ALGEBRAIC NUMBER THEORY

LECTURE 11 NOTES

First we'll prove the proposition from last time:

Proposition 1. *Let A be a Dedekind domain with fraction field K. Let L/K be a finite separable extension, and B the integral closure of A in L. Assume B is* monogenic *over A, i.e. $B = A[\alpha]$ for some $\alpha \in B$. Then let $f(X) \in A[X]$ be the minimal polynomial of α over K. Let $\mathfrak{p}$ be a prime of A and let $\overline{f}$ be the reduction of f mod $\mathfrak{p}$. If $\overline{f}$ factors as*

$$\overline{f}[X] = \overline{P}_1(X)^{e_1} \dots \overline{P}_r(X)^{e_r}$$

where $P_1, \dots, P_r \in (A/\mathfrak{p})[X]$ are irreducible and monic, then

$$\mathfrak{p}B = \mathfrak{B}_1^{e_1} \dots \mathfrak{B}_r^{e_r}$$

where $\mathfrak{B}_i = \mathfrak{p}B + P_i(\alpha)B$, the ramification index of $\mathfrak{B}_i$ is e_i, and the residue degree of $\mathfrak{B}_i$ is $f_i = \deg \overline{P}_i$.

Proof. Let $\overline{P}$ be an irreducible factor of $\overline{f}$, let $\overline{\alpha}$ be a root of $\overline{P}$ (in the algebraic closure of $\overline{A} = A/\mathfrak{p}$), and let $\mathfrak{B}$ be the prime of B which is the kernel of the map

$$A[\alpha] \to \overline{A}[\overline{\alpha}]$$

(the right hand side is a field). It is clear that $\mathfrak{p}B + P(\alpha)B$ is contained in $\mathfrak{B}$. Conversely, if $g(\alpha) \in \mathfrak{B}$, then $\overline{g}(\overline{al}) = 0$, so $\overline{g} = \overline{Ph}$ for some $\overline{h} \in \overline{A}[X]$ since $\overline{P}$ is the minimal polynomial of $\overline{\alpha}$. Then $g - Ph \in A[X]$ must actually have coefficients in $\mathfrak{p}$, so $g(\alpha) \in P(\alpha)B + \mathfrak{p}B$. So we do have $\mathfrak{B} = \mathfrak{p}B + P(\alpha)B$. It's clear that get exactly all the primes in the factorization of $\mathfrak{p}$ in this way, for this construction gives a prime $\mathfrak{B}$ of B lying above $\mathfrak{p}$, and conversely, if $\mathfrak{B}$ lies above $\mathfrak{p}$, then $B/\mathfrak{B}$ is a field extension of $A/\mathfrak{p}$ generated by the image of α in $B/\mathfrak{B}$.

It's clear that the residue degree $[B/\mathfrak{B}_i : A/\mathfrak{p}]$ of $\mathfrak{B}_i$ is $f_i = \deg \overline{\alpha}_i$ (over $\overline{A}$) $= \deg \overline{P}_i$. Now let e_i' be the ramification index of $\mathfrak{B}_i$, so that $\mathfrak{p}B = \mathfrak{B}_1^{e_1} \dots B_r^{e_r}$. Since $f(\alpha) = 0$ and $f(X) - P_1(X)^{e_1} \dots P_r(X)^{e_r} \in \mathfrak{p}A[X]$, it follows that

$$P_1(\alpha)^{e_1} \dots P_r(\alpha)^{e_r} \in \mathfrak{p}B$$

.

