Math 154. A non-primitive ring of integers

The aim of this handout is to explain Dedekind's example of a cubic field K for which $\mathscr{O}_K$ does not have the form $\mathbf{Z}[\alpha]$ for any integral primitive element α of K. In fact, we'll even see that whatever α we choose, the index $[\mathscr{O}_K : \mathbf{Z}[\alpha]]$ is always divisible by a common prime p, so the "Dedekind criterion" for factoring $p\mathscr{O}_K$ really cannot always be expected to work for every p by artful choice of α. This shows that in general, factorization in $\mathscr{O}_K$ lies somewhat deeper than factoring in $\mathbf{F}_p[X]$, at least for a few thorny primes p.

1. Motivation

The basic idea behind Dedekind's example is easier to understand if presented in a slightly more general setting. Suppose $K/\mathbf{Q}$ is a number field of degree d and that some prime $p < d$ is totally split in K (such as 2 being totally split in a cubic field); the real work will be to actually find such an example, since we'll see that in such cases the Dedekind factorization criterion cannot be applied (so we need some new idea to verify that p is really totally split in K in such situations). For now, let us simply accept that we have such a K and p.

I claim that necessarily $p|[\mathscr{O}_K : \mathbf{Z}[\alpha]]$ for *every* integral primitive element α for $K/\mathbf{Q}$ (so in particular, $\mathscr{O}_K \neq \mathbf{Z}[\alpha]$ for any α). The reason is as follows. In the handout on Dedekind's criterion, we saw that if p does not divide the index, then the natural map of *rings* $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \to \mathscr{O}_K/p\mathscr{O}_K$ is an isomorphism. Letting $h \in \mathbf{Z}[X]$ be the minimal polynomial of α, we have $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] = \mathbf{F}_p[X]/(\overline{h})$ with $\overline{h} = h \bmod p$ monic of degree d. Now comes the clever idea: let's count the number of maps $\mathscr{O}_K/p\mathscr{O}_K \to \mathbf{F}_p$ as *rings* in two different ways.

First of all, if there is a presentation as $\mathbf{F}_p[X]/(\overline{h})$ then a ring map $\mathscr{O}_K/p\mathscr{O}_K \to \mathbf{F}_p$ is nothing more or less than a ring map $\mathbf{F}_p[X] \to \mathbf{F}_p$ that kills $\overline{h}$; i.e., it is a root of $\overline{h}$ in $\mathbf{F}_p$. The number of such roots is at most the size of $\mathbf{F}_p$, which is to say that it is at most p. Thus, *if* p does not divide $[\mathscr{O}_K : \mathbf{Z}[\alpha]]$ for some α then the number of ring maps $\mathscr{O}_K/p\mathscr{O}_K \to \mathbf{F}_p$ is at most p.

On the other hand, if p is totally split in K, so $p\mathscr{O}_K = \prod_{i=1}^{d} \mathfrak{p}_i$ for $d = [K : \mathbf{Q}]$ primes ideals $\mathfrak{p}_i$ with $\mathscr{O}_K/\mathfrak{p}_i = \mathbf{F}_p$ for all i then we get d *distinct* ring maps $\mathscr{O}_K/p\mathscr{O}_K \to \mathscr{O}_K/\mathfrak{p}_i = \mathbf{F}_p$ (distinctness due to comparing the kernels, namely $\mathfrak{p}_i/p\mathscr{O}_K$ for all i). But we just got an upper bound of p on the number of such distinct ring maps if p does not divide $[\mathscr{O}_K : \mathbf{Z}[\alpha]]$ for some α. Hence, if $d > p$ then we have more distinct maps than this upper bound, and so have a contradiction! That is, if a prime p totally splits in a number field $K/\mathbf{Q}$ of degree $d > p$ then $p|[\mathscr{O}_K : \mathbf{Z}[\alpha]]$ for *all* integral primitive elements α of K as claimed!

2. The example

The smallest prime p is 2, so the simplest place to search for an example satisfying the above hypotheses is cubic fields in which 2 is totally split. This is what we will now present, but observe that we cannot use the Dedekind criterion to verify the totally split property, since we've just shown that in any possible example there is no α for which Dedekind's criterion actually applies using $\mathbf{Z}[\alpha]$.

