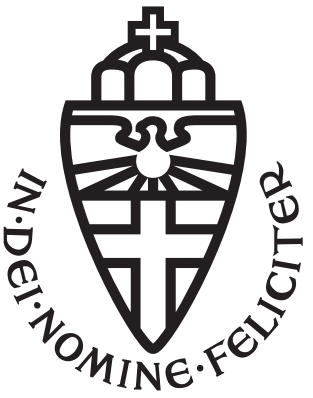
Computing Torsion in Field Extensions

Sep Thijssen

June 21, 2010



Master Thesis in Mathematics
Department of Mathematics
Radboud University Nijmegen
Supervisor: Wieb Bosma
Second reader: Hendrik Lenstra, Jr.

Abstract

Let K/F be a finite separable extension of fields. The object of study in this thesis shall be the torsion subgroup $\mathcal{T}$ of K^*/F^*. $\mathcal{T}$ can be described in terms of 1-cocycles. To do this we will use Galois cohomology. When K contains at most finitely more roots of unity then F, the group $\mathcal{T}$ is finite. In this case, one might wonder whether it is possible to construct a subset S of K^* of representatives of $\mathcal{T}$, i.e. such that $SF^*/F^* = \mathcal{T}$. In the case of number fields an algorithm is given that produces such a set S. The emphasis is on proving that the algorithm is good in terms of complexity, and not in making it practical.

1 Introduction

Notation 1. For any positive integer n and (multiplicatively written) abelian group A, the groups $A[n]$ and A^n denote respectively the kernel and the image of the endomorphism $A \to A$, $x \mapsto x^n$. $A[n]$ is referred to as the *n-torsion* in A, and A^n as the *n-th powers*. The *complete torsion* of A is

$$\mathrm{Tor}(A) = \bigcup_{n \in \mathbb{Z}_{>0}} A[n].$$

For any positive integer n, ζ_n denotes a primitive n-th root of unity.

Let K/F be a finite separable extension of fields. A natural question is: what can be said about the factor group K^*/F^*? For algorithmic purposes there is a negative answer: the group K^*/F^* is not finitely generated when F is infinite and $K \neq F$. This result is due to Brandis, see [2, 6]. So we have to be a bit less ambitious, and restrict ourselves to subgroups M of K^* such that M/F^* is somehow under control, for example the case that M/F^* is finite. In that case M only contains so called radicals over F. In general one has $\#M/F^* \geq [F(M) : F]$ and due to Kneser's Theorem we know exactly when equality holds.

Theorem 2 (Kneser)**.** *Let F be a field with separable closure F_{sep} and let M be a group $F^* \subset M \subset F_{\mathrm{sep}}^*$ such that $[M : F^*] < \infty$. Then one has*

$$\#M/F^* = [F(M) : F]$$

if and only if the following two conditions are satisfied:

(i) If p is an odd prime dividing $[M : F^*]$ and M contains a p-th root of unity ζ_p, then $\zeta_p \in F$.

(ii) If ζ_4 is a 4-th root of unity and M contains $1 + \zeta_4$, then $\zeta_4 \in F$.

For a proof, see for example [7, 15, 6].

Clearly the existence or absence of certain roots of unity plays a central role in Kneser's Theorem. This phenomenon is not unusual when studying radicals. Subgroups of K^* that contain F^* with finite index, say n, certainly are torsion mod F^*. Consider therefore the subgroup T of K^* such that

$T/F^* = (K^*/F^*)[n]$. Let $\mu = K^*[n]$ be the group of all n-th roots of unity in K. Then there is an exact sequence

$$0 \longrightarrow \mu F^*/F^* \longrightarrow T/F^* \longrightarrow T/\mu F^* \longrightarrow 0.$$

It follows that T/F^* is finite if and only if $\mu F^*/F^*$ and $T/\mu F^*$ are. The first is finite when K contains at most finitely many more roots of unity then F. The second is finite, which is a consequence of the following Theorem.

Theorem 3 (van Tieghem)**.** *Let K/F be a finite separable field extension, and let $\mu = \mathrm{Tor}(K^*)$ be the group of all roots of unity in K^*. Then $\mathrm{Tor}(K^*/\mu F^*)$ is a finite group of order dividing $[K : F]$.*

The original proof of van Tieghem [16] is very long. A shorter version, which makes use of Galois Cohomology can be found in [15]. This theorem was also – probably independently – proven by May, see for example [12, 6].

Suppose that K/F is an extension of number fields. Let $d = \#K^*[n]$ be the number of n-th roots of unity in K, and let $m = [K : \mathbb{Q}]$. Then

$$\#(K^*/F^*)[n] \leq d \cdot [K : F] \leq dm.$$

Let φ be Euler's totient function. Then $\varphi(d) \leq m$. Note that $i \leq 2\varphi(i)^2$ for any $i \in \mathbb{Z}_{>0}$. Hence we get

$$\#(K^*/F^*)[n] \leq 2m^3.$$

In particular the group $\mathcal{T} = \mathrm{Tor}(K^*/F^*)$ is finite. This allows us to only worry about the n-torsion for finitely many n. Furthermore, since $\mathcal{T}$ equals the direct product of all of its primary parts it would suffice to consider $\mathrm{Tor}(K^*/F^*)[p^k]$ for primes p and integers $k > 0$.

Another consequence of the bound $\#\mathcal{T} \leq 2m^3$ is that the 'size' of $\mathcal{T}$ is a priori not too large to 'compute' $\mathcal{T}$. It is polynomially bounded in the degree $m = [K : \mathbb{Q}]$, and hence in the 'size of K', which will be part of the input of the algorithm we have in mind. That it is indeed possible to 'compute' $\mathcal{T}$ in a reasonable time is the Main Theorem of this thesis.

Theorem 4 (Main Theorem)**.** *Let K/F be an extension of number fields. Then $\mathrm{Tor}(K^*/F^*)$ is a finite group and there is a polynomial time algorithm that constructs a subset of K^* of representatives of $\mathrm{Tor}(K^*/F^*)$.*

The main object of study is $(K^*/F^*)[n]$ for some integer n and finite separable extension K/F of fields. The next section will contain a superficial study of this group. In Section 4 we will go deeper in the theory to describe $(K^*/F^*)[n]$ in terms of 1-cocycles. Galois cohomology is the main tool used for this. Section 3 will contain the results needed from Galois cohomology, like a cohomological version of Hilbert 90. In Sections 5–7 the group $(K^*/F^*)[n]$ will be cut into smaller pieces that can be calculated individually. This will finish the mathematical analyses and the first half of this thesis.

Algorithms in number fields are the subject of the second half, which contains Sections 8 and 9. An introduction and some basic results are given in Section 8. In Section 9 we will prove the Main Theorem and other crucial theorems such as:

Theorem 5. *Let F be a number field. Then there is a polynomial time algorithm that constructs an integer n such that* $\mathrm{Tor}(F^*) = \langle \zeta_n \rangle$.

2 Reduction

Let K/F be an extension of fields, and let n be a positive integer not divisible by the characteristic. Note that $(K^*/F^*)[n]$ is a subgroup of $(K(\zeta_n)^*/F^*)[n]$. Suppose that $S \subset K(\zeta_n)^*$ is a set of representatives of $(K(\zeta_n)^*/F^*)[n]$. Then a set of representatives for $(K^*/F^*)[n]$ is easily computed:

$$\{s \mid s \in S,\ s \in K\}.$$

Therefore we shall only worry about n-torsion in extensions K/F such that $\zeta_n \in K$.

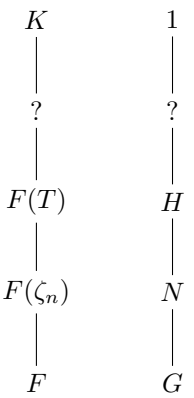
Let $T \subset K^*$ be such that $T/F^* = (K^*/F^*)[n]$. All intermediate fields L in $K/F(T)$ have the same n-torsion over F^*, because

$$T/F^* = \big(K^*/F^*\big)[n] \supset \big(L^*/F^*\big)[n] \supset \big(F(T)^*/F^*\big)[n] \supset T/F^*.$$

We will try to reduce the problem by calculating intermediate fields with nice properties.

Suppose that $\zeta_n \in K$. Then $F(T)/F$ is a normal extension. Suppose also that K/F is separable. Then $F(T)/F$ is Galois. This gives rise to a 'nice' intermediate field of $K/F(T)$, namely the largest Galois extension of F contained in K. That field can actually be calculated because it equals the intersection of all conjugates of K over F.

Remark 6. Let K/F be a finite Galois extension, and n a positive integer such that $\zeta_n \in K$. Let $T \subset K^*$ be such that $T/F^* = (K^*/F^*)[n]$. Let G be the Galois group of K/F, and let $H \subset G$ and $N \subset G$ be the Galois groups of respectively $K/F(T)$ and $K/F(\zeta_n)$. One might wonder how to reduce the problem further. That is to find ever smaller and/or nicer intermediate fields of $K/F(T)$. Perhaps it is possible to reduce to an intermediate field that equals $F(T)$. The equivalent approach for the corresponding groups would be to find ever larger subgroups of H. In Section 4 we will show that H can be computed in the primary case.



$F(T)/F(\zeta_n)$ is a Galois extension with group isomorphic to N/H, which is abelian and annihilated by n. By group theory these two facts come down to respectively: H contains $[N, N]$ – the group generated by the commutators in N, and H contains N^n. So we have the inclusion $[N, N]N^n \subset H$. This leads to a reduction. Instead of K we could consider the field L of invariants of $[N, N]N^n$. This reduction will in general not bring us to the field $F(T)$, see the example below. It turns out that the field $F(T)$ cannot be recognized by the presence of roots of unity in the splitting field and the structure of the Galois group alone. Instead one should consider the Galois group together with an action on the roots of unity, and this brings us to Galois cohomology.