But we also have $\mathfrak{B}_i^{e_i} = (\mathfrak{p}b + P_i(\alpha)B)^{e_i} \subset \mathfrak{p}B + P_i(\alpha)^{e_i}B$ for every i. Multiplying these gives

$$\begin{aligned}\mathfrak{B}_1^{e_1} \dots \mathfrak{B}_r^{e_r} &\subset (\mathfrak{p}B + P_1(\alpha)^{e_1}B) \dots (\mathfrak{p}B + P_r(\alpha)^{e_r}B) \\ &\subset \mathfrak{p}B + P_1(\alpha)^{e_1}P_2(\alpha)^{e_2} \dots P_r(\alpha)^{e_r}\end{aligned}$$

$$= \mathfrak{p}B = \mathfrak{B}_1^{e_1'} \dots \mathfrak{B}_r^{e_r'}$$

which implies $e_i \geq e_i'$ for each i. But we know that $\sum e_i f_i = \deg \overline{f} = \deg f = [E : F] = \sum e_i' f_i$, which forces $e_i = e_i'$ for all i.

□

1. Section 5.3

If L/K is an extension of number fields, we define $D_{L/K}$ to be the discriminant ideal of $\mathcal{O}_L$ over O_K.

The main result of this section says that for a finite separable extension L/K, where $K = Frac(A)$ for a Dedekind domain A, and B the integral closure of$A$ in L, a prime $\mathfrak{p}$ of A ramifies in B iff it divides the discriminant $D_{B/A}$.

We can use this example to compute which primes which ramify in quadratic or cyclotomic fields, in particular.

Example. If $d \equiv 2, 3 \bmod 4$ is squarefree, then the discriminant of $\mathbb{Q}(\sqrt{d})$ is $4d$. So the prime 2 ramifies in the quadratic field. We can check that $(2) = (2, \sqrt{d})^2$ if $d \equiv 2 \bmod 4$ and $1(2) = (2, 1 + \sqrt{d})^2$ if $d \equiv 3 \bmod 4$.

The discriminants D which are equal to d if $d \equiv 1 \bmod 4$ and squarefree and $4d$ if $d \equiv 2, 3 \bmod 4$ and squarefree, are called *fundamental discriminants.*

Example. For the cyclotomic field, $\mathbb{Q}(\zeta_{p^r})$, the discriminant is a power of p. So the only prime which ramifies is p, and p ramifies completely: $(p) = (1 - \zeta_{p^r})^{[\mathbb{Q}(\zeta_{p^r}):\mathbb{Q}]}$. This follows from using $(1 - \zeta_{p^r}^k) = (1 - \zeta_{p^r})$ as ideals whenever k is coprime to p.

2. Section 5.4

Quadratic extensions are monogenic, so we can apply our proposition to figure out how primes decompose.

(1) $d \equiv 2, 3 \bmod 4$. Then $\alpha = \sqrt{d}$ generates the ring of integers. Its minimal polynomial is $X^2 - d$, whose discriminant is $4d$. So p ramifies iff $p|4d$ (i.e. $X^2 - d$ is a square mod p. Note that for $p = 2$, we either get X^2 or $X^2 + 1 \equiv (X + 1)^2 \bmod 2$). Now if p doesn't divide $4d$, then p splits as $\mathfrak{p}_1\mathfrak{p}_2$ (with $e(\mathfrak{p}_i) = 1, f(\mathfrak{p}_i) = 1$) iff $X^2 - d \bmod p$ has two roots in $\mathbb{F}_p$, i.e. iff d is a quadratic residue mod p. Otherwise p is inert (remains prime), with $e = 1, f = 2$.

(2) $d \equiv 1 \bmod 4$. Then $\alpha = (1 + \sqrt{d})/2$ generates the ring of integers, and its minimal polynomial is $X^2 - X + (1 - d)/4$, whose discriminant is d. So p ramifies iff $p|d$. Otherwise, we calculate as follows: if $p = 2$ then p splits iff $(1 - d)/4 \equiv 0 \bmod 2$ iff $d \equiv 1 \bmod 8$. If p is odd then the condition is as before: p splits iff d is a quadratic residue mod p.

