Math 154. Dedekind's factorization criterion

The aim of this handout is to give a proof of Dedekind's criterion for computing the prime factorization of $p\mathscr{O}_K$ for a prime number $p > 0$ and a number field K. The initial setup is to consider $\alpha \in \mathscr{O}_K$ that is primitive for $K/\mathbf{Q}$, so $\mathbf{Z}[\alpha]$ is an order in $\mathscr{O}_K$, and to assume that $p \nmid [\mathscr{O}_K : \mathbf{Z}[\alpha]]$. (Recall that in practice, a sufficient criterion for p to satisfy this condition is that $p^2 \nmid d(1, \alpha, \dots, \alpha^{n-1})$ with $n = [K : \mathbf{Q}]$, so all but finitely many p are covered in this way.) Let $h \in \mathbf{Z}[X]$ denote the minimal polynomial of α over $\mathbf{Q}$, so $\mathbf{Z}[\alpha] \simeq \mathbf{Z}[X]/(h)$. Passing to the reduction modulo p, we get a ring isomorphism $\mathbf{Z}[\alpha]/p \cdot \mathbf{Z}[\alpha] \simeq \mathbf{F}_p[X]/(\overline{h})$ where $\overline{h} := h \bmod p \in \mathbf{F}_p[X]$. The idea behind Dedekind's criterion is to relate the monic irreducible factorization of $\overline{h}$ in $\mathbf{F}_p[X]$ to the prime ideal factorization of $p\mathscr{O}_K$ by interpreting each in terms of the ring structure of $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$. In class we saw some worked examples of this with $K = \mathbf{Q}(\alpha)$ for $\alpha^3 = 10$. Below we also give another class of examples with $\mathbf{Z}[\alpha] = \mathscr{O}_K$.

1. Main result and proof

Here is Dedekind's result.

Theorem 1.1. *With notation and hypotheses as above, especially that $p \nmid [\mathscr{O}_K : \mathbf{Z}[\alpha]]$, let $\prod \overline{h}_i^{e_i}$ denote the monic irreducible factorization of $\overline{h}$. Then the prime factorization of $p\mathscr{O}_K$ has the form*

$$p\mathscr{O}_K = \prod \mathfrak{p}_i^{e_i}$$

where $\mathfrak{p}_i = (p, h_i(\alpha))$ for any $h_i \in \mathbf{Z}[X]$ lifting $\overline{h}_i \in \mathbf{F}_p[X]$. Moreover, there is an isomorphism of residue fields $\mathbf{F}_p[X]/\overline{h}_i \simeq \mathscr{O}_K/\mathfrak{p}$ via $X \mapsto \alpha \bmod \mathfrak{p}$, so the residue field degree $f_i = [\mathscr{O}_K/\mathfrak{p}_i : \mathbf{F}_p]$ is equal to $\deg \overline{h}_i$.

In this theorem, we are not taking $(p, h_i(\alpha))$ as the definition of $\mathfrak{p}_i$; rather, we *define* the $\mathfrak{p}_i$'s to be the pairwise distinct prime factors of $p\mathscr{O}_K$ and are claiming that after suitable re-indexing if necessary we can arrange that $\mathfrak{p}_i = (p, h_i(\alpha))$ for all i.

The key to getting the proof off the ground is the observation that since the injection $\mathbf{Z}[\alpha] \to \mathscr{O}_K$ has finite index not divisible by p (by hypothesis), the induced ring map $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \to \mathscr{O}_K/p\mathscr{O}_K$ is an isomorphism. This is a special case of:

Lemma 1.2. *Let $M' \to M$ be an injective map of abelian groups such that M/M' has finite order not divisible by p. The induced map $M'/pM' \to M/pM$ is an isomorphism.*

Proof. Let $n = \#(M/M')$, so n is not divisible by p and hence multiplication by p on the finite abelian group M/M' is an automorphism (bijective). Hence, for each $m \in M$ there exists $m_1 \in M$ such that $pm_1 \equiv m \bmod M'$, so $m - pm_1 \in M'$. This shows that $M'/pM' \to M/pM$ is surjective. For injectivity, suppose $m' \in M' \cap pM$. We want $m' \in pM'$. Writing $m' = pm$ for some $m \in M$, we have that the residue class $[m] \in M/M'$ is killed by multiplication by p. But this multiplication map is an automorphism on M/M', so $[m] = 0$ and hence $m \in M'$. Thus, $m' = pm \in pM'$ as desired. ■