Example 7. This example is inspired by an article of Bruen, Jensen and Yui [3]. They study Galois extensions that have a Frobenius group of prime degree. Radical extensions give rise to such groups, but it turns out that the converse is in general not true.

Let $a = \zeta_5 + \zeta_5^{-1}$, and α a root of $X^5 - a$. Consider $f = X^5 + 5X^3 + 5X - 1 \in \mathbb{Q}[x]$. By Eisenstein's criterion with $p = 5$, $f(X+1)$ is irreducible, and hence f. The roots of f are

$$1/(\zeta_5^i \alpha) - \zeta_5^i \alpha \qquad \text{for } \ i = 1, 2, \ldots, 5.$$

So f splits into linear factors over $K = \mathbb{Q}(\alpha, \zeta_5)$. Let β be a real valued zero of f and write $E = \mathbb{Q}(\beta)$, then $K = E(\zeta_5)$. The extension $E(\zeta_5)/E$ is cyclic of degree 4. It has a unique proper intermediate field $E(\sqrt{5})$ which is real valued. Because not all zeros of f are real valued, K is a splitting field of f. In other words, $K/\mathbb{Q}$ is Galois, say with group G. Let $N \subset G$ be the Galois group of $K/\mathbb{Q}(\zeta_5)$. Then there is a short exact sequence

$$1 \longrightarrow N \longrightarrow G \longrightarrow G/N \longrightarrow 1.$$

N is of order 5, and hence cyclic. G/N is isomorphic to the Galois group of $\mathbb{Q}(\zeta_5)/\mathbb{Q}$, which is cyclic of order 4. It follows that G is generated by two elements σ, τ with $N = \langle \sigma \rangle$, and $\tau(\zeta_5) = \zeta_5^i$, where i has order 4 in $(\mathbb{Z}/5\mathbb{Z})^*$. Now

$$\tau(a)a = (\zeta_5^2 + \zeta_5^3)(\zeta_5 + \zeta_5^{-1}) = \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = -1.$$

Therefore

$$\tau(\alpha) = \tau(\sqrt[5]{a}) = \sqrt[5]{-a^{-1}} = c\alpha^{-1}$$

for some $c \in \mathbb{Q}(\zeta_5)$. Without loss of generality assume that $\sigma(\alpha) = \zeta_5 \alpha$. Because N is normal in G there is an integer j with $\tau\sigma\tau^{-1} = \sigma^j$. So

$$\tau\sigma(\alpha) = \zeta_5^i c\alpha^{-1} \qquad \text{and} \qquad \sigma^j\tau(\alpha) = \zeta_5^{-j} c\alpha^{-1},$$

and $i \equiv -j \mod 5$.

Let $T \subset K^*$ be such that $T/\mathbb{Q}^* = (K^*/\mathbb{Q}^*)[5]$, and let $H \subset G$ bet the Galois group of $K/F(T)$. Then certainly $H \supset [N,N]N^5$, because $[N,N]N^5$ is the trivial group. So K is already reduced as discussed in Remark 6. But this does in general not mean that $K = F(T)$, as shown below.

Suppose that $K = F(T)$. Then K contains an element γ with $\gamma^5 \in \mathbb{Q}$, and with $\gamma \notin \mathbb{Q}(\zeta_5)$. It follows that γ is a root of the irreducible $X^5 - \gamma^5$. The 5 fields $\mathbb{Q}(\zeta_5^t \gamma)$, for $t = 0, \ldots, 4$, of degree 5 over $\mathbb{Q}$ are conjugate to each other. One of them is K^τ. Assume without loss of generality that $\mathbb{Q}(\gamma) = K^\tau$. Then $\tau(\gamma) = \gamma$. Let k be such that $\sigma(\gamma) = \zeta_5^k \gamma$. Then

$$\tau\sigma(\gamma) = \zeta_5^{ik}\gamma \qquad \text{and} \qquad \sigma^j\tau(\gamma) = \zeta_5^{jk}\gamma.$$

But then $i \equiv j \mod 5$. Contradiction. So $K \neq F(T)$.

3 Galois and Group Cohomology

Definition 8. Let G be a group. If G acts on an abelian group M by means of a homomorphism $G \to \mathrm{Aut}(M)$, then M is called a *G-module*.

Example 9. If K/F is a Galois extension with group G then K^* is a G-module by $\sigma k = \sigma(k)$ for $\sigma \in G$ and $k \in K^*$. In other words: the action is defined by evaluation. Similarly, the additive group of K is a G-module.

Definition 10. Let M be a G-module, and n a non-negative integer. An *n-cochain* is a function $(\prod_{i=1}^{n} G) \to M$. The set of all such functions is denoted by $\mathrm{C}^n(G, M)$. Note that $\mathrm{C}^0(G, M)$ can be identified by M. The *n-th boundary function* $\delta_n : \mathrm{C}^n(G, M) \to \mathrm{C}^{n+1}(G, M)$ is defined by

$$\begin{aligned}\delta_n(f)(\sigma_1, \ldots, \sigma_{n+1}) = {} & \sigma_1 f(\sigma_2, \ldots, \sigma_{n+1}) \\ & + \sum_{i=1}^{n} f(\sigma_1, \ldots, \sigma_i\sigma_{i+1}, \ldots, \sigma_{n+1}) \\ & + (-1)^{n+1} f(\sigma_1, \ldots, \sigma_n).\end{aligned}$$

Theorem 11. *Let G be a group, M be a G-module, and n a non-negative integer. Then*

(i) The set $\mathrm{C}^n(G, M)$ can be made into an abelian group by adding n-cochains component wise.

(ii) $\delta_n \circ \delta_{n-1} = 0$ for $n > 0$.

(iii) δ_n is a homomorphism for all $n \geq 0$.

Statement (i) is easy to verify. A straightforward but tedious calculation shows that (ii) and (iii) are true. There is an indirect proof of (ii) and (iii) in [14], where our n-cochains are given the predicate *inhomogeneous*. In [8] the cohomology of groups is treated in the exercises.

Definition 12. Let G be a group, M be a G-module, and n a positive integer. Define the following abelian groups

(i) $\mathrm{B}^n(G, M) = \operatorname{Im} \delta_{n-1}$, whose elements are called *n-coboundaries*.

(ii) $\mathrm{Z}^n(G, M) = \operatorname{Ker} \delta_n$, whose elements are called *n-cocycles*.

(iii) The *n-th cohomology* of G with coefficients in M is the factor group $\mathrm{H}^n(G, M) = \mathrm{Z}^n(G, M)/\mathrm{B}^n(G, M)$.

Example 13. (i) A 1-cocycle is a function $f\colon G \to M$ satisfying $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$ for $\sigma, \tau \in G$. Such functions are also called *crossed homomorphisms*.

(ii) A 1-coboundary is a function $f\colon G \to M$ satisfying $f(\sigma) = \sigma m - m$ for some $m \in M$ and all $\sigma \in G$.

Definition 14. Let A be a monoid (by convention with a unit element) and let F be a field. A *character* of A in F is a homomorphism $\chi\colon A \to F^*$. Characters $\chi_1, \ldots, \chi_n$ are called *linearly independent* over F when the relation $\sum a_i\chi_i = 0$ for $a_i \in F$ implies that $a_i = 0$ for all i.

Theorem 15 (Artin)**.** *Distinct characters $\chi_1, \ldots, \chi_n$ of a monoid A in a field F are linearly independent.*

Proof. See also [8]. Assume by contradiction that the χ_i are linearly dependent. Take a minimal $m \geq 2$, indices $I = \{i_1, \ldots, i_m\}$, and coefficients $\{a_i \mid i \in I\}$ such that

$$\sum_{i \in I} a_i \chi_i(x) = 0 \qquad \text{for all } x \in A.$$

Note that by minimality of m, all a_i are nonzero. Let $j, k \in I$ distinct. Then χ_j is distinct from χ_k, and there is an $b \in A$ such that $\chi_j(b) \neq \chi_k(b)$. Let $x \in A$. Then

$$0 = \sum_{i \in I} a_i \chi_i(bx) = \sum_{i \in I} a_i \chi_i(b) \chi_i(x) \qquad \text{for all } x \in A.$$

By minimality of m, $\chi_j(b)$ is nonzero. Dividing the last equality by $\chi_j(b)$ and subtracting it from the first yields:

$$\sum_{i \in I} \left(a_i - a_i \frac{\chi_i(b)}{\chi_j(b)} \right) \chi_i = 0.$$

The term with index j disappears, while the k-th has nonzero coefficient. Contradiction by minimality of m. □

Remark 16. The theorem above is called "Linear independence of characters". Dedekind already proved the special case where $A = F^*$ and $\chi_1, \ldots, \chi_n$ are distinct automorphisms of F. This special case is also referred to as Dedekind's Lemma in the literature.

Corollary 17. *Let K/F be a finite Galois extension with group $G = \{\sigma_1, \ldots, \sigma_n\}$, and let $\alpha_1, \ldots, \alpha_n$ be a basis for K as an F-vectorspace. If $\sum_i c_i \sigma_i(\alpha_j) = 0$ for all j, then $c_i = 0$ for all i.*

Proof. Let $x \in K$, and let $b_i \in F$ such that $x = \sum_j b_j \alpha_j$. Then

$$\sum_i c_i \sigma_i(x) = \sum_i c_i \sigma_i \sum_j b_j \alpha_j = \sum_j b_j \sum_i c_i \sigma_i(\alpha_j) = 0.$$

By linear independence of characters, $c_i = 0$ for all i. □

Theorem 18 (Cohomological Hilbert 90)**.** *Let K/F be a Galois extension with group G. Then $\mathrm{H}^1(G, K^*)$ and $\mathrm{H}^1(G, K)$ are trivial for the action of G on respectively the multiplicative group K^* and additive group K defined by evaluation of automorphism.*

Proof. See also [8, 13]. Let f be a multiplicative 1-cocycle. We have to prove that f is a 1-coboundary. By linear independence of characters there is a $\beta \in K$ such that

$$\alpha = \sum_{\sigma \in G} f(\sigma) \sigma(\beta)$$

is non zero. Applying an arbitrary $\tau \in G$ yields

$$\tau(\alpha) = \sum_{\sigma \in G} \tau f(\sigma) \tau\sigma(\beta).$$

The multiplicative 1-cocycle condition is $f(\tau\sigma) = f(\tau)\tau(f(\sigma))$. Hence

$$\begin{aligned}\tau(\alpha) &= \sum_{\sigma\in G} f(\tau\sigma)f(\tau)^{-1}\tau\sigma(\beta)\\ &= f(\tau)^{-1}\sum_{\sigma\in G} f(\tau\sigma)\tau\sigma(\beta)\\ &= f(\tau)^{-1}\sum_{\sigma\in G} f(\sigma)\sigma(\beta)\\ &= f(\tau)^{-1}\alpha.\end{aligned}$$

It follows that f satisfies the multiplicative 1-coboundary condition $f(\tau) = \tau(\alpha^{-1})/\alpha^{-1}$ for all $\tau \in G$.

