Algebraic Number Theory, Math 421
Instructor: Sreekar M. Shastry
Notes on the splitting of primes in extensions and quadratic reciprocity

1. Ramification

Terminology 1. A number ring is the ring of integers in a number field.

Let us mention the following theorem, purely for curiosity.

Theorem 2. *Let $\mathscr{O}$ be a number ring and let $\alpha \in \mathscr{O}$ be of degree n over $\mathbb{Q}$. Then there is an integral basis*

$$\left\{1, \frac{f_1(\alpha)}{d_1}, \dots, \frac{f_{n-1}(\alpha)}{d_{n-1}}\right\}$$

where $d_i \in \mathbb{Z}$ satisfy $d_1 | d_2 | \cdots | d_{n-1}$, the $f_i \in \mathbb{Z}[x]$ are monic, and $\deg f_i = i$. The d_i are uniquely determined. See [Mar77, 13, p.36].

Terminology 3. What is called "inertial degree" on [Mar77, p.64] is more often called the "residual degree."

Definition 4. Let L/K be an extension of number fields. A prime P of $\mathscr{O}_K$ is said to be ramified in $\mathscr{O}_L$ if $e(Q/P) > 1$ for some prime Q of K lying above it, or equivalently, if $P.\mathscr{O}_L$ is not squarefree.

Let us recall the following theorem [Mar77, 21, p.65] and a generalization.

Theorem 5. *Let L/K be a finite extension of number fields and let $Q_1, \dots, Q_g$ be the primes of $\mathscr{O}_L$ lying above a prime P of $\mathscr{O}_K$. Denote by $e_1, \dots, e_r$ and $f_1, \dots, f_r$ the corresponding ramification indices and residual degrees. Then we have*

$$[L : K] = \sum_{i=1}^{g} e_i f_i.$$

Theorem 6. *Moreover, if L/K is Galois then the e_i and f_i are independent of i and we have*

$$[L : K] = efg$$

where g is as above and e,f is the common value of the e_i,f_i, respectively. See [FT91, 20, p.117].

We recall the following result [Mar77, 23, p.70] which was proved in the lecture of 7-Feb-11.

Theorem 7. *Let L/K be a normal extension of number fields with Galois group G. Then G acts transitively on the set of primes of L lying above a given prime of K.*

Notation 8. For an ideal I of a Dedekind ring $\mathscr{O}$, write

$$\|I\| := \#\mathscr{O}/I.$$

We have the following important theorem which we will prove a special case of below.

Remark 9. Passages of the notes bounded by {begin $*$} and {end $*$} are optional and will not be covered on the exams or homework assignments.

{begin $*$}

Let L/K be a finite extension of number fields. Then there is a notion of relative discriminant

$$D_{L/K} \in \mathrm{Cl}(\mathscr{O}_K)^2$$

which is to say, $D_{L/K}$ is a square in the ideal class group of K. We will (perhaps?) see the definition of relative discriminant later on in the course.

Next, let $\mathscr{O}_L^\vee$ be the dual of $\mathscr{O}_L$ with respect to the trace $\mathrm{Tr}_{L/K}$. The inverse of $\mathscr{O}_L^\vee$ in $\mathrm{Cl}(L)$ is known as the *different* and denoted by $\mathscr{D}_{L/K}$. It can be shown that

$$\mathrm{N}_{L/K}(\mathscr{D}_{L/K}) = D_{L/K},$$

i.e. the norm of the different is the discriminant.

The results we want to state are the following.

Theorem 10. *A prime P ramifies in the extension L/K iff $P|D_{L/K}$.*

Theorem 11. *Let $L = K(\alpha)$ and suppose that $f(x)$, the minimal polynomial of α over K, lies in $\mathscr{O}_K[x]$. Then*
(a) $\mathscr{O}_K[\alpha]^\vee = f'(\alpha)\mathscr{O}_K[\alpha]$, and
(b) $\mathfrak{d}(\mathscr{O}_K[\alpha]) = \mathrm{N}_{L/K}(f'(\alpha))\mathscr{O}_K = \mathrm{disc}(f)\mathscr{O}_K$.

