice in there. But every power of α is in the same bounded subset, so two of those finite powers of α must be the same. So $\alpha^k = \alpha^\ell$ for some $k \neq \ell$, giving $\alpha^{k-\ell} = 1$. In other words, α is a root of unity. ♣

So ψ isn't injective, but that's only because it has solved our biggest problem, at least inasmuch as we wanted to get rid of those pesky roots of unity. If Dirichlet's Theorem is correct (which of course it is), then the image $\psi(O_K^*)$ of the unit group under ψ is a free abelian group! It now, finally, has a chance to be a lattice!

The next part of being a lattice is for the rank to equal the dimension. This has two parts: the rank can't be too big, and it can't be too small. We'll do the "not too big" part first.

We'll approach this in a slightly funny way. If you have a subgroup – additive – of a vector space, like we do, then if the rank is greater than the dimension of the space, the vectors have to bunch up, somehow, because the vector space isn't big enough to hold them all discretely. Like $\mathbb{Z}[\sqrt{2}]$ inside $\mathbb{R}$, for example – a rank two group inside a two-dimensional space.

Let's formalize that.

Definition 11.4. *Let S be a subset of a normed real vector space V. Then S is discrete if and only if for each vector $v \in S$, there is a positive real number $B > 0$ such that if $w \in S$ satisfies $|v - w| < B$, then $w = v$.*

In other words, S is discrete if each of its points is isolated from the others. The idea will be that if a subgroup is discrete, then it doesn't have enough room, in an n-dimensional space, to have more than n $\mathbb{Z}$-linearly independent vectors.

Theorem 11.5. *Let L be a subgroup of the additive group of a real vector space V. If L is a discrete subgroup of V, then L is a free abelian group of rank at most* $\dim V$*.*

The proof of this theorem is in the geometry section.

Now to prove that the image of ψ is discrete. Let $v = (v_1, \ldots, v_n)$ be any point in the image $\Psi = \psi(\mathcal{O}_K - \{0\})$. Let $X > 0$, and consider the set $B(X)$:

$$B(X) = \{(w_1, \ldots, w_n) \mid |v_i - w_i| < B \,\text{for all}\, i\}$$

If $\psi(x_1, \ldots, x_n)$ is in $B(X)$, then

$$|\log|x_i| - v_i| < B$$

for all i. Exponentiating gives

$$|x_i|/e^{v_i} < e^B$$

for all i. But this is a bounded subset of V_K, so there are only finitely many points of $\mathcal{O}_K$ in it. This means that there are only finitely many points of $\mathcal{O}_K$ in $B(X)$, so Ψ is discrete, as desired.

So the rank of the unit group (which is the rank of its image under ψ) is at most n. But we can actually do better, because the complex embeddings come in pairs, and the absolute value of a complex number is the same as the absolute value of its conjugate. That gives us s linear relations satisfied by the image of ψ, so the image of ψ is actually of rank no more than $r + s$.

Dirichlet says, however, that the rank is $r + s - 1$. Where's the extra relation?

Well, the norm of a unit is always ±1. So the units are contained in the locus

$$\{(u_1, \ldots, u_n) \mid \prod u_1 = \pm 1\}$$

in V_K. Plugging this into ψ (taking absolute values and then logarithms) shows that the image of ψ is contained in the locus

$$\{(x_1, \ldots, x_n) \mid x_1 + \ldots + x_n = 0\}$$

which is one more linear relation. So the rank of $\psi(\mathcal{O}_K^*)$ (and thus the rank of the unit group $\mathcal{O}_K^*$) is at most $r + s - 1$.

Now for the hard part: to show that the rank is at least that big.

Specifically, let H be the subspace of $\mathbb{R}^n$ given by the following linear relations:

$$x_1 + \ldots + x_n = 0$$

$$x_{r+1} = x_{r+2}, \ldots, x_{n-1} = x_n$$

We will show that $\psi(\mathcal{O}_K^*)$ spans H.

To do this, let W be the span of $\psi(\mathcal{O}_K^*)$ in $\mathbb{R}^n$. If $W \neq H$, then there is some linear relation $\ell(x) = a_1x_1 + \ldots + a_nx_n = 0$ that is satisfied by all the vectors in W, but not by all the vectors in H. Define the following function $f\colon U_K \to \mathbb{R}$:

$$f(u_1, \ldots, u_n) = a_1 \log|u_1| + \ldots + a_n \log|u_n|$$

We're going to find a unit $u \in \mathcal{O}_K^*$ such that $f(u) \neq 0$. That will show that the image of u – which is contained in W – does not satisfy $\ell(\psi(u)) = 0$, which is a contradiction, meaning that $W = H$ after all.

Choose $c = (c_1, \ldots, c_n)$ with positive real coordinates such that

$$\prod c_i = A > \left(\frac{4}{\pi}\right)^s \sqrt{|\mathrm{disc}(K)|}$$

and such that $c_{r+1} = c_{r+2}, \ldots, c_{n-1} = c_n$. Define a bounded set S in V_K by

$$|x_1| \leq c_1, \ldots, |x_r| \leq c_r$$

and

$$|x_{r+1}|^2 + |x_{r+1}|^2 \leq c_{r+1}^2, \ldots, |x_{n-1}|^2 + |x_n|^2 \leq c_{n-1}^2$$

The set S is bounded and symmetric and convex and wonderful for applying Minkowski's Lemma to. As long as it's big enough. Its volume is easy to compute, though: it's a product of r intervals of length $2c_1, \ldots, 2c_r$ and s circles of radius $2c_{r+1}, 2c_{r+3}, \ldots, 2c_{n-1}$, so the volume is $2^r \pi^s \prod c_i > 2^n \sqrt{|\mathrm{disc}(K)|}$.

This is big enough, because the determinant of $\mathcal{O}_K$ in B_K is $\sqrt{|\mathrm{disc}(K)|}$. So there is a nonzero element a of $\mathcal{O}_K$ in S.

We have $N(a) \leq A$, by construction. And none of the conjugates of a can be all that small, because then at least one of the other ones would be too big:

Since $a \neq 0$, we have $|N(a)| \geq 1$, so if $\sigma_1, \ldots, \sigma_n$ are the embeddings of K in $\mathbb{C}$, we have:

$$|\sigma_i(a)| \geq \frac{1}{\prod_{j \neq i} |\sigma_j(a)|} \geq \frac{1}{\prod_{j \neq i} c_j} = \frac{c_i}{A}$$

for all i.

There are only finitely many elements of $\mathcal{O}_K$ of norm at most A, so there are only finitely many principal ideals of $\mathcal{O}_K$ of norm at most A. Pick generators for each of those, and call them $b_1, \ldots, b_k$. Because a has norm at most A, there must be some unit u satisfying $a = ub_m$ for some m.

Our next step is to show that $|f(u) - f(c)|$ is bounded from above *independently of the choice of c*. Then we'll pick a clever c to show that $f(u) \neq 0$.

$$\begin{aligned}
|f(u) - f(c)| &= |f(a) - f(b_m) - f(c)| \\
&\leq |f(b_m)| + |f(a) - f(c)| \\
&= |f(b_m)| + |a_1(\log(|\sigma_1(a)|) - \log|c_1|) + \ldots \\
&+ a_n(\log(|\sigma_n(a)|) - \log|c_n|)| \\
&\leq |f(b_m)| + \log(A)\,(|a_1| + \ldots + |a_n|) \\
&= B
\end{aligned}$$

where B does not depend on the particular choice of c_i!