Now, let f be an additive 1-cocycle. By linear independence of characters there is a $\beta \in K$ with $\mathrm{tr}(\beta) = \sum_{\sigma\in G}\sigma(\beta) \neq 0$. Consider the element

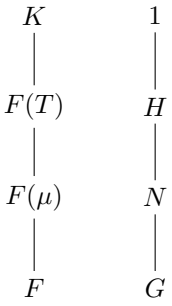
$$\alpha = \frac{1}{\mathrm{tr}(\beta)}\sum_{\sigma\in G} f(\sigma)\sigma(\beta).$$

It is not hard to check that $f(\tau) = \tau(-\alpha) - (-\alpha)$ for all $\tau \in G$. □

4 Torsion and 1-Cocycles

In this section we keep the following notation:

- K/F is a finite Galois extension with Galois group G,
- n is an integer such that $\zeta_n \in K$,
- $\mu = \langle\zeta_n\rangle = K^*[n]$,
- $T \subset K^*$ is such that $T/F^* = (K^*/F^*)[n]$,
- N is the Galois group of $K/F(\mu)$,
- H is the Galois group of $K/F(T)$.



Remark 19. Let $f \in \mathrm{Z}^1(G,\mu)$. Consider the expression $\sum_{\sigma\in G} f(\sigma)\cdot\sigma$. All σ are distinct characters of K^* in K^*, and all the coefficients are nonzero. By linear independence of characters, there is a $\beta \in K^*$ such that

$$\sum_{\sigma\in G} f(\sigma)\cdot\sigma(\beta) \neq 0.$$

Theorem 20 (Dummit [5])**.** *There is an isomorphism of groups $T/F^* \cong \mathrm{Z}^1(G,\mu)$ given by $\alpha F^* \longmapsto (\sigma \mapsto \alpha/\sigma(\alpha))$ with inverse $f \longmapsto \alpha_f F^*/F^*$, where $\alpha_f = \sum_{\sigma\in G} f(\sigma)\cdot\sigma(\beta_f)$, and where $\beta_f \in K$ is any element such that $\alpha_f \neq 0$.*

Proof. By Hilbert 90 $\mathrm{Z}^1(G,K^*) = \mathrm{B}^1(G,K^*)$, and $\mathrm{Z}^1(G,\mu)$ clearly is a subset of this. If $\alpha \in T$ and $\sigma \in G$, then $\sigma(\alpha) = \zeta_n^i\alpha$ for some integer i. Because $\alpha/\sigma(\alpha) = \sigma(\alpha^{-1})/\alpha^{-1}$ the map

$$\begin{aligned}T/F^* &\longrightarrow \mathrm{Z}^1(G,\mu),\\ \alpha F^* &\longmapsto \sigma \mapsto \alpha/\sigma(\alpha).\end{aligned}$$

has its image in $\mathrm{Z}^1(G,\mu)$. It is not hard to check that it is a well-defined homomorphism. Suppose αF^* is in the kernel. Then $\sigma(\alpha)=\alpha$ for all $\sigma\in G$. In other words $\alpha\in K^G=F$, such that αF^* is trivial. It follows that this homomorphism is injective.

Let $f\in \mathrm{Z}^1(G,\mu)$. Then $\sum_{\sigma\in G} f(\sigma)\cdot\sigma$ is a sum of characters with nonzero coefficients. By linear independence of characters there is a $\beta_f\in K^*$ depending on f such that $\alpha_f=\sum_{\sigma\in G} f(\sigma)\cdot\sigma(\beta_f)\neq 0$. Let $\tau\in G$, then

$$\begin{aligned}\tau(\alpha_f) &= \sum_{\sigma\in G} \tau f(\sigma)\cdot\tau\sigma(\beta_f)\\ &= \sum_{\sigma\in G} f(\tau\sigma)\cdot f(\tau)^{-1}\cdot\tau\sigma(\beta_f)\\ &= f(\tau)^{-1}\sum_{\sigma\in G} f(\tau\sigma)\cdot\tau\sigma(\beta_f)\\ &= f(\tau)^{-1}\sum_{\sigma\in G} f(\sigma)\cdot\sigma(\beta_f)\\ &= f(\tau)^{-1}\cdot\alpha_f,\end{aligned}$$

such that

$$f(\tau)=\alpha_f/\tau(\alpha_f).$$

Because $\mathrm{Im}(f)\subset\mu$ the image of f is killed by taking the n-th power. Thus

$$\tau(\alpha_f^n)=\alpha_f^n \qquad \text{for all } \tau\in G.$$

In other words $\alpha_f^n\in K^G=F$ and $\alpha_f\in T$. So the image of the map $f\longmapsto \alpha_f F^*$ is contained in T/F^*. Composing this map with the homomorphism we defined before yields

$$f\longmapsto \alpha_f F^*\longmapsto \big(\tau\mapsto \alpha_f/\tau(\alpha_f)\big).$$

This composition is the identity because $\alpha_f/\tau(\alpha_f)=f(\tau)$. In particular the homomorphism from before is surjective. We already proved that it was injective. It follows that both maps in the composition are bijective and inverse to each other. Furthermore the map $f\longmapsto\alpha_f F^*$ satisfies the homomorphism condition, because the other map in the composition does. □

Example 21. Let F be a field with $\mathrm{char}\, F\neq 2$ and $\zeta_4\notin F$. Suppose that there exists an integer t such that $\zeta_{2^t}\in F(\zeta_4)$ but $\zeta_{2^{t+1}}\notin F(\zeta_4)$. Let $T\subset F(\zeta_4)^*$ be such that $T/F^*=\big(F(\zeta_4)^*/F^*\big)[2^t]$. We shall determine a set $S\subset F(\zeta_4)^*$ of cardinality $\#T/F^*$ such that $SF^*/F^*=T/F^*$. In other words, a set of coset representatives. This special case was also studied by Vélez, see [17].

Let $\mu=\langle\zeta_{2^t}\rangle=F^*[2^t]$. The order of T/F^* is the product of the orders $\#\mu F^*/F^*=2^{t-1}$ and $\#T/\mu F^*$. The latter is a divisor of 2 by van Tieghem. Hence the order of T/F^* is at most 2^t.

The extension $F(\zeta_4)/F$ is Galois of order two, say with group G generated by σ. Then $\sigma(\zeta_4)=\zeta_4^{-1}$. Let j be such that $\sigma(\zeta_{2^t})=\zeta_{2^t}^j$. Using that $\sigma^2=1$ yields

$$j^2\equiv 1 \mod 2^t,$$

which has four solutions mod 2^t:

$$j \in \{1,\ -1,\ 2^{t-1}+1,\ 2^{t-1}-1\}.$$

Using that $\sigma(\zeta_4) \neq \zeta_4$ yields that either $j = -1$ or $j = 2^{t-1} - 1$. Hence one of the following is the case:

(i) $\sigma(\zeta_{2^t}) = \zeta_{2^t}^{-1}$,

(ii) $\sigma(\zeta_{2^t}) = -\zeta_{2^t}^{-1}$.

Case (i). Consider $\alpha_k = 1 + \zeta_{2^t}^k$. Then $\alpha_k/\sigma(\alpha_k) = \zeta_{2^t}^k$. So the map $f_k \colon \sigma \mapsto \zeta_{2^t}^k$ defines an element of $\mathrm{Z}^1(G,\mu)$. When varying k, one finds 2^t distinct f_k. Together they are all of $\mathrm{Z}^1(G,\mu)$, because $\mathrm{Z}^1(G,\mu)$ has order at most 2^t. It follows that the set $S = \{\alpha_k \mid k = 1, \ldots, 2^t\}$ is such that $SF^*/F^* = T/F^*$.

Case (ii). Let $f \in \mathrm{Z}^1(G,\mu)$. Then $f(\sigma) = \zeta_{2^t}^k$ for some $k = 1, \ldots, 2^t$. By the 1-cocycle condition

$$1 = f(\sigma^2) = f(\sigma) \cdot \sigma f(\sigma) = \zeta_{2^t}^k \cdot \sigma(\zeta_{2^t}^k) = \zeta_{2^t}^k \cdot (-1)^k \cdot \zeta_{2^t}^{-k} = (-1)^k.$$

It follows that k is a multiple of 2, and that T/F^* has order at most 2^{t-1}. The group $\mu F^*/F^*$ has already order 2^{t-1}, so $S = \mu$ is as desired.

Proposition 22.

$$H = \bigcap_{f \in \mathrm{Z}^1(G,\mu)} \mathrm{Ker}(f).$$

Proof. Let $\sigma \in H$ and let $f \in \mathrm{Z}^1(G,\mu)$. By Theorem 20, choose $\alpha \in T$ such that $f(\sigma) = \sigma(\alpha)/\alpha$. The action of H on T is trivial because $F(T) = K^H$. So $f(\sigma) = 1$, or equivalently $\sigma \in \mathrm{Ker}(f)$. This holds for all $\sigma \in H$, $f \in \mathrm{Z}^1(G,\mu)$, and therefore $H \subset \bigcap_{f \in \mathrm{Z}^1(G,\mu)} \mathrm{Ker}(f)$.

