Galois Action on Division Points

Master's Thesis by

Willem Jan Palenstijn

supervised by

Dr. Bart de Smit

March 29, 2004

Universiteit Leiden

Contents

Introduction

In this paper we will study the action of Galois groups on division points.

If G is a commutative algebraic group and K is a field with separable closure K^{sep}, we will consider the group of *division points* of $G(K)$, defined as

$$D = \{x \in G(K^{\text{sep}}) : \exists n \in \mathbb{Z}_{>0} : nx \in G(K)\}.$$

There are two important cases: G is the multiplicative group $\mathbb{G}_m$ and G is an elliptic curve E. In the first case division points are often called radicals and are given by $\{x \in K^{\text{sep}*} : \exists n \in \mathbb{Z}_{>0} : x^n \in K^*\}$.

In general $\text{Gal}(K^{\text{sep}}/K)$ acts on $G(K^{\text{sep}})$. The structure of the torsion of $G(K^{\text{sep}})$ is well known in our two cases and the action of $\text{Gal}(K^{\text{sep}}/K)$ on $G(K^{\text{sep}})_{\text{tor}}$ has been studied extensively. See for example Washington [6] and Serre [4].

In this paper we will consider the action of the Galois group on the group of division points. In the cases we consider, this group will be divisible. Some preliminary theory about divisible groups is in section 1.2.

In chapter 2 we will show how to obtain D from $G(K)$ without referring to K^{sep} or to G. To achieve this, we will study extensions of abelian groups $A \subset B$, where B/A is torsion. We will restrict the amount of p-torsion that A and B can have. In the case of field extensions, we will limit the p-torsion of A and B to rank 1 (considered as an $\mathbb{F}_p$-vector space), since the p-th roots of unity of a field have rank at most 1. In the case of elliptic curves, the p-torsion has rank 2, except if $\text{char}\, K = p > 0$, in which case the p-torsion has rank 0 or 1, depending on whether the elliptic curve is supersingular or ordinary.

If $K \subset L$ is a Galois extension, then the Galois group of L over K acts on $G(L)$. An automorphism of L that is the identity on K induces an automorphism of $G(L)$ that is the identity on $G(K)$. Therefore, studying automorphisms of abelian groups can provide insight into Galois groups. In chapter 3 we will provide several tools to describe these automorphism groups. We will introduce analogues of several notions from Galois theory, such as normal extensions and extending automorphisms.

Next, we will consider the Galois action on division points. An easy example of this is the case where $G(K)$ contains enough torsion. In this case the Galois group is abelian and for the multiplicative group the Galois action is then described by Kummer theory. The analogue for elliptic curves is the Kummer pairing, which is treated in Silverman [5], VIII, Proposition 1.2.

In the fourth and last chapter we will study the Galois group in the more general case where $K \subset L$ is a Galois extension where L is formed by adjoining a group of radicals B which satisfies some extra conditions, to K. We will give a description of the image of the Galois group in the automorphism group of B, which will in general not be abelian.

Chapter 1

Preliminaries

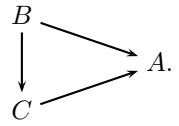
In this chapter we will introduce the concepts of fibered sums, fibered products, divisibility and injectivity, roughly following Lang [2] and Eisenbud [1].

1.1 Fibered sums and products

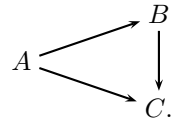
In this section, we will define the fibered product of groups and the fibered sum of abelian groups. We first introduce these notions in a general setting.

Let $\mathfrak{C}$ be a category, and A an object in that category. Consider the following two categories. The objects of the category $\mathfrak{C}_A$ are morphisms $B \to A$, where $B \in \mathfrak{C}$. Dually, the objects of the category $\mathfrak{C}^A$ consist of morphisms $A \to B$, where B is again an object of $\mathfrak{C}$.

A morphism in $\mathfrak{C}_A$ from $B \to A$ to $C \to A$ is a morphism $B \to C$ (in $\mathfrak{C}$) that makes the following diagram commutative:



A morphism in $\mathfrak{C}^A$ from $A \to B$ to $A \to C$ is a morphism $B \to C$ that makes the following diagram commutative:



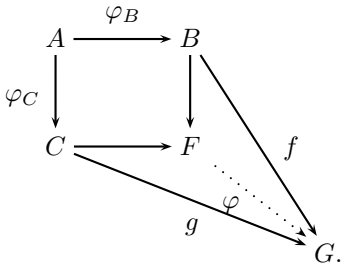
Definition 1.1. *The* product *in* $\mathfrak{C}_A$ *of* $B \to A$ *and* $C \to A$ *is called the* fibered product *of* B *and* C *over* A*. It is written* $B \times_A C$*.*

The coproduct *in* $\mathfrak{C}^A$ *of* $A \to B$ *and* $A \to C$ *is called the* fibered coproduct *or* fibered sum *of* B *and* C *over* A*. It is written* $B \oplus_A C$*.*

Theorem 1.2. *Fibered sums exist in the category of abelian groups. The fibered sum of* B *and* C *over* A*, with homomorphisms* $\varphi_B : A \to B$ *and* $\varphi_C : A \to C$*, is given by* $(B \oplus C)/\{(\varphi_B(a), -\varphi_C(a) : a \in A\}$*.*

Proof. Let G be an abelian group with homomorphisms $f : B \to G$ and $g : C \to G$ such that $f\varphi_B = g\varphi_C$.

Define $F := (B \oplus C)/\{(\varphi_B(a), -\varphi_C(a) : a \in A\}$. We need to show there is a unique homomorphism $\varphi : F \to G$ such that the following diagram is commutative:



Define the map

$$\begin{aligned} \varphi' : B \oplus C &\longrightarrow G \\ (b, c) &\longmapsto f(b) + g(c). \end{aligned}$$

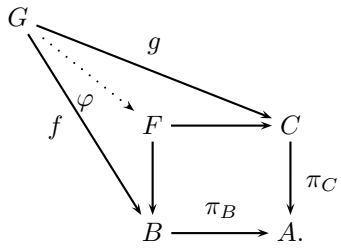
The subgroup $\{(\varphi_B(a), -\varphi_C(a) : a \in A\} \subset B \oplus C$ is in the kernel of φ', since $f(\varphi_B(a)) + g(-\varphi_C(a)) = f(\varphi_B(a)) - g(\varphi_C(a)) = 0$. Therefore, φ' induces an homomorphism $\varphi : F \to G$. It is clear that it makes the above diagram commutative.

The unicity of φ follows directly from the fact that commutativity of the above diagram implies that $\varphi(b, 0) = f(b)$ and $\varphi(0, c) = g(c)$. □

Theorem 1.3. *Fibered products exist in the category of groups. The fibered product of* B *and* C *over* A*, with homomorphisms* $\pi_B : B \to A$ *and* $\pi_C : C \to A$*, is given by* $\{(b, c) \in B \times C : \pi_B(b) = \pi_C(c)\}$*.*

Proof. Let G be a group with homomorphisms $f : G \to B$ and $g : G \to C$ such that $\pi_B f = \pi_C g$.

Define $F := \{(b, c) \in B \times C : \pi_B(b) = \pi_C(c)\}$. We need to show there is a unique homomorphism $\varphi : G \to F$ such that the following diagram is commutative:



Define the map

$$\begin{aligned} \varphi : G &\longrightarrow F \\ x &\longmapsto (f(x), g(x)). \end{aligned}$$

Note that the pair $(f(x), g(x))$ indeed satisfies the required condition, since $\pi_B(f(x)) = \pi_C(g(x))$. Also, φ is a homomorphism because f and g are both homomorphisms.

It is clear that φ is unique, since the commutativity of the diagram directly requires that the B-coordinate of $\varphi(x)$ is $f(x)$ and the C-coordinate is $g(x)$. □

Theorem 1.4. *Let C be an abelian group. If A and B are subgroups of C, then $A + B$ is the fibered sum of A and B over $A \cap B$.*

Proof. Let D be an abelian group and let $f : A \to D$ and $g : B \to D$ be two homomorphisms that are equal on $A \cap B$.

Define a map

$$\begin{aligned} \varphi : A + B &\longrightarrow D \\ a + b &\longmapsto f(a) + g(b). \end{aligned}$$

This is a well defined homomorphism since f and g are equal on $A \cap B$. It is clearly equal to f when restricted to A and equal to g when restricted to B. Also, φ is the only homomorphism with this property, since it is necessary that $\varphi(a) = f(a)$ for $a \in A$ and $\varphi(b) = g(b)$ for $b \in B$. So, $A + B$ has the universal property of the fibered sum, as required. □

Theorem 1.5. *Let K be a field, and let $K \subset L$ and $K \subset M$ be two finite Galois extensions contained in a fixed algebraic closure of K. Then LM and $L \cap M$ are also Galois extensions of K, and the natural map*

$$\mathrm{Gal}(LM/K) \longrightarrow \mathrm{Gal}(L/K) \times_{\mathrm{Gal}((L\cap M)/K)} \mathrm{Gal}(M/K)$$

is an isomorphism.

Proof. Theorem VI, §1.14 from Lang's Algebra [2] states that LM and $L \cap M$ are Galois over K, and that the map

$$\begin{array}{rcl} \mathrm{Gal}(LM/(L\cap M)) & \longrightarrow & \mathrm{Gal}(L/(L\cap M)) \times \mathrm{Gal}(M/(L\cap M)) \\ \sigma & \longmapsto & (\sigma|_L, \sigma|_M) \end{array}$$

is an isomorphism.

Now consider the natural map

$$\begin{array}{rcl} \mathrm{Gal}(LM/K) & \longrightarrow & \mathrm{Gal}(L/K) \times_{\mathrm{Gal}((L\cap M)/K)} \mathrm{Gal}(M/K) \\ \sigma & \longmapsto & (\sigma|_L, \sigma|_M). \end{array}$$

Note that this is well defined, since if $\sigma \in \mathrm{Gal}(LM/K)$, then $\sigma|_L$ and $\sigma|_M$ are equal on $L \cap M$.

It is clear that this map is injective, since if an automorphism is the identity on L and on M, it is also the identity on LM.

For surjectivity, let (σ, τ) be an element of $\mathrm{Gal}(L/K) \times_{\mathrm{Gal}((L\cap M)/K)} \mathrm{Gal}(M/K)$. We can extend σ to an automorphism $\sigma' \in \mathrm{Gal}(LM/K)$ such that $\sigma'|_L = \sigma$. Restricting σ' to M gives an element of $\mathrm{Gal}(M/K)$, which we can invert and compose with τ: define $\varphi = \sigma'|_M^{-1}\tau \in \mathrm{Gal}(M/K)$. Note that φ is the identity on $L \cap M$, because σ' and τ are equal on $L \cap M$.

Because of this, the isomorphism from Lang's Algebra above allows us to extend φ to an automorphism $\varphi' \in \mathrm{Gal}(LM/K)$ such that $\varphi'|_M = \varphi$ and $\varphi'|_L = \mathrm{id}_L$.

