Radicals in arithmetic

Palenstijn, W.J.

Chapter 2

Radical extensions of abelian groups

2.1 Introduction

In the previous chapter, we used radical extensions of abelian groups to gain insight into Galois groups. In this chapter we will build on this idea to set up a theory for automorphisms of such radical group extensions, free from the context of fields. We will derive analogues of a number of results familiar from Galois theory, including basic properties of restrictions and extensions of automorphisms, and also a translation of Kummer theory and Schinzel's theorem for the classification of abelian radical extensions.

As we hinted at in the preface, a key property that we require of our groups of radicals is that all finite subgroups are cyclic. This means that for any prime p, there are no two linearly independent p-torsion elements, and it implies that the automorphism group of the torsion subgroup is abelian.

Specifically, let B be an abelian group of which every finite subgroup is cyclic. We say that an abelian group $C \supset B$ is a *radical extension* of B if the quotient C/B is torsion and all finite subgroups of C are again cyclic. The cardinality of C/B is the *degree* of the extension, and if the degree of the extension is finite, we say that the extension itself is finite.

In Section 2.2 we will define the concept of a maximal radical extension of B, and give its universal properties.

In Chapter 1, we studied the action of the absolute Galois group of a field on a group of radicals. Taking the role of that Galois group in this chapter is an arbitrary profinite group with a continuous action on B, where we give B the discrete topology. Write B^G for the invariants of B under the action of G. In Section 2.3 we will look at extensions of the form $B^G \subset B$ where B/B^G is torsion, which we will call Galois radical extensions of abelian groups.

In Section 2.4 we will then give an analogue of Kummer extensions of fields,

and in Section 2.5 we will show that a Galois radical extension $B^G \subset B$ has a maximal abelian sub-extension B_{ab}. This group B_{ab} has the defining properties that $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ is abelian and that for every sub-extension C with $\mathrm{Aut}_{B^G}(C)$ abelian, we have that B_{ab} contains C. The main ingredient in the definition and construction of B_{ab} will be a generalization of Schinzel's Theorem 1.7.

The main theorem of this chapter is Theorem 2.25 in section 2.6, which is a generalization of Theorem 1.6 to the setting of this chapter. It states that if G is a subgroup of $\mathrm{Aut}(B)$ such that $B^G \subset B$ is a radical extension, then G is a normal subgroup of $\mathrm{Aut}_{B^G}(B)$, and $\mathrm{Aut}_{B^G}(B)/G$ is abelian. We call this quotient $\mathrm{Aut}_{B^G}(B)$ the *entanglement group* of B with the action of G.

We conclude the chapter with a number of results giving more explicit expressions for the entanglement group. These will form the basis for the results of Chapters 3 to 6.

2.2 Maximal radical extensions

In this section we will define the maximal radical extension of an abelian group B of which all finite subgroups are cyclic, and prove its universal property.

We start with a definition. If $B \subset C$ and $B \subset D$ are two radical extensions of B, then a homomorphism from C to D is a *B-homomorphism* if it is the identity on B. A B-homomorphism that is a bijection is a *B-isomorphism*.

Theorem 2.1. *Let B be an abelian group of which every finite subgroup is cyclic. Then there is a group $\bar{B}$ that has the following properties.*

1. *The group $\bar{B}$ is a radical extension of B.*
2. *For every radical extension C of B, there is an injective B-homomorphism $C \to \bar{B}$.*

Up to a not necessarily unique B-isomorphism, there is exactly one group $\bar{B}$ with these two properties. Furthermore, given this group $\bar{B}$, if $\bar{B} \subset F$ is a radical extension, then F equals $\bar{B}$.

Definition 2.2. Let B be an abelian group of which every finite subgroup is cyclic. We call the group $\bar{B}$ given by Theorem 2.1 the *maximal radical extension* of B.