Remark 12. In the statement of the theorem, by $\mathfrak{d}(\mathscr{O}_K[\alpha])$ is meant the absolute discriminant of the ring extension $\mathscr{O}_K[\alpha]/\mathbb{Z}$, regarded as an ideal in $\mathbb{Z}$ Note well that this notion discards the sign of the absolute discriminant $\mathrm{disc}(K) \in \mathbb{Z}$.

{end $*$}

Lemma 13. *Let K be a number field of degree n over $\mathbb{Q}$ and let $\alpha_1, \dots, \alpha_n \in K$. Then*
(a) $\mathrm{disc}(r\alpha_1, \alpha_2, \dots, \alpha_n) = r^2\mathrm{disc}(\alpha_1, \dots, \alpha_n)$ for all $r \in \mathbb{Q}$ and
(b) if β is a $\mathbb{Q}$-linear combination of $\alpha_2, \alpha_3, \dots, \alpha_n$ then

$$\mathrm{disc}(\alpha_1 + \beta, \alpha_2, \dots, \alpha_n) = \mathrm{disc}(\alpha_1, \dots, \alpha_n).$$

Proof. Expand out the determinant which defines the discriminant. (Recall that the discriminant of an n-tuple $(\alpha_i)_{i=1}^n$ in $\mathscr{O}_K$ is $|\sigma_i(\alpha_j)|^2$ i.e. the square of the determinant of the matrix with the given ijth entry, where the σ_i are the embeddings of K into $\mathbb{C}$.) ∎

The following statement and proof are from [Mar77, p. 72ff].

Theorem 14. *Let p be a prime in $\mathbb{Z}$ and suppose that p is ramified in a number ring $\mathscr{O}_K$. Then $p|\mathrm{disc}(\mathscr{O}_K)$.*

Proof. Let P be a prime of $\mathscr{O}_K$ lying over p such that $e(P/p) > 1$. Then $p.\mathscr{O} = P.I$ where I is divisible by all primes of $\mathscr{O}_K$ lying over p, including P.

Let $\{\sigma_1, \dots, \sigma_n\}$ be the embeddings of the fraction field K of $\mathscr{O}_K$ into $\mathbb{C}$ and extend each σ_i to an automorphism of some L/K such that L is normal over $\mathbb{Q}$. Thus the discriminant of an n-tuple $(\alpha_i)_{i=1}^n$ in $\mathscr{O}_K$ is $|\sigma_i(\alpha_j)|^2$ (i.e. the square of the determinant of the matrix with the given ijth entry).

Let $\{\alpha_1, \dots, \alpha_n\}$ be an integral basis for $\mathscr{O}_K$. We will replace one of the α_i by a suitably chosen element which will enable us to see that $p|\mathrm{disc}(\mathscr{O}_K)$. Choose any $\beta \in I \smallsetminus p.\mathscr{O}_K$ (where we know that $p.\mathscr{O}_K \subsetneq I$ — this is in fact the reason that I was defined as it was); then β is in every prime of $\mathscr{O}_K$ lying over p, but not in $p.\mathscr{O}_K$. Writing

$$\beta = m_1\alpha_1 + \cdots + m_n\alpha_n, m_i \in \mathbb{Z},$$

then the fact that $\beta \notin p.\mathscr{O}_K$ implies that $p \nmid m_j$ for some j. Without loss, suppose that $p \nmid m_1$. Put

$$d := \mathrm{disc}(\mathscr{O}_K) = \mathrm{disc}(\alpha_1, \dots, \alpha_n);$$

then we have by the above lemma

$$\mathrm{disc}(\beta, \alpha_2, \dots, \alpha_n) = m_1^2 d.$$

Since $p \nmid m_1$ it will suffice to show that

$$p|\mathrm{disc}(\beta, \alpha_2, \ldots, \alpha_n).$$

Recall that β is in every prime of $\mathscr{O}_K$ lying over p. It follows that β is in every prime of $\mathscr{O}_L$ lying over p. (Each such prime $Q \ni p$ and $Q \cap \mathscr{O}_K$ is a prime lying over p, so that $\beta \in Q \cap \mathscr{O}_K \subset Q$.) Fixing such a Q of $\mathscr{O}_L$ lying over p, we claim that $\sigma(\beta) \in Q$ for each $\sigma \in \mathrm{Aut}(()L/\mathbb{Q})$. To see this, observe that $\sigma^{-1}(Q)$ is a prime of $\sigma^{-1}(\mathscr{O}_L) = \mathscr{O}_L$ lying over p and hence contains β. Thus $\sigma_i(\beta) \in Q$ for all i. It follows by expanding out the determinant which defines the discriminant that Q contains $\mathrm{disc}(\beta, \alpha_2, \ldots, \alpha_n)$. Since the discriminant is in $\mathbb{Z}$, it is in $Q \cap \mathbb{Z} = p.\mathbb{Z}$, as required. ■

