Prime Splitting in Quadratic Fields

Ferran Espuña Bertomeu

December 3, 2023

Claim 1. *Let m be a square-free integer. Let $K = \mathbb{Q}(\sqrt{m})$ and let p be a prime number. Then,*

$$\mathcal{O}_K/p\mathcal{O}_K \cong \begin{cases} \mathbb{F}_p[X]/(X^2 - m), & \text{if } p \text{ odd or } p = 2 \text{ and } \quad m \equiv 2, 3 \pmod 4 \\ \mathbb{F}_2[X]/(X^2 + X), & \text{if } p = 2 \text{ and } \quad m \equiv 1 \pmod 8 \\ \mathbb{F}_2[X]/(X^2 + X + 1), & \text{if } p = 2 \text{ and } \quad m \equiv 5 \pmod 8 \end{cases}$$

Proof. Let us deal with $p = 2$ first. In the first case, we have shown in class that

$$\mathcal{O}_K = \mathbb{Z}\left[\sqrt{m}\right]$$

where $\sqrt{m}$ is a root of the irreducible polynomial $f(X) = X^2 - m$. Therefore, $\mathcal{O}_K/p\mathcal{O}_K = \mathbb{Z}[X]/(f, 2) \cong \mathbb{F}_2[X]/\bar{f})$. Parallely, in the second and third cases, we have shown in class that

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$$

where $\frac{1+\sqrt{m}}{2}$ is a root of the irreducible polynomial $f(X) = X^2 - X - \frac{m-1}{4}$. Modulo 2, in the second case, the polynomial f is $X^2 + X$ and in the third case, it is $X^2 + X + 1$.

Now, let us deal with p odd. We still have that $\mathcal{O}_K$ is generated by either $\sqrt{m}$ or $\frac{1+\sqrt{m}}{2}$ over $\mathbb{Z}$. However, 2 is invertible in $\mathbb{Z}/p\mathbb{Z}$ and, in particular, in $\mathcal{O}_K/p\mathcal{O}_K$. Therefore, $\mathcal{O}_K/p\mathcal{O}_K$ is always generated by $\sqrt{m}$ over $\mathbb{Z}/p\mathbb{Z}$ and $\mathcal{O}_K/p\mathcal{O}_K \cong \mathbb{F}_p[X]/(X^2 - m)$. □

Remark 2. This lets us know how $p\mathcal{O}_K$ factorizes in $\mathcal{O}_K$ in terms of the factorization of a polynomial in $\mathbb{F}_p[X]$:

- If the polynomial is irreducible, then $p\mathcal{O}_K$ is prime because $\mathcal{O}_K/p\mathcal{O}_K$ is a field. we say that p is *inert*.
- Otherwise, $p\mathcal{O}_K$ is of the form $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$, where $\mathfrak{p}_i$ are prime ideals of $\mathcal{O}_K$. because the extension is of degree $2 = n = \Sigma_i e_i f_i$, either $g = 1$ and $e_1 = 2$ (we say that p is *ramified*) or $g = 2$ and $e_1 = e_2 = 1$ (We say that p is *completely split*). In the first case, f factors as a square of an irreducible polynomial, and in the second case, f factors as

a product of two distinct irreducible polynomials. This is because we can differentiate between a quotient by a square of a prime $\mathfrak{p}$ and a product of two distinct primes $\mathfrak{p}$, $\mathfrak{q}$. both in $\mathbb{F}_p[X]$ and in $\mathcal{O}_K$. In the first case, the class of any element of $\mathfrak{p}$ squares to zero, whereas in the second case there are no nilpotent elements (by the Chinese Remainder Theorem, $R/(\mathfrak{p}\mathfrak{q}) \cong R/\mathfrak{p} \times R/\mathfrak{q}$).

Proposition 1. *In the above situation, we get that:*

- *p is inert, when $\left(\frac{m}{p}\right) = -1$, or $p = 2$ and $m \equiv 5 \pmod 8$.*
- *p is ramified, when $\left(\frac{m}{p}\right) = 0$, or $p = 2$ and $m \equiv 2, 3 \pmod 4$.*
- *p is completely split, when $\left(\frac{m}{p}\right) = 1$, or $p = 2$ and $m \equiv 1, \pmod 8$.*

Proof. For the case of p odd, we have seen that the factorization corresponds to the factorization of $X^2 - m$ in $\mathbb{F}_p[X]$. The polynomial has no roots (is irreducible, so p is inert) exactly when $\left(\frac{m}{p}\right) = -1$ (m is not a square modulo p). Otherwise, if u is a root of $X^2 - m$ in $\mathbb{F}_p[X]$, then $X^2 - m = (X - u)(X + u)$, so the factors are distinct unless $u = -u$ (i.e. $u = 0$) and $m = 0$. This happens exactly when $\left(\frac{m}{p}\right) = 0$ (m is a multiple of p).