Before proving this theorem by constructing $\bar{B}$, we first recall the concept of an *essential extension* (see e.g., [13], definition A3.10): an abelian group C is an essential extension of a group $B \subset C$ if every non-zero subgroup of C has a non-zero intersection with B.

Proposition 2.3. *Let B be an abelian group of which all finite subgroups are cyclic. If $B \subset C$ is an essential extension, it is a radical extension.*

Proof. Let $x \neq 0$ be an element of C. Then $\langle x \rangle$ has a non-trivial intersection with B, so a multiple of x is contained in B. Therefore, C/B is torsion. It remains to be

shown that all finite subgroups of C are cyclic, or equivalently, that for every prime p there is at most one subgroup $H \subset C$ of order p.

Suppose p is a prime and H_1 and H_2 are two subgroups of C of order p. Because $B \subset C$ is essential, $H_1 \cap B$ is non-trivial and therefore equal to H_1. The same holds for H_2, so $H_2 \cap B$ equals H_2. All finite subgroups of B are cyclic, so B has a unique subgroup of order p, equal to H_1 and H_2. □

Theorem 2.4. *Let B be an abelian group of which all finite subgroups are cyclic. Then there exists a divisible abelian group E that is an essential extension of B. This group E is unique up to a not necessarily unique B-isomorphism and it has two universal properties: for any essential extension C of B, there is an injective B-homomorphism from C into E, and for any divisible abelian group F containing B, there is an injective B-homomorphism from E into F.*

Proof. See [13], §A3.4, Corollary A3.9 and Proposition A3.10. □

Since a divisible abelian group is the same as an injective $\mathbf{Z}$-module, the group E given by this theorem is called the *injective hull* of B (following [13], section A3.4).

We will use the existence of maximal essential extensions to show the existence of a maximal radical extension $\bar{B}$ of an abelian group B of which all finite subgroups are cyclic. We start by considering torsion subgroups of prime order.

If for a prime q the subgroup $B[q]$ of q-torsion of B is trivial, the direct sum $B \oplus \mathbf{Z}/q\mathbf{Z}$ is a radical extension of B, but not an essential extension. We therefore first define

$$B' = B \oplus \bigoplus_{\substack{q \text{ prime} \\ B[q]=0}} \mathbf{Z}/q\mathbf{Z}.$$

Next, we define $\bar{B}$ to be the injective hull of B'. We can now prove that the group $\bar{B}$ thus constructed satisfies the properties of Theorem 2.1.

Proof of Theorem 2.1. (1). The extension $B \subset B'$ is a radical extension by construction, and $B' \subset \bar{B}$ is an essential extension by definition and therefore also radical by Proposition 2.3. A radical extension of a radical extension of B is again radical over B, so $\bar{B}$ is a radical extension of B.

(2). Define the group $C' \supset C$ as follows:

$$C' = C \oplus \bigoplus_{\substack{q \text{ prime} \\ C[q]=0}} \mathbf{Z}/q\mathbf{Z}.$$

We will construct an injective B-homomorphism $C' \to \bar{B}$, which implies the existence of an injective B-homomorphism $C \to \bar{B}$.

The group C' contains B', and we claim $B' \subset C'$ is an essential extension. Let x be any element of C' C, and pick $n \in \mathbf{Z}_{>0}$ minimal such that nx is in B. We have $x \notin B$, so $n > 1$. If nx is 0, take any prime $p \mid n$, and we then have $\frac{n}{p}x \in C'[p] \setminus \{0\} = B'[p] \setminus \{0\}$. Otherwise, if nx is not 0, then $nx \in B \setminus \{0\} \subset B' \setminus \{0\}$.

We conclude that $B' \subset C'$ is an essential extension, so by Theorem 2.4 there is an injective D-homomorphism $C' \to \bar{B}$.

