Introduction to rings of integers

December 4, 2013

We've been studying cyclotomic fields $\mathbb{Q}(\zeta_n)$, but we decided that it's a good idea to step back and look at more general objects.

Definition 0.1. *A* number field *is a finite extension* $F/\mathbb{Q}$.

Some examples:

1. Hilbert's favorite example: $F = \mathbb{Q}$.
2. Quadratic fields: $F = \mathbb{Q}(\sqrt{d})$, with $d \in \mathbb{Z}$ a square-free integer. (We could actually take any $d \in \mathbb{Q}$, but this would give the same list of fields.)
3. Cyclotomic fields: $F = \mathbb{Q}(\zeta_n)$.
4. More generally, we can adjoin to $\mathbb{Q}$ any *algebraic number*: the root of a polynomial with rational coefficients.

In this lecture, we'll be trying to answer the question: what is the analog of the ring $\mathbb{Z} \subset \mathbb{Q}$ for a general number field F? The answer will be a subring $\mathcal{O}_F \subset F$ called the *ring of integers* of F.

We've already seen such a ring come up in the example $F = \mathbb{Q}(\zeta_p)$. Recall that, as part of the first proof that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$, we needed to pass to the subring $\mathbb{Z}[\zeta_p]$ in order to exploit a certain interesting factorization of p. In general, the ring $\mathcal{O}_F$ lets us ask more refined questions about F, having to do with arithmetic matters such as prime numbers.

We start by abstracting a portion of the argument we used in studying $\mathbb{Z}[\zeta_p]$.

Proposition 0.2. *Let* $\alpha \in \overline{\mathbb{Q}}$ *be an algebraic number, of degree say* $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. *Denote by* $\mathbb{Z}[\alpha]$ *the ring generated by* α. *The following conditions are equivalent:*

1. *This ring* $\mathbb{Z}[\alpha]$ *is finitely generated as an abelian group.*
2. *The minimal polynomial of* α *has integer coefficients.*

Proof. $\underline{1 \Rightarrow 2}$: By the classification of finitely generated abelian groups, we have $\mathbb{Z}[\alpha] = F \oplus \mathbb{Z}^n$ for some finite F and $n \in \mathbb{N}$. But since $\mathbb{Z}[\alpha]$ lies inside a rational vector space, it has no torsion. Thus $F = 0$. So $\mathbb{Z}[\alpha] \simeq \mathbb{Z}^n$ is finite free of rank n. Note that a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$ is necessarily also a $\mathbb{Q}$-basis for $\mathbb{Q}(\alpha)$. Using this, we can compute the characteristic polynomial $p(T)$ of α acting by multiplication on $\mathbb{Q}(\alpha)$ in two ways. One, using the rational basis $1, \alpha, \ldots, \alpha^{d-1}$, shows that $p(T)$ is the minimal polynomial of α. Another using a $\mathbb{Z}$-basis of $\mathbb{Z}[\alpha]$, shows that $p(T)$ has $\mathbb{Z}$-coefficients. Thus we have 2.

$\underline{2 \Rightarrow 1}$: If the minimal polynomial of α has integer coefficients, then we have a relation $\alpha^d = c_{d-1}\alpha^{d-1} + \ldots + c_1\alpha + c_0$ for some integers c_i. Multiplying by powers of α, we see that for every $n \geq d$, the element α^n lies in the span of the previous powers of α. By induction, it follows that every power of α lies in the span of $1, \alpha, \ldots, \alpha^{d-1}$. Thus $\mathbb{Z}[\alpha]$ is generated by $\{1, \alpha, \ldots, \alpha^{d-1}\}$, so α satisfies 1. $\square$

We note that the proof of $2 \Rightarrow 1$ actually gives us extra information. The same argument shows that these equivalent conditions hold even if we only assume a weaker version of 2: it's enough for α to be the root of *some* monic polynomial with integer coefficients. We also get an automatic strengthening of 1: in fact $\mathbb{Z}[\alpha]$ is a free abelian group of rank d, and even admits a $\mathbb{Z}$-basis given by $\{1, \alpha, \ldots, \alpha^{d-1}\}$.

The previous proposition motivates the following definition:

Definition 0.3. *An algebraic number $\alpha \in \overline{\mathbb{Q}}$ is called* integral*, or an* algebraic integer*, if it satisfies the equivalent conditions of the previous proposition (i.e., $\mathbb{Z}[\alpha]$ is finitely generated as an abelian group, or α is the root of a monic polynomial with integer coefficients.)*

So we have both a "linear algebra" criterion for integrality and a "polynomial" criterion. The equivalence of these criteria is akin to the fact from field theory that an element is algebraic if and only if it generates a finite extension field. Now we have this analog "over $\mathbb{Z}$", and we call the resulting notion "integrality".

There's also another way of thinking about this. The ring $\mathbb{Z}[\alpha]$ being finitely generated as an abelian group signifies that, intuitively speaking, α doesn't have any denominators. Reason being, if α had denominators, then the powers of α, which lie in $\mathbb{Z}[\alpha]$, would have denominators which grow without bound. But a finite generating set would give a bound for how bad the denominators could be: namely, the product of the denominators of the generators. So if α had denominators, then $\mathbb{Z}[\alpha]$ couldn't be finitely generated. If we made this rigorous it would lead to another proof of the previous proposition, but we'll just leave it as intuition.

So, it seems that the integrality of α means that $\mathbb{Z}[\alpha]$ is a promising candidate for $\mathcal{O}_F$, at least when $F = \mathbb{Q}(\alpha)$. For example, as we remarked after the proposition, the rank of $\mathbb{Z}[\alpha]$ as a $\mathbb{Z}$-module is the same as the rank of F as a $\mathbb{Q}$-vector space. So $\mathbb{Z}[\alpha]$ has approximately the right size.

