Math 154. Some examples of ideal factorization

Let $K = \mathbf{Q}(\sqrt{-5})$, so $\mathscr{O}_K = \mathbf{Z}[\sqrt{-5}] = \mathbf{Z}[X]/(X^2+5)$. This has discriminant -20, so the ramified primes are precisely 2 and 5. For any prime p, $\mathscr{O}_K/(p) = \mathbf{F}_p[X]/(X^2+5)$. In class we saw that this implies $(2) = \mathfrak{p}_2^2$ for $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$ and that $(5) = \mathfrak{p}_5^2$ for $\mathfrak{p}_5 = (\sqrt{-5})$. We also recorded for the other p exactly which ones satisfy that -5 is a square or not modulo p (using quadratic reciprocity to work out possibilities for the Legendre symbol $(-5|p) = (-1|p)(5|p) = (-1)^{(p-1)/2}(5|p)$ depending on $p \bmod 20$; if you don't see how to do that quadratic reciprocity argument, please ask me about it). In particular, for $p \equiv 11, 13, 17, 19 \bmod 20$ we have that -5 is not a square mod p, so $p\mathscr{O}_K$ is prime. On the other hand, for $p \equiv 1, 3, 7, 9 \bmod 20$ we have that $p\mathscr{O}_K = \mathfrak{p}\mathfrak{p}'$ for distinct primes $\mathfrak{p}$ and $\mathfrak{p}'$. In this handout we use this to work out some prime ideal factorizations for principal ideals $\alpha\mathscr{O}_K$ for several different elements α.

1. Conjugation of prime factors

Before taking up the examples, we address a general fact in the split case. In this case, since $p\mathscr{O}_K$ is preserved under the conjugation automorphism of K (i.e., the nontrivial element of $\mathrm{Gal}(K/\mathbf{Q})$, denoted $z \mapsto \overline{z}$), this conjugation must permute the pair of prime ideals $\mathfrak{p}$ and $\mathfrak{p}'$ dividing $p\mathscr{O}_K$ (as it certainly carries prime ideals to prime ideals, and prime ideal factorization is *unique* up to rearrangement).

Lemma 1.1. *Let K be a quadratic field, and p a rational prime that is split in K: $p\mathscr{O}_K = \mathfrak{p}\mathfrak{p}'$ with $\mathfrak{p}' \neq \mathfrak{p}$. The conjugation element of* $\mathrm{Gal}(K/\mathbf{Q})$ *swaps $\mathfrak{p}$ and $\mathfrak{p}'$; equivalently, $\mathfrak{p}' = \overline{\mathfrak{p}}$.*

Proof. We know that $\overline{\mathfrak{p}}$ is a prime ideal factor of $\overline{p\mathscr{O}_K} = p\mathscr{O}_K$, so it is equal to $\mathfrak{p}$ or $\mathfrak{p}'$. Hence, it would suffice to rule out the first option. Let us begin by presenting a bogus method to rule it out. Suppose that $\overline{\mathfrak{p}} = \mathfrak{p}$. By uniqueness of prime factorization, we likewise would have that $\overline{\mathfrak{p}'} = \mathfrak{p}'$. This says that the ideals $\mathfrak{p}$ and $\mathfrak{p}'$ in $\mathscr{O}_K$ are carried to themselves the Galois group, so surely by Galois theory it should be the case that each arises from an ideal of $\mathbf{Z}$, say $n\mathbf{Z}$ and $n'\mathbf{Z}$ for positive integers n and n'. That is, $\mathfrak{p} = n\mathscr{O}_K$ and $\mathfrak{p}' = n'\mathscr{O}_K$, so $p\mathscr{O}_K = nn'\mathscr{O}_K$. Intersecting with $\mathbf{Z}$, this says $p\mathbf{Z} = nn'\mathbf{Z}$, so either $n = 1$ or $n' = 1$, contradicting that $n\mathscr{O}_K = \mathfrak{p}$ and $n'\mathscr{O}_K = \mathfrak{p}'$ are proper ideals in $\mathscr{O}_K$. The error in the argument is that a Galois-stable ideal need *not* arise from an ideal in the ring of integers of the ground field. For example, with $K = \mathbf{Q}(\sqrt{-5})$ the unique prime ideals $\mathfrak{p}_2$ and $\mathfrak{p}_5$ of $\mathscr{O}_K$ over 2 and 5 respectively are Galois-stable by uniqueness. Since $(2) = \mathfrak{p}_2^2$ and $(5) = \mathfrak{p}_5^2$, taking norms gives $4 = \mathrm{N}\mathfrak{p}_2^2$ and $25 = \mathrm{N}\mathfrak{p}_5^2$, or in other words $\mathrm{N}\mathfrak{p}_2 = 2$ and $\mathrm{N}\mathfrak{p}_5 = 5$. Neither of these is a square in $\mathbf{Z}$, so neither of $\mathfrak{p}_2$ or $\mathfrak{p}_5$ can have the form $n\mathscr{O}_K$ for $n \in \mathbf{Z}$ (though note that $\mathfrak{p}_5$ *is* a principal ideal of $\mathscr{O}_K$, just not with a generator from $\mathbf{Z}$).