Let $\sigma \in \bigcap_{f \in \mathrm{Z}^1(G,\mu)} \mathrm{Ker}(f)$. Then $f(\sigma) = 1$ for all $f \in \mathrm{Z}^1(G,\mu)$. Let $\alpha \in T$. The map $\tau \mapsto \tau(\alpha)/\alpha$ is an element of $\mathrm{Z}^1(G,\mu)$. So $\sigma(\alpha) = \alpha$. It follows that σ acts trivially on T, and hence on $F(T)$. Therefore σ is contained in the corresponding group H. □

Definition 23. Let φ be the composition of the homomorphisms $G \to \mathrm{Aut}(\mu) \to (\mathbb{Z}/n\mathbb{Z})^*$. That is defined by $\varphi(\sigma) = i + n\mathbb{Z}$, where i is such that $\sigma(\zeta_n) = \zeta_n^i$.

Remark 24. Note that μ is contained in $F(\mu)$, the field of invariants of N. In other words, the action of N on μ is trivial. The action on μ completely determines the F-automorphism of $F(\mu)$. This action is described by the homomorphism φ in terms of 'taking powers'. In particular $N = \mathrm{Ker}(\varphi)$. Because the action of N on μ is trivial, the 1-cocycle condition becomes the homomorphism condition: let $\sigma, \tau \in N$, then

$$f(\sigma\tau) = f(\sigma) \cdot \sigma f(\tau) = f(\sigma) \cdot f(\tau).$$

It follows that $\mathrm{Z}^1(N,\mu) = \mathrm{Hom}(N,\mu)$.

Proposition 25. *Let $f \in \mathrm{Z}^1(G,\mu)$, and let $\sigma \in G$, $\tau \in N$. Then*

(i) $f(\sigma\tau\sigma^{-1}\tau^{-i}) = 1$, for all $i \in \mathbb{Z}$ with $\varphi(\sigma) = i + n\mathbb{Z}$.

(ii) $\varphi(\sigma) = -1 + n\mathbb{Z} \quad \Longrightarrow \quad f(\sigma^2) = 1.$

Proof. (i) Let $\sigma \in G$ $\tau \in N$, and $i \in \mathbb{Z}$ such that $\varphi(\sigma) = i + n\mathbb{Z}$. Recall that τ acts trivially on μ. Using the 1-cocycle condition we obtain

$$\begin{aligned} f(\sigma\tau\sigma^{-1}) &= f(\sigma\tau) \cdot \sigma\tau f(\sigma^{-1}) \\ &= f(\sigma\tau) \cdot \sigma f(\sigma^{-1}) \\ &= f(\sigma) \cdot \sigma f(\tau) \cdot \sigma f(\sigma^{-1}) \\ &= f(\sigma\sigma^{-1}) \cdot \sigma f(\tau) \\ &= f(\tau)^i. \end{aligned}$$

The group N is normal in G, because the corresponding field $F(\mu)$ is Galois over the ground field F. So $\sigma\tau\sigma^{-1} \in N$. Using that the restriction of f to N is a homomorphism, yields $f(\sigma\tau\sigma^{-1}\tau^{-i}) = 1$.

(ii) $f(\sigma^2) = f(\sigma)\sigma f(\sigma) = f(\sigma)f(\sigma)^{-1} = 1.$ □

Notation 26. In the remainder of this section J will be the following subset of G:

$$\begin{aligned} J = &\langle \sigma\tau\sigma^{-1}\tau^{-i} \mid \sigma \in G,\ \tau \in N,\ i \in \mathbb{Z},\ i + n\mathbb{Z} = \varphi(\sigma) \rangle \\ &\cdot \langle \sigma^2 \mid \sigma \in G,\ \varphi(\sigma) = -1 + n\mathbb{Z} \rangle. \end{aligned}$$

Proposition 27. *J is a normal subgroup of G.*

Proof. Let $\sigma, \gamma \in G$ and $\tau \in N$. Let $x = \sigma\tau\sigma^{-1}\tau^{-i}$ for some $i \in \mathbb{Z}$ such that $i + n\mathbb{Z} = \varphi(\sigma)$. Then

$$\gamma x \gamma^{-1} = (\gamma\sigma\gamma^{-1})(\gamma\tau\gamma^{-1})(\gamma\sigma\gamma^{-1})^{-1}(\gamma\tau\gamma^{-1})^{-i},$$

and $\varphi(\gamma\sigma\gamma^{-1}) = \varphi(\sigma)$.

Suppose there is an element $y = \sigma^2$ for some $\sigma \in G$ with $\varphi(\sigma) = -1 + n\mathbb{Z}$. Let $\gamma \in G$. Then

$$\gamma y \gamma^{-1} = (\gamma\sigma\gamma^{-1})^2,$$

and $\varphi(\gamma\sigma\gamma^{-1}) = \varphi(\sigma) = -1 + n\mathbb{Z}$.

It follows that the $J \subset G$ is the product of two normal subgroups of G. Therefore J is a group that is normal in G. □

Proposition 28.

$$[N, N]N^n \subset J \subset H.$$

Proof. The inclusion $J \subset H$ follows from Proposition 25. Let $\sigma, \tau \in N$. Note that $\varphi(\sigma) = 1 \mod n$. Hence $[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} \in J$. Note also that $\varphi(\sigma) = -n + 1 \mod n$, such that $\tau^n = \sigma^0\tau\sigma^{-0}\tau^{n-1} \in J$. It follows that $[N, N]N^n \subset J$. □

Corollary 29. *The factor group N/J is abelian of exponent n.*

Theorem 30 (Zordan)**.** *Let $n = p^k$ for a prime p and integer $k \geq 1$ and let $f \in \mathrm{Hom}(N, \mu)$. Then* $\mathrm{Ker}(f) \supset J$ *if and only if f can be extended to an element of* $\mathrm{Z}^1(G, \mu)$.

One implication follows from Proposition 25. The other implication is due to Michele Zordan [19], who is writing a master thesis on this subject.

Corollary 31. *If $n = p^k$ for a prime p and integer $k \geq 1$ and*

$$\bigcap_{f \in \mathrm{Hom}(N,\mu)} \mathrm{Ker}(f) \supset J,$$

then the restriction map $\mathrm{Z}^1(G,\mu) \to \mathrm{Hom}(N,\mu)$ is surjective.

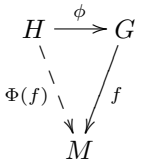
Remark 32. The object of study is $(K^*/F^*)[n]$. This group is isomorphic to $\mathrm{Z}^1(G,\mu)$, which maps onto $\mathrm{Hom}(N,\mu)$ under certain conditions. Therefore it is natural to consider the image and kernel of this map. To do so, we will introduce some more theory about 1-cocycles in the next section.

Corollary 33. *If $n = p^k$ for a prime p and integer $k \geq 1$ then $K^J = F(T)$, in other words $H = J$.*

Proof. Suppose $\sigma \in N/J$ is non trivial. By the Structure Theorem of finitely generated abelian groups, N/J is the direct product of cyclic groups. Consider the homomorphism $f\colon N/J \to \mu$ that is the composition of a projection of N/J onto one of its cyclic components in which σ maps to a non trivial element, together with an injective homomorphism from the cyclic component to μ. Then $f(\sigma) \neq 1$. By Zordan's Theorem f can be extended to an element $\bar{f}$ of $\mathrm{Z}^1(G/J,\mu)$, and $H/J \subset \mathrm{Ker}\,\bar{f}$ by Proposition 22. Hence, σ is non trivial implies that $\sigma \notin H/J$. The contraposition now yields that $H = J$. □

5 Dividing the Torsion

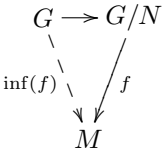
Remark 34. Let $\phi : H \to G$ be a homomorphism of groups and let M be a G-module. Then M is also a H-module by letting $\sigma \in H$ act on $m \in M$ via ϕ, i.e. $\sigma m = \phi(\sigma)m$. Furthermore ϕ induces a homomorphism Φ between 1-cocycles with the arrow reversed.



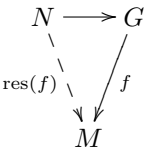
$$\begin{aligned} \Phi : \mathrm{Z}^1(G,M) &\longrightarrow \mathrm{Z}^1(H,M) \\ f &\longmapsto \big(\sigma \mapsto f \circ \phi(\sigma)\big) \end{aligned}$$

Definition 35. Let G be a group with a normal subgroup N, and let M be an abelian group. Consider the following special cases of Remark 34.

(i) If M is a G/N-module then the projection homomorphism $G \to G/N$ naturally induces a homomorphism $\mathrm{Z}^1(G/N,M) \longrightarrow \mathrm{Z}^1(G,M)$ that is given by $f \longmapsto (\sigma \mapsto f(\sigma N))$. This homomorphism is called *inflation* and is denoted by inf.



(ii) Similar, if M is a G-module, then the embedding $N \to G$ gives rise to a homomorphism called *restriction*, or res, with $\mathrm{res} : \mathrm{Z}^1(G,M) \to \mathrm{Z}^1(N,M)$ and is given by restriction of domain.



Remark 36. Let M be a G/N-module for some group G with normal subgroup N. This induces the structure of a G-module M, and this induces the structure of an N-module M. The latter is of course given by the trivial action. The short exact sequence $1 \to N \to G \to G/N \to 1$ induces a sequence

$$\mathrm{Z}^1(G/N, M) \xrightarrow{\inf} \mathrm{Z}^1(G, M) \xrightarrow{\mathrm{res}} \mathrm{Z}^1(N, M) = \mathrm{Hom}(N, M).$$

As explained in Remark 24, $\mathrm{Z}^1(N, M) = \mathrm{Hom}(N, M)$ because the action of N on M is trivial. The homomorphism inf is injective, because $G \to G/N$ is surjective. The composition is trivial, because the composition $N \to G \to G/N$ is. In other words $\mathrm{Im}(\inf) \subset \mathrm{Ker}(\mathrm{res})$. The other inclusion is also true because N acts trivially on M.