We can now deliver the coup de grace. If $r + s - 1 = 0$, then there is nothing to prove – $H = 0$, and the lower bound for the rank is trivial. Otherwise, there are at least two different c_i, and we can choose one of them freely. In that case, as $c_1 \to \infty$, we have $|f(c)| \to \infty$ as well. As long as $|f(c)| > B$, we must have $f(u) \neq 0$, as desired. ♣

12 Showing an ideal is not principal: using the units

Let's say you have an ideal I in the ring of integers O_K of a number field K, and you want to prove that it's not principal. Here's one idea for how you might do it.

Compute the norm $N(I)$ of I. Any generator of I must have norm $\pm N(I)$. So if $I = (x)$, then $\psi(x) = (y_1, \ldots, y_n)$ must satisfy

$$y_1 + \ldots + y_n = \log N(I)$$

as well as $y_{r+1} = y_{r+2}, \ldots, y_{n-1} = y_n$.

But if $I = (x)$, then for any unit u of $\mathcal{O}_K$, we also have $I = (ux)$. The units of $\mathcal{O}_K$ (or, more accurately, their image under ψ) is a lattice in the subspace H from the previous section. So, by judicious adding and subtracting of lattice vectors in H from $\psi(x)$, we can find a generator of I that lies in a bounded, computable subset of $\mathbb{R}^n$. Search for generators of I in that subset – it's a finite search – and if you don't find any, then you know that I is not principal.

Let's do an example. Let K be the number field $\mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^3 + 4x + 1$. A calculation (which I will not do here) shows that $\mathbb{Z}[\alpha]$ is the ring of integers of K, and that $P = (\alpha + 1, 2)$ is a prime ideal of $\mathcal{O}_K$ of norm 2. We want to show that P is not a principal ideal.

First, we need to find a unit. The polynomial $x^3 + 4x + 1$ has exactly one real root, so it has exactly one real embedding, and one complex embedding. Therefore, the unit group has rank $1 + 1 - 1 = 1$.

The norm of α is -1, so it is a unit! Let's compute its image under ψ.

A bit of Newton's method (or some other root approximation technique, like Maple) shows that the real root of $x^3 + 4x + 1$ is a little bit greater than $-1/4$. This means, since the norm of α is -1, that the complex roots have absolute value a little bit less than 2. So as a vector, we have

$$\psi(\alpha) \sim (\log(1/4), \log(2), \log(2)$$

Thus, if there is a generator x for P, then there must be a generator y such that

$$\psi(y) = (\log(|y_1|), \log(|y_2|), \log(|y_2|))$$

with

$$0 \leq \log(|y_1|) \leq \log(4)$$

or, equivalently

$$1 \leq |y_1| \leq 4$$

and therefore also (since $|y_1 y_2^2| = 2$)

$$1/\sqrt{2} \leq |y_2| \leq \sqrt{2}$$

The rest is a bit tedious. We have now defined a bounded subset of Minkowski space. We know a basis for the lattice $\mathcal{O}_K$ in V_K, namely $\{1, \alpha, \alpha^2\}$, and we know approximately what coordinates these basis vectors have in V_K. The three vectors $\{1, \alpha, \alpha^2\}$ are pretty close to orthogonal, so it's easy to calculate how large a linear combination of them is ... and it's easy to check that not very many of those linear combinations have length 8 or less. Once you've got that short list, it's pretty easy to check that none of those vectors have norm 2.

For a quadratic extension, there's a much easier trick. Let's say you want to check if the ideal $P = (5, 6 + \sqrt{11})$ is a principal ideal of $\mathbb{Z}[\sqrt{11}]$. (Notice that $\mathbb{Z}[\sqrt{11}]$ is indeed the ring of integers of $\mathbb{Q}(\sqrt{11})$.)

Well, the norm of P is 5, because

$$\begin{aligned} \mathbb{Z}[\sqrt{11}]/P &\cong \mathbb{Z}[x]/(x^2 - 11, 6 + x, 5) \\ &\cong \mathbb{F}_5[x]/(x^2 - 1, x + 1) \\ &\cong \mathbb{F}_5[x]/(x + 1) \\ &\cong \mathbb{F}_5 \end{aligned}$$

so we just need to check if there's an element of norm 5 in $\mathbb{Z}[\sqrt{11}]$. So we set $N(a + b\sqrt{11}) = 5$:

$$a^2 - 11b^2 = 5$$

This equation looks difficult to solve. But in practice, either there is a solution lying around that's not too hard to stumble onto just by a brute force search, or else there's a small prime q such that the equation has no solutions modulo q^r for some small r. And the likely primes q are things like 5 and 11, which are staring you in the face anyway.

In this particular case, there are solutions modulo 5 and 11, so we suspect that there is a solution more generally. And indeed, $a = 4$ and $b = 1$ gives you a winner! But then, $a = \pm 4$ and $b = \pm 1$ are all solutions to the equation. Are they all generators of P?

No. We know that (5) factors as the product of two prime ideals of $\mathbb{Z}[\sqrt{11}]$, because (5) is not prime (it's properly contained in P!), and it's not ramified (the discriminant here is 44). So there is another prime ideal $Q = (5, 6 - \sqrt{11})$ such that

$PQ = (5)$. Our four solutions above must include generators for Q. (Notice that Q has to be principal because it's $(5)P^{-1}$, and (5) and P are both principal!)

So which solutions correspond to generators of P? We must check. All the solutions will divide into 5 because any element of norm 5 is a divisor of 5. So we just need to check which solutions divide $6 + \sqrt{11}$. And we can ignore the $a = -1$ case, because we can multiply $a + b\sqrt{11}$ by -1 without changing the ideal it generates. So:

$$\begin{aligned}\frac{6+\sqrt{11}}{4+\sqrt{11}} &= \frac{(6+\sqrt{11})(4-\sqrt{11})}{(4+\sqrt{11})(4-\sqrt{11})} \\ &= \frac{13-2\sqrt{11}}{5}\end{aligned}$$

which is not in $\mathbb{Z}[\sqrt{11}]$, but

$$\begin{aligned}\frac{6+\sqrt{11}}{4-\sqrt{11}} &= \frac{(6+\sqrt{11})(4+\sqrt{11})}{(4-\sqrt{11})(4+\sqrt{11})} \\ &= \frac{35+10\sqrt{11}}{5} \\ &= 7+2\sqrt{11}\end{aligned}$$

which *is* an element of $\mathbb{Z}[\sqrt{11}]$. So $P = (4 - \sqrt{11})$ is principal, and incidentally, $Q = (4 + \sqrt{11})$ is also principal.

13 Modules

Let R be a commutative ring. An R-module is a bunch of things that you can add and subtract, and that you can multiply by elements of R.

OK, that's obviously a terrible definition. But it captures very well what a module is. We're pure math types, though, so we want a definition.

Definition 13.1. *Let R be a commutative ring. An R module is an abelian group M and a function $\cdot\colon R \times M \to M$ satisfying*

- $r(m_1 + m_2) = rm_1 + rm_2$
- $(r_1 + r_2)m = r_1 m + r_2 m$
- $r_1(r_2 m) = (r_1 r_2)m$
- $1m = m$

for all r, r_1, r_2 in R and all m, m_1, m_2 in M.

So for a module to make sense, you need to have a ring and a group. The actual module is the group, but you need to have the ring around to do the multiplying for you.