Modulo 2, we have:

- $X^2 + 0 = X^2$ and $X^2 + 1 = (X + 1)^2$, so p is ramified when $m \equiv 2, 3 \pmod 4$.
- $X^2 + X$ factors as $X(X + 1)$, so p is completely split when $m \equiv 1 \pmod 8$.
- $X^2 + X + 1$ is irreducible, so p is inert when $m \equiv 5 \pmod 8$.

$\square$

Proposition 2. *The same proposition, but without using Claim 1.*

Proof. We will examine each of the six cases separately, and give appropriate factorizations of $p\mathcal{O}_K$. We will start by the inert cases:

- p odd, $\left(\frac{m}{p}\right) = -1$: We just need to show that $p\mathcal{O}_K$ is prime in $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{m}\right]$. Indeed, if

  $$p\left(a + b\sqrt{m}\right) = \left(c + d\sqrt{m}\right)\left(e + f\sqrt{m}\right) = (ec + mfd) + (ed + fc)\sqrt{m}$$

  then $p \mid ec + mfd$ and $p \mid ed + fc$ so

  $$p \mid d(ec + mdf) - c(ed + fc) = mfd^2 - fc^2 = f(md^2 - c^2)$$

  Since p is prime, $p \mid f$ or $p \mid md^2 - c^2$. The first case implies $p \mid ec$ and $p \mid ed$, so either $p \mid e$, in which case $p \mid (e + f\sqrt{m})$, or $p \mid c$ and $p \mid d$, in which case $p \mid (c + d\sqrt{m})$. In the second case, if $p \mid d$ we can play the same game as in the case $p \mid f$, because $p \nmid m$. Otherwise, working modulo p, let x be the inverse of d. $0 \equiv md^2 - c^2 \equiv m - x^2c^2 \equiv m - (xc)^2$ so m is a square modulo p, a contradiction.

- $p = 2$, $m \equiv 5 \pmod 8$: We have $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. We will show that 2 is prime in $\mathcal{O}_K$. Assume that we have a factorization:

$$2\left(a + b\frac{\sqrt{m}+1}{2}\right) = \left(c + d\frac{\sqrt{m}+1}{2}\right)\left(e + f\frac{\sqrt{m}+1}{2}\right) \Rightarrow \tag{1}$$
$$8a + 4b + 4b\sqrt{m} = (2c + d\sqrt{m} + d)(2e + f\sqrt{m} + f) =$$
$$(4ce + 2cf + 2de + (m+1)\,df) + 2(cf + de + df)\sqrt{m}$$

Because $m + 1$ is even, we can divide by 2 and get

$$4a + 2b = 2ce + cf + de + rdf \tag{2}$$
$$2b = cf + de + df \tag{3}$$

where $r = \frac{m+1}{2} \equiv 3 \pmod 4$. Subtracting (3) from (2), we get

$$4a = 2ce + (r-1)\,df$$

$r - 1 \equiv 2 \pmod 4$ so $\frac{r-1}{2}$ is odd. Dividing the equation by 2, ce and df must have the same parity. They can't be both odd, because that would imply c, d, e, f odd, contradicting (3). Therefore, they are both even. If both c and d are even, or both e and f are even, then we have shown that 2 divides one of the factors on the right hand side of (1), so we are done. By symmetry, we may assume that c and f are even. Looking at (3), we realize that now de is even, so d or e must be even, again showing that one of the factors on the right hand side of (1) is divisible by 2.

Because the extension is of degree 2, $p\mathcal{O}_K$ must have at most two prime factors, by the same argument as before. Therefore, In the cases where $p\mathcal{O}_K$ is not prime, it is enough to show that a product of two proper ideals (the same one repeated twice, or two different ones, depending on the case)contains in $p\mathcal{O}_K$. This will imply equality, and that th ideals are prime.

- p odd, $\left(\frac{m}{p}\right) = 0$: We have $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{m}\right]$ and $p \mid m$. we will show that $p\mathcal{O}_K = (p, \sqrt{m})^2$. Indeed, let $m = kp$, $p \nmid k$ because m is square-free. By the Bezout identity, there exist $a, b \in \mathbb{Z}$ such that $ap + bk = 1$ so $p = p(ap+bk) = ap^2 + bm = ap^2 + b\left(\sqrt{m}\right)^2 \in (p, \sqrt{m})^2$. The ideal $(p, \sqrt{m})$ is proper, as its intersection with $\mathbb{Z}$ is $p\mathbb{Z} + m\mathbb{Z} = p\mathbb{Z}$.