Proof. Let $f \in \mathrm{Ker}(\mathrm{res})$ and let $\sigma \in G$, $\tau \in N$. Then

- $f(\tau) = 1$,
- $f(\sigma\tau) = f(\sigma) \cdot \sigma f(\tau) = f(\sigma)$,
- $f(\tau\sigma) = f(\tau) \cdot \tau f(\sigma) = f(\sigma)$.

It follows that f induces an element $g \in \mathrm{Z}^1(G/N, M)$ defined by $g : \sigma N \mapsto f(\sigma)$, with $f = \inf(g)$. □

Corollary 37. *Let M be a G/N-module for some group G with normal subgroup N. Then there is an exact sequence*

$$0 \longrightarrow \mathrm{Z}^1(G/N, M) \xrightarrow{\inf} \mathrm{Z}^1(G, M) \xrightarrow{\mathrm{res}} \mathrm{Z}^1(N, M) = \mathrm{Hom}(N, M).$$

Corollary 38. *Let K/F be a finite Galois extension with group G. Let n be an integer such that $\zeta_n \in K$. Let $\mu = \langle \zeta_n \rangle = K^*[n]$, and let $N = \mathrm{Gal}(K/F(\mu))$. Then there is a commutative diagram*

$$\begin{array}{ccccccc}
0 & \longrightarrow & \mathrm{Z}^1(G/N, \mu) & \xrightarrow{\inf} & \mathrm{Z}^1(G, \mu) & \xrightarrow{\mathrm{res}} & \mathrm{Z}^1(N, \mu) \\
 & & \downarrow{\scriptstyle \psi'}\sim & & \downarrow{\scriptstyle \psi}\sim & & \downarrow{\scriptstyle \psi''}\sim \\
0 & \longrightarrow & \big(F(\mu)^*/F^*\big)[n] & \xrightarrow{\phi} & \big(K^*/F^*\big)[n] & \xrightarrow{\phi'} & \big(K^*/F(\mu)^*\big)[n],
\end{array}$$

in which the rows are exact. The isomorphisms ψ, ψ', ψ'' are as in Theorem 20. The homomorphisms ϕ and ϕ' are the natural injection $F(\mu)^*/F^* \to K^*/F^*$ and projection $K^*/F^* \to K^*/F(\mu)^*$, restricted to the n-torsion.

Proof. Let $f \in \mathrm{Z}^1(G/N, \mu)$, Choose a $\beta \in K$ such that $\alpha = \sum_{\sigma \in G} \inf f(\sigma) \cdot \sigma(\beta) \neq 0$. Then $\alpha F^* = \psi \inf(f)$. Let S be a set of coset representatives of

G/N. Note that

$$\begin{aligned}\alpha &= \sum_{\sigma\in S}\sum_{\tau\in N} \inf f(\sigma\tau)\cdot\sigma\tau(\beta)\\ &= \sum_{\sigma\in S}\sum_{\tau\in N} \inf f(\sigma)\cdot\sigma\inf f(\tau)\cdot\sigma\tau(\beta)\\ &= \sum_{\sigma\in S}\sum_{\tau\in N} \inf f(\sigma)\cdot\sigma\tau(\beta)\\ &= \sum_{\sigma\in S} \inf f(\sigma)\cdot\sigma\sum_{\tau\in N}\tau(\beta)\\ &= \sum_{\sigma\in G/N} f(\sigma)\cdot\sigma\sum_{\tau\in N}\tau(\beta).\end{aligned}$$

Now $\sum_{\tau\in N}\tau(\beta)\in F^N = F(\mu)$. Therefore $\alpha F^* = \phi\psi'(f)$. It follows that the block on the left is exact.

Let $f\in \mathrm{Z}^1(G,\mu)$, Choose a $\beta\in K$ such that $\alpha = \sum_{\sigma\in G} f(\sigma)\cdot\sigma(\beta)\neq 0$. Then $\alpha F^* = \phi'\psi(f)$. Let S be a set of coset representatives of G/N. Note that

$$\begin{aligned}\alpha &= \sum_{\tau\in N}\sum_{\sigma\in S} f(\tau\sigma)\cdot\tau\sigma(\beta)\\ &= \sum_{\tau\in N}\sum_{\sigma\in S} f(\tau)\cdot\tau f(\sigma)\cdot\tau\sigma(\beta)\\ &= \sum_{\tau\in N} f(\tau)\cdot\tau\sum_{\sigma\in S} f(\sigma)\cdot\sigma(\beta)\\ &= \sum_{\tau\in N} \mathrm{res}\, f(\tau)\cdot\tau\sum_{\sigma\in S} f(\sigma)\cdot\sigma(\beta).\end{aligned}$$

It follows that $\alpha F^* = \psi''\,\mathrm{res}(f)$. □

Remark 39. If furthermore the following two hold,

(i) $n = p^k$ for some prime p and integer $k\geq 1$,

(ii) $\bigcap_{f\in\mathrm{Hom}(N,\mu)}\mathrm{Ker}(f)\supset J = \langle \sigma\tau\sigma^{-1}\tau^{-i} \mid \sigma\in G,\ \tau\in N,\ i\in\mathbb{Z},\ i+n\mathbb{Z} = \varphi(\sigma)\rangle\cdot\langle\sigma^2\mid\sigma\in G,\ \varphi(\sigma) = -1+n\mathbb{Z}\rangle$,

then by Corollary 31, the rows are surjective on the right, and hence the diagram can be extended with trivial groups on the right. In that case $(K^*/F^*)[n]$ is the product of $(F(\zeta_n)^*/F^*)[n]$ and $\mathcal{S}$. Where $\mathcal{S}$ is any subset of $(K^*/F^*)[n]$ that maps onto $(K^*/F(\zeta_n)^*)[n]$.

Remark 40. This marks the path to the solution of the main problem of computing the complete torsion in K^*/F^*. The problem can be split into two 'smaller' ones: the torsion of the 'Kummer part', which corresponds to $(K^*/F(\zeta_n)^*)[n]$, and the torsion of the 'cyclotomic part', which is $(F(\zeta_n)^*/F^*)[n]$. Of course this strategy is only viable if (i) and (ii) of the previous remark can be made true. Condition (i) is not a problem, we might just as well compute the torsion per primary part. The complete torsion is then the direct product of those. Condition (ii) can be forced by reducing to the field of invariants of J. In Section 6 we will further analyze the 'Kummer part', and in Section 7 the 'cyclotomic part'.

6 Torsion in Kummer Extensions

Remark 41. Let K/F be a finite separable extension, and let $n = p^k$ for some prime p and integer k such that $\zeta_n \in K^*$. In this Section we shall first introduce Kummer theory, and then investigate the 'Kummer part' of $(K^*/F^*)[n]$. The goal is to construct a set $S \subset K^*$ such that $SF(\zeta_n)^*/F(\zeta_n)^* = (K^*/F(\zeta_n)^*)[n]$. Furthermore, S needs to represent elements in $(K^*/F^*)[n]$, in other words the set S should be such that $S^n \subset F^*$.

Definition 42. An extension K/F is called a *Kummer extension of exponent* n for some integer $n > 1$ if:

(i) There are n distinct n-th roots of unity in F,

(ii) K/F is an abelian extension of exponent n.

Theorem 43. *Let F be a field with $\zeta_n \in F$. Then there is a one to one correspondence between groups W with $F^{*n} \subset W \subset F^*$ and Kummer extensions K/F of exponent n, given by the map*

$$W \longmapsto F(W^{1/n}) = K,$$

with inverse

$$K \longmapsto F^* \cap K^{*n} = W.$$

For a proof see for example [8, 13]. This result is known as classical ablelian Kummer theory.

Corollary 44. *Let F be a field with $\zeta_n \in F$. Suppose that $\alpha^n \in F^*$ and that $\beta^n \in F^*$. Then $\alpha \in F(\beta)$ if and only if $\alpha = b\beta^k$ for some $k \in \mathbb{Z}$ and $b \in F^*$.*

Proof. Suppose $\alpha \in F(\beta)$. Let $K = F(\beta)$ and let $W = \langle \beta^n \rangle F^{*n}$. Then $F(W^{1/n}) = F(\beta) = K$, and hence $F^* \cap K^{*n} = W$. So $\alpha^n \in W$, say

$$\alpha^n = (\beta^n)^k b^n$$

for some $b \in F^*$ and $k \in \mathbb{Z}$. But then

$$\alpha = \beta^k \zeta_n^l b$$

for some $l \in \mathbb{Z}$. Because $\zeta_n \in F$, α is of the right form. The converse implication is trivial. □

Remark 45. As in Remark 41, let K/F be a finite separable extension with $\zeta_n \in K$ for some $n = p^k$. Let $T \subset K^*$ be such that $T/F^* = (K^*/F^*)[n]$. Then $F(T)/F$ is a Galois extension – say with group G, and $F(T)/F(\zeta_n)$ is a Kummer extension of exponent n – say with Galois group $N \subset G$. Let $\mu = \langle \zeta_n \rangle$, then by Corollary 31 and 38 there is a commutative diagram

$$\begin{array}{ccccc} \mathrm{Z}^1(G,\mu) & \xrightarrow{\text{res}} & \mathrm{Hom}^1(N,\mu) & \longrightarrow & 0 \\ \downarrow{\scriptstyle \psi}\,\sim & & \downarrow{\scriptstyle \psi''}\,\sim & & \\ T/F^* & \xrightarrow{\phi'} & T/F(\zeta_n)^* & \longrightarrow & 0. \end{array}$$

We plan to make a set $S \subset T$ such that $SF(\zeta_n)^*/F(\zeta_n)^* = T/F(\zeta_n)^*$. This can be done in three steps.