The composed automorphism $\sigma'\varphi'$ is equal to σ when restricted to L, since $\sigma'|_L = \sigma$ and $\varphi'|_L = \mathrm{id}_L$. Also, when restricting to M, it is equal to τ, because $(\sigma'\varphi')|_M = \sigma'|_M\varphi'|_M = \sigma'|_M\sigma'|_M^{-1}\tau = \tau$. □

1.2 Divisibility

Definition 1.6. *An abelian group A is* divisible *if for all $a \in A$, $n \in \mathbb{Z}_{>0}$, there is an element $b \in A$ with $nb = a$.*

Lemma 1.7. *If A is a divisible abelian group, then every quotient group Q of A is also divisible.*

Proof. Let $q \in Q$, $\tilde{q} \in A$ such that $\tilde{q} \mapsto q \in Q$ and $n \in \mathbb{Z}_{>0}$. Because A is divisible, there is an element $b \in A$ with $nb = \tilde{q}$. Let $\bar{b}$ be the image of b in Q. Then $n\bar{b} = q$ in Q, so Q is divisible. □

Lemma 1.8. *Every abelian group A can be embedded in a divisible abelian group.*

Proof. Let F be the free $\mathbb{Z}$-module $\bigoplus_A \mathbb{Z}$ and let K be the kernel of the surjective homomorphism $F \to A$ given by $(n_a)_{a\in A} \mapsto \sum_{a\in A} n_a a$. We find an isomorphism $A \cong F/K$. The tensor product $F \otimes_{\mathbb{Z}} \mathbb{Q}$ is divisible, and it contains F because F is torsion-free. By lemma 1.7, $(F \otimes_{\mathbb{Z}} \mathbb{Q})/K$ is also divisible, and it contains F/K. □

Definition 1.9. *An abelian group D is called* injective *if every exact sequence of abelian groups $0 \to D \to M \to N \to 0$ splits.*

Theorem 1.10. *A divisible abelian group D is injective.*

Proof. Let D be a divisible abelian group and $0 \to D \xrightarrow{f} M \to N \to 0$ an exact sequence of abelian groups. We will prove the existence of a homomorphism $M \to D$ which splits f, with Zorn's lemma.

Consider the set of all pairs (M', φ) for which M' is an abelian group with $D \subset M' \subset M$ and φ is a group homomorphism $M' \to D$ for which $\varphi_i f = \mathrm{id}_D$. We index this set with J and define an ordering by setting $(M_i, \varphi_i) \leq (M_j, \varphi_j)$ when $M_i \subset M_j$ and φ_j restricted to M_i is equal to φ_i, for $i, j \in J$.

Now consider a totally ordered subset $\{(M_i, \varphi_i)\}_{i\in I}$ with $I \subset J$. Define a map $\psi : \bigcup_{i\in I} M_i \to D$ by mapping $x \in \bigcup_{i\in I} M_i$ to the image of x under any φ_i for which $x \in M_i$. Note that this is well-defined, since if $x \in M_j$ for $j \neq i$, then, because our subset is totally ordered, either φ_i restricted to M_j is equal to φ_j, or vice versa. It is a homomorphism since if $x, y \in \bigcup_{i\in I} M_i$, then there is an $i \in I$ for which $x, y \in M_i$. Then $\varphi_i(x+y) = \varphi_i(x) + \varphi_i(y)$, so $\psi(x+y) = \psi(x) + \psi(y)$. Therefore, the pair $(\bigcup_{i\in I} M_i, \psi)$ is an upper bound of our totally ordered subset.

By Zorn's Lemma, there is a maximal pair (M', φ). If $M' = M$, then the homomorphism φ splits the sequence $0 \to D \to M \to N \to 0$, as required. If $M' \neq M$, let $x \in M' \setminus M$. We will now extend φ to a homomorphism φ' from $\langle M', x\rangle$ to D. From theorem 1.4 we know that $\langle M', x\rangle = M' \oplus_{M'\cap\langle x\rangle} \langle x\rangle$. Therefore, a homomorphism from $\langle M', x\rangle$ to D is specified by an homomorphism from M' to D (we take φ for this), and one from $\langle x\rangle$ to D, such that they are the same on $M' \cap \langle x\rangle$. Since there is an $n \in \mathbb{Z}_{\geq 0}$ such that $\langle x\rangle \cap M' = \langle nx\rangle$, the map φ' has to map x to an element $d \in D$ for which $nd = \varphi(nx)$. If $n = 0$, any d suffices. If $n \neq 0$, such a d exists because D is divisible. Note that $x \notin \mathrm{im} f \subset M$, so we still have that $\varphi' f = \mathrm{id}_D$. The pair $(\langle M', x\rangle, \varphi')$ contradicts the maximality of (M', φ). □

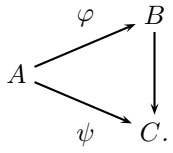
Chapter 2

Adding division points to abelian groups

We are interested in adjoining division points to an abelian group A. Specifically, let A be an abelian group and r a map from the set of primes to the set of non-negative integers. We will consider extensions of the following form:

Definition 2.1. *Let B be an abelian group. We call an injective homomorphism of abelian groups $A \hookrightarrow B$ an* r-extension *if B/A is torsion and if for all primes p the rank of the p-torsion of B is at most $r(p)$.*

Definition 2.2. *Let B and C be abelian groups. If $\varphi : A \hookrightarrow B$ and $\psi : A \hookrightarrow C$ are both injections, an* A-homomorphism *from B to C is a group homomorphism of B to C that makes the following diagram commutative:*



Given a group A and a map r, we will construct a maximal r-extension of A. To do this, we first need to define the *injective hull* of an abelian group.

2.1 Injective Hull

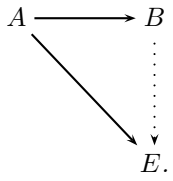
Before we can define the injective hull of a group, we first need some preliminary definitions and lemmas. Key concepts are divisibility, mentioned in section 1.2, and essential extensions.

Definition 2.3. *Let $A \hookrightarrow B$ be an injective homomorphism of abelian groups. Then, B is an* essential extension *of A if the pre-image of every non-zero subgroup of B in A is non-zero. Note that this implies that the cokernel of an essential extension is torsion.*

Lemma 2.4. *The only essential extension of a divisible abelian group E is E itself.*

Proof. Let E be a divisible abelian group, and $E \subset F$ an essential extension. Assume that $E \neq F$ is not surjective. Then there are a prime p and $y \in F$ such that $y \notin E$ and $py \in E$. Since E is divisible, there is an element $e \in E$ such that $pe = py$. So, $e - y$ is a p-torsion element in $\langle E, y\rangle \setminus E$, which means that $\langle e - y\rangle \cap E = 0$. This contradicts the fact that $E \subset \langle E, y\rangle$ is essential. □

Theorem 2.5. *Let A be an abelian group. Then there is an essential extension $i : A \hookrightarrow E$ such that for every essential extension $A \hookrightarrow B$ there is an essential extension $B \hookrightarrow E$ such that the following diagram commutes:*



Moreover, E is divisible and the only essential extension of E is E itself. Also, E is unique up to isomorphism in the sense that every essential extension of A satisfying the same universal property as $A \hookrightarrow E$ is A-isomorphic to E.

This group E is called the injective hull *of A.*

Proof. As we have seen in lemma 1.8, there is a divisible abelian group B with an injection $A \hookrightarrow B$.

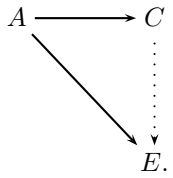
Consider all essential extensions of A in B. Note that this is not an empty set since it contains A itself. If we have a chain E_i of such extensions $A \subset E_i \subset B$, then $\bigcup_i E_i$ is again essential over A and contained in B, since every nonzero subgroup of $\bigcup_i E_i$ intersects some E_i nontrivially and therefore intersects A nontrivially. By Zorn's lemma, there is now a maximal essential extension E of A that is contained in B.

We will now prove that E is divisible. Assume that it is not. Then there is an $x \in E$ and a prime p such that there is no $y \in E$ with $py = x$. Since B is divisible, there is a $y \in B$ with $py = x$. Now consider the A-injection $E \subset \langle E, y\rangle$. Since E is a maximal essential extension of A inside B, this is not an essential extension. So, there exists a subgroup $F \subset \langle E, y\rangle$ such that $F \cap E = 0$. Let $a \neq 0$ be an element of F. Then a is of the form $e + ky$ for some $e \in E$, $k \in \mathbb{Z}$, $k \neq 0$. Because $\gcd(k, p) = 1$, a multiple of a is of the form $e' + y$, so we can let $k = 1$ without loss of generality. Because $py \in E$, we find that

$pa = pe + py \in E \cap F$ and therefore $pa = pe + py = 0$. So, $p(-e) = py = x$. This contradicts the assumption that x was not divisible by p in E, so E is divisible.

Because of lemma 2.4, the only essential extension of E is E itself.

Let $A \hookrightarrow C$ be any essential extension of A. We will show there is an injection $C \hookrightarrow E$ such that



is a commutative diagram.

Since E is divisible and therefore injective (theorem 1.10), the exact sequence $0 \to E \xrightarrow{i} C \oplus_A E$ splits. This means there is a homomorphism $\varphi : C \oplus_A E \to E$.

Define from this a new homomorphism:

$$\begin{array}{rcl} \varphi' : C & \longrightarrow & E \\ c & \longmapsto & \varphi(c, 0). \end{array}$$

Assume that φ' is not injective. Then the kernel of φ' is a nontrivial subgroup of C, and since C is essential over A, the kernel intersects A nontrivially. So, there is an $a \in A \setminus \{0\}$ for which $\varphi(a, 0) = \varphi'(a) = 0$. Because $(a, 0) = (0, a) = i(a) \in C \oplus_A E$, we find that $\varphi(i(a)) = 0$, which contradicts the fact that φ splits the sequence above. We find that φ' is the required injection from C to E respecting A.

Finally, let $A \hookrightarrow E'$ be an essential extension that has the same universal property as $A \hookrightarrow E$. Then, by this property, there is an essential extension $E \hookrightarrow E'$. This injection is an isomorphism because of lemma 2.4. □

2.2 Maximal r-extensions

In this section, A will be a fixed abelian group, and r a fixed map from the set of primes to the set of non-negative integers.

If G is an abelian group and n a positive integer, we denote the subgroup of G of n-torsion elements by $G[n]$. In particular, if p is a prime, $G[p]$ is the p-torsion of G, which can be considered as an $\mathbb{F}_p$-vector space. We denote the dimension of this vector space by $\operatorname{rank} G[p]$.

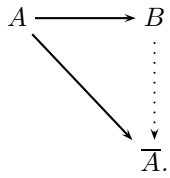
Theorem 2.6. *Define*

$$\widetilde{A} := A \oplus \bigoplus_{p \text{ prime}} (\mathbb{Z}/p\mathbb{Z})^{r(p)-\operatorname{rank} A[p]}.$$

Consider the r-extension

$$A \hookrightarrow \overline{A} := \operatorname{InjHull}(\widetilde{A}).$$

For every r-extension $A \hookrightarrow B$ there is an r-extension $B \hookrightarrow \overline{A}$ such that the following diagram is commutative:



The only r-extension of $\overline{A}$ is $\overline{A}$ itself. Up to isomorphism of $\overline{A}$, the r-extension $A \hookrightarrow \overline{A}$ is the only r-extension satisfying the universal property.

We will use the following lemmas in the proof.