Now we give a valid proof, using our concrete understanding of the prime factors of $p\mathscr{O}_K$ in the split case. (Later we will see a more conceptual approach to such matters.) We have $K = \mathbf{Q}(\sqrt{d})$ for a unique squarefree $d \in \mathbf{Z}$. To give a uniform treatment of all cases, and especially not to have to do extra contortions for $p = 2$, we let $D = \mathrm{disc}(K/\mathbf{Q})$, so $D = 4d$ if $d \equiv 2, 3 \bmod 4$ and $D = d$ if $d \equiv 1 \bmod 4$. Recall that $\mathscr{O}_K = \mathbf{Z}[X]/(X^2 - DX + (D^2-D)/4)$ always. Since we are in the split case, $p \nmid D$ and in $\mathbf{F}_p[X]$ we have

$$X^2 - DX + (D^2 - D)/4 = (X - u_0)(X - D + u_0)$$

for some $u_0 \in \mathbf{F}_p$. At the expense of possibly swapping the labels of $\mathfrak{p}$ and $\mathfrak{p}'$ if necessary, we have

$$\mathfrak{p} = (p, (D+\sqrt{D})/2 - u),\ \ \mathfrak{p}' = (p, (D+\sqrt{D})/2 - D + u) = (p, (-D+\sqrt{D})/2 + u) = (p, (D-\sqrt{D})/2 - u)$$

for any $u \in \mathbf{Z}$ lifting $u_0 \in \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$; the final equality above comes from negating one of the generators of the ideal, a harmless operation. (Note that if we replace u with $u + pt$ for some $t \in \mathbf{Z}$ then these formulas for the ideals really do not change, as we know they cannot, since p visibly lies in each ideal.) Now from the formula for $\mathfrak{p}$ we see that

$$\overline{\mathfrak{p}} = (\overline{p}, \overline{(D+\sqrt{D})/2 - u}) = (p, (D-\sqrt{D})/2 - u) = \mathfrak{p}'.$$