For example. If R is a field, then an R-module is a vector space.

If $R = \mathbb{Z}$, notice that a $\mathbb{Z}$-module is the same thing as an abelian group. One direction is obvious – any R-module is an abelian group regardless of what R is – and to go the other way, notice that an abelian group is an abelian group (yeah), and you can multiply it by elements of $\mathbb{Z}$ (heck yeah!). I mean, to multiply m by 5, just compute $m + m + m + m + m$.

If R is any ring, then any ideal I of R is an R-module. In fact, you could *define* an ideal to be an R-submodule of R. (An R-submodule of M is exactly what you think it is: it's an R-module whose elements are contained in M, and whose operations are the restrictions of the operations of M.)

Better yet, R/I is an R-module, for any commutative ring R and ideal I. Morally speaking: you can add and subtract the elements of R/I, and you can multiply them by elements of R (by reducing them mod I first). Technically speaking ... it's really boring and silly. Check it yourself, if you like. But bring a pillow.

An example that's a little more directly related to this course: the Gaussian integers $\mathbb{Z}[i]$ are a $\mathbb{Z}$-module. You can add and subtract them, and multiply them by elements of $\mathbb{Z}$. (Again, I leave it to you to check that all the axioms of the technical definition are satisfied.)

More generally, if T is any ring containing R, then T is an R-module. So, for example, $\mathbb{Q}$ is a $\mathbb{Z}$-module. So is $\mathbb{R}$.

More more generally, if $\phi\colon R \to T$ is a homomorphism, then T is an R-module. This explains the R/I example too.

As in any part of mathematics, once you define the objects, you have to define the morphisms.

Definition 13.2. *Let M and N be R-modules. An R-module homomorphism from M to N is a homomorphism $f\colon M \to N$ of abelian groups such that $f(rm) = rf(m)$ for all r in R and m in M. An R-module isomorphism is an R-module homomorphism that admits a two-sided inverse that is also an R-module homomorphism.*

In other words, an R-module homomorphism is a function that plays nice (commutes) with the addition, subtraction, and

R-multiplication.

Notice that because R-module homomorphisms are always homomorphisms of abelian groups, it follows that an R-module homomorphism is an R-module isomorphism if and only if it's bijective:

$$f^{-1}(rn) = f^{-1}(rf(f^{-1}(n))) = f^{-1}(f(rf^{-1}(n))) = rf^{-1}(n)$$

For example, if R is a field, then an R-module homomorphism is the same thing as a linear transformation of vector spaces. (Check it out – the proof is really easy!)

Complex conjugation defines a $\mathbb{Z}$-module homomorphism from $\mathbb{Z}[i]$ to $\mathbb{Z}[i]$. This is also a homomorphism of rings.

The function $x \to 2x$ is a $\mathbb{Z}$-module homomorphism from $\mathbb{Z}[i]$ to $\mathbb{Z}[i]$, but it's not a ring homomorphism, because 1 doesn't map to 1.

And complex conjugation defines a ring homomorphism $\mathbb{Q}(i) \to \mathbb{Q}(i)$, but this homomorphism of rings is *not* a homomorphism of $\mathbb{Q}(i)$-modules.

Notice – and the proof here is very easy – that the image and preimage of a submodule under a module homomorphism are again submodules.

But there is more work to do before we leave the warm embrace of the modules section.

Definition 13.3. *Let M be an R-module, S a subset of M. The submodule generated by S is the intersection of all submodules containing S.*

It's easy to check that any intersection of R-modules is again an R-module, so this definition makes sense. And this definition leads to a few more, but most especially, we say that an R-module M is finitely generated if there is a finite set S that generates M.

I guess we should actually prove some stuff.

Theorem 13.4. *Let M be an R-module, $N \subset M$ a submodule. If M is finitely generated, then so is M/N.*

Proof: If you can write $m \in M$ as a linear combination of generators $\{x_i\}$, then that linear combination still works after you reduce modulo N. ♣

For the next theorem, we will recall a definition.

Definition 13.5. *A ring R is noetherian if and only if every ideal of R is finitely generated.*

Theorem 13.6. *Let M be a finitely generated module over a noetherian ring R. Then every submodule of M is also finitely generated.*

Proof: We're going to start by proving the theorem in the case that $M = R^n = R \times R \times \ldots \times R$. We will then use a cunning trick to prove it for a general M. Let N be a submodule of $M = R^n$.

If $n = 1$, then an R-submodule of M is better known as an ideal of R, and is therefore finitely generated by assumption.

We will now induce on n. (The verb "to induct" is what you use to admit people to a Hall of Fame. "Deduce" gives "deduction", so "induce" gives "induction". I know, I know. I'm telling the tide not to come in.)

If $n \geq 2$, then we can write $R^n = R^{n-1} \times R$. Let $N_1 = \{(r_1, \ldots, r_n) \in N \mid r_n = 0\}$. Then N_1 is isomorphic to an R-submodule of R^{n-1}, and so it is finitely generated.

Let $N_2 = \pi_n(N) \subset R$, where $\pi_n \colon R^n \to R$ is the projection onto the nth coordinate. In other words, let N_2 be the set of elements of R that appear as the nth coordinate of some element of N. Since it's the image of a submodule under a homomorphism, it's a submodule of R, and therefore an ideal, and therefore finitely generated.

Let $x_1, \ldots, x_s$ be generators for N_1, and let $y_1, \ldots, y_t$ be elements of N whose nth coordinates are generators for N_2. For any $m \in N$, we can find an R-linear combination of the y_i whose nth coordinate is the same as that of m. In other words, we can find $r_1, \ldots, r_t \in R$ such that the nth coordinate of the following element of M is zero:

$$m - r_1 y_1 - \ldots - r_t y_t$$

But this means that this element is in M_1! So it's a linear combination of the x_i:

$$m - r_1 y_1 - \ldots - r_t y_t = r_1' x_1 + \ldots r_s' x_s$$

Reorganising this shows that m is in the R-linear span of the set $\{x_1, \ldots, x_s, y_1, \ldots, y_t\}$. So N is finitely generated.

Now let's do the general case. Since M is finitely generated, there is a surjective R-module homomorphism $\phi \colon R^n \to M$, mapping the standard basis vectors to the n generators $\{x_1, \ldots, x_n\}$ of M:

$$\phi(r_1, \ldots, r_n) = r_1 x_1 + \ldots + r_n x_n$$

(It's easy to check that this is indeed a surjective homomorphism. This is, by the way, a standard trick in algebra. Remember it.)

Let N be a submodule of M. Its preimage $\phi^{-1}(N)$ is a submodule of R^n, and is therefore finitely generated. The images of these generators under ϕ therefore generate N, and so N is finitely generated. ♣

14 Algebra that isn't really number theory

Theorem 14.1. *Let D be a finite commutative domain. Then D is a field.*

Proof: Let $a \in D$ be any nonzero element, and define a function $\phi\colon D \to D$ be the function $\phi(x) = ax$. Since D is a domain, ϕ is injective. But D is finite, so ϕ must also be surjective! So there is some element $b \in D$ such that $\phi(b) = 1$. Which is to say, $ab = 1$, so a is a unit. Since a was arbitrary, D is a field. ♣

The following theorem is known as the "Linear independence of characters" theorem, because a homomorphism from a group to a field is called a character.