Lemma 2.7. *Let A be an abelian group, p a prime and suppose that $A[p]$ is finite. Then, $A[p^n]$ is finite for all $n \in \mathbb{Z}_{>0}$.*

Proof. We use induction to n. For $n = 1$ we assumed that $A[p^1]$ is finite. For $n > 1$, let $B := A[p^n]$. Then we have the exact sequence

$$0 \longrightarrow p^{n-1}B/p^nB \longrightarrow B \longrightarrow B/p^{n-1}B \longrightarrow 0.$$

Note that $p^nB = 0$. Because B/pB is finite and there is a natural surjection $B/pB \twoheadrightarrow p^{n-1}B/p^nB$, we see that $p^{n-1}B/p^nB$ is also finite. By the induction hypothesis, $B/p^{n-1}B$ is finite and therefore $\#B = \#(p^{n-1}B/p^nB)\#(B/p^{n-1}B)$ is finite. □

Lemma 2.8. *Let B be an r-extension of A such that for all primes p, the rank of the p-torsion of A and B is equal. Then B is an essential extension.*

Proof. Let $C \neq 0$ be a subgroup of B that intersects (the image of) A trivially. Since B is torsion over A, there is an element $x \neq 0$ in C such that $px \in A$ for some prime p. Since $px \in C \cap A$, it is 0, so x is a p-torsion element of B that is not contained in the image of A. This contradicts the fact that A and B have p-torsion of equal rank. So, every non-trivial subgroup of B intersects A non-trivally, and B is an essential extension. □

Proof of theorem 2.6. First, we need to show that the extension $A \subset \overline{A}$ has the required properties. That is, $\overline{A}/A$ is torsion, and $\operatorname{rank} \overline{A}[p] \leq r(p)$.

Let $x \in \overline{A}$. Because $\overline{A}$ is essential over $\widetilde{A}$, the subgroup $\langle x \rangle \subset \overline{A}$ has a non-trivial intersection with $\widetilde{A}$. So, there is an $n \in \mathbb{Z}$, $n > 0$ such that $nx \in \widetilde{A}$. By definition, $\widetilde{A}$ is a direct sum of A and a number of torsion groups. There is an $m \in \mathbb{Z}$, $m > 0$ that annihilates the torsion part of $nx \in \widetilde{A}$, so $(mn)x \in A$. Therefore, $\overline{A}/A$ is torsion.

By construction, $\operatorname{rank} \widetilde{A}[p] = r(p)$. Since $\overline{A}$ is an essential extension, it also has $\operatorname{rank} \overline{A}[p] = r(p)$.

Now let $\varphi : A \hookrightarrow B$ be an r-extension. From this we will first construct an injective homomorphism $A \oplus \bigoplus_p (\mathbb{Z}/p\mathbb{Z})^{\operatorname{rank} B[p] - \operatorname{rank} A[p]} \to B$.

Since $A[p]$ and $B[p]$ are both $\mathbb{F}_p$-vector spaces, we know that $B[p] = \varphi(A[p]) \oplus V_p$, where V_p is an $\mathbb{F}_p$-vector space of dimension $(\operatorname{rank} B[p] - \operatorname{rank} A[p])$. Consider the homomorphism

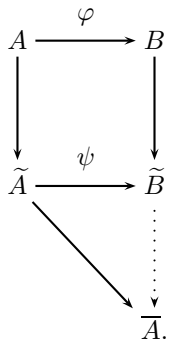
$$\begin{aligned} \varphi' : A \oplus \bigoplus_p V_p &\longrightarrow B \\ (a, (t_p)) &\longmapsto \varphi(a) + \sum_p t_p. \end{aligned}$$

Let $(a, (t_p))$ be an element of the kernel of φ'. Then $\varphi(a) + \sum_p t_p = 0$, so $\varphi(a)$ is torsion. Because φ is an injection, a is also torsion. So, we see that $\ker \varphi'$ is torsion.

Let q be a prime number, and let $(a, (t_p))$ be a q-torsion element of $\ker \varphi'$. This means that $t_p = 0$ unless $p = q$. The image of $(a, (t_p))$ is $\varphi(a) + t_q = 0$, which means that $\varphi(a) = -t_q$. Here $\varphi(a)$ is a q-torsion element in $\varphi(A)$ and $t_q \in V_q$. However, by definition of V_q, we know that $V_q \cap \varphi(A[q]) = \{0\}$. So, $\varphi(a) = t_q = 0$. The injectivity of φ now implies that $a = 0$. Therefore, $\ker \varphi'$ has trivial q-torsion for all primes q and since $\ker \varphi'$ is a torsion group, it is trivial.

By taking the direct sum of φ' with the identity map on $\bigoplus_p (\mathbb{Z}/p\mathbb{Z})^{r(p) - \operatorname{rank} B[p]}$ we obtain an injective homomorphism $\psi : \widetilde{A} \to \widetilde{B}$ (where $\widetilde{B}$ is defined analogously to $\widetilde{A}$).

Because the rank of the p-torsion of $\widetilde{A}$ is equal to that of $\widetilde{B}$, we can apply lemma 2.8, which implies that ψ is essential. The universal property of the injective hull $\overline{A}$ of $\widetilde{A}$ now provides an injection $\widetilde{B} \to \overline{A}$.



This gives the required injection $B \hookrightarrow \overline{A}$.

Let $\varphi : \overline{A} \hookrightarrow E$ be an r-extension. Then we have that $\operatorname{rank} \overline{A}[p] = \operatorname{rank} E[p] = r(p)$. So, by lemma 2.8, this extension is essential, and since $\overline{A}$ is divisible, the only essential of $\overline{A}$ is $\overline{A}$ itself (lemma 2.4).

Now assume that $A \hookrightarrow E$ is another r-extension of A satisfying the same universal property as $A \hookrightarrow \overline{A}$. Then by this universal property, there is an r-extension $\overline{A} \hookrightarrow E$. We have just seen that any such r-extension must be an isomorphism. □

Corollary 2.9. *$\overline{A}$ is closed under r-extensions, in the sense that $\overline{\overline{A}} = \overline{A}$*

Example 2.10 Let $A = \mathbb{Q}^*$. Since the unit group of an algebraic field extension of $\mathbb{Q}$ has p-torsion of at most rank 1, we set $r(p) = 1$. Then $\overline{A} = \{x \in \overline{\mathbb{Q}}^* : \exists n \in \mathbb{N}, x^n \in \mathbb{Q}^*\}$.

Alternatively, if we write $A = \mathbb{Q}^* \cong \langle -1 \rangle \oplus \bigoplus_p (p^{\mathbb{Z}})$, $\overline{A} \cong \mu \oplus \bigoplus_p (p^{\mathbb{Q}})$

Example 2.11 Let E be an elliptic curve over $\mathbb{Q}$ and $A = E(\mathbb{Q})$. Because the p-torsion of an elliptic curve over $\overline{\mathbb{Q}}$ has rank 2, we set $r(p) = 2$ for all primes p. Then $\overline{A} = \{P \in E(\overline{\mathbb{Q}}) : \exists n \in \mathbb{Z}_{>0} : nP \in E(\mathbb{Q})\}$.

If E is an elliptic curve over $\mathbb{F}_p$, we set $r(l) = 2$ for all primes $l \neq p$, and $r(p) = 0$ or 1, depending on whether E is supersingular or ordinary.

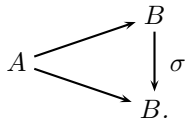
Chapter 3

Galois theory for abelian groups

3.1 Normal extensions

In this section we will describe A-automorphisms of r-extensions of a fixed abelian group A. As in the previous section, r is a fixed map from the set of primes to the set of non-negative integers.

Definition 3.1. *Let $A \hookrightarrow B$ be abelian groups. We define $\mathrm{Aut}_A(B)$ as the subgroup of all $\sigma \in \mathrm{Aut}(B)$ for which the following diagram commutes:*



Definition 3.2. *Let $A \hookrightarrow B$ be an r-extension of abelian groups. We call B* normal *over A if all injective A-homomorphisms (A-*embeddings*) from B into $\overline{A}$ have the same image.*

Theorem 3.3. *Let $A \hookrightarrow B$ be an r-extension of abelian groups. If for every $n \in \mathbb{Z}$ that occurs as the order of an element of B/A we have that $\#B[n] = \#\overline{A}[n]$, then B is normal over A.*

Proof. Let n be an integer that occurs as the order of some element of B/A. The injection f maps the (finite) set of n-th roots of unity in B injectively to the set of n-th roots of unity in $\overline{A}$. By our assumption, both sets have the same cardinality, so f is also surjective. It follows that the image of f contains all of the n-torsion of $\overline{A}$

Let b be an element of B and let n be the order of n in B/A. Then $f(nb) = g(nb)$, so $f(b) - g(b) = \zeta$ where ζ is an n-torsion element in $\overline{A}$. As we have seen, all the n-torsion of $\overline{A}$ is contained in the image of f, so $\zeta \in \mathrm{Im}(f)$. We find that $f(b - f^{-1}(\zeta)) - g(b) = 0$. So, $g(b) \in \mathrm{Im}(f)$. Because of symmetry, we find that $f(b) \in \mathrm{Im}(g)$. So, $f(B) = g(B)$. □

Example 3.4 The converse of this theorem does not hold. As an example, let $A = \langle 2 \rangle \subset \mathbb{C}^*$ and $B = \langle 2, \alpha \rangle$, where α is a fixed element of $\mathbb{C}$ such that $\alpha^4 = -4$.

When embedding B into $\overline{A}$, we only have to give the image of α. There are eight possible images, since $\overline{A}$ has eight 8th roots of unity. However, four of these have 4th power 4, and do therefore not induce an injection.

The remaining four embeddings send α to $i^k\alpha$, where $i = \alpha^2/2 \in B$. Note that $i^2 = -1$. Since $i \in B$, these four embeddings have the same image in $\overline{A}$. This means that $A \subset B$ is normal.

However, there is an element in B/A of order 8, but B does not contain any primitive 8th roots of unity.

Theorem 3.5. *Let $A \hookrightarrow B \hookrightarrow C$ be abelian groups. Assume that B is normal over A. Then there is a homomorphism $\mathrm{Aut}_A(C) \to \mathrm{Aut}_A(B)$ such that the following sequence is exact:*

$$0 \longrightarrow \mathrm{Aut}_B(C) \longrightarrow \mathrm{Aut}_A(C) \longrightarrow \mathrm{Aut}_A(B)$$

Proof. Since B is normal over A, every A-injection from B to $\overline{A}$ has the same image. Therefore, every A-injection from B to C also has the same image. In particular, if $\sigma \in \mathrm{Aut}_A(C)$, the restriction of σ to B maps B onto itself, since its image must be the same as that of the identity on C restricted to B. Therefore, there is a well-defined restriction map from $\mathrm{Aut}_A(C) \to \mathrm{Aut}_A(B)$.

The kernel of this map consists of exactly those automorphisms in $\mathrm{Aut}_A(C)$ that are the identity on B, so the kernel is $\mathrm{Aut}_B(C)$. □

Example 3.6 The last map is generally not a surjection. As an example, choose a fixed $\alpha \in \mathbb{C}^*$ such that $\alpha^8 = -9$ and let $i = \alpha^4/3$. Note that $i^2 = -1$. Now consider the extension $\langle \mathbb{Q}^*, i \rangle \subset \langle \mathbb{Q}^*, \alpha \rangle$. The torsion subgroup of $\langle \mathbb{Q}^*, \alpha \rangle$ is $\langle i \rangle$.