Let $K = \mathbf{Q}(\theta)$ where $\theta^3 + \theta^2 - 2\theta + 8 = 0$. (You should check that this cubic is indeed irreducible over $\mathbf{Q}$.) One computes via traces of powers of θ (with the help of the cubic minimal polynomial of θ) that $D(1, \theta, \theta^2) = -4 \cdot 503$, so since $D(1, \theta, \theta^2) = [\mathscr{O}_K : \mathbf{Z}[\theta]]^2 \mathrm{disc}(K)$, we must have that either $\mathscr{O}_K = \mathbf{Z}[\theta]$ with discriminant $-4 \cdot 503$ or $[\mathscr{O}_K : \mathbf{Z}[\theta]] = 2$ and K has discriminant -503. We verify that the latter option is what occurs by exhibiting an explicit element $\beta \in \mathscr{O}_K$ not in $\mathbf{Z}[\theta]$. Define $\beta = (\theta + \theta^2)/2$. Using the minimal polynomial for θ over $\mathbf{Q}$, one can compute the matrix for multiplication by β on K relative to the ordered basis $\{1, \theta, \theta^2\}$. This matrix comes out to be

$$\begin{pmatrix} 0 & -4 & 0 \\ 1/2 & 1 & -4 \\ 1/2 & 0 & 1 \end{pmatrix},$$

so its characteristic polynomial is $X^3 - 2X^2 + 3X - 10 \in \mathbf{Z}[X]$. Thus, by Cayley-Hamilton (as we saw in an earlier class), β must satisfy this cubic polynomial; it is even the minimal polynomial, since visibly $\beta \notin \mathbf{Q}$

(forcing $\mathbf{Q}(\beta) = K$ for degree reasons). This shows that $\beta \in \mathscr{O}_K$, and by inspection $\beta \notin \mathbf{Z}[\theta]$ (as $\mathbf{Z}[\theta]$ is spanned over $\mathbf{Z}$ by $\{1, \theta, \theta^2\}$).

So far we have proved that $\mathrm{disc}(K) = -503$. This is not divisible by 2, so 2 is *unramified* in K. Let's show by an indirect argument that it must be totally split. To factor $2\mathscr{O}_K$, we will get some nontrivial relations by computing a few norms of elements of K. We compute $\mathrm{N}_{K/\mathbf{Q}}(\theta)$ and $\mathrm{N}_{K/\mathbf{Q}}(\theta + 1)$. Inspecting the minimal polynomial of θ over $\mathbf{Q}$, we see that $\mathrm{N}_{K/\mathbf{Q}}(\theta) = -8$, so $\theta\mathscr{O}_K$ is a product of primes over 2 (perhaps with some multiplicity). Likewise, the minimal polynomial of $\theta + 1$ is

$$(X-1)^2 + (X-1)^2 - 2(X-1) + 8 = X^3 - 2X^2 - X + 10,$$

so $\mathrm{N}_{K/\mathbf{Q}}(\theta + 1) = -10$. It follows that the prime factorization of $(\theta + 1)$ must have the form

$$(\theta + 1) = \mathfrak{p}_2\mathfrak{p}_5$$

for some prime ideals $\mathfrak{p}_2$ and $\mathfrak{p}_5$ with respective norms 2 and 5.

Aha, so we found a prime ideal $\mathfrak{p}_2$ with norm 2! This must be one of the prime factors of $2\mathscr{O}_K$, and by *unramifiedness* we know that $2\mathscr{O}_K$ is a product of distinct primes without repetition. Hence, either $2\mathscr{O}_K = \mathfrak{p}_2\mathfrak{p}'_2$ with $\mathfrak{p}'_2$ of norm 4 or else $2\mathscr{O}_K = \mathfrak{p}_2\mathfrak{p}'_2\mathfrak{p}''_2$ with $\mathfrak{p}'_2$ and $\mathfrak{p}''_2$ both of norm 2. This latter case is exactly the totally split case, so we just have to rule out the possibility $2\mathscr{O}_K = \mathfrak{p}_2\mathfrak{p}'_2$ with $\mathfrak{p}'_2$ a prime of norm 4. Suppose we're in the latter case. Since $\mathrm{N}_{K/\mathbf{Q}}(\theta) = -8$, so the ideal (θ) has norm 8, we know that (θ) is a product of powers of $\mathfrak{p}_2$ and $\mathfrak{p}'_2$ (the only primes over 2). But we constructed $\mathfrak{p}_2$ as one of the prime factors of $(\theta + 1)$, so $\theta + 1 \in \mathfrak{p}_2$ and hence certainly $\theta \notin \mathfrak{p}_2$ (why not?). It follows that $\mathfrak{p}_2$ *cannot* appear as a prime factor of (θ), leaving as the only possibility that (θ) is a power of $\mathfrak{p}'_2$. But that's impossible, since if $(\theta) = {\mathfrak{p}'_2}^r$ for some integer r then taking norms of both sides gives that $8 = 4^r$, an absurdity. This contradiction rules out the case $2\mathscr{O}_K = \mathfrak{p}_2\mathfrak{p}'_2$, leaving as the only remaining option that 2 is totally split in K. Observe how indirect this argument is.