(i) Construct $\mathrm{Hom}(N, \mu)$. Note that N is finite abelian of exponent n, and μ is cyclic of order n. N is a direct product of cyclic groups of order dividing n. From each cyclic component C of N of order d there are d homomorphisms $C \to \mu$, because a generator of C can be sent to any element of order dividing d in μ, and there are exactly d of such elements. This way we find exactly $\#N$ homomorphisms.

(ii) Extend those homomorphisms to $\mathrm{Z}^1(G, \mu)$. Suppose that p is odd. Then G/N is cyclic. It follows that G is generated by N and by one other element γ. A homomorphism $f\colon N \to \mu$ can be extended by sending γ to any element in μ such that the 1-cocycle condition

$$f(\sigma\tau) = f(\sigma) \cdot \sigma f(\tau),$$

holds for all $\sigma, \tau \in G$. If $p = 2$ then G/N is generated by two elements. The 1-cocycles can be constructed similar with one choice more.

(iii) Map the 1-cocycles with ψ to T/F^*. The map ψ from Theorem 20 is defined with representatives. So we can actually construct an element in T corresponding to the 1-cocycle.

7 Torsion in Cyclotomic Extensions

Proposition 46. *Let p be a prime, F a field and $a \in F$ such that $a \notin F^p$. Then:*

(i) If p is odd, or $p = 2$ and $\mathrm{char}\, F = 2$, then $X^{p^n} - a$ is irreducible over F for all integers $n \geq 0$.

(ii) If $p = 2$, $n \geq 2$ and $\mathrm{char}\, F \neq 2$, then $X^{2^n} - a$ is irreducible over F if and only if $a \notin -4F^4$.

For a proof see for example [8, 6].

Remark 47. Suppose F is a field and $a \in F$ with $a \notin F^2$ and with $\zeta_4 \in F$. Then $(1 + \zeta_4)^4 = -4 \in F^4$. So $a \notin -4F^4$ is equivalent to $a \notin F^4$, which is true because $a \notin F^2$. So in this case $X^{2^n} - a$ is irreducible.

Lemma 48. *Let $n = p^k$ for a prime p and a positive integer k. Let $\mu = \langle \zeta_n \rangle$. Let F be a field of characteristic not equal to p. Suppose that $F(\mu)/F$ is a proper extension. Let $T \subset F(\mu)^*$ be such that $T/F^* = \big(F(\mu)^*/\mu F^*\big)[n]$. Then*

(i) If p is odd and $\zeta_p \in F$, or if $p = 2$ and $\zeta_4 \in F$, then $T/\mu F^*$ is trivial.

(ii) If p is odd, then $T/\mu F^*$ is trivial.

(iii) If $p = 2$ and $\zeta_4 \notin F$, then $T/\mu F^*$ equals $\big(F(\zeta_4)^*/\mu F^*\big)[n]$.

Proof. (i) Let $\alpha \in T$. We shall prove that $\alpha \in \mu F^*$ with induction on the degree of α over F. If $\alpha \in F^*$ then $\alpha(\mu F^*)$ is trivial.

Otherwise consider the extension $F(\alpha)/F$. It is cyclic of order a power of p, because $\zeta_p \in F$ when p is odd, and $\zeta_4 \in F$ when $p = 2$. So the collection of intermediate fields form a chain. By Proposition 46 and the

remark following it, this chain equals $F = F(\alpha^{p^r}) \subsetneq \ldots \subsetneq F(\alpha^p) \subsetneq F(\alpha)$ for some $r \geq 1$. But also $F(\alpha^{p^i}) = F(\zeta^{p^i})$ for some $\zeta \in \mu$. By Corollary 44, $\alpha = \zeta^i \beta$ for some $\beta \in F(\zeta^p) \subsetneq F(\alpha)$. Note that $\beta^n \in \mu F^*$, and that the degree of β over F is smaller than that of α. By induction $\beta \in \mu F^*$, and hence $\alpha = \zeta^i \beta \in \mu F^*$.

(ii) Let $\alpha \in T$. If $\alpha \in F$ then surely $\alpha \in \mu F^*$. Otherwise $F(\alpha)/F$ is a proper extension. It follows from Proposition 46 that $X^{p^r} - \alpha^{p^r}$ is an irreducible polynomial for some $r \geq 1$. Since $F(\alpha)/F$ is Galois, $F(\alpha)$ must contain ζ_{p^r}. The degree of ζ_p over F divides $p-1$, and must also divide p^r. This is only possible when $\zeta_p \in F$. Now the problem is reduced to case (i).

(iii) There is an exact sequence

$$0 \rightarrowtail \big(F(\zeta_4)^*/\mu F^*\big)[n] \rightarrowtail \big(F(\mu)^*/\mu F^*\big)[n] \rightarrowtail \big(F(\mu)^*/\mu F(\zeta_4)^*\big)[n].$$

Because of (i), the group on the right is trivial. The group in the middle is $T/\mu F^*$. It is isomorphic to the group on the left, which is $\big(F(\zeta_4)^*/\mu F^*\big)[n]$. □

Remark 49. The group that arises in case (iii) was completely determined in Example 21.

8 Basic Algorithms in Number Fields

As in many texts about computational mathematics, we will not go into the details of basic notions such as *algorithm* or *bit-operations*. It is assumed that the reader is familiar with these notions. It will suffice to think of an algorithm as a step by step description that, given an *input* in the form of a finite sequence of integers, produces another, called the *output*. A bit-operation then is a most simple form of a step in the algorithm. The total of bit-operations needed as a function of number of input bits is called the *running time*. For a finite sequence $a_1, a_2, \ldots, a_n$ of integers the number

$$\sum_{i=1}^{n} \big\lceil {}^2\log\left(|a_i| + 2\right)\big\rceil$$

measures its *size*. One should think of the size as the number of bits needed tot spell out the sequence. An algorithm is said to run in *polynomial time*, when the running time is bounded by a polynomial function in the size of the input.

For more background on this subject see [11].

Definition 50. A *number field* F of degree n over $\mathbb{Q}$ is encoded as an n-dimensional $\mathbb{Q}$-vector space together with a multiplication table $F \times F \to F$.

Remark 51. Let F be a number field with basis $\{v_1, \ldots, v_n\}$ over $\mathbb{Q}$. Let a_{ijk} be the k-th component of $v_i v_j$. Then the multiplication table consists of the n^3 rational numbers a_{ijk}. There are more than n bits needed to spell out this information. So the size of F is at least n. Keep in mind that this is one order of magnitude larger than the size of the integer n. There exists for example no polynomial time algorithm that calculates 2^n with input n. This is because

there are at least n bits needed to spell out 2^n (as a binary number), and n is exponentially large compared to the size of n. On the other hand, with input F, one can compute 2^n in polynomial time. It is also possible to construct a prime factorization of n in polynomial time in the size of F.

Definition 52. An $m \times n$ matrix $M = (m_{ij})$ over $\mathbb{Z}$ is in *Hermite normal form (HNF)* if there is an $0 \leq r \leq n$, and a strictly increasing function $f\colon [r+1, n] \to [1, m]$ such that:

(i) The first r columns of M are zero,

(ii) $m_{f(j)j} \geq 1$ for all $r + 1 \leq j \leq n$,

(iii) $m_{ij} = 0$ for all $r + 1 \leq j \leq n$ and $i > f(j)$,

(iv) $m_{f(k)j} < m_{f(k)k}$ for all $r + 1 \leq k < j \leq n$.

Theorem 53. *Let A be an $m \times n$ matrix over $\mathbb{Z}$. Then there is a unique $m \times n$ matrix B in HNF such that $B = AU$ for some $U \in \mathrm{Gl}_n(\mathbb{Z})$ (i.e. U is unimodular).*

For a proof see for example [4, 18]. Note that U is in general not unique. For example when $A = 0$, all $U \in \mathrm{Gl}_n(\mathbb{Z})$ are such that $AU = B = 0$ is in HNF.

Corollary 54. *Notation as above. The rank of A equals the rank of B, which is $n - r$.*

Proposition 55. *Let A be an $m \times n$ matrix over $\mathbb{Z}$. Then there is a polynomial time algorithm that constructs a unimodular matrix U such that AU is in HNF.*

An actual algorithm, including proofs about its complexity, is given in [18]. It is based on the so called Bareiss Algorithm.

Corollary 56. *Let A be an $m \times n$ matrix over $\mathbb{Q}$. Then there is a polynomial time algorithm that constructs matrices X and Y such that the columns of X and AY are bases for respectively* $\mathrm{Ker}(A)$ *and* $\mathrm{Im}(A)$.

Proof. First we will bring this back to a problem over $\mathbb{Z}$. Let (x_i) be a sequence of integers that represents A. Let z be the product of all denominators of the nonzero entries of A. Then z is the product of the elements in some subsequence of (x_i). It follows that the size of z is smaller than the size of A. The matrix zA, has entries in $\mathbb{Z}$. It is represented by a sequence that has piecewise smaller entries than the sequence (zx_i). It follows that the size of zA is bounded by the square of the size of A.

Construct the unimodular matrix U such that zAU is in HNF. Let r be the number of zero columns of zAU. Let $\{e_1, \ldots, e_n\}$ be the standard basis for $\mathbb{Q}^n$. Now take

$$X = U(e_1, \ldots, e_r), \qquad Y = U(e_{r+1}, \ldots, e_n). \qquad \square$$

Corollary 57. *Let N and N' two matrices over $\mathbb{Q}$ whose columns are respectively bases for the linear subspaces V and V' of $\mathbb{Q}^m$. Then there is a polynomial time algorithm that constructs two matrices whose columns are bases for the subspaces $V \cap V'$ and $\langle V \cup V' \rangle$ of $\mathbb{Q}^m$.*

Proof. Let n and n' be the dimension of respectively V and V' and let A be the $m \times (n+n')$ matrix obtained by putting N next to N'. Construct matrices X and Y as above. Note that Y is an $(n+n') \times (n-r)$ matrix. Furthermore the columns of AY form a basis for $\langle V \cup V' \rangle$.