Consider an automorphism $\sigma \in \mathrm{Aut}_{\mathbb{Q}^*}(\langle \mathbb{Q}^*, \alpha \rangle)$. We know that $\sigma(\alpha)^8 = -9$, so $\sigma(\alpha) = i^k\alpha$, for a $k \in \mathbb{Z}$. This means that $\sigma(i) = (i^k\alpha)^4/3 = \alpha^4/3 = i$, so i is fixed under all automorphisms in $\mathrm{Aut}_{\mathbb{Q}^*}(\langle \mathbb{Q}^*, \alpha \rangle)$

However, $\mathrm{Aut}_{\mathbb{Q}^*}(\langle \mathbb{Q}^*, i \rangle)$ contains an automorphism that sends i to $-i$.

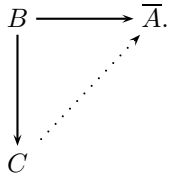
Theorem 3.7. *Let $A \hookrightarrow B \hookrightarrow C$ be abelian groups such that B and C are both normal over A. Then the following sequence is exact:*

$$0 \longrightarrow \mathrm{Aut}_B(C) \longrightarrow \mathrm{Aut}_A(C) \longrightarrow \mathrm{Aut}_A(B) \longrightarrow 0.$$

The proof of this theorem depends on the following lemmas.

Lemma 3.8. *Let $A \hookrightarrow B$ and $B \hookrightarrow C$ be r-extensions of abelian groups. Then the restriction map $\mathrm{Emb}_A(C, \overline{A}) \to \mathrm{Emb}_A(B, \overline{A})$ is a surjection.*

Proof. Let ϕ be an element of $\mathrm{Emb}_A(B, \overline{A})$. Because every r-extension of B is also an r-extension of A, this embedding ϕ has the universal property of $B \hookrightarrow \overline{B}$. Then, since $B \hookrightarrow C$ is an r-extension, there is an injection $C \hookrightarrow \overline{A}$ such that the following diagram commutes:



Therefore, the restriction map $\mathrm{Emb}_A(C, \overline{A}) \to \mathrm{Emb}_A(B, \overline{A})$ is a surjection. □

Lemma 3.9. *Let $A \hookrightarrow B$ be a normal extension and $\sigma \in \mathrm{Emb}_A(B, \overline{A})$. Then the map*

$$\begin{array}{rcl} \sigma_* : \mathrm{Aut}_A(B) & \longrightarrow & \mathrm{Emb}_A(B, \overline{A}) \\ \varphi & \longmapsto & \sigma\varphi \end{array}$$

gives a bijection between $\mathrm{Emb}_A(B, \overline{A})$ and $\mathrm{Aut}_A(B)$.

Proof. Consider the map

$$\begin{array}{rcl} \mathrm{Emb}_A(B, \overline{A}) & \longrightarrow & \mathrm{Aut}_A(B) \\ \tau & \longmapsto & \sigma^{-1}\tau \end{array}$$

This map is well-defined since $\tau(B) = \sigma(B)$ by the definition of a normal extension, and therefore σ^{-1} is defined on the image of τ.

It is clear from the definition that this map is a two-sided inverse of σ_*. This means that σ_* is a bijection. □

Proof of theorem 3.7. Because of theorem 3.5, we only need to prove that the restriction map $\mathrm{Aut}_A(C) \to \mathrm{Aut}_A(B)$ is a surjection.

Choose $\sigma \in \mathrm{Emb}_A(C, \overline{A})$ and let $\sigma' \in \mathrm{Emb}_A(B, \overline{A})$ be the restriction of σ to B. As shown in lemma 3.9, these two embeddings induce bijections $\sigma_* : \mathrm{Aut}_A(C) \xrightarrow{\sim} \mathrm{Emb}_A(C, \overline{A})$ and $\sigma'_* : \mathrm{Aut}_A(B) \xrightarrow{\sim} \mathrm{Emb}_A(B, \overline{A})$.

$$\begin{array}{ccc} \mathrm{Aut}_A(C) & \xrightarrow{\text{res}} & \mathrm{Aut}_A(B) \\ {\scriptstyle \sigma_*}\downarrow\wr & & {\scriptstyle \sigma'_*}\downarrow\wr \\ \mathrm{Emb}_A(C, \overline{A}) & \xrightarrow{\text{res}} & \mathrm{Emb}_A(B, \overline{A}) \end{array}$$

An automorphism of C composed with σ, restricted to B gives the same embedding of B into $\overline{A}$ as first restricting to B and then composing with σ', so the above diagram is commutative. Since we already know the restriction map $\mathrm{Emb}_A(C, \overline{A}) \to \mathrm{Emb}_A(B, \overline{A})$ is surjective (lemma 3.8), the restriction $\mathrm{Aut}_A(C) \to \mathrm{Aut}_A(B)$ is a surjection. □

The following theorem is the analogue of theorem 1.5.

Theorem 3.10. *Let A be an abelian group, and $A \subset B$ and $A \subset C$ two r-extensions contained in $\overline{A}$. If B and C are both normal over A, then $B+C$ and $B \cap C$ are also normal over A, and there is a natural isomorphism*

$$\mathrm{Aut}_A(B + C) \xrightarrow{\sim} \mathrm{Aut}_A(B) \times_{\mathrm{Aut}_A(B \cap C)} \mathrm{Aut}_A(C).$$

Proof. All embeddings of B into $\overline{A}$ have the same image because B is normal over A, and the same holds for C. Therefore, all embeddings of $B \cap C$ into $\overline{A}$ have the same image: the intersection of the images of B and C. So, $B \cap C$ is normal over A.

Similarly, every embedding of $B + C$ into $\overline{A}$ can be restricted to embeddings of B and C into $\overline{A}$. The image of $B+C$ in $\overline{A}$ is the sum of the images of B and C, and therefore all embeddings of $B + C$ into $\overline{A}$ have the same image and $B + C$ is normal over A.

Because of theorem 3.5 there are restriction maps from $\mathrm{Aut}_A(B+C)$ to $\mathrm{Aut}_A(B)$ and $\mathrm{Aut}_A(C)$, and from $\mathrm{Aut}_A(B)$ and $\mathrm{Aut}_A(C)$ to $\mathrm{Aut}_A(B \cap C)$. Clearly, restricting an automorphism from $\mathrm{Aut}_A(B + C)$ first to B and then to $B \cap C$ gives the same automorphism as first restricting to C and then to $B \cap C$. So, the universal property of $\mathrm{Aut}_A(B) \times_{\mathrm{Aut}_A(B \cap C)} \mathrm{Aut}_A(C)$ gives a homomorphism from $\mathrm{Aut}_A(B + C)$ to this fibered product.

The kernel of this homomorphism consists of those automorphisms that are the identity on B and on C. Those automorphisms are clearly also the identity on $B + C$, so, the kernel is trivial.

To prove that it is surjective, let $(\sigma_B, \sigma_C) \in \mathrm{Aut}_A(B) \times_{\mathrm{Aut}_A(B \cap C)} \mathrm{Aut}_A(C)$. Define an automorphism in $\mathrm{Aut}_A(B + C)$ by sending elements $b + c \in B + C$ (where $b \in B$ and $c \in C$) to $\sigma_B(b)+\sigma_C(c) \in B+C$. This is well defined since σ_B and σ_C are equal on $B \cap C$. It is an automorphism since it maps B to B, C to C and $B \cap C$ to $B \cap C$ and therefore the inverse is given by the homomorphism analogously derived from $(\sigma_B^{-1}, \sigma_C^{-1})$. □

3.2 Computing automorphism groups

Let $0 \to A \to B \xrightarrow{g} C \to 0$ be an exact sequence of abelian groups. Consider all automorphisms σ of B for which the following diagram is commutative:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0 \\ & & \| & & \sigma\downarrow\wr & & \| & & \\ 0 & \longrightarrow & A & \longrightarrow & B & \longrightarrow & C & \longrightarrow & 0. \end{array}$$

We will call the group of these automorphisms $\mathrm{Aut}_A^1(B)$. If we make the condition that the diagram has to commute explicit, we get the following alternate description:

$$\mathrm{Aut}_A^1(B) = \{\sigma \in \mathrm{Aut}(B) : \forall x \in A : \sigma(x) = x \text{ and } \forall y \in B : g(\sigma(y) - y) = 0\}.$$

Using the exactness of $0 \to A \to B \to C \to 0$, we can rewrite the second condition, yielding:

$$\mathrm{Aut}_A^1(B) = \{\sigma \in \mathrm{Aut}(B) : \forall x \in A : \sigma(x) = x \text{ and } \forall y \in B : \sigma(y) - y \in A\}.$$

Lemma 3.11. *If $0 \to A \to B \xrightarrow{g} C \to 0$ is an exact sequence of abelian groups, then the map*

$$\begin{array}{rcl} \varphi : \mathrm{Aut}_A^1(B) & \longrightarrow & \mathrm{Hom}(C, A) \\ \sigma & \longmapsto & (c \mapsto \sigma(\tilde{c}) - \tilde{c}, \text{ where } \tilde{c} \in g^{-1}(c).) \end{array}$$

is a well defined isomorphism of abelian groups.

Proof. By definition of $\mathrm{Aut}_A^1(B)$, we know that $\sigma(\tilde{c}) - \tilde{c}$ is really an element of A for all $\tilde{c} \in B$. Also, if $\tilde{c}'$ is another element in the inverse image of c, then the difference $\tilde{c} - \tilde{c}'$ is contained in A, so σ maps $\tilde{c} - \tilde{c}'$ to itself. Because of that, $\sigma(\tilde{c}) - \tilde{c} = \sigma(\tilde{c}') - \tilde{c}'$, so the above map is well-defined.

It is clear that the identity is mapped to 0, so to show that φ is a homomorphism, we only need to consider $\varphi(\sigma\tau)$ for $\sigma, \tau \in \mathrm{Aut}_A^1(B)$:

$$\begin{array}{rcl} \varphi(\sigma\tau)(c) & = & \sigma\tau(\tilde{c}) - \tilde{c} = \sigma\tau(\tilde{c}) - \sigma(\tilde{c}) + \sigma(\tilde{c}) - \tilde{c} \\ & = & \sigma(\tau(\tilde{c}) - \tilde{c})) + \sigma(\tilde{c}) - \tilde{c} = \tau(\tilde{c}) - \tilde{c} + \sigma(\tilde{c}) - \tilde{c} \\ & = & \varphi(\sigma)(c) + \varphi(\tau)(c) \end{array}$$

Now consider the following map:

$$\begin{array}{rcl} \psi : \mathrm{Hom}(C, A) & \longrightarrow & \mathrm{Aut}_A^1(B) \\ h & \longmapsto & (b \mapsto b + hg(b)) \,. \end{array}$$

Note that if $h \in \mathrm{Hom}(C, A)$, the homomorphism $b \mapsto hg(b) + b$ is indeed an element of $\mathrm{Aut}^1_A(B)$: it is an automorphism since $b \mapsto b - hg(b)$ is the inverse; if $b \in A$, then $g(b) = 0$, so $b + hg(b) = b$, and $g(b + hg(b)) = 0 + g(b) = g(b)$.

