Student seminar solutions Week 13

1. *Proof.* Let K/F be a cyclic extension of number fields of degree n, let $\mathcal{S}$ be a finite set of rational primes, and let $\mathfrak{p}$ be a prime of $\mathcal{O}_F$. We follow the four steps of the exercise sheet.

   (1) Construction of m and proof of (iii): $K \cap F(\zeta_m) = F$.

   Enlarge $\mathcal{S}$ so that it contains all rational primes that ramify in $F/\mathbb{Q}$ and in $K/\mathbb{Q}$, and also the rational prime below $\mathfrak{p}$. We now apply Lemma 0.1 with this $\mathcal{S}$ and $n = [K : F]$ and obtain an integer $m > 1$, prime to every element of $\mathcal{S}$ and to $\mathfrak{p}$, such that:

   (i) $\mathrm{Gal}(F(\zeta_m)/F) \cong (\mathbb{Z}/m\mathbb{Z})^\times$;

   (ii) $\left(\frac{\mathfrak{p}}{F(\zeta_m)/F}\right)$ has order divisible by n;

   (iii) there exists $\tau \in \mathrm{Gal}(F(\zeta_m)/F)$ of order divisible by n independent from $\left(\frac{\mathfrak{p}}{F(\zeta_m)/F}\right)$.

   Since every rational prime ramifying in $F/\mathbb{Q}$ lies in $\mathcal{S}$ and m is prime to $\mathcal{S}$, no prime dividing m ramifies in $F/\mathbb{Q}$. Conversely, a rational prime $q \nmid m$ cannot ramify in $\mathbb{Q}(\zeta_m)/\mathbb{Q}$. Hence $F \cap \mathbb{Q}(\zeta_m)$ is everywhere unramified over $\mathbb{Q}$, and by the given fact that $\mathbb{Q}$ has no nontrivial everywhere unramified extensions,

   $$F \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$

   The same argument (using that $\mathcal{S}$ contains the primes ramifying in $K/\mathbb{Q}$) gives

   $$K \cap \mathbb{Q}(\zeta_m) = \mathbb{Q}.$$

   Set $L := K \cap F(\zeta_m)$. A standard degree identity yields

   $$[F(\zeta_m) : L] = [K(\zeta_m) : K].$$

   Moreover, thanks to the same identity we have

   $$[F(\zeta_m) : F] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m), \qquad [K(\zeta_m) : K] = [\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \varphi(m).$$

   Therefore

   $$\varphi(m) = [F(\zeta_m) : F] = [F(\zeta_m) : L][L : F] = [K(\zeta_m) : K][L : F] = \varphi(m)[L : F],$$

   so $[L : F] = 1$ and hence

   $$K \cap F(\zeta_m) = F,$$

   which proves (iii).

(2) Description of $\mathrm{Gal}(K(\zeta_m)/F)$.

Let $G = \mathrm{Gal}(K/F) = \langle \sigma \rangle$. Since $K \cap F(\zeta_m) = F$, the extensions K/F and $F(\zeta_m)/F$ are linearly disjoint over F, and restriction induces an isomorphism

$$\mathrm{Gal}(K(\zeta_m)/F) \;\cong\; G \times \mathrm{Gal}(F(\zeta_m)/F).$$

Under this identification,

$$\Big(\frac{\mathfrak{p}}{K(\zeta_m)/F}\Big) = \Big(\frac{\mathfrak{p}}{K/F}\Big) \times \Big(\frac{\mathfrak{p}}{F(\zeta_m)/F}\Big).$$

(3) Definition of H and E, proofs of (iv) and (i).

Assume $\mathfrak{p}$ is unramified in K/F (so Frobenius elements are defined); since $\mathfrak{p} \nmid m$, it is also unramified in $F(\zeta_m)/F$ and in $K(\zeta_m)/F$. Let τ be as in (1) and define

$$H := \big\langle\, \sigma \times \tau,\ \big(\tfrac{\mathfrak{p}}{K(\zeta_m)/F}\big) \big\rangle \subseteq \mathrm{Gal}(K(\zeta_m)/F), \qquad E := K(\zeta_m)^H.$$

(iv) Since $\mathfrak{p}$ is unramified in $K(\zeta_m)/F$, its decomposition group is cyclic generated by the Frobenius element $\big(\frac{\mathfrak{p}}{K(\zeta_m)/F}\big)$, which lies in H. Hence the decomposition group of $\mathfrak{p}$ in E/F is trivial, so $\mathfrak{p}$ splits completely in E/F.

(i) Notice that $\sigma \times \tau \in H$ fixes E and $1 \times \tau \in G \times \mathrm{Gal}(F(\zeta_m)/F)$ fixes K. Therefore, the element

$$\sigma \times 1 = (\sigma \times \tau)(1 \times \tau)^{-1}$$

fixes $K \cap E$. As σ generates $G = \mathrm{Gal}(K/F)$, this implies $K \cap E = F$.

(4) Proof of (ii): $K(\zeta_m) = E(\zeta_m)$.