Next, we show that every group X that has properties 1 and 2 has no non-trivial radical extensions. Let X be such a group, and suppose $X \subset F$ is a radical extension. Let f be any element of F, and $n \in \mathbf{Z}_{>0}$ such that $nf \in B$. By property 2, there is a B-injection $\varphi : F \to X$. We have $n\varphi(f) = \varphi(nf) = nf$, so $n(\varphi(f) - f)$ equals 0, and $\varphi(f) - f$ is an n-torsion element of F. Because F and X both have the property that their finite subgroups are cyclic, they share a unique subgroup of order n, so we see $\varphi(f) - f \in F[n] = X[n] \subset X$. We conclude that f is an element of X, so F equals X.

We conclude the proof of Theorem 2.1 by showing unicity. If there are two extensions $B \subset X$ and $B \subset Y$ both satisfying the properties from the theorem, then there is a B-injection $\varphi : X \to Y$ (by property 1 of X and 2 of Y). The image $\varphi(X)$ clearly also satisfies these properties, and $\varphi(X) \subset Y$ is a radical extension, so $\varphi(X)$ equals Y (since $\varphi(X)$ has no non-trivial radical extensions) and φ is a B-isomorphism. □

2.3 Galois radical extensions

Since we aim to study Galois groups of fields using similar structures for radical group extensions, in this section we will explore analogous concepts. We will look at some of the different properties characterizing Galois field extensions and what these lead to in our current setting, such as the ground field being the invariant subfield of some automorphism group, or all embeddings into a fixed algebraic closure having the same image.

Lemma 2.5. *Let C be an abelian group with all finite subgroups of C cyclic. Let $G \subset \mathrm{Aut}(C)$ be a subgroup, and write C^G for the G-invariants of C. Then the following three properties are equivalent.*

1. *$C^G \subset C$ is a radical extension, i.e., C/C^G is torsion;*
2. *$I_G \cdot C$ is torsion, where I_G is the augmentation ideal $\langle 1 - \sigma : \sigma \in G \rangle \subset \mathbf{Z}[G]$;*
3. *G acts trivially on C/C_{tors}.*

We start the proof of this lemma with a small proposition about the augmentation ideal.

Proposition 2.6. *Let C and G be as above, and let x be an element of C and $\bar{x}$ its image in C/C^G. If $I_G \cdot x$ or $\langle \bar{x} \rangle$ is finite, then $I_G \cdot x$ and $\bar{x}$ are cyclic of the same order.*

Proof. For any positive integer n we have $nI_G \cdot x = I_G \cdot nx$, so $nI_G \cdot x$ is 0 if and only if nx is invariant under G. The proposition immediately follows from this observation and the fact that all finite subgroups of C are cyclic. □

Proof of Lemma 2.5. (1) $\Leftrightarrow$ (2): This follows directly from the proposition.

(2) $\Leftrightarrow$ (3): Both statements are equivalent to G only shifting elements of C by torsion elements of C. □

These properties lead to the following definition.

Definition 2.7. A *Galois radical extension* is a radical extension $B \subset C$ such that there is a subgroup $G \subset \mathrm{Aut}(C)$ with $B = C^G$.

Note that despite the name we have given these Galois extensions, there is in general no one to one correspondence between subgroups of the radical group and subgroups of its automorphism group. Most extensions generated by elements of prime order do not have this property, for example: if we take $C = \mathbf{Z}/p\mathbf{Z}$ for a prime $p > 3$, and $G = \mathrm{Aut}(C) = (\mathbf{Z}/p\mathbf{Z})^*$, then C^G is $\{1\}$ and C/C^G is a Galois radical extension. It has no subextensions other than C and C^G, but G does have non-trivial subgroups.

This also implies that there are possibly multiple choices for the group G from the definition.

Galois radical extensions do share a number of properties with Galois field extensions, some of which are given by the following theorem. Other parallels are explored in the next two sections.