This is a two-sided inverse of φ, since

$$(\varphi\psi(h))(c) = \psi(h)(\tilde{c}) - \tilde{c} = (hg(\tilde{c}) + \tilde{c}) - \tilde{c} = hg(\tilde{c}) = h(c)$$

and

$$\psi\varphi(\sigma)(b) = b + \varphi(\sigma)(g(b)) = b + \sigma(\widetilde{g(b)}) - \widetilde{g(b)} = b + \sigma(b) - b = \sigma(b).$$

□

Corollary 3.12. *If $A \hookrightarrow B$ is an r-extension, then*

$$\mathrm{Aut}_{A+B_{\mathrm{tor}}}(B) \cong \mathrm{Hom}(B/(A + B_{\mathrm{tor}}), B_{\mathrm{tor}})$$

Proof. We apply the previous lemma to the exact sequence $0 \to A + B_{\mathrm{tor}} \to B \to B/(A + B_{\mathrm{tor}}) \to 0$. This gives us an isomorphism between $\mathrm{Aut}^1_{A+B_{\mathrm{tor}}}(B)$ and $\mathrm{Hom}(B/(A + B_{\mathrm{tor}}), A + B_{\mathrm{tor}})$.

Claim: $\mathrm{Aut}^1_{A+B_{\mathrm{tor}}}(B) = \mathrm{Aut}_{A+B_{\mathrm{tor}}}(B)$. By the definition of the left-hand automorphism group, it is sufficient to show that for all $\sigma \in \mathrm{Aut}_{A+B_{\mathrm{tor}}}(B)$ and all $b \in B$ we have that $\sigma(b) - b \in A + B_{\mathrm{tor}}$.

Since $A \hookrightarrow B$ is an r-extension, the group $B/(A + B_{\mathrm{tor}})$ is torsion. Therefore, there is an $n \in \mathbb{Z}_{>0}$ such that nb is mapped to zero in $B/(A + B_{\mathrm{tor}})$. Therefore, $nb \in AB_{\mathrm{tor}}$, and $\sigma(nb) - nb = 0$. So, $n(\sigma(b) - b) = 0$, which means that $\sigma(b) - b \in B_{\mathrm{tor}}$.

Claim: $\mathrm{Hom}(B/(A + B_{\mathrm{tor}}), A + B_{\mathrm{tor}}) = \mathrm{Hom}(B/(A + B_{\mathrm{tor}}), B_{\mathrm{tor}})$. We have already seen that $B/(A + B_{\mathrm{tor}})$ is torsion. Therefore, the image of any homomorphism from $B/(A + B_{\mathrm{tor}})$ to $A + B_{\mathrm{tor}}$ is torsion as well and therefore contained in B_{tor}. □

Corollary 3.13. $\mathrm{Aut}_{A+B_{\mathrm{tor}}}(B)$ *is abelian.*

Define the *Tate-module* $T(A) := \varprojlim \overline{A}_{\mathrm{tor}}[n]$ (cf. Silverman [5] III, §7). The projective limit ranges over all positive integers n, with projection maps $\overline{A}_{\mathrm{tor}}[m'] \to \overline{A}_{\mathrm{tor}}[m]$ if $m \mid m'$.

Theorem 3.14. *The map*

$$\begin{aligned} \chi : \mathrm{Hom}(\overline{A}/(A + \overline{A}_{\mathrm{tor}}), \overline{A}_{\mathrm{tor}}) &\longrightarrow \mathrm{Hom}(A, T(A)) \\ \varphi &\longmapsto (x \mapsto (\varphi(x/n))_n) \end{aligned}$$

is a well defined isomorphism of abelian groups.

Proof. Let x be an element of A and $n \in \mathbb{Z}_{>0}$. Then $\frac{x}{n}$ is an element of $\overline{A}$ of which the n-th power is in $A + \overline{A}_{\text{tor}}$. Therefore, $\varphi(\frac{x}{n}) \in \overline{A}[n]$. Note that while $\frac{x}{n}$ is only defined up to n-torsion, $\overline{A}_{\text{tor}}$ is contained in the kernel of φ, so $\varphi(\frac{x}{n}$ is properly defined. If $m \mid n$, then $\varphi(\frac{x}{m}) \in \overline{A}[m]$, and $\frac{n}{m}\varphi(\frac{x}{n}) = \varphi(\frac{x}{m})$. So, $(\varphi(\frac{x}{n}))_n$ is a proper element of $T(A)$. It is clear that the map χ respects the group operation, so it remains to prove that χ is an isomorphism.

If $\varphi(\frac{x}{n}) = 0$ for all $x \in A$ and $n \in \mathbb{Z}_{>0}$, and assume that $\varphi \neq 0$. Then there is an $a \in \overline{A}/(A+\overline{A}_{\text{tor}})$ such that $\varphi(a) \neq 0$. Let n be the order of a in $\overline{A}/(A+\overline{A}_{\text{tor}})$ and let $x = na$. Then, $\varphi(\frac{x}{n}) = \varphi(a) \neq 0$. Therefore, the homomorphism is an injection.

To prove surjectivity, let $\psi \in \text{Hom}(A, T(A))$. Define a homomorphism φ' from $\overline{A}$ to $\overline{A}_{\text{tor}}$ as follows: let $x \in \overline{A}$. Then there is an $y \in A$ and an $n \in \mathbb{Z}_{>0}$ such that $nx = y$. Now set $\varphi'(x) = \psi(y)_n$. Here $\psi(y)_n$ means the n-th component of the projective limit $\psi(y)$. This is an element of $\overline{A}[n] \subset \overline{A}_{\text{tor}}$. This map is well defined because of the restriction properties of the projective limit. It is a homomorphism because ψ is a homomorphism. If $x \in A$, then we can take $y = x$ and $n = 1$, and since $\psi(x)_1 \in A_{\text{tor}}[1] = \{0\}$, $\varphi'(x) = 0$ If $x \in \overline{A}_{\text{tor}}$, we can take $y = 0$, so $\varphi'(x) = \psi(0)_n = 0$. Therefore, $A + \overline{A}_{\text{tor}} \subset \ker \varphi'$, which means that φ induces a homomorphism φ from $\overline{A}/(A + \overline{A}_{\text{tor}})$ to $\overline{A}_{\text{tor}}$. It is clear that χ maps φ to ψ. So, χ is an isomorphism, as required. □

Let $0 \to A \to B \to C \to 0$ again be an exact sequence of abelian groups, and let D be a subgroup of A.

Consider the automorphisms of B that map A to itself: $\text{Aut}(A, B) := \{\sigma \in \text{Aut}(B) : \sigma(A) = A\}$. Define $\text{Aut}_D(A, B)$ to be the subgroup consisting of those automorphisms that are the identity when restricted to D.

Lemma 3.15. *The sequence*

$$0 \longrightarrow \text{Aut}^1_A(B) \longrightarrow \text{Aut}_D(A, B) \longrightarrow \text{Aut}_D(A) \times \text{Aut}(C)$$

is exact. Additionally, if the exact sequence $0 \to A \to B \to C \to 0$ *splits, the sequence*

$$0 \longrightarrow \text{Aut}^1_A(B) \longrightarrow \text{Aut}_D(A, B) \longrightarrow \text{Aut}_D(A) \times \text{Aut}(C) \longrightarrow 0$$

is exact and it splits.

Proof. First, we will show the first sequence is indeed exact. The automorphisms in $\text{Aut}^1_A(B)$ are the identity when restricted to A, so they clearly map A to itself and are the identity when restricted to D. Therefore, $\text{Aut}^1_A(B)$ is a subgroup of $\text{Aut}_D(A, B)$. The sequence is exact at $\text{Aut}_D(A, B)$, since the image of the first map and kernel of the second map are both exactly those automorphisms in $\text{Aut}_D(A, B)$ that are the identity when restricted to A and induce the identity on C.

Now assume that $0 \to A \to B \to C \to 0$ splits. Then, $B \cong A \oplus C$. This means that, given an automorphism in $\mathrm{Aut}_D(A)$ and an automorphism of C, we can compose them into an automorphism of $B \cong A \oplus C$ that maps A to itself and is the identity on D. This gives a map $\mathrm{Aut}_D(A) \times \mathrm{Aut}(C) \to \mathrm{Aut}_D(A, B)$ which splits the exact sequence. □

Now define $\mathrm{Aut}^1_D(A, B)$ as the subgroup of $\mathrm{Aut}_D(A, B)$ consisting of the automorphism that induce the identity on C. This means that

$$\mathrm{Aut}^1_D(A, B) = \{\sigma \in \mathrm{Aut}(B) : \sigma|_A \in \mathrm{Aut}_D(A) \text{ and } \forall b \in B : \sigma(b) - b \in A\}.$$

We can restrict the exact sequence from lemma 3.15 to these automorphisms:

Lemma 3.16. *The sequence*

$$0 \longrightarrow \mathrm{Aut}^1_A(B) \longrightarrow \mathrm{Aut}^1_D(A, B) \longrightarrow \mathrm{Aut}_D(A)$$

is exact. If the sequence $0 \to A/D \to B/D \to C \to 0$ *splits, the sequence*

$$0 \longrightarrow \mathrm{Aut}^1_A(B) \longrightarrow \mathrm{Aut}^1_D(A, B) \longrightarrow \mathrm{Aut}_D(A) \longrightarrow 0$$

is exact and splits.

Proof. Since automorphisms in $\mathrm{Aut}^1_A(B)$ are automorphisms of B that are the identity on D and C and map A to itself, $\mathrm{Aut}^1_A(B) \subset \mathrm{Aut}^1_D(A, B)$, so the sequence is exact at $\mathrm{Aut}^1_A(B)$.

The image of the first map and kernel of the second map in $\mathrm{Aut}^1_D(A, B)$ are exactly those automorphisms of $\mathrm{Aut}^1_D(A, B)$ that are the identity on A, so the sequence is exact at $\mathrm{Aut}^1_D(A, B)$.

Now assume that $0 \to A/D \to B/D \to C \to 0$ splits.

There is an abelian group $\widetilde{C}$ with $D \subset \widetilde{C} \subset B$ such that the map $B/D \to C$ induces an isomorphism $\widetilde{C}/D \to C$. Because $\widetilde{C} \cap A = D$, theorem 1.4 implies that $B = \widetilde{C} \oplus_D A$. Because of this, we can extend an automorphism of A that is the identity on D to an automorphism of B: the image of the map

$$\begin{array}{rcl} \mathrm{Aut}_D(A) & \longrightarrow & \mathrm{Aut}_D(A) \times \mathrm{Aut}_D(\widetilde{C}) \hookrightarrow \mathrm{Aut}_D(B) \\ \sigma & \longmapsto & (\sigma \oplus \mathrm{id}_{\widetilde{C}}) \end{array}$$

is contained in $\mathrm{Aut}^1_D(A, B)$ and this map gives the required splitting. □

Corollary 3.17. *If* $0 \to B_{\mathrm{tor}}/A_{\mathrm{tor}} \to B/A$ *splits, the following sequence is exact and splits:*

$$0 \longrightarrow \mathrm{Aut}_{A+B_{\mathrm{tor}}}(B) \longrightarrow \mathrm{Aut}_A(B) \longrightarrow \mathrm{Aut}_{A_{\mathrm{tor}}}(B_{\mathrm{tor}}) \longrightarrow 0$$

Proof. We will apply lemma 3.16 to the exact sequence $0 \to AB_{\text{tor}} \to B \to B/AB_{\text{tor}} \to 0$, with $A \subset AB_{\text{tor}}$ taking the role of D.

Since $AB_{\text{tor}}/A = B_{\text{tor}}/A_{\text{tor}}$, the exact sequence $0 \to AB_{\text{tor}}/A \to B/A \to B/AB_{\text{tor}} \to 0$ splits.