We have $\mathrm{Gal}(K(\zeta_m)/F(\zeta_m)) \cong G \times 1$. The fixed field of $H \cap (G \times 1)$ is therefore

$$K(\zeta_m)^{H \cap (G \times 1)} = E(\zeta_m).$$

Let $b \in H \cap (G \times 1)$. Since $b \in G \times 1$, we can write $b = \sigma^a \times 1$ for some $a \in \mathbb{Z}$. On the other hand, since $H = \langle\, \sigma \times \tau,\ \big(\frac{\mathfrak{p}}{K(\zeta_m)/F}\big) \rangle$, there exist integers i, j such that

$$b = (\sigma \times \tau)^i \Big(\frac{\mathfrak{p}}{K(\zeta_m)/F}\Big)^j.$$

Using the identification of (2),

$$\Big(\frac{\mathfrak{p}}{K(\zeta_m)/F}\Big) = \Big(\frac{\mathfrak{p}}{K/F}\Big) \times \Big(\frac{\mathfrak{p}}{F(\zeta_m)/F}\Big),$$

we obtain

$$b = \Big(\sigma^i \Big(\frac{\mathfrak{p}}{K/F}\Big)^j\Big) \times \Big(\tau^i \Big(\frac{\mathfrak{p}}{F(\zeta_m)/F}\Big)^j\Big).$$

Comparing second coordinates (since $b = \sigma^a \times 1$) gives

$$\tau^i \Big(\frac{\mathfrak{p}}{F(\zeta_m)/F}\Big)^j = 1.$$

By Lemma 0.1(iii) the subgroups $\langle\tau\rangle$ and $\left\langle \left(\frac{\mathfrak{p}}{F(\zeta_m)/F}\right)\right\rangle$ intersect trivially, hence the equality above forces $\tau^i = 1$ and $\left(\frac{\mathfrak{p}}{F(\zeta_m)/F}\right)^j = 1$. Since both τ and $\left(\frac{\mathfrak{p}}{F(\zeta_m)/F}\right)$ have order divisible by n, we conclude

$$n \mid i \qquad \text{and} \qquad n \mid j.$$

Now compare first coordinates:

$$\sigma^i \left(\frac{\mathfrak{p}}{K/F}\right)^j = \sigma^a.$$

Because $G = \langle\sigma\rangle$ has order n, from $n \mid i$ we get $\sigma^i = 1$, and from $n \mid j$ we get $\left(\frac{\mathfrak{p}}{K/F}\right)^j = 1$. Hence $\sigma^a = 1$ and therefore $b = 1$. Thus $H \cap (G \times 1) = \{1\}$, and consequently

$$K(\zeta_m)^{H\cap(G\times 1)} = K(\zeta_m).$$

But the fixed field of $H \cap (G \times 1)$ is $E(\zeta_m)$, so we obtain

$$K(\zeta_m) = E(\zeta_m),$$

which proves (ii). All four properties are proved. □

2. *Proof.* Let F be a number field and let E be an intermediate field

$$F \subseteq E \subseteq F(\zeta_m),$$

with E/F abelian. We prove that statement (ii) of Artin Reciprocity holds for the extension E/F.

For the cyclotomic extension $F(\zeta_m)/F$, Artin Reciprocity has already been proved. In particular, there exists an ideal $\mathfrak{m}$ of $\mathcal{O}_F$, divisible only by the primes that ramify in $F(\zeta_m)/F$, such that

$$\mathcal{P}^+_{F,\mathfrak{m}} \subseteq \ker\left(\mathcal{A}_{F(\zeta_m)/F} : \mathcal{I}_F(\mathfrak{m}) \longrightarrow \mathrm{Gal}(F(\zeta_m)/F)\right).$$

Since E is an intermediate field of $F(\zeta_m)/F$, every prime of F that ramifies in E/F also ramifies in $F(\zeta_m)/F$. Hence the same ideal $\mathfrak{m}$ is admissible for the extension E/F.

Let $\mathfrak{a} \in \mathcal{P}^+_{F,\mathfrak{m}}$. By the choice of $\mathfrak{m}$, the Artin symbol of $\mathfrak{a}$ in $F(\zeta_m)/F$ is trivial:

$$\left(\frac{\mathfrak{a}}{F(\zeta_m)/F}\right) = 1.$$

By the Consistency Property of the Artin symbol, the Artin symbol of $\mathfrak{a}$ in E/F is the restriction of its Artin symbol in $F(\zeta_m)/F$. Therefore

$$\left(\frac{\mathfrak{a}}{E/F}\right) = \left(\frac{\mathfrak{a}}{F(\zeta_m)/F}\right)\Big|_E = 1.$$

This shows that $\mathfrak{a}$ lies in the kernel of the Artin map for E/F, and hence

$$\mathcal{P}^+_{F,\mathfrak{m}} \subseteq \ker\left(\mathcal{A}_{E/F} : \mathcal{I}_F(\mathfrak{m}) \longrightarrow \mathrm{Gal}(E/F)\right).$$

Thus statement (ii) of Artin Reciprocity holds for the extension E/F, as required. □