Applying this lemma as indicated above, the assumption $p \nmid [\mathscr{O}_K : \mathbf{Z}[\alpha]] = \#(\mathscr{O}_K/\mathbf{Z}[\alpha])$ (a quotient of additive groups) implies that the natural ring map

$$\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \to \mathscr{O}_K/p\mathscr{O}_K \tag{1}$$

is an isomorphism. In particular, this isomorphism carries ideals to ideals in both directions, yet the ideals on the left side are $I/p\mathbf{Z}[\alpha]$ for ideals $I \subseteq \mathbf{Z}[\alpha]$ which contain p. Under the ring map the image is $(I + p\mathscr{O}_K)/p\mathscr{O}_K$ and this must be $J/p\mathscr{O}_K$ for the ideal $J \subseteq \mathscr{O}_K$ generated by I (which contains p). In other words, necessarily $J = I\mathscr{O}_K$. Thus, the ring isomorphism (1) carries $I/p\mathbf{Z}[\alpha]$ isomorphically over to $I\mathscr{O}_K/p\mathscr{O}_K$ for ideals $I \subseteq \mathbf{Z}[\alpha]$ containing p, and so injectivity of the resulting map $I/p\mathbf{Z}[\alpha] \to I\mathscr{O}_K/p\mathscr{O}_K$ implies that $\mathbf{Z}[\alpha] \cap I\mathscr{O}_K = I$ for all such I. In particular, *every* ideal J of $\mathscr{O}_K$ containing p has the form $J = I\mathscr{O}_K$ for a *unique* ideal I of $\mathbf{Z}[\alpha]$ that contains p.

Since the ring isomorphism (1) carries $I/p\mathbf{Z}[\alpha]$ over onto $I\mathscr{O}_K/p\mathscr{O}_K$, passing to the induced isomorphism of quotients by these ideals gives that the natural map $\mathbf{Z}[\alpha]/I \to \mathscr{O}_K/I\mathscr{O}_K$ is an isomorphism. In particular, one side is a domain if and only if the other is, which is to say that I is a prime ideal if and only if $I\mathscr{O}_K$ is a prime ideal, where I is an ideal of $\mathbf{Z}[\alpha]$ containing p. From this we see that the *pairwise distinct* prime ideals $\mathfrak{p}_i$ of $\mathscr{O}_K$ containing p (i.e., dividing $p\mathscr{O}_K$, as $\mathscr{O}_K$ is Dedekind, in possible contrast with $\mathbf{Z}[\alpha]$) are $\wp_i\mathscr{O}_K$ where $\wp_i$ ranges through the *pairwise distinct* prime ideals of $\mathbf{Z}[\alpha]$ containing p. Also, the isomorphism $\mathbf{Z}[\alpha]/I \simeq \mathscr{O}_K/I\mathscr{O}_K$ as explained already includes as a special case $\mathbf{Z}[\alpha]/\wp_i \simeq \mathscr{O}_K/\wp_i\mathscr{O}_K = \mathscr{O}_K/\mathfrak{p}_i$.

Suppose we could show (after suitable rearranging of the irreducible factors of $\overline{h}$ over $\mathbf{F}_p$) that $\wp_i = p\mathbf{Z}[\alpha] + h_i(\alpha)\mathbf{Z}[\alpha]$ for all i. Then we would have $\mathfrak{p}_i = \wp_i\mathscr{O}_K = (p, h_i(\alpha))$ as ideals in $\mathscr{O}_K$, as desired. Let us now establish this description of the $\wp_i$'s. A prime ideal of $\mathbf{Z}[\alpha]$ containing p corresponds to the kernel of a quotient mapping from $\mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \simeq \mathbf{F}_p[X]/(\overline{h})$ onto a finite domain (and so equivalently, onto a finite field). By the Chinese Remainder Theorem, we have a ring isomorphism

$$\mathbf{F}_p[X]/(\overline{h}) \simeq \prod_i \mathbf{F}_p[X]/(\overline{h}_i)^{e_i'}.$$

The field quotients of this ring correspond to the monic irreducible factors $\overline{h}_i$ of $\overline{h}$, which is to say that the kernels of its maps onto fields are the ideals $(\overline{h}_i)$. But $h_i(\alpha) \in \mathbf{Z}[\alpha]$ maps to $\overline{h}_i \bmod \overline{h}$ in $\mathbf{F}_p[X]/(\overline{h}) = \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$, so the ideals $p\mathbf{Z}[\alpha] + h_i(\alpha)\mathbf{Z}[\alpha]$ in $\mathbf{Z}[\alpha]$ are the preimages of the ideals $(\overline{h}_i)$ in $\mathbf{F}_p[X]/(\overline{h}) = \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha]$. Hence, after suitable re-indexing if necessary, there are precisely the $\wp_i$'s, as desired.