We can now apply lemma 3.16. Together with the fact that $\text{Aut}_A(A + B_{\text{tor}}) = \text{Aut}_{A_{\text{tor}}}(B_{\text{tor}})$, this shows that the sequence

$$0 \longrightarrow \text{Aut}^1_{A+B_{\text{tor}}}(B) \longrightarrow \text{Aut}_A(B) \longrightarrow \text{Aut}_{A_{\text{tor}}}(B_{\text{tor}}) \longrightarrow 0$$

splits. As we have seen in the proof of corollary 3.12, the groups $\text{Aut}^1_{A+B_{\text{tor}}}(B)$ is equal to $\text{Aut}_{A+B_{\text{tor}}}(B)$. □

Corollary 3.18. *The following sequence is exact and splits:*

$$0 \longrightarrow \text{Aut}_{A+\overline{A}_{\text{tor}}}(\overline{A}) \longrightarrow \text{Aut}_A(\overline{A}) \longrightarrow \text{Aut}_{A_{\text{tor}}}(\overline{A}_{\text{tor}}) \longrightarrow 0$$

Proof. $\overline{A}$ is divisible by definition. For all $a \in \overline{A}_{\text{tor}}$, $n \in \mathbb{Z}$, $n \neq 0$, there is a $b \in \overline{A}$ with $nb = a$. Since a is torsion and a multiple of b, the element b is also torsion. Therefore, $\overline{A}_{\text{tor}}$ is also divisible. By lemma 1.7, $\overline{A}_{\text{tor}}/A_{\text{tor}}$ is divisible. This means that it is injective (theorem 1.10), so we can apply corollary 3.17 to $B = \overline{A}$. □

Corollary 3.19. *Using the previous corollary and theorem 3.14, we find that*

$$\text{Aut}_A(\overline{A}) \cong \text{Hom}(A, \varprojlim \overline{A}[n]) \rtimes \text{Aut}_{A_{\text{tor}}}(\overline{A}_{\text{tor}}).$$

Example 3.20 Let A be $\mathbb{Q}^*$ and $r(p) = 1$ for all primes p. Define $\hat{\mu} = T(\mathbb{Q}^*) = \varprojlim \mu_n$, where n ranges over the positive integers, with projection maps $\mu_m \to \mu_{m'}$ given by raising to the power m/m', if $m' \mid m$.

Then the following map is an isomorphism:

$$\begin{array}{rcl} \text{Aut}_A(\overline{A}) & \xrightarrow{\sim} & \text{Hom}(\mathbb{Q}^*, \hat{\mu}) \rtimes \hat{\mathbb{Z}}^* \\ \sigma & \longmapsto & (x \mapsto (\sigma(\sqrt[n]{x})/\sqrt[n]{x})_n, \sigma|_{\overline{A}_{\text{tor}}}). \end{array}$$

Note that this isomorphism depends on the choice of n-th roots.

Example 3.21 The sequence from corollary 3.17, $0 \longrightarrow \text{Aut}_{A+B_{\text{tor}}}(B) \longrightarrow \text{Aut}_A(B) \longrightarrow \text{Aut}_{A_{\text{tor}}}(B_{\text{tor}}) \longrightarrow 0$ is not always exact.

Consider the extensions from example 3.6. Let A be $\mathbb{Q}^*$, and $B = \langle \mathbb{Q}^*, \alpha \rangle$. As seen before, the image of $\text{Aut}_A(B)$ in $\text{Aut}_{A_{\text{tor}}}(B_{\text{tor}})$ is trivial, while on the other hand, $\text{Aut}_{A_{\text{tor}}}(B_{\text{tor}}) = \text{Aut}_{\langle -1 \rangle}(\langle i \rangle) \cong \mathbb{Z}/2\mathbb{Z}$.

Example 3.22 Even if the sequence is exact, it does not always have to split.

As an example, let $A = \langle -1, \sqrt[4]{-3} \rangle$, and $B = \langle \zeta_8, \sqrt[8]{3} \rangle$. Denote $\sqrt[4]{-3}$ by α and $\sqrt[8]{3}$ by β. Choose the roots in such a way that $\beta^2 = \zeta^8 \alpha$. The torsion subgroup A_{tor} is equal to $\langle -1 \rangle$ and $B_{\text{tor}} = \langle \zeta_8 \rangle$.

Since $\beta^2 = \zeta_8 \alpha$, the automorphism group $\text{Aut}_{AB_{\text{tor}}}(B) = \mathbb{Z}/2\mathbb{Z}$. The automorphism group of the torsion $\text{Aut}_{A_{\text{tor}}}(B_{\text{tor}})$ is $(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

So, if the sequence were to split, $\text{Aut}_A(B)$ would be of exponent 2. However, B has an automorphism σ that sends ζ_8 to ζ_8^3 and β to $\zeta_8 \beta$. This automorphism is the identity on A, since it maps $-1 = \zeta_8^4$ to $\zeta_8^{12} = -1$ and $\alpha = \zeta_8^{-1} \beta^2$ to $\zeta_8^{-3} \zeta_8^2 \beta^2 = \alpha$. It does not have order 2, however, since σ^2 maps β to $\zeta_8^2 \beta$, which is not equal to β. Therefore, the sequence does not split.

Chapter 4

Galois theory

4.1 Kummer theory

Let K be a field with algebraic closure $\overline{K}$ and m a positive integer such that $\operatorname{char} K$ does not divide m. Define the subgroup of K^* of m-th roots of unity as

$$\mu_m(K) := \{\zeta \in K^* : \zeta^m = 1\}.$$

Denote $\mu_m(\overline{K})$ by μ_m. For a subgroup W of K^* define the subgroup of $\overline{K}^*$ of m-th roots of W as

$$W^{1/m} := \{x \in \overline{K}^* : x^m \in W\}.$$

Theorem 4.1. *(Kummer theory) Let K be a field and $m \in \mathbb{Z}_{>0}$ such that $\operatorname{char} K$ does not divide m, and μ_m is contained in K^*. Then, the map from groups to fields*

$$\begin{array}{rcl} \{W : K^{*m} \subset W \subset K^*\} & \longrightarrow & \{L : K \subset L \subset \overline{K}, L/K \text{ abelian of exponent } m\} \\ W & \longmapsto & K(W^{1/m}) \end{array}$$

is a bijection.

Additionally, if $K^{*m} \subset W \subset K^*$ and $[W : K^{*m}] < \infty$, then $[K(W^{1/m}) : K] = [W : K^{*m}]$ and the map

$$\begin{array}{rcl} \operatorname{Gal}(K(W^{1/m})/K) & \longrightarrow & \operatorname{Hom}(W/K^{*m}, \mu_m) \\ \sigma & \longmapsto & (\alpha \mapsto \sigma(\beta)/\beta, \text{ for } \beta \in W \text{ satisfying } \beta^m = \alpha) \end{array}$$

is an isomorphism.

Proof. See Lang's Algebra [2], section VI, theorems §8.1 and §8.2. □

Corollary 4.2. *Let K and m be as above. Let W is an abelian group with $K^{*m} \subset W \subset K^*$, where $K(W^{1/m})/K$ may be infinite. Then, the map*

$$\begin{array}{rcl} \mathrm{Gal}(K(W^{1/m})/K) & \longrightarrow & \mathrm{Hom}(W/K^{*m}, \mu_m) \\ \sigma & \longmapsto & (\alpha \mapsto \sigma(\beta)/\beta, \textit{ for } \beta \in W \textit{ satisfying } \beta^m = \alpha) \end{array}$$

is an isomorphism.

Proof. From infinite Galois theory, we know that

$$\mathrm{Gal}(K(W^{1/m})/K) = \varprojlim \mathrm{Gal}(K(W_0^{1/m})/K),$$

where W_0 ranges over all abelian groups $K^{*m} \subset W_0 \subset W$ for which the field extension $K(W_0^{1/m})/K$ is finite.

Because $W/K^{*m} = \varinjlim W_0/K^{*m}$, the universal property of the injective limit gives us that

$$\mathrm{Hom}(W/K^{*m}, \mu_m) \cong \varprojlim \mathrm{Hom}(W_0/K^{*m}, \mu_m).$$

Theorem 4.1 tells us that the maps $\mathrm{Gal}(K(W_0^{1/m})/K) \to \mathrm{Hom}(W_0, \mu_m)$ are isomorphisms, and since these maps are respected by the inclusions between the W_0's, the corollary follows. □

Theorem 4.3. *Let K, m and W be as in the previous theorem. Then the natural restriction map*

$$\mathrm{Gal}(K(W^{1/m})/K) \longrightarrow \mathrm{Aut}_{K^*}(W^{1/m})$$

is an isomorphism.

Proof. Consider the sequence

$$1 \longrightarrow K^* \longrightarrow W^{1/m} \xrightarrow{m} W/K^{*m} \longrightarrow 1.$$

It is exact, since the elements of $W^{1/m}$ that are $1 \in W/K^{*m}$ after taking the m-th power are exactly those in K^* (note that $\mu_m \in K^*$), and every element in W has an m-th root in $W^{1/m}$.

In lemma 3.11 we have seen that there is an isomorphism

$$\begin{array}{rcl} \mathrm{Aut}^1_{K^*}(W^{1/m}) & \longrightarrow & \mathrm{Hom}(W/K^{*m}, K^*) \\ \sigma & \longmapsto & (\alpha \mapsto \sigma(\beta)/\beta, \text{ where } \beta^m = \alpha.) \end{array}$$

Since W/K^{*m} is a subgroup of K^*/K^{*m}, if an automorphism of $W^{1/m}$ is the identity on K^*, it also induces the identity on W/K^{*m}. Because of this, $\mathrm{Aut}^1_{K^*}(W^{1/m})$ is equal to $\mathrm{Aut}_{K^*}(W^{1/m})$.

Also, $W/{K^*}^m$ is a group of exponent m, and therefore the image of any homomorphism from $W/{K^*}^m$ to K^* is in fact contained in μ_m. This means that $\mathrm{Hom}(W/{K^*}^m, K^*) = \mathrm{Hom}(W/{K^*}^m, \mu_m)$.

Combining this with corollary 4.2 proves the theorem. □

We can generalize the above to (suitably defined) infinite values of m. A Steinitz number m is a formal expression

$$m = \prod_{p \text{ prime}} p^{m(p)}$$

where $m(p) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$.

We can define a natural multiplication on Steinitz numbers, as well as the concept of divisibility: if $m = \prod_{p \text{ prime}} p^{m(p)}$ and $n = \prod_{p \text{ prime}} p^{n(p)}$ are Steinitz numbers, then $mn = \prod_{p \text{ prime}} p^{m(p)+n(p)}$ and $m \mid n$ if $\forall p$ prime : $m(p) \leq n(p)$.

Note that the positive integers form a subset of the Steinitz numbers. If n is a positive integer, $n = \prod_{p \text{ prime}} p^{\mathrm{ord}_p(n)}$

If K is again a field with algebraic closure $\overline{K}$ and m a Steinitz number, define

$$\mu_m(K) = \{\zeta \in K^* : \exists n \in \mathbb{Z}_{>0}, n \mid m \text{ with } \zeta^n = 1\}$$

and again denote $\mu_m(\overline{K})$ by μ_m. Also define, for a subgroup W of K^*,

$$W^{1/m} = \{x \in \overline{K}^* : \exists n \in \mathbb{Z}_{>0}, n \mid m \text{ with } x^n \in W\}.$$

Theorem 4.4. *(Kummer theory for Steinitz numbers) Let K be a field and m a Steinitz number with* $\mathrm{char}\, K$ *not dividing m such that $\mu_m \subset K^*$. Then there is a bijection*

$$\begin{array}{rcl} \{B : K^* \subset B \subset {K^*}^{1/m}\} & \longrightarrow & \{L : K \subset L \subset \overline{K}, L/K \textit{ abelian of exponent } m\} \\ B & \longmapsto & K(B) \end{array}$$

Additionally, if B is an abelian group with $K^* \subset B \subset {K^*}^{1/m}$, then the natural restriction

$$\mathrm{Gal}(K(B)/K) \longrightarrow \mathrm{Aut}_{K^*}(B)$$

is an isomorphism.