Corollary 15. *Only finitely many primes of $\mathbb{Z}$ are ramified in a given number ring $\mathscr{O}_K$.*

Corollary 16. *Let L/K be an extension of number fields. Then only finitely many primes of K are ramified in L.*

2. Inertia and Decomposition

Definitions 17. Let L/K be a normal extension of number fields with group G and degree $n = [L : K]$ with rings of integers $\mathscr{O}_L$,$\mathscr{O}_K$. Let P be a prime of K so that all primes Q of L lying above it have common ramification index e and residual degree f, and if there are r such primes, we have $efr = n$.

Fix such a Q lying over P. The *decomposition group* is

$$D(Q/P) := \{\sigma \in G : \sigma Q = Q\}.$$

The *inertia group* is

$$I(Q/P) := \{\sigma \in G : \sigma(\alpha) \equiv \alpha \pmod{Q}, \forall \alpha \in \mathscr{O}_L\}.$$

These are subgroups of G and we have $I \subset D$.

For each $\sigma \in G$ we have the commutative diagram

$$\begin{tikzcd}
\mathscr{O}_L \arrow[r, "\sigma"] \arrow[d] & \mathscr{O}_L \arrow[d] \\
\mathscr{O}_L/Q \arrow[r, "\overline{\sigma}"] & \mathscr{O}_L/Q
\end{tikzcd}$$

which gives us the group homomorphism

$$D(Q/P) \to \mathrm{Gal}(k(Q)/k(P))$$

where we write $k(Q) = \mathscr{O}_L/Q$ and $k(P) = \mathscr{O}_K/P$ for the resdidue field; these are finite fields.[1]

[1] In fact the whole of algebraic number theory can be developed for a certain class of Dedekind domains such that the residue fields at maximal ideals are finite fields. Such fields are called "global fields" and consist of number fields which are finite extensions of $\mathbb{Q}$ and the function fields which are finite extensions of $\mathbb{F}_q(t)$.

The function field case is generally regarded as "easier" than the number field case, primarily because there is an algebro-geometric interpretation of these fields in terms of algebraic curves over finite fields, so that one may apply the language and results of algebraic geometry to their study.

For instance, in the function field case, we can easily write down examples of extensions with prescribed ramification index and residual degree: $\mathbb{F}_q(t^{1/e})/\mathbb{F}_q(t)$ has ramification index e and $\mathbb{F}_{q^f}(t)/\mathbb{F}_q(t)$ has residual degree f, in both cases relative to the prime ideal (t) in the "ring of integers" $\mathbb{F}_q[t] \subset \mathbb{F}_q(t)$.

In addition to the above notation, we write L^H for the fixed field of L under the subgroup $H \subset G$, and Q^H for the prime $Q \cap L^H$ of L^H.

Let us state without proof the following theorem ([Mar77, Theorem 28, p. 100]).

Theorem 18. *In addition to the above notation, write $I := I(Q/P), D := D(Q/P)$. Then we have the following.*

$$\begin{tikzcd}
{} \arrow[dddd, phantom, "G\{"'] & {} \arrow[dd, phantom, "D\{"'] & {} \arrow[d, phantom, "I\{"'] & L \arrow[d, dash, "{e=[L:L^I]}"'] & Q \arrow[d, dash, "{e(Q/Q^I)=e,\ f(Q/Q^I)=1}"] \\
 & & {} & L^I \arrow[d, dash, "{f=[L^I:L^D]}"'] & Q^I \arrow[d, dash, "{e(Q^I/Q^D)=1,\ f(Q^I/Q^D)=f}"] \\
 & {} & & L^D \arrow[d, dash, "{r=[L^D:K]}"'] & Q^D \arrow[d, dash, "{e(Q^D/P)=f(Q^D/P)=1}"] \\
 & & & K & P. \\
{} & & & &
\end{tikzcd}$$

Remark 19. Given L/K, we may figuratively say that all ramification of P occurs between $L^I \subset L$, all residual extension at P occurs between $L^D \subset L^I$, and all "topological covering near P" occurs between $K \subset L^D$ (or perhaps we might say that

$$\operatorname{Spec} \mathscr{O}_{L^D} \to \operatorname{Spec} \mathscr{O}_K$$

is a regular covering space in a sufficiently small neighborhood of $P \in \operatorname{Spec} \mathscr{O}_K$).

