Math 154. Some quadratic factoring

In this handout we work out some examples of prime ideal factorization of principal ideals in the ring of integers of $\mathbf{Q}(\sqrt{-5})$. But first we review the story of the prime factorization of $p\mathscr{O}_K$ for a rational prime $p > 0$ and general quadratic field $K = \mathbf{Q}(\sqrt{d})$ with a squarefree integer $d \neq 1$.

1. General considerations

Define $D = \mathrm{disc}(K)$, so $D = 4d$ when $d \equiv 2, 3 \bmod 4$ (i.e., when $\mathscr{O}_K = \mathbf{Z}[\sqrt{d}]$) and $D = d$ when $d \equiv 1 \bmod 4$ (i.e., when $\mathscr{O}_K = \mathbf{Z}[(1+\sqrt{d})/2]$). Note in particular that if D is even then necessarily $\mathscr{O}_K = \mathbf{Z}[\sqrt{d}]$ and $D = 4d$. As we saw in HW3, Exercise 3,

$$\mathscr{O}_K \simeq \mathbf{Z}[(D+\sqrt{D})/2] = \mathbf{Z}[X]/(X^2 + DX + (D^2 - D)/4).$$

In that HW3 exercise you also showed that the structure of $\mathscr{O}_K/p\mathscr{O}_K$ *as a ring* falls into three cases:

(i) It is $\mathbf{F}_p[t]/(t^2)$ precisely when $p|D$.
(ii) It is $\mathbf{F}_p \times \mathbf{F}_p$ precisely when $p \nmid D$ with $D \bmod p$ a square for odd p and $D \equiv 1 \bmod 8$ for $p = 2$.
(iii) It is $\mathbf{F}_{p^2}$ precisey when $p \nmid D$ with $D \bmod p$ a nonsqaure for odd p and $D \equiv 5 \bmod 8$ for $p = 2$.

These three cases are distinguished ring-theoretically as follows: (i) is the case when there is a nonzero nilpotent element, (iii) is the field case, and (ii) is the rest (or alternatively the case when there is a nontrivial idempotent; i.e., an element e satisfying $e^2 = e$ with $e \neq 0, 1$). In class we exploited the low-degree nature of quadratic fields to carry out a systematic exhaustion of cases (done more systematically later with a "Chinese Remainder Theorem for Dedekind domains") to show that the factorization of $p\mathscr{O}_K$ breaks up into three respective possibilities as well:

(i′) $p\mathscr{O}_K = \mathfrak{p}^2$,
(ii′) $p\mathscr{O}_K = \mathfrak{p}\mathfrak{p}'$ with $\mathfrak{p} \neq \mathfrak{p}'$,
(iii′) $p\mathscr{O}_K$ is prime,

and these are respectively called the *ramified*, *split*, and *inert* cases.

We can describe these prime ideal factors in the ramified and split cases (there being nothing to do in the inert cases!):

Proposition 1.1. *Let $\alpha_D = (D+\sqrt{D})/2$. In the ramified case, $p\mathscr{O}_K = \mathfrak{p}^2$ where $\mathfrak{p} = (p, \alpha_D)$. In the split case, if u represents one of the two distinct roots of $X^2 - DX + (D^2 - D)/4$ in $\mathbf{F}_p$ then the distinct prime factors of $p\mathscr{O}_K$ are $(p, \alpha_D - u)$ and $(p, \alpha_D^* - u)$ where $z \mapsto z^*$ denotes the nontrivial automorphism of K.*

Note that in the split case, the effect of the nontrivial element of $\mathrm{Gal}(K/\mathbf{Q})$ swaps the two distinct primes dividing $p\mathscr{O}_K$.

Proof. We have $\mathscr{O}_K/p\mathscr{O}_K = \mathbf{F}_p[X]/(X^2 - DX + (D^2 - D)/4)$ as rings, and by separately considering when p is odd or $p = 2$ we see that in the ramified case (i.e., $p|D$) the quadratic polynomial is *always* X^2 in $\mathbf{F}_p[X]$, whence the unique (!) prime ideal $\mathfrak{p}/p\mathscr{O}_K$ in $\mathscr{O}_K/p\mathscr{O}_K = \mathbf{F}_p[X]/(X^2)$ corresponds to $(X)/(X^2)$. But X corresponds to α_D, so $\mathfrak{p}/p\mathscr{O}_K$ is generated by α_D, or in other words $\mathfrak{p} = (p, \alpha_D)$.