Proof. A group B with $K^* \subset B \subset {K^*}^{1/m}$ is the union of a number of groups $W^{1/n}$, where n is a positive integer and ${K^*}^n \subset W \subset K^*$. Similarly, a field L with $K \subset L \subset \overline{K}$ such that L/K is abelian of exponent m is the union of a number of fields L_0, where L_0/K is of finite exponent $n \mid m$.

Because of this, the bijection between $\{W : {K^*}^m \subset W \subset K^*\}$ and $\{L : K \subset L \subset \overline{K}, L/K$ abelian of exponent $m\}$ from theorem 4.1 now extends to the case where m is a Steinitz number.

For the second part of the proof, consider all groups W for which there is a positive integer n such that $W^{1/m} \subset B$ and $K^{*n} \subset W \subset K^*$. For such pairs (W, n), we can apply theorem 4.3, which states that the natural restriction $\mathrm{Gal}(K(W^{1/n})/K) \to \mathrm{Aut}_{K^*}(W^{1/n})$ is an isomorphism.

We now take the projective limit over all such pairs (W, n) on both sides. Since the inclusions between such W respect these restriction maps, the natural restriction between the projective limits is an isomorphism as well. The left-hand projective limit is $\mathrm{Gal}(K(B)/K)$.

Because $K^* \subset W^{1/n}$ is normal, each automorphism of B maps $W^{1/n}$ to itself. Since we also have that $\bigcup W^{1/n} = B$, the right-hand projective limit $\varprojlim \mathrm{Aut}_{K^*}(W^{1/n})$ is $\mathrm{Aut}_{K^*}(B)$.

Therefore, the restriction is an isomorphism:

$$\mathrm{Gal}(K(B)/K) \xrightarrow{\sim} \mathrm{Aut}_{K^*}(B).$$

□

4.2 Galois groups of radical field extensions

Let K again be a field with fixed algebraic closure $\overline{K}$. Let B be a group such that $K^* \subset B \subset K^{*1/m}$, for a Steinitz number m for which $\mathrm{char}\, K$ does not divide m. Assume that μ_m is contained in B. Note that this implies that $K(B)$ is normal over K.

In this section we will describe the Galois group $\mathrm{Gal}(K(B)/K)$.

Let w be the Steinitz number for which $\mu_w = \mu_m \cap K^*$. In the case where m is finite, this means that w is the number of m-th roots of unity in K. Define B_w as $B \cap K^{*1/w}$. This makes $K(B_w)$ over K a Kummer extension.

Additionally, assume that there is a Steinitz number t such that $\mu_m \subset \mu_t \subset B$ and μ_t satisfies the condition $K(\mu_t B_w) \cap B = \mu_t B_w$.

In the Kummer case, if $\mu_m \subset K^*$, taking $\mu_t = \mu_m$ is sufficient: $K(\mu_m B_w) \cap B = K(B_w) \cap B = B_w = \mu_m B_w$. In corollary 4.7 below we will prove that if $\mu_{mw} \subset B$, taking $\mu_t = \mu_{mw}$ also satisfies this condition.

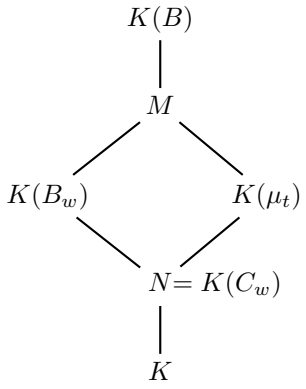
Since B contains μ_t, we can split up our extension into a cyclotomic part $K \subset K(\mu_t)$ and $K(\mu_t) \subset K(B)$. There is a natural injection $\mathrm{Gal}(K(\mu_t)/K) \to \mathrm{Aut}_{\mu_w}(\mu_t)$. We call the image of this map H. So, $H \cong \mathrm{Gal}(K(\mu_t)/K)$.

If we restrict the image of $\mathrm{Gal}(K(B)/K)$ in $\mathrm{Aut}_{K^*}(B)$ to $\mathrm{Aut}_{\mu_w}(\mu_t)$, it is clearly contained in H. Therefore, the image of $\mathrm{Gal}(K(B)/K)$ is contained in

$$\mathrm{Aut}_{K^*,\,H}(B) := \{\sigma \in \mathrm{Aut}_{K^*}(B) : \sigma \text{ restricted to } \mu_t \text{ belongs to } H\}.$$

Let M be the compositum of $K(B_w)$ and $K(\mu_t)$ and N the intersection. Write $C_w := B_w \cap K(\mu_t)^*$. It is clear that $K(C_w) \subset N = K(B_w) \cap K(\mu_t)$. The opposite inclusion is derived from Kummer theory as follows. We know from theorem 4.4 that $K(B_w) \cap K(\mu_t)$ is obtained by adjoining a subgroup C of B_w to K. Additionally, $C \subset K(\mu_t)^*$ because $K(C) \subset K(\mu_t)$. Therefore, $C \subset C_w$ and $N \subset K(C_w)$. So, N is equal to $K(C_w)$.

The various fields we are considering are shown in the following diagram.



We can describe $\mathrm{Gal}(K(B_w)/K)$ and $\mathrm{Gal}(N/K)$ in terms of automorphism groups of abelian groups with Kummer theory: theorem 4.4 states that the natural restriction maps $\mathrm{Gal}(K(B_w)/K) \xrightarrow{\sim} \mathrm{Aut}_{K^*}(B_w)$ and $\mathrm{Gal}(N/K) \xrightarrow{\sim} \mathrm{Aut}_{K^*}(C_w)$ are isomorphisms.

We have homomorphisms $\psi_1 : H \cong \mathrm{Gal}(K(\mu_t)/K) \to \mathrm{Gal}(N/K) \cong \mathrm{Aut}_{K^*}(C_w)$ and $\psi_2 : \mathrm{Aut}_{K^*}(B_w) \to \mathrm{Aut}_{K^*}(C_w)$. By definition of $\mathrm{Aut}_{K^*,H}(B)$, we also have a homomorphism from $\mathrm{Aut}_{K^*,H}(B)$ to H. Combined with the natural restriction from $\mathrm{Aut}_{K^*,H}(B)$ to $\mathrm{Aut}_{K^*}(B_w)$, this gives two maps from $\mathrm{Aut}_{K^*,H}(B)$ to $\mathrm{Aut}_{K^*}(C_w)$:

$$\begin{aligned} \varphi_1 : &\quad \mathrm{Aut}_{K^*,H}(B) \longrightarrow H \xrightarrow{\psi_1} \mathrm{Aut}_{K^*}(C_w) \\ \varphi_2 : &\quad \mathrm{Aut}_{K^*,H}(B) \longrightarrow \mathrm{Aut}_{K^*}(B_w) \xrightarrow{\psi_2} \mathrm{Aut}_{K^*}(C_w). \end{aligned}$$

These two maps allow us to describe $\mathrm{Gal}(K(B)/K)$.

Theorem 4.5. *The natural homomorphism* $\mathrm{Gal}(K(B)/K) \longrightarrow \mathrm{Aut}_{K^*,H}(B)$ *gives an isomorphism of* $\mathrm{Gal}(K(B)/K)$ *with the subgroup* Γ *of* $\mathrm{Aut}_{K^*,H}(B)$ *consisting of the elements that have the same image under the two maps* φ_1 *and* φ_2 *defined above.*

Proof. Let Γ' be the fibered product $H \times_{\mathrm{Aut}_{K^*}(C_w)} \mathrm{Aut}_{K^*}(B_w)$. From theorem 1.5 we know that the natural map from Γ' to $\mathrm{Gal}(M/K)$ is an isomorphism. Because of the universal property of the fibered product, the homomorphisms

φ_1 and φ_2 from $\mathrm{Aut}_{K^*,\,H}(B)$ restricted to Γ to $\mathrm{Aut}_{K^*}(C_w)$ both factor through Γ' with the same map $\pi : \Gamma \to \Gamma'$.

Galois theory gives us the following short exact sequence:

$$0 \longrightarrow \mathrm{Gal}(K(B)/M) \xrightarrow{f} \mathrm{Gal}(K(B)/K) \xrightarrow{g} \mathrm{Gal}(M/K) \longrightarrow 0.$$

We will use this sequence to describe $\mathrm{Gal}(K(B)/K)$.

The image of the map $\mathrm{Gal}(K(B)/K) \to \mathrm{Aut}_{K^*,\,H}(B)$ is contained in Γ, because if we restrict an automorphism in $\mathrm{Aut}_{K^*,\,H}(B)$ to $H \cong \mathrm{Gal}(K(\mu_t)/K)$ and to $\mathrm{Aut}_{K^*}(B_w) \cong \mathrm{Gal}(K(B_w)/K)$, then they are the same when further restricted to $\mathrm{Aut}_{K^*}(C_w) \cong \mathrm{Gal}(N/K)$. This gives us an induced map $h : \mathrm{Gal}(K(B)/K) \to \Gamma$.

Since applying π after h is the same as first applying g and then applying the isomorphism from $\mathrm{Gal}(M/K)$ to Γ', the following diagram is commutative.

$$\begin{array}{ccccc} \mathrm{Gal}(K(B)/K) & \xrightarrow{g} & \mathrm{Gal}(M/K) & \longrightarrow & 0 \\ \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle \wr} & & \\ \Gamma & \xrightarrow{\pi} & \Gamma' & & \end{array}$$

Since g and the isomorphism are both surjective, π has to be surjective. The kernel of π consists of exactly those elements of Γ that are the identity when mapped to H and when mapped to $\mathrm{Aut}_{K^*}(B_w)$. So, $\ker \pi = \mathrm{Aut}_{\mu_t B_w}(B)$.

We also have a restriction map $\mathrm{Gal}(K(B)/M) \to \mathrm{Aut}_{\mu_t B_w}(B)$, which makes the following square commutative:

$$\begin{array}{ccccc} 0 & \longrightarrow & \mathrm{Gal}(K(B)/M) & \xrightarrow{g} & \mathrm{Gal}(K(B)/K) \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathrm{Aut}_{\mu_t B_w}(B) & \longrightarrow & \Gamma. \end{array}$$

Since $K(B)/M$ is a Kummer extension, we know from theorem 4.4 that the restriction $\mathrm{Gal}(K(B)/M) \to \mathrm{Aut}_{M^* \cap B}(B)$ is an isomorphism. This automorphism group is equal to $\mathrm{Aut}_{\mu_t B_w}(B)$ by our assumption on t, which makes the restriction map mentioned above an isomorphism.