Remark 20. The fields L^I, L^D are called the "inertia field" and "decomposition field," respectively.

It follows from the above theorem (see [Mar77, Cor. 1,p. 101]) that the homomorphism from the decomposition group to the residual Galois group is surjective with kernel I so that we have the exact sequence

$$1 \longrightarrow I(Q/P) \longrightarrow D(Q/P) \longrightarrow \operatorname{Gal}(k(Q)/k(P)) \longrightarrow 1.$$

Recall that the the extension of finite fields $k(Q)/k(P)$ has degree f so that its Galois group is cyclic of order f.

Corollary 21. *If D is a normal subgroup of G then P splits into r distinct primes in L^D. If, moreover, I is normal in G, then each of them remains prime (is "inert") in L^I. Each one becomes an eth power in L.*

Proof. [Mar77, Cor. 2, p. 102]. ∎

Put $\omega := e^{2\pi i/m}$ and fix a prime $p \in \mathbb{Z}$. Then we have (see [Mar77, p. 75])

$$p.\mathbb{Z}[\omega] = (Q_1 \cdots Q_r)^e$$

with the Q_i distinct primes of $\mathbb{Z}[\omega]$, all of which have the same residual degree f over p. We also have $efr = \varphi(m)$. Moreover, a theorem from [Mar77, p. 76] tells us that if we write $m = p^k n$ with $p \nmid n$, then we have $e = \varphi(p^k)$ and f is the order of p in the group $(\mathbb{Z}/n)^\times$.

Now let us consider how the theory above applies to the splitting of the prime 2 in the field $\mathbb{Q}[\omega_{23}]$ where $\omega_{23} := e^{2\pi i/23}$.

We know that 2 splits into two primes in $\mathbb{Q}[\omega_{23}]$ since $efr = 22$ (because 23 is prime), and $e = 1, f = 11$. Thus the decomposition field $\mathbb{Q}[\omega_{23}]^D$ has degree 2 over $\mathbb{Q}$. Moreover, there is exactly one quadratic subfield of $\mathbb{Q}[\omega_{23}]$ since the Galois group is cyclic of order 22. Thus the decomposition field must be $\mathbb{Q}[\sqrt{-23}]$ (since by [Mar77, Ch. 2, Ex. 8], $\mathbb{Q}[\sqrt{-23}] \subset \mathbb{Q}[\omega_{23}]$ — the exercise says that if p is an odd prime then $\mathbb{Q}[e^{2\pi i/p}]$ contains $\sqrt{p}$ if $p \equiv 1 \pmod 4$ and $\sqrt{-p}$ if $p \equiv -1 \pmod 4$). Since 2 is unramified in $\mathbb{Q}[\omega_{23}]$ the inertia field is all of $\mathbb{Q}[\omega_{23}]$.

In the same vein, if L/K is Galois with cyclic Galois group and P is a prime in K which splits into r primes in L then the decomposition field is the unique intermediate field of degree r over K and P splits into r primes in every intermediate field containing the decomposition field.

Let us state without proof the following result ([Mar77, Theorem 29,p. 104]).

Theorem 22. *With the notations above, among field extensions K' intermediate to L/K, we have that*

(1) L^D is maximal such that there is a prime P'/P such that

$$e(P'/P) = f(P'/P) = 1,$$

(2) L^D is minimal such that Q is the only prime of L lying over some prime P',

(3) L^I is maximal such that $e(P'/P) = 1$; thus it is also known as the maximal unramified subextension of L/K, and

(4) L^I is minimal such that Q is totally ramified over P' (i.e. such that $e(Q/P') = [L : K']$).

We turn our attention next to quadratic reciprocity.

3. Quadratic Reciprocity

Definition 23. A prime P of a number field K is said to split completely in a extension field F if P splits into $[F : K]$ distinct primes, so that all must have $e = f = 1$.