Now suppose we are in the split case, so in $\mathbf{F}_p[X]$ we have

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

for $u \in \mathbf{Z}$ representing a root in $\mathbf{F}_p$. (The sum of the roots is D, hence the form of the other term.) Thus, the two prime ideals $\mathfrak{p}/p\mathscr{O}_K$ and $\mathfrak{p}'/p\mathscr{O}_K$ in

$$\mathscr{O}_K/p\mathscr{O}_K = \mathbf{F}_p[X]/(X-u)(X-(D-u))$$

are respectively generated by $X-u$ and $X-(D-u) = X+u-D$. But X corresponds to α_D, so $\mathfrak{p}$ and $\mathfrak{p}'$ correspond (as an unordered pair of ideals) to $(p, \alpha_D - u)$ and $(p, \alpha_D - D + u)$. But by inspection we see that $\alpha_D - D = (-D + \sqrt{D})/2 = -\alpha_D^*$. Thus, the second ideal is $(p, -\alpha_D^* + u)$, and we may negative the second member of the generating set without harm. ■

In numerical examples one doesn't try to memorize these formulas for the prime factors as in Proposition 1.1, but rather work it out from first principles each time, as we shall illustrate below.

2. The case $K = \mathbf{Q}(\sqrt{-5})$

In this case $D = -20$, and in class we worked out the factorization of the two ramified primes: $2\mathscr{O}_K = \mathfrak{p}_2^2$ for $\mathfrak{p}_2 = (2, 1+\sqrt{-5})$ and $5\mathscr{O}_K = (\sqrt{-5})^2$. We also saw via quadratic reciprocity that for $p \neq 2, 5$, the split case (i.e., -5 mod p is a square) occurs exactly for $p \equiv 1, 3, 7, 9 \bmod 20$ and the inert case (i.e., -5 mod p is a non-square) occurs exactly for $p \equiv 11, 13, 17, 19 \bmod 20$. Explicitly, since $\mathscr{O}_K = \mathbf{Z}[\sqrt{-5}] = \mathbf{Z}[X]/(X^2-5)$, for the split case (i.e., -5 mod p is a square) we have

$$\mathscr{O}_K/p\mathscr{O}_K \simeq \mathbf{F}_p[X]/(X^2+5) = \mathbf{F}_p[X]/(X-u)(X+u)$$

where $u^2 \equiv -5 \bmod p$, so by reasoning as in the proof of Proposition 1.1 via chasing of prime ideals we find that $p\mathscr{O}_K$ has as its two distinct prime factors $(p, \sqrt{-5} \pm u) = (p, u \pm \sqrt{-5})$.

For example, 3 and 7 are split with prime factorizations

$$3\mathscr{O}_K = \mathfrak{p}_3\mathfrak{p}_3', \;\; 7\mathscr{O}_K = \mathfrak{p}_7\mathfrak{p}_7'$$

where $\mathfrak{p}_3 = (3, 1+\sqrt{-5})$, $\mathfrak{p}_3' = (3, 1-\sqrt{-5})$ (as $-5 \equiv 1^2 \bmod 3$) and $\mathfrak{p}_7 = (7, 3+\sqrt{-5})$, $\mathfrak{p}_7' = (7, 3-\sqrt{-5})$ (as $-5 \equiv 3^2 \bmod 7$). Note that these prime ideals have respective norms 3 and 7 (as always in the split case for a quadratic field for reasons we discussed in class), and hence they are *non-principal* because no element $x + y\sqrt{-5} \in \mathbf{Z}[\sqrt{-5}] = \mathscr{O}_K$ (with $x, y \in \mathbf{Z}$) has norm $x^2 + 5y^2$ equal to 3 or 7. By similar reasoning, the unique prime factor of (2) is non-principal (but its square (2) is principal).