Theorem 14.2 (Linear independence of characters)**.** *Let $f_1, \ldots, f_n$ be distinct homomorphisms from an abelian group G to the multiplicative group F^* of a field F. Then $f_1, \ldots, f_n$ are linearly independent over F.*

Proof: We proceed by induction on n. If $n = 1$, then we are done before we start. Now assume that $n \geq 2$, and that there are $a_1, \ldots, a_n \in F$ such that

$$a_1 f_1(g) + \ldots + a_n f_n(g) = 0$$

for all $g \in G$. We want to show that all the a_i are zero.

Since $f_1 \neq f_n$, there is some $g_0 \in G$ such that $f_1(g_0) \neq f_n(g_0)$. Applying the linear dependence relation to an element $g_0 g \in G$ gives:

$$a_1 f_1(g_0) f_1(g) + \ldots + a_n f_n(g_0) f_n(g) = 0$$

and if we multiply the original dependence relation by $f_n(g_0)$ we get:

$$a_1 f_n(g_0) f_1(g) + \ldots + a_n f_n(g_0) f_n(g) = 0$$

Subtracting the two equations cancels the last term, and gives:

$$a_1(f_1(g_0) - f_n(g_0)) f_1(g) + \ldots + a_{n-1}(f_{n-1}(g_0) - f_n(g_0)) f_{n-1}(g) = 0$$

which is a linear dependence relation between $f_1, \ldots, f_{n-1}$. By induction, this means that all the coefficients in this relation are zero! In particular, we get $a_1 = 0$, since $f_1(g)(f_1(g_0) - f_n(g_0)) \neq 0$.

But if $a_1 = 0$, then our original dependence relation becomes a relation between the $n-1$ homomorphisms $f_2, \ldots, f_n$! So all the other a_i have to be zero too. ♣

Theorem 14.3 (Chinese Remainder Theorem)**.** *Let R be a domain, I and J ideals of R. Let IJ be the product ideal:*

$$IJ = \{a_1 b_1 + \ldots + a_r b_r \mid a_i \in I,\ b_i \in J\}$$

If $I + J = R$, then $R/IJ \cong (R/I) \times (R/J)$.

Proof: If you want to show that two things are isomorphic, probably you should write down an isomorphism. So, define the following function from R to $(R/I) \times (R/J)$:

$$f(r) = (r \pmod{I}, r \pmod{J})$$

The kernel of f is clearly $I \cap J$. To show that it induces an isomorphism from R/IJ to $(R/I) \times (R/J)$, all we need to do is show that $I \cap J = IJ$ and that f is onto.

The first of these, that $I \cap J = IJ$, is mere algebraic trickery. The inclusion $IJ \subset I \cap J$ is obvious from the definition of ideal. For the reverse inclusion, note that $I \cap J = (I \cap J)(I + J) \subset JI + IJ = IJ$. (Remember that $I \cap J$ is a subset of both I and J!)

Surjectivity of f is a little more involved. A useful shortcut is to notice that if we can show that both $(0, 1)$ and $(1, 0)$ are in the image of f, then f must be surjective. (Say $f(a) = (0, 1)$ and $f(b) = (1, 0)$. Then for any x and y, we get $f(xa+yb) = (x, y)$.)

We know that $I + J = R$. So there are some $a \in I$ and $b \in J$ such that $a + b = 1$. Then $f(a) = (a \pmod{I}, a \pmod{J}) = (0, 1)$, and similarly $f(b) = (1, 0)$. So we're done. ♣

Theorem 14.4. *Let F be a field, and $f(x)$ a nonconstant polynomials with coefficients in F. The prime ideals of $F[x]/(f(x))$ are all maximal, and they are the ideals generated by the irreducible factors of $f(x)$ over F.*

Proof: First off, notice that if $q(x)$ is an irreducible factor of $f(x)$, then the ideal $(q(x))$ is certainly prime. By the Third Isomorphism Theorem for rings, if you like.

So now assume that P is a prime ideal of $F[x]/(f(x))$. Then it is the reduction modulo $(f(x))$ of a prime ideal of $F[x]$ that contains $(f(x))$. Prime ideals of $F[x]$ are either 0, or they're generated by irreducible polynomials. Since f is nonconstant, P can't be generated by 0, so it must be generated by an irreducible polynomial $q(x)$.

But P contains $f(x)$, so $q(x) \mid f(x)$, as desired. ♣

Theorem 14.5. *Let R be a noetherian ring, $I \subset R$ an ideal. Then there is a finite sequence of primes $P_1, \ldots, P_n$ such that $I \subset P_i$ for each i, and $\prod P_i \subset I$.*

Proof: If I is prime, we're done, so assume that I is not prime. Since R is noetherian, assume further that I is maximal with respect to the property of not satisfying the conclusion of the theorem. Then there are a, b such that $a, b \notin I$, but $ab \in I$, so I is a proper subset of both $Ra + I$ and $Rb + I$. Hence – by the maximality of I – there are primes $P_1, \ldots P_n$ and $Q_1, \ldots Q_m$ such that $\prod P_i \subset Ra + I$ and $\prod Q_j \subset Rb + I$. Then $\prod P_i \prod Q_j \subset (I + Ra)(I + Rb) \subset I$, and for each i, j, $I \subset P_i$ and $I \subset Q_j$, as desired. ♣

Theorem 14.6. *Let R be a domain, and let I and J be coprime ideals. Then for all positive integers n and m, the ideals I^n and J^m are also coprime.*

Proof: The ideal $I^n + J^m$ is either equal to R (in which case we're done), or else it's contained in some maximal ideal M. If $I^n + J^m \subset M$, then $I^n \subset M$ and $J^m \subset M$. But M is maximal, so it's prime. In particular, this means that $I^n \subset M$ means $I \subset M$, and similarly $J \subset M$, implying $I + J \subset M$ ... which is impossible since I and J are coprime. So I^n and J^m are coprime too. $\clubsuit$

The following is not the strongest version of this theorem that's known. But it will do for us.

Theorem 14.7. *Let R be a noetherian ring, and let $I_1 \subset I_2 \subset \ldots$ be an increasing chain of ideals. Then for some k, $I_k = I_m$ for all $m \geq k$.*

Proof: Define $I = \bigcup_k I_k$. It's an ideal: given any x and y in I, there is some k such that $x, y \in I_k$. Then $x \pm y \in I_k \subset I$, so I is closed under plus and minus. And if $r \in R$, then $rx \in I_k \subset I$ as well, so I is indeed an ideal.

But R is noetherian, so I is finitely generated, by $\{x_1, \ldots, x_n\}$. For each i, there is some k_i such that $x_i \in I_{k_i}$. Letting k be the largest of the k_i, we get $x_i \in I_k$ for all i. But then $I_k = I$, so $I_m = I_k$ for all $m \geq k$, as desired. $\clubsuit$

The following is not the only version of Nakayama's Lemma that's around. But it will do for what we want, and the proof is nicely illustrative.

Theorem 14.8 (Nakayama's Lemma)**.** *Let A be a ring, $I \neq A$ an ideal of A, and M a finitely-generated A-module. If $IM = M$, then there exists some $a \in A$ with $a \equiv 1 \pmod{I}$ such that $aM = 0$.*

Proof: Let $M = x_1 A + \ldots + x_n A$. Since $IM = M$, we know that for each x_i, we can write:

$$x_i = a_{1i} x_1 + \ldots + a_{ni} x_n$$

where $a_{ji} \in I$ for each i. This looks a lot like linear algebra, so let's define the matrix $B = (\delta_{ij} - a_{ij})$, where δ_{ij} is the Kronecker delta: it equals 1 if $i = j$, and equals 0 if $i \neq j$.