Having described each $\wp_i$, we also get a description of the residue field: the isomorphism (1) carries $\wp_i/(p\mathbf{Z}[\alpha])$ over to $\mathfrak{p}_i/p\mathscr{O}_K$ and hence passing to the quotient gives an isomorphism of finite fields $\mathbf{Z}[\alpha]/\wp_i \simeq \mathscr{O}_K/\mathfrak{p}_i$. But

$$\mathbf{Z}[\alpha]/\wp_i = \mathbf{Z}[X]/(h, p, h_i) \simeq \mathbf{F}_p[X]/(\overline{h}, \overline{h}_i) \simeq \mathbf{F}_p[X]/(\overline{h}_i)$$

with α corresponding to the residue class of X, so this gives the desired description of the residue fields (and formula for the residue field degrees over $\mathbf{F}_p$).

Finally, we have to show that the multiplicity e_i' of $\mathfrak{p}_i$ in $p\mathscr{O}_K$ is equal to the multiplicity e_i of $\overline{h}_i$ as an irreducible factor of $\overline{h}$. For this we revisit the Chinese Remander Theorem. This gives a ring-theoretic isomorphism

$$\mathscr{O}_K/p\mathscr{O}_K \simeq \prod \mathscr{O}_K/\mathfrak{p}_i^{e_i'},$$

so the number of distinct positive powers of the ideal $\mathfrak{p}_i/p\mathscr{O}_K$ is e_i' by inspection. But the ring isomorphism

$$\mathbf{F}_p[X]/(\overline{h}) \simeq \mathbf{Z}[\alpha]/p\mathbf{Z}[\alpha] \simeq \mathscr{O}_K/p\mathscr{O}_K$$

carries the ideal $(\overline{h}_i)/(\overline{h})$ over to the ideal $\mathfrak{p}_i/p\mathscr{O}_K$, so the number of distinct positive powers of $(\overline{h}_i)/(\overline{h})$ is e_i'. However, this count is also visibly equal to the multiplicity e_i of $\overline{h}_i$ as an irreducible factor of $\overline{h}$, so $e_i = e_i'$.

2. A cubic example

Let $K = \mathbf{Q}(\alpha)$ with $\alpha^3 + 10\alpha + 1 = 0$. The cubic polynomial $f = X^3 + 10X + 1 \in \mathbf{Z}[X]$ is irreducible over $\mathbf{Q}$ because it does not have a rational root, and $\mathbf{Z}[\alpha]$ is an order in $\mathscr{O}_K$. A direct calculation shows $\operatorname{disc}(\mathbf{Z}[\alpha]/\mathbf{Z}) = -4027$, and this is prime. Hence, $\mathscr{O}_K = \mathbf{Z}[\alpha]$ and so Dedekind's criterion is applicable for all p and the only ramified prime is 4027.

The prime $p = 2$ is unramified, and in fact

$$X^3 + 10X + 1 \equiv (X+1)(X^2+X+1) \bmod 2$$

is the irreducible factorization in $\mathbf{F}_2[X]$. We use the obvious lifts of these monic irreducibles to $\mathbf{Z}[X]$, so $2\mathscr{O}_K = (2, \alpha+1)(2, \alpha^2+\alpha+1) = \mathfrak{P}_1\mathfrak{P}_2$ with $f_1 = \deg(X+1) = 1$ and $f_2 = \deg(X^2+X+1) = 2$. Note that $\sum e_i f_i = 1 + 2 = 3 = [K : \mathbf{Q}]$, as it should be.

The prime $p = 4027$ is ramified, and in fact one checks

$$X^3 + 10X + 1 \equiv (X + 2215)^2(X + 3624) \bmod 4027$$

in $\mathbf{F}_{4027}[X]$. Using the obvious lifts of these monic linear factors to $\mathbf{Z}[X]$, we get

$$4027\mathscr{O}_K = (4027, \alpha + 2215)^2(4027, \alpha + 3624) = \mathfrak{Q}_1^2\mathfrak{Q}_2,$$

so $e_1 = 2$ and $e_2 = 1$ with both $\mathfrak{Q}_i$'s having residue field degree 1 over $\mathbf{F}_{4027}$. Note that $\sum e_i f_i = 2 + 1 = 3 = [K : \mathbf{Q}]$, as it should be.