Math 676. Some vertical factorizations

Let us recall the general result on "vertical factorization" as proved in class. We let A be a Dedekind domain with fraction field F, and let F'/F be a finite separable extension such that the integral closure A' of A in F' is monogenic; that is, $A' = A[a']$ for some $a' \in A'$. (After we study the theory of completions later on, we will see that the monogenicity hypothesis is *always* satisfied when A is a discrete valuation ring.) The minimal polynomial f of a' over F lies in $A[X]$, and the map of A-algebras $A[X]/(f) \to A'$ uniquely determined by $X \mapsto a'$ is an *isomorphism*. Indeed, it is visibly surjective, and to check injectivity we note that the source is a finite free A-module and so it is enough to verify injectivity after applying $F \otimes_A (\cdot)$. Such extension of scalars gives rise to the map $F[X]/(f) \to F'$, and this is indeed injective (even an isomorphism) because it is a map of fields (as f is irreducible in $F[X]$).

The result from class was that if $\mathfrak{p}$ is a (nonzero) prime ideal of A and the reduction $\overline{f} \in \kappa(\mathfrak{p})[X]$ of f has factorization $\overline{f} = \prod_{i=1}^{g} \overline{f}_i^{e_i}$ for pairwise distinct monic irreducibles $\overline{f}_i$ then upon choosing monic lifts $f_i \in A[X]$ of $\overline{f}_i$ for all i then there is the prime factorization

$$\mathfrak{p}A' = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$$

with $\mathfrak{P}_i = (\mathfrak{p}, f_i(a'))$ and $\kappa(\mathfrak{P}_i) \simeq \kappa(\mathfrak{p})[X]/(\overline{f}_i)$ over $\kappa(\mathfrak{p})$ for all i. In particular, $[\kappa(\mathfrak{P}_i) : \kappa(\mathfrak{p})] = \deg \overline{f}_i$ for all i. In view of the fact that monogenicity always holds when A is local, and that the problem of factoring $\mathfrak{p}A'$ may be worked out after first localizing throughout at the multiplicative set $A - \mathfrak{p}$, it follows that by first localizing to $A_{\mathfrak{p}}$ the problem of vertical factorization of a prime may always be carried out by the above procedure (provided that we can find an a' whose existence is guaranteed by general theory; in practice, this amounts to carrying out an instance of weak approximation).

We wish to work out some examples of this theorem with $A = \mathbf{Z}$. In class, the general case of factorization of $p\mathbf{Z}$ in quadratic fields K was discussed; recall that $\mathscr{O}_K$ is always monogenic over $\mathbf{Z}$ in such cases. In Homework 4, Exercise 1, you showed that when carrying out prime factorization in a Galois extension one has that $e(\mathfrak{P}_i|\mathfrak{p})$ and $f(\mathfrak{P}_i|\mathfrak{p})$ are independent of i. We will illustrate the case of a non-Galois extension of $\mathbf{Q}$ as well as the general case of cyclotomic extensions of $\mathbf{Q}$.

1. A non-Galois 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 $\mathrm{disc}(\mathbf{Z}[\alpha]/\mathbf{Z}) = -4027$, and this is prime. Hence, $\mathscr{O}_K = \mathbf{Z}[\alpha]$ is monogenic and so the preceding general technique is applicable 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 $f(\mathfrak{P}_1|2\mathbf{Z}) = \deg(X+1) = 1$ and $f(\mathfrak{P}_2|2\mathbf{Z}) = \deg(X^2+X+1) = 2$. Note that $\sum e(\mathfrak{P}_i|2\mathbf{Z})f(\mathfrak{P}_i|2\mathbf{Z}) = 1 + 2 = 3 = [K : \mathbf{Q}]$, 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 $e(\mathfrak{Q}_1|4027\mathbf{Z}) = 2$ and $e(\mathfrak{Q}_2|4027\mathbf{Z}) = 1$ with both $\mathfrak{Q}_i$'s having residue field degree 1 over $\mathbf{F}_{4027}$. Note that $\sum e(\mathfrak{Q}_i|4027\mathbf{Z})f(\mathfrak{Q}_i|4027\mathbf{Z}) = 2 + 1 = 3 = [K : \mathbf{Q}]$, as it should be.

2. Cyclotomic fields

Let $K = \mathbf{Q}(\zeta_n)$ be a splitting field of $X^n - 1$ for a positive integer n. Letting $\Phi_n \in \mathbf{Z}[X]$ denote the nth cyclotomic polynomial, this is the minimal polynomial of ζ_n over $\mathbf{Q}$, and $\mathbf{Z}[\zeta_n] \simeq \mathbf{Z}[X]/(\Phi_n)$ is an order in $\mathscr{O}_K$. We have proved earlier that $\mathbf{Z}[\zeta_n] = \mathscr{O}_K$ if n is a prime power, and we will soon prove that this equality holds in general, with $\mathrm{disc}(K/\mathbf{Q})$ divisible by exactly the primes that divide n (so the primes of $\mathbf{Q}$ that ramify in K are precisely the prime factors of n, though this latter fact can be proved by other methods once one knows a bit more about general ramification theory). For now we will grant the equality $\mathbf{Z}[\zeta_n] = \mathscr{O}_K$, so in particular $\mathscr{O}_K$ is monogenic over $\mathbf{Z}$. We wish to work out how most primes of $\mathbf{Z}$ factor in $\mathscr{O}_K$. The case of ramified primes is a little complicated, so we just work out one ramified case and then we work out the general unramified case.