X is an $(n+n') \times r$ matrix. Let X_1 be the matrix formed by the first n rows of X, and X_2 by the last n' rows. Then

$$NX_1 + N'X_2 = AX = 0.$$

It is now clear that the columns in NX_1 form a basis for $V \cap V'$. □

Definition 58. An *extension of number fields* K/F is encoded as the number field K together with a sequence of elements in K that forms a basis for the subspace F.

Corollary 59. *Let F be a number field with subfields K and L. Then one can construct the fields $K \cap L$ and KL as subfields of F in polynomial time.*

Proposition 60. *Let F be a number field and $\alpha \in F$. Then there is a polynomial time algorithm that constructs the subfield $\mathbb{Q}(\alpha)$ of F.*

Proof. Let $n = [F : \mathbb{Q}]$ and compute the rank r of the matrix A with columns α^i for $i = 0, \ldots, n-1$. This can be done by computing the HNF of a multiple of A that has integer coefficients. It follows that $\alpha^0, \ldots, \alpha^{r-1}$ is a basis for $\mathbb{Q}(\alpha)$. It not hard to compute its multiplication table. □

Proposition 61. *Let F be a number field of degree n over $\mathbb{Q}$ and let α be a primitive element for F over $\mathbb{Q}$. Then there is a polynomial time algorithm that constructs an irreducible polynomial f over $\mathbb{Q}$ such that $\mathbb{Q}(\alpha) \cong \mathbb{Q}[X]/(f)$.*

Proof. Let M be the $(n+1) \times n$ matrix with rows α^i for $0 \leq i \leq n$. Then a vector in the 1-dimensional kernel defines a polynomial of degree n over $\mathbb{Q}$ of which α is a zero. □

Lemma 62. *Let $F(\alpha, \beta)/F$ be an algebraic extension of fields such that β is separable over F. Let K be the normal closure of $F(\alpha, \beta)/F$, and let f and g be the minimal polynomial of respectively α and β. Then $F(\alpha, \beta) = F(\alpha + t\beta)$ for all $t \in F$ with*

$$t \notin \left\{ \frac{x - \alpha}{\beta - y} \mid x, y \in K,\ f(x) = g(y) = 0,\ y \neq \beta \right\}.$$

Proof. Let y be a zero of g with $y \neq \beta$. Then $f(\alpha + t(\beta - y)) \neq 0$, because otherwise $t = \frac{\alpha + t(\beta - y) - \alpha}{\beta - y}$. It follows that the polynomials $g(X)$ and $f(\alpha + t(\beta - X))$ have exactly one zero in common, namely β. Because g is separable we get

$$\gcd\big(g(X), f(\alpha + t(\beta - X))\big) = X - \beta.$$

In particular $\beta \in F(\alpha + t\beta)$, and hence also $\alpha \in F(\alpha + t\beta)$. So $F(\alpha, \beta) = F(\alpha + t\beta)$. □

Proposition 63. *Let F be a number field, and let $\alpha, \beta \in F$. Then there is a polynomial time algorithm that constructs a primitive element for $\mathbb{Q}(\alpha, \beta)$.*

Proof. Let $n = [F : \mathbb{Q}]$, then there are at most n^2 values t in $\mathbb{Q}$ such that $\alpha + t\beta$ is not a primitive element for $\mathbb{Q}(\alpha, \beta)$. So the element $\alpha + t\beta$ for $t = 0, \ldots, n^2$ with the largest degree over $\mathbb{Q}$ is a primitive element for $\mathbb{Q}(\alpha, \beta)$. □

Corollary 64. *Giving a number field F is polynomial time equivalent to giving an irreducible polynomial f over $\mathbb{Q}$ with $F \cong \mathbb{Q}[X]/(f)$.*

Proof. Given such f of degree n it is not hard to construct the multiplication table of $\mathbb{Q}[X]/(f)$ in polynomial time.

Conversely, let F be a number field of degree n over $\mathbb{Q}$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for F over $\mathbb{Q}$. Then $F = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. After n iterations of Proposition 63 we find a primitive element for F. Now apply Proposition 61. □

Proposition 65. *Let F be a number field and let $\sigma \in \mathrm{Aut}(F)$. Then there is a polynomial time algorithm that constructs F^σ.*

Proof. Note that σ is a linear map $F \to F$, when F is regarded as an $\mathbb{Q}$-vector space. Now construct a basis for $\mathrm{Ker}(\sigma - \mathrm{id}) = F^\sigma$, and compute a multiplication table. □

9 Advanced Algorithms in Number Fields

Proposition 66. *Let F be a number field and let $f \in F[X]$ be monic. Then there is a polynomial time algorithm that factors f into irreducible monic polynomials.*

See [9, 10, 11].

Lemma 67. *Let K/F be separable. Let H be the set of all F-embeddings of K in a normal closure that leave F invariant. Then $E = \cap_{\sigma \in H} \sigma(K)$ is the largest Galois extension of F that is contained in K.*

Proof. Restriction of a $\sigma \in H$ to E induces an F-embedding $\sigma|_E : E \to K$. The group, say G, of all these restrictions has order $[E : F]$. Note that all $\sigma \in G$ are bijections of E. So E/F is Galois with group G. If $x \in K$ is contained in a Galois extension over F then so is $\sigma(x)$ for all $\sigma \in H$. It follows that $x \in E$, and that E is the largest Galois extension over F in K. □

Proposition 68. *Let K/F be an extension of number fields. Then there is a polynomial time algorithm that constructs the subfield E that is the largest Galois extension of F contained in K.*

Proof. Let f be an irreducible polynomial over F with $K \cong F[X]/(f)$. For each irreducible factor g of f over K construct the field $K[X]/(g)$. Find a zero β of g in $K[X]/(g)$ and construct the subfield $L_g = F(\beta) \cap K$ of K. Then construct the intersection

$$E = \bigcap_g L_g,$$

which is the largest Galois extension of F in K. □

Theorem 5. *Let F be a number field. Then there is a polynomial time algorithm that constructs an integer n such that $\mathrm{Tor}(F^*) = \langle \zeta_n \rangle$.*

Proof. Let m be the degree of $F/\mathbb{Q}$. For each $i = 2, 3, \ldots, m+1$ calculate the largest integer k_i such that $X^{i^{k_i}} - 1$ splits into linear factors over F. This can be done in polynomial time over F because the degree has an upper bound $i^{k_i} \leq 2(\phi(i^{k_i}))^2 \leq 2m^2$, that is polynomial in m. Now construct:

$$n = \operatorname{lcm}\{i^{k_i} \mid i = 2, 3, \ldots, m+1\}.$$

Then clearly $\zeta_n \in \operatorname{Tor}(F^*)$. Conversely, if $\zeta_p \in \operatorname{Tor}(F^*)$ for a prime p then $\phi(p) = p-1$ divides $m = [F : \mathbb{Q}]$ and hence $p \leq m+1$. So if $\zeta_{p^k} \in \mu(F)$ then p^k divides the constructed integer n. This is true for all primes p and all integers k, and therefore $\operatorname{Tor}(F^*) \subset \langle \zeta_n \rangle$. So n is as desired. □

Proposition 69. *Let K/F be an extension of number fields. Let $n = p^k$ for a prime p and integer $k \geq 1$ such that $\zeta_n \in K$, and write $\mu = \langle \zeta_n \rangle$. Suppose that $\zeta_{p^{k+1}} \notin K$. Then there is a polynomial time algorithm that constructs a set $S \subset K$ that is a set of representatives of $\big(F(\mu)^*/F^*\big)[n]$.*

Proof. Let $T \subset K$ be such that $T/F^* = \big(F(\mu)^*/F^*\big)[n]$. There is a short exact sequence

$$0 \longrightarrow \mu F^*/F^* \longrightarrow T/F^* \longrightarrow T/\mu F^* \longrightarrow 0.$$

By Lemma 48 the group $T/\mu F^*$ is trivial when p is odd or when $\zeta_4 \in F$. So in that case $S = \mu$ is as desired. If $p = 2$ and $\zeta_4 \notin F$, then $T/\mu F^*$ equals $\big(F(\zeta_4)^*/\mu F^*\big)[n]$. Construct a maximal integer t such that $\zeta_{2^t} \in F(\zeta_4)$. Let $\sigma \colon F(\zeta_4) \to F(\zeta_4)$ be the non trivial F-automorphism of $F(\zeta_4)$. Then $\sigma(\zeta_{2^t}) = \pm\zeta_{2^t}^{-1}$. From Example 21 it follows that the $\pm$ determines whether $T/\mu F^*$ is trivial or not.

(i) If $\sigma(\zeta_{2^t}) = \zeta_{2^t}^{-1}$, then $T/\mu F^*$ is of order two. A representative of the non trivial element is $1 + \zeta_{2^t}$. It follows that $S = \mu \cup (1 + \zeta_{2^t})\mu$ is a set of representatives of T/F^*.