The determinant of B is clearly congruent to 1 modulo I, because B itself is congruent to the identity matrix modulo I. By Cramer's Rule, the classical adjoint matrix B^* of B satisfies $B^*B = (\det B)\mathrm{Id}_n$, where Id_n denotes the N by n identity matrix.

Now write $B^* = (c_{ij})$, and multiply out that matrix equation entry by entry. (Yuck.) You get, for each i and k between 1 and n:

$$\sum_{j=1}^{n} c_{ij}(\delta_{jk} - a_{jk}) = \delta_{ik}(\det B)$$

Multiplying both sides by x_k gives:

$$\sum_{j=1}^{n} c_{ij}(\delta_{jk} - a_{jk})x_k = \delta_{ik}(\det B)x_k$$

If we sum over k, this becomes:

$$\sum_{j,k=1}^{n} c_{ij}(\delta_{jk} - a_{jk})x_k = \sum_{k=1}^{n} \delta_{ik}(\det B)x_k$$

But now we reap the benefits of all this crunchy calculation, with a festival of cancellation. We already know that

$$\sum_{k=1}^{n}(\delta_{jk} - a_{jk})x_k = 0$$

by definition of the a_{jk}. So the left hand monstrosity is just a bunch of zeroes added together! And by the definition of δ_{ik}, we have:

$$\sum_{k=1}^{n} \delta_{ik}(\det B)x_k = (\det B)x_i$$

So we get $(\det B)x_i = 0$ for all i, and so $(\det B)M = 0$. Setting $a = \det B$ allows us to put our feet up and celebrate our success.

♣

15 Geometry that's not really number theory

Theorem 15.1. *Let V be a real vector space with a nondegenerate symmetric bilinear pairing $\langle \cdot, \cdot \rangle$, and let $\{v_1, \ldots, v_n\}$ be a basis for V. Let B be an orthonormal basis of V with respect to the pairing. Then*

$$\det \begin{pmatrix} [v_1]_B & \ldots & [v_n]_B \end{pmatrix}^2 = \det \begin{pmatrix} \langle v_1, v_1 \rangle & \ldots & \langle v_n, v_1 \rangle \\ \vdots & & \vdots \\ \langle v_1, v_n \rangle & \ldots & \langle v_n, v_n \rangle \end{pmatrix}$$

where $[v_i]_B$ denotes the column vector of v_i written in B-coordinates.

Proof: Write $B = \{e_1, \ldots, e_n\}$, and let $T\colon V \to V$ be the linear transformation satisfying $T(e_i) = v_i$. Then we have

$$\det \begin{pmatrix} [v_1]_B & \ldots & [v_n]_B \end{pmatrix}^2 = (\det[T]_B)^2$$

where $[T]_B$ denotes the matrix of T with respect to the basis B.

But because B is orthonormal, we know that $[v]_B \cdot [w]_B =$

$\langle v, w\rangle$ for any vectors v and w in V. So we can compute

$$\begin{pmatrix} \langle v_1, v_1\rangle & \dots & \langle v_n, v_1\rangle \\ \vdots & & \vdots \\ \langle v_1, v_n\rangle & \dots & \langle v_n, v_n\rangle \end{pmatrix}$$

$$= \left(\begin{array}{ccc} [v_1]_B & \dots & [v_n]_B \end{array} \right)^t \left(\begin{array}{ccc} [v_1]_B & \dots & [v_n]_B \end{array} \right)$$

$$= [T]_B^t [T]_B$$

That pretty much does it, given that $\det A = \det A^t$ for any square matrix A. ♣

Theorem 15.2. *Let $M \subset \mathbb{Z}^d$ be a lattice in $\mathbb{R}^d$ with $M \cong \mathbb{Z}^d$, and let $T\colon \mathbb{R}^d \to \mathbb{R}^d$ be a linear transformation such that $T(\mathbb{Z}^d) = M$. Then*

$$[\mathbb{Z}^d : M] = |\det T|$$

where $[\mathbb{Z}^d : M]$ is the index of M in $\mathbb{Z}^d$.

Proof: Let $\{e_1, \dots, e_d\}$ be the standard basis for $\mathbb{Z}^d$, and let $\{v_1, \dots, v_d\}$ be the basis of M for which $v_i = T(e_i)$.

Consider the following two sets:

$$D = \{(x_1, \dots, x_d) \in \mathbb{R}^d \mid 0 \leq x_i < 1 \text{ for all}\, i\}$$

and

$$F = \{\{a_1 v_1 + \dots + a_d v_d \in \mathbb{R}^d \mid 0 \leq a_i < 1 \text{ for all}\, i\}\}$$

The set D is a fundamental domain for $\mathbb{Z}^d$. That is, for every vector $v \in \mathbb{R}^d$, there is a unique vector $y \in D$ such that $v = y + z$

for some $z \in \mathbb{Z}^d$. Similarly, $F = T(D)$ is a fundamental domain for M. (This is fancy geometric language for "D is a complete set of representatives for $\mathbb{R}^d$ modulo $\mathbb{Z}^d$.")

Let $\{w_1, \ldots, w_n\}$ be a complete set of representatives for $\mathbb{Z}^d$ modulo M, so that every element of $\mathbb{Z}^d$ can be written uniquely as $w_i + m$ for some $m \in M$. (Notice here that $n = [\mathbb{Z}^d : M]$.) Then the set

$$S = (w_1 + D) \cup \ldots \cup (w_n + D)$$

is also fundamental domain for M. To see this, notice that for any $v \in \mathbb{R}^d$, there is a unique vector $y \in D$ and $z \in \mathbb{Z}^d$ such that $v = y + z$. But for z, there is a unique $i \in \{1, \ldots, n\}$ and $m \in M$ such that $z = w_i + m$, giving $v = (w_i + y) + m$ uniquely, as desired.

All three of the sets D, F, and S are bounded. So there are finitely many translates of F by elements of M whose union contains S. (Translates of F by elements of M cover the whole of $\mathbb{R}^d$, remember – this is part of what "fundamental domain" means.) Let $m_1, \ldots, m_r$ be the finitely many elements of M associated to those finitely many translates, so that

$$S \subset \bigcup_{i=1}^{r} (m_i + F)$$

If we define $S_i = S \cap (m_i + F)$, then S is the disjoint union of the S_i.

Now define $F_i = -m_i + S_i$. I claim that F is the disjoint union of the F_i.

To see this, notice first that the F_i are certainly disjoint, because if $v \in F_i \cap F_j$, then $v = m_i + s = m_j + s'$ for some

$s, s' \in S$, giving $s - s' \in M$. Since S is a fundamental domain for M in $\mathbb{R}^d$, it follows that $s = s'$, and so $m_i = m_j$, giving $i = j$.

Now choose any $v \in F$. There is a unique $s \in S$ such that $v - s = m \in M$, since S is a fundamental domain for M in $\mathbb{R}^d$. But then $s \in -m + F$, meaning that $-m = m_i$ for some i (m is unique!), so $s \in S_i$ and $v \in F_i$, as desired.