- $p = 2, m \equiv 2, 3 \pmod 4$: We have $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{m}\right]$. If $m \equiv 2 \pmod 4$, we can do exatly the same as in the previous case. Let us assume that $m \equiv 3 \pmod 4$. We will show that $2\mathcal{O}_K = (2, 1 + \sqrt{m})^2$. An element of this product of ideals is

$$(1+\sqrt{m})^2 - 2(1+\sqrt{m}) = 1 + 2\sqrt{m} + m - 2 - \sqrt{m} = m - 1 \equiv 2 \pmod 4$$

$4 = 2^2$ also belongs here, and therefore so does 2. We can see that the ideal $(2, 1+\sqrt{m})$ is proper by trying to find 1 as a combination of 2 and $1 + \sqrt{m}$:

$$1 = 2\left(a + b\sqrt{m}\right) + \left(1 + \sqrt{m}\right)\left(c + d\sqrt{m}\right) = (2a + c + dm) + (2b + c + d)\sqrt{m}$$

Equating terms, we obtain:

$$2b + c + d = 0$$
$$2a + c + dm = 1$$

Because m is odd, reducing modulo 2, we get $c + d \equiv 0$ and $c + d \equiv 1$, a contradiction.

- p odd, $\left(\frac{m}{p}\right) = 1$: We have $\mathcal{O}_K = \mathbb{Z}[\sqrt{m}]$ and, for some n, $p \mid n^2 - m$, $p \nmid n$. We will show that $p\mathcal{O}_K \subset (p, n+\sqrt{m})(p, n-\sqrt{m})$, and that the two ideals in the product are distinct (by symmetry, this will imply that they are both proper ideals). For the first part, observe that $2np = p(n+\sqrt{m}) + p(n-\sqrt{m})$ is in the relevant ideal product. $p \nmid 2n$ so, by the Bezout identity, there exist $a, b \in \mathbb{Z}$ such that

  $$ap + b(2n) = 1 \Rightarrow p = a\left(p^2\right) + b\,(2np) \in \left(p, n+\sqrt{m}\right)\left(p, n-\sqrt{m}\right)$$

  We will prove that the ideals are different by contradiction. Without loss of generality, we will assume that $n - \sqrt{m} \in (p, n+\sqrt{m})$:

  $$n - \sqrt{m} = p\left(a + b\sqrt{m}\right) + \left(n+\sqrt{m}\right)\left(c + d\sqrt{m}\right) = (ap + cn + dm) + (bp + nd + c)\sqrt{m}$$

  Equating terms, we get

  $$\begin{aligned} bp + nd + c &= -1 \\ ap + cn + dm &= n \end{aligned}$$

  Now, working modulo p, and multiplying the first equation by n, we get

  $$\begin{aligned} md + nc &\equiv -n \\ cn + dm &\equiv n \end{aligned}$$

  Subtracting the first equation from the second, we get $p \mid 2n \Rightarrow p \mid n$, against our assumptions.

- $p = 2$, $m \equiv 1 \pmod 8$: We have $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$. Similarly to the previous case, We will show that $2\mathcal{O}_K \subset \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right)$, and that the two ideals in this product are distinct. For the first part,

  $$2 = 2\frac{1+\sqrt{m}}{2} + 2\frac{1-\sqrt{m}}{2} \in \left(2, \frac{1+\sqrt{m}}{2}\right)\left(2, \frac{1-\sqrt{m}}{2}\right)$$

  For the seccond, again, by symmetry, we may assume that $\frac{1-\sqrt{m}}{2} \in \left(2, \frac{1+\sqrt{m}}{2}\right)$:

  $$\frac{1-\sqrt{m}}{2} = 2\left(a + b\frac{1+\sqrt{m}}{2}\right) + \frac{1+\sqrt{m}}{2}\left(c + d\frac{1+\sqrt{m}}{2}\right) =$$
  $$\left(2a + b + \frac{c}{2} + \frac{d}{4} + \frac{md}{4}\right) + \left(b + \frac{c}{2} + 2\frac{d}{4}\right)\sqrt{m}$$

  Equating terms and multiplying everything by 4 we get:

  $$\begin{aligned} 2 &= 8a + 4b + 2c + (m+1)\,d \\ -2 &= 4b + 2c + 2d \end{aligned}$$

  And subracting the two equations we obtain:

  $$4 = 8a + (m-1)\,d$$

  Which is a contradiction because both terms on the right are multiples of 8.

$\square$