(ii) If $\sigma(\zeta_{2^t}) = -\zeta_{2^t}^{-1}$, then $T/\mu F^*$ is trivial and $S = \mu$ is a set of representatives of T/F^*. □

Proposition 70. *Let K/F be a Galois extension of number fields. Let $n = p^k$ for a prime p and integer $k \geq 1$ such that $\zeta_n \in K$, and write $\mu = \langle \zeta_n \rangle$. Let $T \subset K$ be such that $T/F^* = (K^*/F^*)[n]$. Then there is a polynomial time algorithm that constructs the subfield $F(T)$ of K.*

Proof. Let f be an irreducible polynomial over F with $K = F[X]/(f)$. Then all zeros of f are contained in K. Let α be a zero of f. Elements σ of the Galois group G of K/F can be constructed as a linear map $\sigma \colon K \to K$ defined by $\sigma \colon \alpha \mapsto \beta$ for some zero β of f. Construct a map $\varphi \colon G \to \{1, \ldots, n\}$ such that $\varphi(\sigma) = i$ when $\sigma(\zeta_n) = \zeta_n^i$. Determine $N = \operatorname{Ker}(\varphi)$. Then N is the Galois group of $K/F(\zeta_n)$. Now construct the group

$$\begin{aligned} J = &\langle \sigma\tau\sigma^{-1}\tau^{-i} \mid \sigma \in G,\ \tau \in N,\ i \in \mathbb{Z},\ i + n\mathbb{Z} = \varphi(\sigma) \rangle \\ &\cdot \langle \sigma^2 \mid \sigma \in G,\ \varphi(\sigma) = -1 + n\mathbb{Z} \rangle. \end{aligned}$$

By Proposition 65 we can construct K^J, which is equal to $F(T)$ by Corollary 33. □

Proposition 71. *Let A be an abelian group of exponent n, and C a cyclic group of order n. Then there is a polynomial time algorithm that constructs* $\mathrm{Hom}(A, C)$.

Note that this Proposition is needed for part (i) of the sketch in Remark 45.

Proof. we shall construct $\mathrm{Hom}(A, C)$ inductively. There is only one homomorphism from the trivial group to C. Suppose we have constructed $\mathrm{Hom}(B, \mu)$ for some subgroup $B \subset A$. If $B = A$ then we are done. Otherwise take a $\sigma \in A - B$. Let $i > 0$ be minimal such that $\sigma^i \in B$. Note that i divides n. Let $f \in \mathrm{Hom}(B, C)$ and let k be such that $f(\sigma^i) = \zeta_n^k$. Then f can be extended to $\langle \sigma, B \rangle$ by $f(\sigma) = \zeta_n^j$ for all j with $ij \equiv k \mod n$. This induces i elements of $\mathrm{Hom}(\langle \sigma, B \rangle, C)$. Doing this for all $f \in \mathrm{Hom}(B, C)$ we find $\mathrm{Hom}(\langle \sigma, B \rangle, C)$. Repeating this process we find $\mathrm{Hom}(A, C)$. □

Proposition 72. *Let K/F be a Galois extension of number fields with Galois group G. Let $n = p^k$ for a prime p and integer $k \geq 1$ such that $\zeta_n \in K$, and write $\mu = \langle \zeta_n \rangle$. Let $f \colon N \to \mu$ be a homomorphism. There is a polynomial time algorithm that with input G, N, f extends f to $\mathrm{Z}^1(G, \mu)$.*

This Proposition is the product of Remark 45 part (ii).

Proof. G/N is isomorphic to to $\mathrm{Gal}(F\zeta_n)/F)$ and hence to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. If p is odd, then G/N is cyclic, if $p = 2$, then G/N is generated by two elements. It follows that G is generated by N and (at most) two other elements, say γ_1, γ_2. A homomorphism $f \colon N \to \mu$ can be extended by sending γ_i to any element in μ such that the 1-cocycle condition

$$f(\sigma\tau) = f(\sigma) \cdot \sigma f(\tau),$$

holds for all $\sigma, \tau \in G$. This can be done by trial and error. □

Proposition 73. *Let K/F be a Galois extension of number fields with Galois group G. Let $n = p^k$ for a prime p and integer $k \geq 1$ such that $\zeta_n \in K$, and write $\mu = \langle \zeta_n \rangle$. Let $f \in \mathrm{Z}^1(G, \mu)$. There is a polynomial time algorithm that constructs an element $\alpha \in K^*$ such that $\alpha/\sigma(\alpha) = f(\sigma)$ for all $\sigma \in G$.*

And this is part (iii) of Remark 45.

Proof. By Theorem 20 we can take for α the element

$$\alpha = \sum_{\sigma \in G} f(\sigma)\sigma(\beta),$$

where $\beta \in F(T)$ is such that $\alpha \neq 0$. It is not hard to find a good β. At least one element in a basis for $F(T)$ as F-vectorspace will do, see Corollary 17. The field $F(T)$ can be constructed by Proposition 70. □

Proposition 74. *Let K/F be a Galois extension of number fields. Let $n = p^k$ for a prime p and integer $k \geq 1$ such that $\zeta_n \in K$, and write $\mu = \langle \zeta_n \rangle$. Let $T \subset K$ be such that $T/F^* = (K^*/F^*)[n]$. Then there is a polynomial time algorithm that constructs a set S of representatives of $T/F(\zeta_n)^*$, such that $S^n \subset F^*$.*

Proof. Construct the field $F(T)$ as described in Proposition 70 and construct the Galois groups G of $F(T)/F$, and N of $F(T)/F(\zeta_n)$. As in Proposition 71, construct $\mathrm{Hom}(N, \mu)$. Extend those homomorphisms to 1-cocycles $\mathrm{Z}^1(G, \mu)$ as described in Proposition 72. Finally apply Proposition 73 to get a set of representatives of T/F^*. □

Theorem 4 (Main Theorem)**.** *Let K/F be an extension of number fields. Then* $\mathrm{Tor}(K^*/F^*)$ *is a finite group and there is a polynomial time algorithm that constructs a subset of K^* of representatives of* $\mathrm{Tor}(K^*/F^*)$*.*

Proof. As described in Theorem 5, construct integers m_1, m_2 such that $\mathrm{Tor}\, K^* = \langle \zeta_{m_1} \rangle$ and $\mathrm{Tor}\, F^* = \langle \zeta_{m_2} \rangle$. Then $\mathrm{Tor}(K^*/F^*)$ is annihilated by $n = [K : F]m_1/m_2$, such that

$$\mathrm{Tor}(K^*/F^*) = (K^*/F^*)[n].$$

As described in Proposition 68, construct the largest subfield E of $K(\zeta_n)$ that is Galois over F. Note that $\zeta_n \in E$. Find all primes p_i and powers $n_i = p_i^{e_i}$ such that

$$n = \prod_i p_i^{e_i} = \prod_i n_i.$$

Let $T_i \subset E^*$ be such that $T_i/F^* = (E^*/F^*)[n_i]$. Then By Corollary 38 and the Remark following it, there is a short exact sequence

$$0 \longrightarrow (F(\zeta_{n_i})^*/F^*)[n_i] \longrightarrow T_i/F^* \longrightarrow T_i/F(\zeta_{n_i})^* \longrightarrow 0.$$

For all i construct a set S_i as described in Proposition 69 such that

$$S_i F^*/F^* = \big(F(\zeta_{n_i})^*/F^*\big)[n_i].$$

Also construct the sets S_i' as described in Proposition 74 such that

$$S_i' F(\zeta_{n_i})^*/F(\zeta_{n_i})^* = T_i/F(\zeta_{n_i})^* = \big(F(T_i)^*/F(\zeta_{n_i})^*\big)[n_i],$$

and such that

$$S_i'^{n_i} \subset F^*.$$

Then $S_i S_i'$ is a set of representatives for T_i/F^*, and $\prod_i S_i S_i'$ for $(E/F^*)[n]$. Now the set

$$S = \{s \mid s \in K \cap \prod_i S_i S_i'\}$$

is such that $SF^*/F^* = \mathrm{Tor}(K^*/F^*)$. □

References

[1] Emil Artin, *Galois Theory*, Notre Dame: University of Notre Dame Press, 1971 (sixth printing)

[2] Albrecht Brandis, *Über die multiplikative Struktur von Körpererweiterungen*, Math. Zeitschr. **87**, 71-73, 1965

[3] Aiden A. Bruen, Christian U. Jensen, Noriko Yui, *Polynomials with frobenius groups of prime degree as Galois groups II*, Number Theory **24**, 305-359, 1986

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, New York: Springer-Verlag, 1993

[5] D.S. Dummit, *On the torsion in quotients of the multiplicative groups in abelian extensions*, in: J.M. DeKoninck and C. Levesque, Proceedings of the International Conference, Berlin: Walter de Gruyter, 1989

[6] Gregory Karpilovsky, *Unit Groups of Classical Rings*, Oxford: Clarendon Press, 1988

[7] M. Kneser, *Lineare Abhängigkeit von Wurzeln*, Acta Arith. **26**, 307-8, 1974

[8] Serge Lang, *Algebra, revised third edition*, Springer-Verlag, 2002

[9] A. K. Lenstra, *Factoring polynomials over algebraic number fields*, Computer Algebra, LNCS 162, Springer-Verlag, 1983

[10] A. K. Lenstra, H. W. Lenstra Jr., L. Lovász, *Factoring Polynomials with Rational Coefficients*, Math. Ann. 261, 1982

[11] H. W. Lenstra Jr., *Algorithms in algebraic number theory*, Bulletin of the American Mathematical Society **26**(2), 211244, 1992.

[12] W. May, *Fields with free multiplicative groups modulo torsion*, Rocky Mountain Math. **10**(3), 599-604, 1980

[13] Patrick Morandi, *Field and Galois Theory*, Springer-Verlag, 1996

[14] Jürgen Neukirch, Alexander Schmidt, Kay Wingberg *Cohomology of Number Fields*, Springer-Verlag, 2000

[15] Peter Stevenhagen, *Ray Class Groups and Governing Fields*, PHD thesis, Universiteit van Amsterdam, 1989

[16] E. van Tieghem, *Radikalen van multiplikatieve groepen in de algebraïsche getaltheorie*, PHD thesis, Katholieke Universiteit Leuven, 1975

[17] William Yslas Vélez, *A generalization of Schinzel's theorem on radical extensions of fields and an application* Acta Arith. **51**(2), 119-130, 1988

[18] Chee Keng Yap, *Fundamental Problems of Algorithmic Algebra*, Oxford: Oxford University Press, 2000

[19] Michele Zordan, *On Galois extensions generated by radicals*, Master thesis, Universiteit Leiden, 2010