Each F_i is the translate of S_i, and so they have the same volume. Since F is the disjoint union of the F_i and S is the disjoint union of the S_i, it follows immediately that F and S have the same volume. But the volume of S is $n = [\mathbb{Z}^d : M]$ – it's the union of n hypercubes of volume 1! So we're done. $\clubsuit$

Theorem 15.3 (Minkowski)**.** *Let L be a lattice in $\mathbb{R}^n$. Let S be a subset of $\mathbb{R}^n$ with the following properties:*

- *S is symmetric: if $v \in S$, then $-v \in S$*
- *S is convex: if v and w are in S, then the line segment joining v to w is entirely contained in S.*
- *S has volume strictly greater than $2^n|\det(L)|$.*

Then S contains a nonzero vector in L.

Proof: Choose a basis $\{v_1, \ldots, v_n\}$ be a basis for L over $\mathbb{Z}$. Let T be the subset of $\mathbb{R}^n$ defined by

$$T = \{v = a_1v_1 + \ldots + a_nv_n \in \mathbb{R}^n \mid 0 \leq a_i \leq 2 \,\text{for all}\, i\}$$

The volume of T is just $2^n|\det(L)|$, by definition, almost – the 2^n comes from the stretching factor by 2.

Define $f\colon S \to T$ by

$$f(a_1 v_1 + \dots a_n v_n) = (a_1 \pmod 2) v_1 + \dots + (a_n \pmod 2) v_n$$

where $a_n \pmod 2$ denotes the unique real number r such that $r - a_n \in 2\mathbb{Z}$. So, for example, $47.23452 \pmod 2 = 1.23452$.

Now, f is the disjoint union of a bunch of translations, so on each of those pieces, it is volume-preserving. Since the volume of S is strictly greater than the volume of T, there must be some overlap between the images of those pieces. In other words, f is not injective, and there are v and w in S such that $v \neq w$ and $f(v) = f(w)$.

But this means that $v - w$ is a nonzero vector of the form $b_1 v_1 + \dots b_n v_n$, where the b_i are all even integers! Since S is convex, the vector $(v-w)/2$ is in S, because it's exactly halfway between v and w ... and it's a point in L! We retire victorious.

♣

Theorem 15.4. *Let L be a subgroup of the additive group of a normed real vector space V. If L is a discrete subgroup of V, then L is a free abelian group of rank at most* $\dim V$*.*

Proof: Let $n = \dim V$, and let $A \subset L$ be any finitely generated subgroup. We will show that A is a free abelian group of rank at most $\dim V$ – it will immediately follow that L is also a free abelian group of rank at most $\dim V$.

So assume that A is generated by $\{v_1, \dots, v_m\}$. Then A is a free abelian group (since V has no torsion), so we may assume that $\{v_1, \dots, v_m\}$ is a basis of A over $\mathbb{Z}$.

Since A is discrete, there is some $\epsilon > 0$ such that A contains no nonzero vectors of length at most ϵ. Therefore, there are no two vectors $v, w \in A$ such that $|v - w| < \epsilon$ unless $v = w$. In other words, if no nonzero vector can get within ϵ of 0, then no two distinct vectors can get within ϵ of each other. Fix this ϵ for A.

If $m > n$, then there is a linear dependence relation between the v_i. After reordering the v_i, we may assume that $\{v_1, \ldots, v_k\}$ is a maximal linearly independent subset of the v_i, and that

$$v_{k+1} = a_1 v_1 + \ldots + a_k v_k$$

where some a_i is irrational (because $\{v_1, \ldots, v_{k+1}\}$ is linearly independent over $\mathbb{Z}$). Fix this index i.

We will show that A is not discrete. Let B be the subgroup of A generated by $\{v_1, \ldots, v_k\}$, and let D be the fundamental parallelepiped for B:

$$D = \{b_1 v_1 + \ldots + b_k v_k \mid 0 \le b_j < 1 \, \text{for all} \, j\}$$

For each positive integer r, define the point

$$P_r = c_1 v_1 + \ldots + c_k v_k$$

where $c_j = r a_j \pmod 1$. That is, c_j is the unique real number in $[0, 1)$ such that $c_j - r a_j$ is an integer.

Then P_r is in D. If $P_r = P_s$ for some r and s, then $r a_j - s a_j \in \mathbb{Z}$ for all j. But then $(r - s) a_i \in \mathbb{Z}$, which because a_i is irrational means that $r = s$.

So the P_r are all different! And they're all crammed into the set D, which has bounded area. Since no two vectors in A are closer than ϵ, it follows that the balls of radius $\epsilon/2$ around the P_r are disjoint. (Any overlap would lead to a distance of less than ϵ.) Since the volume of D is finite, this is impossible, so the rank of A is at most n, as desired. ♣

16 Finite rings

Theorem 16.1. *Every prime ideal of a finite ring is maximal.*

Proof: Let P be a prime ideal of a finite ring R. Then R/P is a finite domain, so it's a field, so P is maximal. Notice that this works even if $P = 0$. ♣

We're ready to characterise finite rings now.

Theorem 16.2. *If R is a finite ring, then*

$$R \cong (R/P_1^{a_1}) \times \ldots \times (R/P_n^{a_n})$$

where the a_i are positive integers and the P_i are prime ideals of R.

Proof: Let R be a finite ring. Then it's noetherian (think about that for a sec!), so there are primes $P_1, \ldots, P_m$ of R such that $\prod P_i \subset 0$. But then for any prime P, we have $\prod P_i \subset P$, so for some i, $P_i \subset P$, and thus $P_i = P$ (since every prime ideal of a finite ring is maximal). Thus, there are only finitely many distinct primes $P_1, \ldots, P_n$ of R, satisfying $\prod P^{m_i} = 0$, where m_i is some positive integer depending only on i. Since each P_i is maximal, they're pairwise coprime, so by the Chinese Remainder Theorem, R is isomorphic to $\prod R/(P_i^{m_i})$. ♣

There's one more handy thing about finite rings.

Theorem 16.3. *Let L be a finite ring that contains a field K. The trace pairing $\langle x, y\rangle = Tr(xy)$ on L is nondegenerate if and only if L is isomorphic to a product of fields.*

Proof: We know from the previous theorem that

$$L \cong (L/P_1^{a_1}) \times \ldots (L/P_n^{a_n})$$

If some $a_i \geq 2$, then $L/P_i^{a_i}$ contains a nilpotent element: if $x \in P_i$ is nonzero, then $x^{a_i} = 0$. But then we can define the element $(0, \dots, x, \dots, 0) \in L$, where the x is in the ith place, and this element X will also be nilpotent.

This means that for any $y \in L$, the element Xy is also nilpotent (or zero) – remember that L is commutative! So the linear transformation T_{Xy} is nilpotent, so all its eigenvalues are zero, so its trace is zero. Thus, if the pairing is nondegenerate, then $a_i = 1$ for all i, and L is the product of fields.

Conversely, if L is the product of fields, then all the a_i are equal to 1. Let $x = (x_1, \dots, x_n) \in L$ be any nonzero element. We want to find another element $y \in L$ such that $\operatorname{Tr}(xy) \neq 0$.

Well, L/P_i is a field, and it must contain K. (L contains K, and L maps onto L/P_i via the ith projection homomorphism. Since homomorphisms of fields are always injective, the restriction of the ith projection to K must be injective as well.)

If for just one index i, we can find a $y_i \in L/P_i$ such that $\operatorname{Tr}_{(L/P_i)/K}(x_i y_i) \neq 0$, then we'll be done, because then $\operatorname{Tr}(xy) \neq 0$, where $y = (0, \dots, y_i, \dots, 0)$.