Conversely, if all primes of F above P have $e = f = 1$ then P must split completely in F. (All of these statements follow from the $n = efr$ theorem.) Thus if a prime splits completely in some extension, then it splits completely in every intermediate extension.

The results from the last lecture easily imply (in our usual notational setup) the following

Corollary 24. *If $D := D(Q/P)$ is a normal subgroup of $G := \mathrm{Gal}(L/K)$ then P splits completely in K' iff $K' \subset L^D$.*

For the proof, see [Mar77, p. 105]. We will be interested in applying this in the case where G is abelian so that all subgroups are automatically normal.

Definition 25. Let $p \in \mathbb{Z}$ be an odd prime. For $n \in \mathbb{Z}$ prime to p, we define the Legendre symbol by

$$\left(\frac{n}{p}\right) := \begin{cases} 1 & \text{if } n \text{ is a square mod } p, \\ -1 & \text{otherwise.} \end{cases}$$

Theorem 26 (Quadratic Reciprocity)**.** *We have*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \textit{if } p \equiv \pm 1 \pmod 8, \\ -1 & \textit{if } p \equiv \pm 3 \pmod 8 \end{cases}$$

and for odd primes $q \neq p$ we have

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \textit{if } p \textit{ or } q \equiv 1 \pmod 4, \\ -\left(\frac{p}{q}\right) & \textit{if } p \equiv q \equiv 3 \pmod 4. \end{cases}$$

Let us establish a criterion for a prime to be a dth power mod p, for any $d|p-1$. Put $\omega := \omega_p := e^{2\pi i/p}$ and consider $\mathbb{Q}[\omega]$. Since $\mathrm{Gal}(\mathbb{Q}[\omega]/\mathbb{Q}) \simeq \mathbb{Z}/(p-1)$, there exists for each $d|p-1$ a unique subfield $F_d \subset \mathbb{Q}[\omega]$ of degree d over $\mathbb{Q}$, and $F_d \subset F_{d'}$ iff $d|d'$.

Theorem 27. *Let p be an odd prime and $q \neq p$ be any other prime. Let $d|p-1$. Then q is a dth power mod p iff q splits completely in F_d.*

Proof. We know[2] that q splits into r distinct primes in $\mathbb{Q}[\omega]$, where $f := (p-1)/r$ is the order of q in $(\mathbb{Z}/p)^\times$. This group is cyclic of order $p-1$ so the map $x \mapsto x^d$ is a group homomorphism whose image is the unique subgroup of order $(p-1)/d$; it consists of all the elements of $(\mathbb{Z}/p)^\times$ whose orders divide $(p-1)/d$. Thus the following are equivalent

(i) q is a dth power mod p
(ii) $f|(p-1)/d$
(iii) $d|r$
(iv) $F_d \subset F_r$

Now, the decomposition field of a prime Q of $\mathbb{Q}[\omega]$ lying over $q \in \mathbb{Z}$ must have degree r, and therefore this decomposition field must be F_r since that is the only intermediate field of degree r.

Therefore the condition $F_d \subset F_r$ is equivalent to the condition that q splits completely in F_d, by Corollary 24, and the theorem is proved. ∎

Lemma 28. *If p is an odd prime then $\mathbb{Q}[e^{2\pi i/p}]$ contains $\sqrt{p}$ if $p \equiv 1 \pmod 4$ and $\sqrt{-p}$ if $p \equiv -1 \pmod 4$*

Proof. This is exercise 8 of chapter 2 of [Mar77]. ∎

Proof of Quadratic Reciprocity. We have

$$\left(\frac{q}{p}\right) = 1$$

iff q splits completely in F_2 iff $F_2 \subset F_r$ where $r :=$ the number of distinct primes that q splits into in $\mathbb{Q}[\omega_p]$, and where $\omega_p := e^{2\pi i/p}$. Now F_2 is the unique quadratic extension of $\mathbb{Q}$ intermediate to $\mathbb{Q}[\omega_p]/\mathbb{Q}$. By the above lemma, we see that

$$F_2 = \begin{cases} \mathbb{Q}[\sqrt{p}] & \text{if } p \equiv 1 \pmod 4, \\ \mathbb{Q}[\sqrt{-p}] & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

Thus by Theorem 27 we are reduced to determining how q factors in $\mathbb{Q}[\sqrt{\pm p}]$. This is accomplished by the following Proposition. In greater detail, we argue as follows.