Summarizing, we have the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Gal}(K(B)/M) & \xrightarrow{f} & \mathrm{Gal}(K(B)/K) & \xrightarrow{g} & \mathrm{Gal}(M/K) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \wr} & & \downarrow{\scriptstyle h} & & \downarrow{\scriptstyle \wr} & & \\ 0 & \longrightarrow & \mathrm{Aut}_{\mu_t B_w}(B) & \xrightarrow{\iota} & \Gamma & \xrightarrow{\pi} & \Gamma' & \longrightarrow & 0. \end{array}$$

Let σ be an element of the kernel of h. Then $\pi h(\sigma) = 1$, and therefore $g(\sigma) = 1$. Because of the exactness of the top row, this means that $\sigma \in \mathrm{Gal}(K(B)/M)$.

So, $\iota(\sigma) = h(\sigma) = 1$. Because ι is an injection, we find that $\sigma = 1$, and h is injective.

To show that h is surjective, let τ be any element of Γ. Since g is a surjection, there is an element $\tilde{\tau} \in \mathrm{Gal}(K(B)/B)$ such that $g(\tilde{\tau}) = \pi(\tau)$. Therefore, τ and $h(\tilde{\tau})$ have the same image under π, so $h(\tilde{\tau})^{-1}\tau \in \mathrm{Aut}_{\mu_t B_w}(B)$. This means that $\tau \in h(\tilde{\tau})\mathrm{Aut}_{\mu_t B_w}(B) = h(\tilde{\tau}\mathrm{Aut}_{\mu_t B_w}(B)) \subset \mathrm{im}\, h$.

So, h is an isomorphism. This proves the theorem, up to the existence of μ_t if $\mu_{mw} \subset B$, which we prove below. □

Theorem 4.6. *(Schinzel) Let K be a field and n a positive integer not divisible by* $\mathrm{char}\, K$*. Let w be the number of n-th roots of unity in K. Then, the splitting field of $X^n - a$ over K is abelian over K if and only if there is an element $b \in K$ with $a^w = b^n$.*

Proof. See [3]. □

Corollary 4.7. *If $\mu_{mw} \subset B$, then $K(\mu_{mw}B_w) \cap B = \mu_{mw}B_w$.*

Proof. The inclusion $K(\mu_{mw}B_w) \cap B \supset \mu_{mw}B_w$ is clear, since $\mu_{mw} \subset B$ and $B_w \subset B$, so we only need to prove $K(\mu_{mw}B_w) \cap B \subset \mu_{mw}B_w$.

Let x be an element of $K(\mu_{mw}B_w) \cap B$. Because $x \in B$, there is an $n \geq 0$, $n \mid m$ and an element $a \in K$ such that $x^n = a$.

$K(\mu_{mw}B_w)$ contains μ_n, so the splitting field of $X^n - a$ over K is contained in $K(\mu_{mw}B_w)$, which is abelian over K. This means that we can apply theorem 4.6. Let v be the number of nth roots of unity in K. Then there is an element $b \in K$ such that $a^v = b^n$.

We have $x^n = a$, so $x^{nv} = a^v = b^n$. Therefore, there is an $\varepsilon \in \mu_n$ such that $x^v = b\varepsilon$. Because B contains μ_{mw} and $nv \mid mw$, there is a $\xi \in \mu_{nv}$ such that $(x\xi)^v = b \in K$. This means that $x\xi \in K^{*1/w}$. We know that $\xi \in \mu_{nv}$ and $x \in B$, so $x\xi \in B_w$ and $x \in \mu_{mw}B_w$. □

Example 4.8 Taking $\mu_t = \mu_m$ as in the Kummer case does not always work.

Let $K = \mathbb{Q}(\sqrt{2})$ and $B = \langle K^*, \zeta_8 \rangle$. Then, $m = 4$, $w = 2$ and $B_w = \langle K^*, i \rangle$. Take $\mu_t = \mu_m = \langle i \rangle$. Then, $K(\mu_t B_w) = K(i)$. Note that $\mu_8 \subset K(i)$, since $\mu_8 = \langle (1+i)/\sqrt{2} \rangle$. Therefore, $\mu_8 \subset K(\mu_t B_w) \cap B$, while $\zeta_8 \not\subset \mu_t B_w$.

We will now apply theorem 4.5 to some examples.

Example 4.9 Consider the Galois extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{-9})$. We take $K = \mathbb{Q}$, $B = \langle \mathbb{Q}^*, \sqrt[4]{-9} \rangle$. We find that $m = 4$, $w = 2$ and we set $t = 4$. This results in $B_w = \langle \mathbb{Q}^*, \sqrt{-9} \rangle = \langle \mathbb{Q}^*, i \rangle$ and $C_w = B_w$. Note that μ_t indeed satisfies the

required condition, since indeed $\mathbb{Q}(\mu_4 B_w) \cap B = \mu_4 B_w$. In the next example we will handle a case where taking $m = t$ does not work.

The automorphism group $\mathrm{Aut}_{K^*}(B)$ consists of the automorphisms mapping $\sqrt[4]{-9}$ to $\sqrt[4]{-9}$, $i\sqrt[4]{-9}$, $-\sqrt[4]{-9}$ and $-i\sqrt[4]{-9}$. Note that this group is isomorphic to the V_4 because all automorphisms have order 2. Because the restriction map $\mathrm{Gal}(\mathbb{Q}(i)/Q) \to \mathrm{Aut}_{\langle -1\rangle}(\langle i\rangle)$ is a surjection, we find that $\mathrm{Aut}_{K^*,H}(B) = \mathrm{Aut}_{K^*}(B)$.

Since $K(\mu_t) = K(B_w) = K(C_w)$, the two maps φ_1 and φ_2 are equal on all of $\mathrm{Aut}_{K^*,H}(B)$, so theorem 4.5 states that $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{-9})/\mathbb{Q}) \cong V_4$.

Example 4.10 Now consider the Galois extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{-4})$. We take $K = \mathbb{Q}$, $B = \langle \mathbb{Q}^*, \sqrt[4]{-4}\rangle$. As in the previous example, we find that $m = 4$, $w = 2$. However, no value of t satisfies the condition on μ_t.

We therefore add ζ_8 to B, so that $B = \langle \mathbb{Q}^*, \zeta_8, \sqrt[4]{-4}\rangle$ and we set $t = 8$. Now that we have added ζ_8, we see that we can also write B as $\langle \mathbb{Q}^*, \zeta_8, \sqrt{2}\rangle$. Therefore, $\mathrm{Aut}_{K^*}(B) \cong V_4 \oplus \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/2\mathbb{Z})^3$. Since the restriction $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \to \mathrm{Aut}_{\langle -1\rangle}(\langle \zeta_8\rangle)$ is a surjection, $\mathrm{Aut}_{K^*,H}(B) = \mathrm{Aut}_{K^*}(B)$.

The group B_w is equal to $\langle \mathbb{Q}^*, i, \sqrt{2}\rangle$ and $C_w = B_w$, since $\sqrt{2} \in \mathbb{Q}(\zeta_8)$.

The map φ_1 maps an automorphism of B to one of C_w through the Galois group of $\mathbb{Q}(\zeta_8)/\mathbb{Q}$. The map φ_2 maps an automorphism of B to one of C_w by restricting it to C_w. Thus, we see that the image $\mathrm{Gal}(\zeta_8, \sqrt[4]{-4})$ in $\mathrm{Aut}_{K^*,H}(B)$ consists of exactly those automorphisms σ for which $\sigma(\zeta_8) + \sigma(\zeta_8^{-1}) = \sigma(\sqrt{2})$ (where we choose ζ_8 such that $\zeta_8 + \zeta_8^{-1} = \sqrt{2}$ in $\mathbb{Q}(\zeta_8)$).

We find that $\mathrm{Gal}(\mathbb{Q}(\zeta_8, \sqrt[4]{-4})/\mathbb{Q}) \cong V_4$ as expected, since $\mathbb{Q}(\zeta_8, \sqrt[4]{-4}) = \mathbb{Q}(\zeta_8)$. The Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt[4]{-4})/\mathbb{Q})$ is a quotient of order 2 of $\mathrm{Gal}(\mathbb{Q}(\zeta_8, \sqrt[4]{-4})/\mathbb{Q})$ and is therefore isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Example 4.11 Consider the Galois extension $\mathbb{Q} \subset \mathbb{Q}(\zeta_3, \sqrt[3]{2})$. We take $K = \mathbb{Q}$ and $B = \langle \mathbb{Q}^*, \zeta_3, \sqrt[3]{2}\rangle$. We find that $m = 3$, $w = 1$ and $t = 3$. Because of this, $B_w = C_w = \mathbb{Q}^*$. It is easy to see from corollary 3.12 and corollary 3.17 that $\mathrm{Aut}_{K^*}(B) = \mathbb{Z}/3\mathbb{Z} \rtimes (\mathbb{Z}/3\mathbb{Z})^* = S_3$. All 6 of these automorphisms induce an automorphism on $\langle \mathbb{Q}^*, \zeta_3\rangle$ that comes from an automorphism of $\mathbb{Q}(\zeta_3)$, so $\mathrm{Aut}_{K^*,H}(B) = \mathrm{Aut}_{K^*}(B)$. Since $K(C_w) = \mathbb{Q}$, the image of both φ_1 and φ_2 is trivial, so $\mathrm{Gal}(K(B)/K) \cong \mathrm{Aut}_{K^*,H}(B) \cong S_3$.

Example 4.12 Let $K = \mathbb{Q}$, $m = \prod_p p^\infty$ and $B = \mathbb{Q}^{*1/m}$, i.e., B consists of all radicals. It follows that $w = 2$ and $t = m$. So, B_w consists of all square roots in B. If we define $p^* = \pm p$ such that $p^* \equiv 1 \bmod 4$, then $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$ (see Lang's Algebra [2], VI, theorem §3.3). Also, $i = \sqrt{-1}$ is itself cyclotomic, so we can conclude that every square root is contained in a cyclotomic extension. It follows that $C_w = B_w$.

We have the following diagram:

$$\begin{array}{ccccc} \mathrm{Aut}_{K^*}(B) & \longrightarrow & \hat{\mathbb{Z}}^* = \mathrm{Gal}(\mathbb{Q}(\mu)/\mathbb{Q}) \\ \downarrow & & \downarrow \\ \mathrm{Aut}_{K^*}(B_w) & = & \mathrm{Aut}_{K^*}(B_w). \end{array}$$

The map on the right maps an element $a \in \hat{\mathbb{Z}}^*$ to the automorphism of B_w given by $i \mapsto i^{a \bmod 4}$ and $\sqrt{p^*} \mapsto (\frac{a}{p})\sqrt{p^*}$.

The image of the Galois group $\mathrm{Gal}(\mathbb{Q}(B)/\mathbb{Q})$ in $\mathrm{Aut}_{K^*}(B)$ now consists of those automorphisms that have the same image under both maps to $\mathrm{Aut}_{K^*}(B_w)$ in this diagram.

Bibliography

[1] D. Eisenbud. *Commutative Algebra with a view toward algebraic geometry.* Springer-Verlay, 1995.

[2] S. Lang. *Algebra.* Addison Wesley, 1993.

[3] A. Schinzel. Abelian binomials, power residues and exponential congruences. *Acta Arithmetica*, 8:245–274, 1977.

[4] J.-P. Serre. *Abelian l-Adic Representations and Elliptic Curves.* Addison Wesley, 1989.

[5] J.H. Silverman. *The Arithmetic of Elliptic Curves.* Springer-Verlag, 1986.

[6] L.C. Washington. *Introduction to Cyclotomic Fields.* Springer-Verlag, 1982.