But there's a problem, which is that the ring $\mathbb{Z}[\alpha]$ can depend on α, even if the field $\mathbb{Q}(\alpha)$ didn't. You can convince yourself of this by considering both α and 5α, say. Furthermore, and this is a subtle point which we'll come back to later, these rings $\mathbb{Z}[\alpha]$ are not as well-behaved as they could be. They're trying their darndest, but the little guys don't quite get there. It turns out we sort of got lucky in the cyclotomic case with $\mathbb{Z}[\zeta_p]$. In general, one actually needs to take the ring generated by more than one integral element of F: the "primitive element theorem" fails over $\mathbb{Z}$.

But how do we know which elements to pick, how many we need, and so on? Those are not easy questions to answer. Thankfully, it's possible to give a tricky (but beautiful!) definition of $\mathcal{O}_F$ which dodges them (at first):

Definition 0.4. *We define $\mathcal{O}_F \subset F$ to be the set of all integral elements of F.*

Don't worry about which α's to pick: just take them all! The trickiness is in the fact that many properties which were easy to see for the rings $\mathbb{Z}[\alpha]$ are not at all obvious for this $\mathcal{O}_F$. Chief among these are:

1. $\mathcal{O}_F$ is indeed a ring.

2. $\mathcal{O}_F$ is finitely generated as an abelian group.

But this defect of $\mathcal{O}_F$ will be overcome once we prove these properties, and anyway it's well offset by the fact that $\mathcal{O}_F$ was canonically described in terms of F, no ad hoc choices of generator α being required.

We'll prove 1 right now, but 2 will wait until next time, when we introduce the Geometry of Numbers, which enhances all of this business with a beautiful picture of $\mathcal{O}_F$.

The proof of 1 is an integral adaptation of the proof of the analogous result in field theory.

Proposition 0.5. *$\mathcal{O}_F$ is a subring of F.*

Proof. First, note that certainly 0 and ± 1 are integral, and so lie in $\mathcal{O}_F$. To see that $\mathcal{O}_F$ is closed under $+$ and $\times$, suppose that α and β are integral. Thus $\mathbb{Z}[\alpha]$ and $\mathbb{Z}[\beta]$ are finitely generated as abelian groups, say by $a_1, \ldots, a_n$ and $b_1, \ldots, b_m$. Then the subring $\mathbb{Z}[\alpha, \beta]$ generated by both α and β is generated by the $n \cdot m$ different products $a_i b_j$. In particular, it is finitely generated. But the rings $\mathbb{Z}[\alpha+\beta]$ and $\mathbb{Z}[\alpha\beta]$ lie inside $\mathbb{Z}[\alpha, \beta]$, and a subgroup of a finitely generated abelian group is also finitely generated. We conclude that $\alpha + \beta$ and $\alpha\beta$ are integral, making $\mathcal{O}_F$ a ring as claimed. □

To finish this lecture, we'll discuss some simple examples.

Example 1: We had better check that $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. Well, the minimal polynomial of $\alpha \in \mathbb{Q}$ is $X - \alpha$. So the minimal polynomial has integer coefficients if and only if $\alpha \in \mathbb{Z}$. You could also do this example using the "linear algebra" definition of integral, by making precise the "has no denominators" picture discussed above.

Example 2: Let's look at quadratic fields, say $\mathbb{Q}(\sqrt{d})$ with d a square-free integer. Which elements $\alpha = a + b\sqrt{d}$ are integral? We again check the minimal polynomial. This is given by $(X - \alpha)(X - \alpha')$, where α' is the nontrivial Galois conjugate of α, i.e. $\alpha' = a - b\sqrt{d}$. Expanding out we get

$$X^2 - 2aX + [a^2 - db^2].$$

Thus α is integral if and only if $2a \in \mathbb{Z}$ and $a^2 - db^2 \in \mathbb{Z}$. So a is allowed to be a half-integer, but then looking at the second equation, we see that b must also be a half-integer to get the denominator of 4 to cancel. Moreover, this cancellation can only happen if d is congruent to $1 \pmod 4$. The upshot is that unless d is $1 \pmod 4$, the only integers are the "obvious" ones: $a + b\sqrt{d}$ with $a, b \in \mathbb{Z}$. In other words, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$. But if d is $1 \pmod 4$, then a and b are allowed to simultaneously be half-integers as well. In this case we can say $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$.

Example 3: It turns out that the cyclotomic fields $\mathbb{Q}(\zeta_n)$ are less exotic than the quadratic fields in this regard: we actually have the simple answer $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ for all n. We'll probably prove this later.

Note that examples 2 and 3 are compatible: recall that the cyclotomic field $\mathbb{Q}(\zeta_n)$ is quadratic when $n = 3, 4$ or 6. In the first and last cases we get $\mathbb{Z}[\sqrt{-3}]$, but the cyclotomic picture gives us the more refined integral generators $\zeta_3 = \frac{-1+\sqrt{-3}}{2}$ and $\zeta_6 = \frac{1+\sqrt{-3}}{2}$, denominator of 2 and all. In the second case, of course, we just get $\mathbb{Z}[\sqrt{-1}]$ in any case. But note the consistency with the fact that -1 is $3 \pmod 4$ but -3 is $1 \pmod 4$.

I was reminded by Martin after class that $d = 5$ also gives a good example of this phenomenon. The golden ratio has a 2 in the denominator. (Actually, that's a bad way of speaking. You should think of it as having no denominators. Instead think that the numerator has a hidden factor of 2 in it.) And the golden ratio is perhaps the simplest algebraic integer out there!