Let us compute $(\frac{2}{p})$. We perform a case analysis on $p \pmod 8$.

$p \equiv 1 \pmod 8 \Rightarrow p \equiv 1 \pmod 4 \Rightarrow \mathbb{Q}[\sqrt{p}] \subset \mathbb{Q}[\omega_p]$. Then, in the notation of the next proposition, we have $m = p \equiv 1 \pmod 4$ so that 2 is split by $(*)$. Therefore $(\frac{2}{p}) = 1$.

$p \equiv 7 \pmod 8 \Rightarrow p \equiv -1 \pmod 4 \Rightarrow \mathbb{Q}[\sqrt{-p}] \subset \mathbb{Q}[\omega_p] \Rightarrow m = -p \equiv -7 \pmod 8 \Rightarrow m \equiv 1 \pmod 8 \Rightarrow$ 2 is split by $(*)$ and therefore $(\frac{2}{p}) = 1$.

$p \equiv 3 \pmod 8 \Rightarrow p \equiv -1 \pmod 4 \Rightarrow \mathbb{Q}[\sqrt{-p}] \subset \mathbb{Q}[\omega_p] \Rightarrow m = -p \equiv -3 \equiv 5 \pmod 8 \Rightarrow$ 2 is inert and therefore $(\frac{2}{p}) = -1$.

$p \equiv 5 \pmod 8 \Rightarrow p \equiv 1 \pmod 4 \Rightarrow \mathbb{Q}[\sqrt{p}] \subset \mathbb{Q}[\omega_p] \Rightarrow m = p \equiv 5 \pmod 8 \Rightarrow 2$ is inert and therefore $(\frac{2}{p}) = -1$.

Let us now compute $(\frac{q}{p})$ for p, q distinct odd primes.

We have:

$p \equiv 1 \pmod 4$ and $(\frac{q}{p}) = 1 \Leftrightarrow q.\mathcal{O}$ splits completely in $\mathbb{Q}[\sqrt{p}] \Leftrightarrow m = p$ and $p \equiv a^2 \pmod q$ for some $a \Leftrightarrow (\frac{p}{q}) = 1$.

[2] This result was reviewed in the previous lecture in the course of working out the example on the splitting of 2 in $\mathbb{Q}[\omega_{23}]$.

$p \equiv 3 \pmod 4$ and $(\frac{q}{p}) = 1 \Leftrightarrow q.\mathcal{O}$ splits completely in $\mathbb{Q}[\sqrt{-p}] \Leftrightarrow m = -p$ and $-p \equiv a^2 \pmod q$ for some $a \Leftrightarrow 1 = (\frac{q}{p}) = (\frac{-p}{q}) = (-1)^{\frac{q-1}{2}}(\frac{p}{q})$. Thus in this case we have:
(case $(\frac{p}{q}) = 1$): $1 = (\frac{q}{p}) = (-1)^{\frac{q-1}{2}} \Leftrightarrow q \equiv 1 \pmod 4$ (i.e. p or $q \equiv 1 \pmod 4$)
and
(case $(\frac{p}{q}) = -1$): $1 = (\frac{q}{p}) = -(-1)^{\frac{q-1}{2}} \Leftrightarrow q \equiv 3 \pmod 4$ (i.e. $p \equiv q \equiv 3 \pmod 4$). ■

Remarks 29. (a) We may give a concise statement of quadratic reciprocity, valid in all cases:

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right).$$

(b) In the above proof, we used the fact that the quadratic symbol may alternatively be defined by

$$\left(\frac{a}{p}\right) := a^{\frac{p-1}{2}} \pmod p$$

which makes it clear that it is gives rise to a homomorphism $(\mathbb{Z}/p)^\times \to \{\pm 1\}$. [see, for instance, the Wikipedia page on the Legendre symbol.]