Example 2.1. Let's factor $(1+\sqrt{-5})$ into primes. This has norm $|\mathrm{N}(1+\sqrt{-5})| = 6 = 2 \cdot 3$, so the factorization must be $\mathfrak{p}_2\mathfrak{p}_3$ or $\mathfrak{p}_2\mathfrak{p}_3'$. But the second option is ruled out since $\mathfrak{p}_3'$ does not contain $1+\sqrt{-5}$ (indeed, it contains $1-\sqrt{-5}$, so if it also contains $1+\sqrt{-5}$ then it would contain 2, contradicting that its intersection with $\mathbf{Z}$ is $3\mathbf{Z}$), whence the former is what occurs. You may check by bare hands as well via considering products among generators that $\mathfrak{p}_2\mathfrak{p}_3 = (1+\sqrt{-5})$.

Example 2.2. Next, we factor $(2+\sqrt{-5})$ into primes. Its norm is $9 = 3^2$, so it must be a product of two prime ideals of norm 3 (as the only prime ideals whose norm is a power of 3 are the two primes over $3\mathbf{Z}$, each of which must have norm 3 as always in the split case for a quadratic field). The case of two distinct primes over 3 is ruled out since $\mathfrak{p}_3\mathfrak{p}_3' = 3\mathscr{O}_K \neq (2+\sqrt{-5})$ (since 3 is not a unit multiple of $2+\sqrt{-5}$ in $\mathscr{O}_K$, as $\mathscr{O}_K^\times = \{\pm 1\}$).

Hence, the two options are $\mathfrak{p}_3^2$ or $(\mathfrak{p}_3')^2$. Which one occurs? Well, a nonzero prime ideal divides a nonzero ideal I in a Dedekind domain if and only if it contains I, so the question is this: which among $\mathfrak{p}_3$ or $\mathfrak{p}_3'$ contains $2+\sqrt{-5}$? We know that only one of these can hold (due to the two options that remain!), and easily $2+\sqrt{-5} \in (3, 1-\sqrt{-5}) = \mathfrak{p}_3'$. Thus, $(2+\sqrt{-5}) = (\mathfrak{p}_3')^2$, as may be verified by bare hands (try!). In particular, the non-principal (!) prime ideal $\mathfrak{p}_3'$ has square that is principal.

Example 2.3. Finally, we factor $(1+2\sqrt{-5})$, an ideal with norm $21 = 3 \cdot 7$. Thus, this ideal must be a product of one among the two primes over 3 and one among the two primes over 7. Which among each occurs? By uniqueness of prime factorization this is exactly the question which which among each pair actually contains $1+2\sqrt{-5}$ (and so equivalently occurs as a prime factor of $(1+2\sqrt{-5})$).

Put another way: in the fields $\mathscr{O}_K/\mathfrak{p}_3$ and $\mathscr{O}_K/\mathfrak{p}_7$ is the image of $1+2\sqrt{-5}$ equal to 0 or not? In these respective quotients that must be $\mathbf{F}_3$ and $\mathbf{F}_7$ (as the respective primes have been seen to have norms 3 and 7), the *definition* of the primes $\mathfrak{p}_3$ and $\mathfrak{p}_7$ implies that the residue class of $\sqrt{-5}$ in each is equal to -1 and -3 respectively (why?). Thus, the respective residue classes of $1+2\sqrt{-5}$ in each of these finite fields are $1+2(-1) = -1 \not\equiv 0 \bmod 3$ and $1+2(-3) = -5 \not\equiv 0 \bmod 7$. We conclude that

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

as may also be verified by bare hands.

As an amusing consequence, since we have seen above that $(\mathfrak{p}_3')^2$ is principal and we have just shown that $\mathfrak{p}_3'\mathfrak{p}_7'$ coincides with the principal ideal $I = (1+2\sqrt{-5})$, it follows that $(\mathfrak{p}_7')^2$ is principal! Explicitly,

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

and by direct calculation with elements we have

$$\frac{(1+2\sqrt{-5})^2}{2+\sqrt{-5}} = -2+3\sqrt{-5},$$

so $(\mathfrak{p}_7')^2 = (-2+3\sqrt{-5})$. The interested reader can verify this latter equality by bare hands too.