■

2. Examples

Recall that for $\mathfrak{a} = (\alpha)$ with $\alpha \in \mathscr{O}_K$, necessarily $\mathrm{N}\mathfrak{a} = |\mathrm{N}_{K/\mathbf{Q}}(\alpha)|$. We first compute the prime ideal factorization of $(1+\sqrt{-5})$. This has norm $|\mathrm{N}_{K/\mathbf{Q}}(1+\sqrt{-5})| = 6 = 2 \cdot 3$, so necessarily $(1+\sqrt{-5}) = \mathfrak{p}_2\mathfrak{p}_3$ for some prime ideals $\mathfrak{p}_2$ and $\mathfrak{p}_3$ over 2 and 3 respectively. But there is only one prime over 2 (recall the discriminant is 20, and the ramified primes are precisely the prime factors of the discriminant, due to our general list of prime factorization in quadratic fields), and explicitly we worked out in class what it is: $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$. (As a safety check, uniqueness implies that this prime ideal must be conjugation-invariant, and indeed is it: $\overline{\mathfrak{p}}_2 = (2, 1-\sqrt{-5}) = (2, -1+\sqrt{-5})$ by negation of the second generator. Then adding 2 to the second generator is harmless and returns the formula for $\mathfrak{p}_2$.) Meanwhile, in $\mathbf{F}_3[X]$ we have $X^2+5 = X^2-1 = (X-1)(X+1)$, so

$$(3) = (3, \sqrt{-5}+1)(3, \sqrt{-5}-1)$$

is the prime ideal factorization of (3). Hence, the unique prime ideal $\mathfrak{p}_3$ dividing $(1+\sqrt{-5})$ is equal to exactly one among the pair $(3, 1+\sqrt{-5})$, $(3, -1+\sqrt{-5}) = (3, 1-\sqrt{-5})$. Which is it? Well, divisibility is related to containment in the opposite direction, so an equivalent issue is which of these contains $1+\sqrt{-5}$? By inspection we see the answer: $\mathfrak{p}_3 = (3, 1+\sqrt{-5})$. For later use, we let $\mathfrak{p}_3'$ denote the other prime over 3, which is to say $\mathfrak{p}_3' := (3, 1-\sqrt{-5})$.

Next, we factor $(2+\sqrt{-5})$. This has norm $4+5\cdot 1 = 9 = 3^2$, so $(2+\sqrt{-5})$ is a product of two prime ideals over 3. The only possibilities are $\mathfrak{p}_3^2$, $\mathfrak{p}_3\mathfrak{p}_3' = (3)$, or ${\mathfrak{p}_3'}^2$. Which is it? Well, the second option is clearly impossible: we can see by hand that $(2+\sqrt{-5}) \neq (3)$, as the ratio $(2+\sqrt{-5})/3$ is visibly not in $\mathscr{O}_K = \mathbf{Z}[\sqrt{-5}]$. How to distinguish among the two remaining possibilities? Well, each says that exactly one prime over 3 divides $(2+\sqrt{-5})$, which is to say that $2+\sqrt{-5}$ lies in exactly one among $\mathfrak{p}_3$ and $\mathfrak{p}_3'$. Staring at the formulas above which defined these two, we see the answer: $2+\sqrt{-5} = 3+(-1+\sqrt{-5}) \in \mathfrak{p}_3'$. So $(2+\sqrt{-5}) = {\mathfrak{p}_3'}^2$. Here is another way to get the answer: in the alternative case $(2+\sqrt{-5}) = \mathfrak{p}_3^2$ we would have that $\mathfrak{p}_3$ contains both $2+\sqrt{-5}$ as well as $1+\sqrt{-5}$, so it would contain their difference 1, which is absurd. This case shows us something interesting: the prime ideal $\mathfrak{p}_3'$ has square $(2+\sqrt{-5})$ which is principal, but it is itself *not* principal: the norm of this prime is 3, and $x^2+5y^2 = 3$ has no solution in $\mathbf{Z}$, so an ideal of norm 3 cannot be principal in $\mathscr{O}_K = \mathbf{Z}[\sqrt{-5}]$. Applying conjugation, likewise $\mathfrak{p}_3$ is not principal but its square is principal (in fact, its square is the conjugate principal ideal $(2-\sqrt{-5})$).