Proposition 30. *Let $\ell \in \mathbb{Z}$ be a prime and let $\mathcal{O}$ be the ring of integers in the quadratic field $\mathbb{Q}[\sqrt{m}]$ where m is squarefree. Recall that $\mathcal{O}$ has integral basis $\{1, \sqrt{m}\}$ and discriminant $4m$ when $m \equiv 2, -1 \pmod 4$ and integral basis $\{1, (1+\sqrt{m})/2\}$ and discriminant m when $m \equiv 1 \pmod 4$.*

We have
(i) if $\ell | m$ then $\ell.\mathcal{O} = (\ell, \sqrt{m})^2$,
(ii) if m is odd then

$$2.\mathcal{O} = \begin{cases} (2, 1+\sqrt{m})^2 & \text{if } m \equiv -1 \pmod 4, \\ (2, (1+\sqrt{m})/2)(2, (1-\sqrt{m})/2 & \text{if } m \equiv 1 \pmod 8, \\ \text{prime if } m \equiv 5 \pmod 8. \end{cases} \qquad (*)$$

(iii) if ℓ is odd and $\ell \nmid m$ then

$$\ell.\mathcal{O} = \begin{cases} (\ell, n+\sqrt{m})(\ell, n-\sqrt{m}) & \text{if } m \equiv n^2 \pmod p, \\ \text{prime if } m \text{ is not a square mod } p. \end{cases} \qquad (**)$$

and in cases $(*)$ and $(**)$, the factors are distinct.

Proof. See [Mar77, 25, p. 74]. ■

We now turn our attention to the Frobenius automorphism.

Definition 31. Assume that the prime P of K is unramified in L, so that $I(Q/P)$ is trivial. Then we have an isomorphism

$$D(Q/P) \xrightarrow{\sim} \mathrm{Gal}(k(Q)/k(P)).$$

The latter Galois group has the distinguished generator

$$\overline{x} \mapsto \overline{x}^{\|P\|}$$

and the corresponding automorphism $\varphi \in D$ has the property that

$$\varphi(x) \equiv x^{\|P\|} \pmod Q$$

for all $x \in \mathscr{O}_L$. Moreover, φ is uniquely determined in D and hence in G. We denote this automorphism by

$$\mathrm{Fr}_{Q/P}.$$

It is known as the *Frobenius automorphism* of Q/P. One directly verifies that

$$\mathrm{Fr}_{\sigma Q/P} = \sigma \mathrm{Fr}_{Q/P} \sigma^{-1}$$

for $\sigma \in G$ so that the conjugacy class of $\mathrm{Fr}_{Q/P}$ depends only on P, thus if $G = \mathrm{Gal}(L/K)$ is abelian, the Frobenius automorphism depends only on P and we may write Fr_P for the element of G such that

$$\mathrm{Fr}_P(x) \equiv x^{\|P\|} \pmod{P.\mathscr{O}_L}.$$

Let us see what all this means for the cyclotomic fields. Put $L := \mathbb{Q}[\omega], \omega := e^{2\pi i/m}$ and $K := \mathbb{Q}$. Then $G \simeq (\mathbb{Z}/m)^\times$ with $\sigma \in G$ corresponding to $k \in (\mathbb{Z}/m)^\times$ iff $\sigma(\omega) = \omega^k$. We may consider Fr_p for all unramified primes, i.e. for all primes $p \nmid m$ (this is explicitly proved in Washington, Introduction to Cyclotomic Fields, page 10). We have

$$\mathrm{Fr}_p(x) \equiv x^p \pmod{p.\mathbb{Z}[\omega]}$$

for all $x \in \mathbb{Z}[\omega]$. Since the automorphism $\sigma_p : \omega \mapsto \omega^p \in G$ satisfies this congruence, and since G is abelian so that the Frobenius automorphism is uniquely determined as an element of G, we must have that $\sigma_p : \omega \mapsto \omega^p \in G$ coincides with Fr_p. For an arbitrary element $x = \sum a_i \omega^i \in \mathbb{Z}[\omega]$ we have

$$\sigma_p\left(\sum a_i \omega^i\right) = \sum a_i \omega^{pi}$$

and thus

$$\sum a_i \omega^i \equiv \left(\sum a_i \omega^i\right)^p \pmod{p.\mathbb{Z}[\omega]}.$$

Remark 32. It follows from the results proved in chapter 4 that p is ramified in an extension of $\mathbb{Q}$ iff p divides the discriminant. See [Mar77, Theorem 34, p. 112].

References

[FT91] A. Frölich and M. J. Taylor. *Algebraic Number Theory.* Cambridge University Press, 1991. Cambridge Studies in Advanced Mathematics, 27.

[Mar77] Daniel A. Marcus. *Number Fields.* Springer-Verlag, 1977. Universitext.