3. *Proof.* Let K/F be an abelian extension with Galois group G, and fix an element $\sigma \in G$. Let $\mathfrak{m}$ be a modulus divisible only by the primes that ramify in K/F. The Artin map

$$\mathcal{A} : \mathcal{I}_F(\mathfrak{m}) \longrightarrow G$$

is surjective, and its kernel is

$$H := \mathcal{P}^+_{F,\mathfrak{m}} \mathcal{N}_{K/F} \mathcal{I}_K(\mathfrak{m}), \qquad \mathcal{I}_F(\mathfrak{m})/H \cong G.$$

Choose an ideal $\mathfrak{a} \in \mathcal{I}_F(\mathfrak{m})$ such that $\mathcal{A}(\mathfrak{a}) = \sigma$. Since only finitely many primes divide $\mathfrak{m}$, removing them does not change Dirichlet density, so it suffices to consider primes $\mathfrak{p} \nmid \mathfrak{m}$. For a prime ideal $\mathfrak{p} \nmid \mathfrak{m}$ we have

$$\left(\frac{\mathfrak{p}}{K/F}\right) = \sigma \quad \Longleftrightarrow \quad \mathcal{A}(\mathfrak{p}) = \mathcal{A}(\mathfrak{a}) \quad \Longleftrightarrow \quad \mathfrak{p}\mathfrak{a}^{-1} \in H.$$

Thus the set S_σ of primes of $\mathcal{O}_F$ whose Frobenius equals σ is precisely the set of primes contained in the coset $\mathfrak{a}H$.

Since $\mathcal{P}^+_{F,\mathfrak{m}} \subset H$, the hypotheses of Proposition 2.3 of chapter 3 are satisfied. Applying this proposition to the coset $\mathfrak{a}H$, we obtain

$$\delta_F(S_\sigma) = \frac{1}{[\mathcal{I}_F(\mathfrak{m}) : H]}.$$

Finally, because $\mathcal{I}_F(\mathfrak{m})/H \cong G$, we have $[\mathcal{I}_F(\mathfrak{m}) : H] = |G| = [K : F]$, and therefore

$$\delta_F(S_\sigma) = \frac{1}{[K : F]}.$$

□

4. *Proof.* Let K/F be an abelian extension of number fields. By Artin reciprocity, the idelic Artin map

$$\mathcal{A} : J_F \longrightarrow \mathrm{Gal}(K/F)$$

is surjective and has kernel

$$\ker(\mathcal{A}) = F^\times N_{K/F} J_K.$$

Recall that the idèle class group of F is defined by

$$C_F := J_F/F^\times.$$

Since $\mathcal{A}(f) = 1$ for every $f \in F^\times$, we have $F^\times \subseteq \ker(\mathcal{A})$. Therefore $\mathcal{A}$ is constant on cosets of $F^\times$ and factors through the quotient C_F, inducing a map

$$\overline{\mathcal{A}} : C_F \longrightarrow \mathrm{Gal}(K/F), \qquad \overline{\mathcal{A}}(xF^\times) := \mathcal{A}(x).$$

This map is well defined: if $xF^\times = yF^\times$, then $y = xf$ for some $f \in F^\times$, and hence

$$\mathcal{A}(y) = \mathcal{A}(x)\mathcal{A}(f) = \mathcal{A}(x),$$

because $f \in \ker(\mathcal{A})$. Moreover, $\overline{\mathcal{A}}$ is surjective, since $\mathcal{A}$ is surjective and the natural projection $J_F \twoheadrightarrow C_F$ is surjective.

By definition, the kernel of $\overline{\mathcal{A}}$ is

$$\ker(\overline{\mathcal{A}}) = \{\, xF^\times \in C_F : \mathcal{A}(x) = 1 \,\} = \frac{\ker(\mathcal{A})}{F^\times} = \frac{F^\times N_{K/F} J_K}{F^\times}.$$

The idelic norm map

$$N_{K/F} : J_K \longrightarrow J_F$$

sends principal idèles of $K^\times$ to principal idèles of $F^\times$ and thus induces a homomorphism on idèle class groups,

$$N_{K/F} : C_K = J_K/K^\times \longrightarrow C_F = J_F/F^\times, \qquad jK^\times \longmapsto N_{K/F}(j)F^\times.$$

Its image is

$$N_{K/F}C_K = \{\, N_{K/F}(j)F^\times : j \in J_K \,\} \subseteq C_F.$$

By construction, this image coincides with the image of $N_{K/F}J_K$ in C_F, and therefore

$$N_{K/F}C_K = \frac{F^\times N_{K/F} J_K}{F^\times} = \ker(\overline{\mathcal{A}}).$$

Thus the induced Artin map

$$\overline{\mathcal{A}} : C_F \longrightarrow \mathrm{Gal}(K/F)$$

is surjective with kernel $N_{K/F}C_K$, and by the First Isomorphism Theorem we obtain

$$\frac{C_F}{N_{K/F}C_K} \;\cong\; \mathrm{Gal}(K/F).$$

This gives the desired reformulation of the idelic Artin map. □