Finally, consider $(1+2\sqrt{-5})$. This has norm $1^2+5\cdot 2^2 = 21 = 3\cdot 7$, so $(1+2\sqrt{-5}) = \mathfrak{p}\mathfrak{q}$ for a prime $\mathfrak{p}$ over 3 and a prime $\mathfrak{q}$ over 7. Which of $\mathfrak{p}_3$ or $\mathfrak{p}_3'$ appears here, or equivalently contains $1+2\sqrt{-5}$? Rather than fiddling around with generators and hoping for divine inspiration, we use intelligence: the unique isomorphism $\mathscr{O}_K/\mathfrak{p}_3 \simeq \mathbf{F}_3$ carries $\sqrt{-5}$ to -1 (since it kills $1+\sqrt{-5}$!), whereas the unique isomorphism $\mathscr{O}_K/\mathfrak{p}_3' \simeq \mathbf{F}_3$ carries $\sqrt{-5}$ to 1, so the first map carries $1+2\sqrt{-5}$ to $1+2\cdot(-1) = -1$ whereas the second carries it to $1+2\cdot 1 = 3 = 0$. Aha, so in fact it is $\mathfrak{p}_3'$ that contains $1+2\sqrt{-5}$. (Now we can even see this explicitly: $1+2\sqrt{-5} = -2(1-\sqrt{-5})+3$. But the point is that one need not actually be clever with arithmetic by instead using the artful trick of remembering how the unique (!) isomorphisms $\mathscr{O}_K/\mathfrak{p} \simeq \mathbf{F}_p$ are actually obtained in the split case!) So now we have $(1+2\sqrt{-5}) = \mathfrak{p}_3'\mathfrak{p}_7$ for some prime ideal $\mathfrak{p}_7$ over 7.

What are the prime ideals over 7? We know that -5 is a square mod 7: explicitly, $-5 \equiv 3^2 \bmod 7$, so

$$(7) = (7, \sqrt{-5}+3)(7, \sqrt{-5}-3)$$

is the prime ideal factorization. Which among $\mathfrak{p}_\pm = (7, \sqrt{-5}\pm 3)$ is the prime ideal $\mathfrak{p}_7$ that divides $1+2\sqrt{-5}$? Well, let us again use the intelligent method of contemplating the unique isomorphism $\mathscr{O}_K/\mathfrak{p}_\pm \simeq \mathbf{F}_7$. This kills $\sqrt{-5}\pm 3$, so it sends $\sqrt{-5}$ to ∓ 3 and hence sends $1+2\sqrt{-5}$ to $1+2\cdot(\mp 3)$. Which of these vanishes in $\mathbf{F}_7$? Clearly it is $1+2\cdot 3$, so $\mathfrak{p}_-$ is the desired prime. That is, $\mathfrak{p}_7 = (7, \sqrt{-5}-3)$.

Notice that this final calculation shows us something interesting: since we already know that $\mathfrak{p}_3'$ is non-principal but has square that is principal, the equation $\mathfrak{p}_3'\mathfrak{p}_7' = (1+2\sqrt{-5})$ shows that $\mathfrak{p}_7'$ cannot be principal but its square is principal. Explicitly, since $x^2+5y^2 = 7$ has no solution in $\mathbf{Z}$ an ideal with norm 7 cannot be principal in $\mathscr{O}_K$, and by squaring

$$(1+2\sqrt{-5})^2 = (\mathfrak{p}_3')^2(\mathfrak{p}_7')^2 = (2+\sqrt{-5})(\mathfrak{p}_7')^2,$$

so $(\mathfrak{p}_7')^2 = ((1+2\sqrt{-5})^2/(2+\sqrt{-5}))\mathscr{O}_K$. This ratio is easily worked out to be $-2+3\sqrt{-5}$, which lies in $\mathscr{O}_K = \mathbf{Z}[\sqrt{-5}]$ as we knew it must, so $(\mathfrak{p}_7')^2 = (-2+3\sqrt{-5})$. It would be a mild annoyance to work that out by hand just from the explicit description of $\mathfrak{p}_7'$ in terms of two generators. Of course, conjugating this gives $\mathfrak{p}_7^2 = (2-3\sqrt{-5})$.