3. Extensions of local fields

Let K be a nonarchimedean local field: for us, a finite extension of $\mathbb{Q}_p$. Let L/K be a finite extension (separable since K has characteristic 0). Let $\mathfrak{p} = (\pi)$ be the prime ideal of $\mathfrak{o} = \mathcal{O}_K$, where $\pi = \pi_K$ is a uniformizer. Then there is only one prime $\mathfrak{B}$ above $\mathfrak{p}$, since L is a nonarchimedean local field too (unique extension of the valuation), so $\mathcal{O}_L$ is a DVR and has a unique nonzero prime ideal. So $\mathfrak{p}\mathcal{O}_L = \mathfrak{B}^e$, where f =residue class degree of $\mathfrak{B}$ satisfies $ef = n := [L : K]$. Now if $e = 1, f = n$ we say the extension is unramified, and if $e = n, f = 1$ we say the extension is totally ramified.

Proposition 2. *There is only one unramified extension of degree n of K.*

Proof. Let $\kappa = \mathcal{O}_K/\mathfrak{p}$ be the residue field of $\mathcal{O}_K$. It is a finite field $\mathbb{F}_q$, with q a power of p (since if K is a finite extension of $\mathbb{Q}_p$, κ is a finite extension of $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$). Now if L/K is an unramified extension of degree n, we see that $[\mathcal{O}_L/\mathfrak{B} : \mathcal{O}_K/\mathfrak{p}] = f = n$. So $\mathcal{O}_L/\mathfrak{B} \cong \mathbb{F}_{q^n}$, the unique extension of $\mathbb{F}_q$ of degree n. Now fix a generator $\overline{\alpha}$ of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ and let $\overline{f} \in \mathbb{F}_q[X]$ be its minimal polynomial. Then f has degree n and is separable, since the extension of finite fields is separable (finite fields are perfect). Let f be a lift of $\overline{f}$ to $\mathcal{O}_K[X]$ and choose it to be monic (and hence of degree n). Then by Hensel's lemma applied to $\mathcal{O}_L$ and its residue field, f has a root α in $\mathcal{O}_L$. This α, being of degree n, must generate the field L over K. Therefore this L must be isomorphic to $K[X]/(f)$. Conversely, it is an easy check that $K[X]/(f)$ is unramified of degree $n = \deg f$. Since the construction of f depends only on K and on n, this shows that L must be unique once these are fixed. In other words, there is exactly one unramified extension of K of every degree. $\square$

Now let's look at the totally ramified case. On the homework, you will show that totally ramified extensions are given by specifying an Eisenstein polynomial

$$X^n + a_{n-1}X^{n-1} + \cdots + a_0$$

with $\pi | a_i$ for all i, and $\pi^2 \nmid a_0$; this is the minimal polynomial of a uniformizer of $\mathcal{O}_L$.

Combining these, one can show that there are only finitely many extensions of degree n of a nonarchimedean local field K. The proof uses the following argument, which is a corollary of Krasner's lemma (Problem 4 on Problem Set 4).

Let $f, g \in K[X]$ be monic polynomials. Define $|f|$ to be the maximum of the absolute values of the coefficients of f. If $|f|$ is bounded then the absolute values of the roots of f are also bounded (for instance, by looking at the Newton polygon). Now fix f, and suppose $|f - g|$ is small. Then if β is any root of g, we have that $|f(\beta) - g(\beta)| = |f(\beta)|$ is small. So β must be close to a root of f, since $f(\beta) = \prod(\beta - \alpha_i)$ where α_i are the roots of f. As β comes close to say $\alpha = \alpha_1$, its distance from the other roots of f approaches the distance of α_1 from ther other roots, so it is bounded from below. We say that β belongs to α. Now if f is irreducible and g is sufficiently close to f, then Krasner's lemma applied to any root β of g shows that $\alpha \in K(\beta)$, where α is the root of f to which β belongs. But since $\deg g = \deg f$, we must have $K(\alpha) = K(\beta)$ and g is irreducible as well. So this tells us that polynomials which are close enough to a given irreducible polynomial f are also irreducible and generate the same extension.