Let us first consider the special case $n = p^e$ with $e \geq 1$ and we wish to study how p factors in $\mathscr{O}_K = \mathbf{Z}[\zeta_{p^e}]$. (Recall that we have already proved that this is the full ring of integers in $K = \mathbf{Q}(\zeta_{p^e})$.) The general procedure for monogenic cases tells us that we should first factor Φ_{p^e} in $\mathbf{F}_p[X]$. Since $X^{p^e} - 1 = \Phi_{p^e} \cdot (X^{p^{e-1}} - 1)$ in $\mathbf{Z}[X]$, by passing to $\mathbf{F}_p[X]$ we get $(X-1)^{p^e} = \Phi_{p^e}(X-1)^{p^{e-1}}$ in $\mathbf{F}_p[X]$, and so $\Phi_{p^e} \equiv (X-1)^{p^{e-1}(p-1)} \bmod p$. Thus, $p\mathbf{Z}[\zeta_{p^e}] = \mathfrak{P}^{p^{e-1}(p-1)}$ with $\mathfrak{P} = (p, \zeta_{p^e} - 1)$, and so $e(\mathfrak{P}|p\mathbf{Z}) = p^{e-1}(p-1)$ and $f(\mathfrak{P}|p\mathbf{Z}) = 1$.

In fact, we can describe $\mathfrak{P}$ more succinctly: $\mathfrak{P} = (\zeta_{p^e} - 1)$. That is, we claim that p already lies in the principal ideal $(\zeta_{p^e} - 1)$ of $\mathbf{Z}[\zeta_{p^e}]$. To see this most easily, we just have to show that the quotient $\mathbf{Z}[\zeta_{p^e}]/(\zeta_{p^e} - 1)$ is killed by p. In fact, via the isomorphism $\mathbf{Z}[\zeta_{p^e}] \simeq \mathbf{Z}[X]/(\Phi_{p^e})$ we have

$$\mathbf{Z}[\zeta_{p^e}]/(\zeta_{p^e} - 1) \simeq \mathbf{Z}[X]/(\Phi_{p^e}, X - 1) \simeq \mathbf{Z}/(\Phi_{p^e}(1)) = \mathbf{Z}/p\mathbf{Z}$$

because $\Phi_{p^e}(1) = p$ (as $\Phi_{p^e}(X) = \Phi_p(X^{p^{e-1}})$ with $\Phi_p(T) = (T^p - 1)/(T - 1) = \sum_{0 \leq j < p} T^j$).

Now we turn to the general unramified case with $K = \mathbf{Q}(\zeta_n)$ for any $n \geq 1$. We take p to be a prime not dividing n, so

$$p\mathscr{O}_K = \mathfrak{p}_1 \cdots \mathfrak{p}_g$$

with $\phi(n) = [K : \mathbf{Q}] = fg$ with f denoting the common residue field degree $[\kappa(\mathfrak{p}_i) : \mathbf{F}_p]$ over $\mathbf{F}_p = \kappa(p\mathbf{Z})$. We need to determine f (and then we know g).

Lemma 2.1. *The order of p in $(\mathbf{Z}/n\mathbf{Z})^\times$ equals f.*

Proof. Consider the factorization $\Phi_n = h_1 \cdots h_g$ into monic irreducibles in $\mathbf{F}_p[X]$, with no extra multiplicities. (Note that *a priori* $\Phi_n \bmod p$ is separable over $\mathbf{F}_p$ because Φ_n divides $X^n - 1$ and $p \nmid n$). We have $f = \deg(h_j)$ for any j, so we need to compute the common degree of the h_j's. By construction, the finite field $k = \mathbf{F}_p[X]/(h_j)$ with order p^f is a quotient of $\mathbf{Z}[\zeta_n]$ and so k is generated over $\mathbf{F}_p$ by a primitive nth root of unity ζ (that is, an nth root of unity whose powers provide a splitting of $X^n - 1$ into monic linear factors). By Galois theory for finite fields, since $\mathrm{Gal}(k/\mathbf{F}_p)$ is generated by the Frobenius element whose order is f we have $\zeta^{p^i} = \zeta$ if and only if $f|i$. However, since ζ is a primitive nth root of unity in characteristic $p \nmid n$ we have $\zeta^a = \zeta^b$ if and only if $a \equiv b \bmod n$. Hence, $f|i$ if and only if $p^i \equiv 1 \bmod n$. This says exactly that f is the order of $p \in (\mathbf{Z}/n\mathbf{Z})^\times$. ■

Of course, in practice if we were to want to actually compute the primes over p in $\mathbf{Z}[\zeta_n]$ (for $p \nmid n$) we would have to compute the h_j's in $\mathbf{F}_p[X]$ and lift each h_j to a monic $H_j \in \mathbf{Z}[X]$. The ideals $(p, H_j(\zeta_n))$ of $\mathbf{Z}[\zeta_n]$ would then be the primes over $p\mathbf{Z}$.