Since x is nonzero, there is some index i such that $x_i \neq 0$. Our problem thus reduces to showing that if L/K is an extension of finite fields, then for every $x \in L$, there is some $y \in L$ such that $\operatorname{Tr}(xy) \neq 0$.

Let $L = K(\alpha)$ by the Primitive Element Theorem. (Recall that L and K are perfect, so L/K is separable.) Consider the following matrix:

$$M = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ \alpha & \sigma_2(\alpha) & \ldots & \sigma_n(\alpha) \\ \alpha^2 & \sigma_2(\alpha)^2 & \ldots & \sigma_n(\alpha)^2 \\ \vdots & \vdots & & \vdots \\ \alpha^{n-1} & \sigma_2(\alpha)^{n-1} & \ldots & \sigma_n(\alpha)^{n-1} \end{pmatrix}$$

where $\sigma_1 = \mathrm{id}, \sigma_2, \ldots, \sigma_n$ are the elements of $\mathrm{Gal}(L/K)$.

That matrix right there brings back memories of that Vandermonde guy. In particular, the determinant of M is just

$$\det M = \prod (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

which is nonzero because L/K is separable and so all the conjugates of α are different.

Thus, the columns of this matrix are linearly independent over K. In particular, if you add them all together, you don't get the zero vector. So, for some j, we have

$$\alpha^j + \sigma_2(\alpha)^j + \ldots + \sigma_n(\alpha)^j \neq 0$$

Therefore, we conclude that

$$\mathrm{Tr}(\alpha^j) = \alpha^j + \sigma_2(\alpha)^j + \ldots + \sigma_n(\alpha)^j \neq 0$$

So let $y_i = x_i/\alpha^j$. Then $\mathrm{Tr}(x_i y_i) = \mathrm{Tr}(\alpha^j) \neq 0$, as desired. ♣

17 Finite Fields

This section is dedicated to describing all the finite fields, how they fit together, and what their Galois theory is.

The first, somewhat odd thing, is that none of this really depends on the characteristic of the fields. So we will fix a prime number p right now, for the whole section, and then pretty much forget about it.

Theorem 17.1. *Every finite field of characteristic p has cardinality p^n for some positive integer n.*

Proof: Let F be a finite field of characteristic p. Then F contains a subfield B isomorphic to $\mathbb{Z}/p\mathbb{Z}$. This means that F is a B-module, which since B is a field, is the same things as a B-vector space.

Let $v_1, \ldots, v_n$ be a basis for F as a B-vector space. Then the elements of F are precisely the linear combinations $a_1v_1 + \ldots + a_nv_n$, where $a_i \in B$. And by the magic of bases, all of those p^n linear combinations are different. So the cardinality of F is exactly p^n. ♣

Ok, ok, fine. We didn't forget about p. But we stopped worrying about what it might be.

Theorem 17.2. *Let F and F' be finite fields with p^n elements, where p is prime and n is a positive integer. Then F and F' are isomorphic. Moreover, if K is a field (possibly infinite) that contains two subfields F and F' with p^n elements, then $F = F'$.*

Proof: The nonzero elements of F form a group F^* under multiplication, and F^* has $p^n - 1$ elements. By Lagrange's Theorem, they're all roots of the polynomial $m(x) = x^{p^n-1} - 1$, which has coefficients in $\mathbb{Z}/p\mathbb{Z}$. This means that F is isomorphic to the splitting field of $m(x)$ over $\mathbb{Z}/p\mathbb{Z}$.

But F' is also isomorphic to the splitting field of $m(x)$ over $\mathbb{Z}/p\mathbb{Z}$, by the same argument with judiciously placed $'$ markers here and there. So F is isomorphic to F', as desired.

And if F and F' are both contained in some larger field K, then they are both the set of roots of $m(x)$ (plus zero) in K. There's only one such set, so $F = F'$. ♣

Theorem 17.3. *Let p be a prime number, n a positive integer. Then there is a finite field of cardinality p^n.*

Proof: Let K be a splitting field of the polynomial $m(x) = x^{p^n-1} - 1$ over $\mathbb{Z}/p\mathbb{Z}$. Then K has at least p^n elements, because it contains all the roots of $m(x)$, and it contains 0. (Note that $m(x)$ has distinct roots because its derivative $m'(x) = -x^{p^n-2}$ has only the root zero, which is not a root of $m(x)$.)

So all we need to do is show that K contains no further elements. So let a and b be two roots of $m(x)$ (or zero). We need to show that $a \pm b$, ab, and $1/a$ (if $a \neq 0$) are also roots of $m(x)$ (or zero). If we do that, then we'll know that the roots of $m(x)$ (with zero) form a field, which must therefore be its splitting field.

If a or b are zero, that's all easy, so let's assume $ab \neq 0$. We know that $a^{p^n-1} = b^{p^n-1} - 1$. So $a^{p^n} = a$ and $b^{p^n} = b$. Therefore

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n} = a \pm b$$

and

$$(ab)^{p^n} = a^{p^n} b^{p^n} = ab$$

so that $a \pm b$ and ab are roots of $xm(x)$, as desired. (Remember that $(a+b)^p = a^p + b^p$ in characteristic p, and iterating that gives $(a+b)^{p^n} = a^{p^n} + b^{p^n}$.)

Finally, if $a \neq 0$, then $1/a \in K$, and $(1/a)^{p^n} = 1/a^{p^n} = 1/a$, so $1/a$ is also a root of $m(x)$. So K is exactly the roots of $xm(x)$, and therefore has p^n roots. ♣

Theorem 17.4. *Let F be a field with p^n elements. Then F contains a subfield with p^m elements if and only if $m \mid n$.*

Proof: If $m \mid n$, then $x^{p^m} - 1$ is a factor of $x^{p^n} - 1$, so all the roots of $x^{p^m} - 1$ are also roots of $x^{p^n} - 1$, and so F contains a subfield with p^m elements.

Conversely, if F contains a subfield B with p^m elements, then F is a B-vector space. In that case, F has b^ℓ elements, where b is the cardinality of B and ℓ is the dimension of F as a B-vector space. But then $(p^m)^\ell = p^n$, so $m\ell = n$ and we're done. ♣

Theorem 17.5. *The multiplicative group of a finite field is cyclic.*

Proof: Let F be a finite field. Then F^* is a finite abelian group, so it's isomorphic to the product of cyclic groups:

$$F^* \cong (\mathbb{Z}/a_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/a_r\mathbb{Z})$$

Better yet, we can insist that $a_{i+1} \mid a_i$ for each i. To show that F^* is cyclic, it's enough to show that $a_2 = 1$.

So, assume $a_2 \neq 1$. Then there is a prime number p that divides evenly into a_2. Then p also divides evenly into a_1, because $a_2 \mid a_1$. This means that there are at least p^2 elements of F^* of order p.

But the polynomial $x^p - 1$ has at most p roots in F. So there can't be at least p^2 elements of F^* of order p in F, and so $a_2 = 1$ and F^* is cyclic, as desired. ♣

Theorem 17.6. *Let K be the finite field with p^n elements, and let L be the finite field with p^{kn} elements. Then the extension L/K is Galois, with cyclic Galois group generated by the automorphism $Frob_{L/K}(x) = x^{p^n}$.*

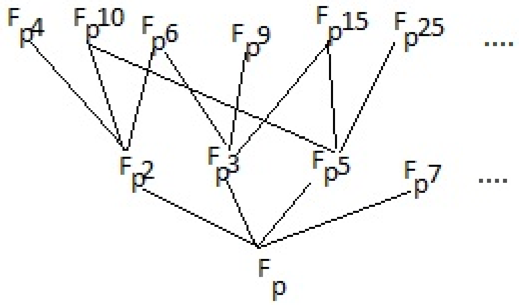
Proof: First, notice that L is a splitting field over $\mathbb{Z}/p\mathbb{Z}$, and so it's Galois over that field. Since K also contains $\mathbb{Z}/p\mathbb{Z}$, it immediately follows that L is Galois over K.

Furthermore, the automorphism $\mathrm{Frob}_{L/K}$ is an automorphism of L that fixes K pointwise. So it's an element of the Galois group $\mathrm{Gal}(L/K)$. I claim that, in fact, $\mathrm{Frob}_{L/K}$ generates the Galois group.

If you iterate $\mathrm{Frob}_{L/K}$ ℓ times, you get the automorphism $a \mapsto a^{p^{\ell n}}$. If $2 \leq \ell \leq k-1$, then the fixed set of $a \mapsto a^{p^{\ell n}}$ is exactly the roots of $x^{p^{\ell n}} - x$, which is strictly smaller than L because $\ell n < kn$. So $\mathrm{Frob}_{L/K}$ has order (in the Galois group) at least k.

But the degree $[L : K] = k$, so $\mathrm{Frob}_{L/K}$ has order at most k as well! So its order is exactly k, and so it's a generator of the cyclic Galois group $\mathrm{Gal}(L/K)$. ♣

We now have enough theorems to have a picture of how the finite fields of characteristic p fit together. Because there is a unique field (up to isomorphism, in a strong sense) with p^n elements for every prime p and positive integer n, let's give the name $\mathbb{F}_{p^n}$ to the unique (isomorphism class of) field with p^n elements. Then the lattice of finite fields of characteristic p by inclusion looks like this:



I mean, there are infinitely many of those finite fields, so we had to leave a few out. But hopefully that gives you the general idea.

And in that picture, every extension is Galois, with cyclic Galois group, generated by the appropriate Frobenius automorphism. Life is good.

18 Local rings and DVRs

Local rings are extremely useful objects in algebra. The name "local" comes from algebraic geometry, and unfortunately it's a little too much to explain the origin of the name here. But honestly, algebraic geometry is awesome and you should go learn some.

Definition 18.1. *Let A be a domain, P a prime ideal of A, K the fraction field of A. The localisation of A at P is the set*

$$A_P = \left\{ \frac{a}{b} \mid a, b \in A,\, b \notin P \right\}$$

Notice that if $a/b \in A_P$, it's still possible that $b \in P$! There are many different fractions that represent the same element of K – all you need is for *one* of them to have a denominator outside P, and the fraction ends up in A_P. Otherwise, nothing would be in A_P: if $p \in P$, then $a/b = pa/pb$.

Theorem 18.2. *The localisation of A at P is a local ring.*

Recall that a local ring is a ring with a unique maximal ideal; that is, the set of all non-units is an ideal.

Proof: Let a/b and c/d be in A_P, such that b and d are not in P. Then all of $a/b \pm c/d$ and $(a/b)(c/d)$ can be written with denominator bd. Since neither of them is in P and since P is prime, it follows that $bd \notin P$ and so A_P is closed under plus, minus, and times. Since A_P clearly contains 0 and 1, it's a subring of K.

To see the local part: the non-units are exactly the elements of K of the form a/b, where $a \in P$. (If $a/b = c/d$, then $bc = ad \in P$, so $b \notin P$ means $c \in P$. So you can't have one representation with numerator in P, but a different one where the numerator isn't in P.) This is an ideal, because if a/b and c/d satisfy $a, c \in P$ and $b, d \notin P$, then $a/b \pm c/d$ also satisfies that, as does $(a/b)(u/v)$ for any $u/v \in A_P$.

In other words, the unique maximal ideal of A_P is the ideal (of A_P) generated by P, often written P_P, or even just P if the context is clear. ♣

The magic of this section is that the localisation of $\mathcal{O}_K$ at a nonzero prime ideal is a very special and pleasant ring, called a Discrete Valuation Ring. Because of how many syllables that is, modern types call that a DVR.

Definition 18.3. *A Discrete Valuation Ring (DVR) is a noethe-*

rian local ring whose unique (nonzero) maximal ideal is principal. A generator of the maximal ideal is called a uniformizer.

The easiest example of a DVR is $\mathbb{Z}_{(p)}$, the localisation of $\mathbb{Z}$ at the prime ideal (p). This ring is all the fractions whose denominators are not divisible by p. The maximal ideal of $\mathbb{Z}_{(p)}$ is the fractions a/b where $p \mid a$, which is exactly the ideal generated by p.

Crucially important is that the quotients work out the same for the localisation as they do for $\mathcal{O}_K$ – remember that paragraph above! And indeed, in this example, we see that $\mathbb{Z}_{(p)}/p^n \cong \mathbb{Z}/p^n$, just like we want – all the extra stuff in the localisation is just units that wash away when you mod out by the nonunits.

Um. We will, um, prove all that. But first, we'll start by characterising the ideals of any DVR.

Theorem 18.4. *Let D be a DVR, I a nonzero, proper ideal of D. Then for some positive integer n, $I = M^n = (\pi^n)$, where $M = (\pi)$ is the unique maximal ideal of D. In particular, a DVR is a PID.*

Proof: Since M is principal, it's invertible, with inverse $M^{-1} = \pi^{-1}D \subset K$, where K is the fraction field of D.

Let $I_1 = IM^{-1}$. Then $I \subset I_1 \subset D$, because $D \subset M^{-1}$ and $I \subset M$. Nakayama's Lemma says we can't have $I = I_1$, so I_1 must be a strictly larger ideal than I.

If $I_1 = D$, then $I = M$ and we're done. Otherwise, $I_1 \subset M$ (remember every nonunit is contained in M!), so let $I_2 = M^{-1}I_1$. Again, $I_2 \neq I_1 = MI_2$ by Nakayama, and $I_2 \subset D$. If $I_2 = D$, then $I = M^2$ and we're done. Otherwise, we can keep going by defining, at each stage, $I_{n+1} = I_n M^{-1}$, with $I_n \subsetneqq I_{n+1} \subset D$.

Since D is noetherian, this can't go on forever, so eventually we have $I = M^n$, as desired. ♣

Another useful fact about localisation.

Theorem 18.5. *Let A be a noetherian domain, P a prime ideal of A. Then the localisation A_P is noetherian.*

Proof: Let I be an ideal of A_P. We want to show that I is finitely generated.

Consider $J = I \cap A$. Since A is noetherian, J is finitely generated, say, by $\{x_1, \ldots, x_n\}$.

If $x \in I$, then we can write $x = a/b$ for some $a, b \in A$, $b \notin P$, and so $a = xb \in I$ as well. But $a \in A$, so $a \in J$, so we can write

$$a = a_1 x_1 + \ldots + a_n x_n$$

for some $a_1, \ldots, a_n \in A$. Dividing both sides by b gives

$$x = (a_1/b)x_1 + \ldots + (a_n/b)x_n$$

with $a_i/b \in A_P$ because $b \notin P$. So I is generated by $\{x_1, \ldots, x_n\}$ as well. ♣