Theorem 2.8. *Let $B \subset C$ be a Galois radical extension, and choose a fixed maximal radical extension $\bar{B}$ of B. Then the following three statements hold.*

1. *For every $x \in C$ there is an integer $n > 0$ such that we have $nx \in B$ and C contains an element of order n;*
2. *All injective B-homomorphisms $C \to \bar{B}$ have the same image;*
3. *$B[2]$ equals $C[2]$.*

Proof. (1.) Let $B \subset C$ be a Galois radical extension, write $G = \mathrm{Aut}_B(C)$, and let x be any element of C. Let k be the order of $\bar{x} \in C/B$, which is well-defined because C/B is torsion. Consider the group $Z = I_G \cdot x \subset C$. Since C/B is torsion, Proposition 2.6 implies Z is finite. Because Z is finite, it is cyclic (by assumption on C). Let z be a generator of Z, and write n for the order of z and Z. Then, again by the proposition, nx is invariant under G and therefore an element of B. This means n satisfies the requirements of the statement.

(2.) We will proceed from statement 1. Suppose φ_1 and φ_2 are two injective B-homomorphisms from C to $\bar{B}$. Let $y = \varphi_1(x)$ be an element of the image of φ_1. It suffices to show y is in the image of φ_2.

Since $B \subset C$ satisfies statement 1, there is a positive integer n such that nx is in B and C contains an element z of order n. The image $\varphi_2(z)$ in $\bar{B}$ also has order n because φ_2 is an injection. Because φ_1 and φ_2 are the identity on B, we find $n\varphi_1(x) = n\varphi_2(x) \in B \subset \bar{B}$, which implies that $\varphi_1(x)$ equals $\varphi_2(x) + z'$ for some element z' of order dividing n. Using that all finite subgroups of $\bar{B}$ are cyclic, we conclude that z' is a multiple of $\varphi_2(z)$, so $y = \varphi_1(x)$ is in the image of φ_2.

(3.) If C contains an element of order 2, that element is unique and therefore invariant under all automorphisms of C and contained in C^G. □

Theorem 2.9. *If $B \subset C$ is a radical extension with $B[2]$ equal to $C[2]$ that satisfies statement 1 or statement 2 from Theorem 2.8, then it is a Galois radical extension.*

Proof. Since the proof of Theorem 2.8 shows that statement 1 implies statement 2, we only need to show the following statement:

If $B[2]$ equals $C[2]$ and all injective B-homomorphisms $C \to \bar{B}$ have the same image, then $B \subset C$ is a Galois radical extension.

To prove this, it suffices to show that $\mathrm{Aut}_B(C)$, the group of automorphisms of C that are the identity on B, does not have a set of invariants larger than B.

Suppose x is an element of $C \setminus B$ of order $p > 1$ in the quotient C/B. We will show there is an automorphism $\sigma \in \mathrm{Aut}_B(C)$ with $\sigma x \neq x$. Since every such x has a multiple of prime order, we can assume that p is prime without loss of generality.

We start by looking at the sub-extension $D = \langle B, x\rangle = B \oplus_{\langle px\rangle} \langle x\rangle$ and classifying the B-homomorphisms $D \to \bar{B}$.

Not all of these homomorphisms are necessarily injections. Suppose y is an element of the kernel of $\varphi \in \mathrm{Hom}_B(D, \bar{B})$. Then py is an element of B and also $\varphi(py) = p\varphi(y) = 0$. However, φ is a B-homomorphism, so φ restricted to B is injective. We see that py is 0 and y is p-torsion. We conclude that if there is no p-torsion in the kernel of φ, then φ is an injection.

If B contains an element of order p, there will clearly be no p-torsion in the kernel of any B-homomorphism (since the p-torsion is a cyclic group by assumption).

If B does not contain an element of order p, but D does, then B has index p in both $B + D[p]$ and in D, so $B + D[p]$ equals D. Then by the same reasoning as above, $\#\mathrm{Hom}_B(D, \bar{B}) = \#\mathrm{Hom}_B(B + D[p], \bar{B})$ equals p, and clearly exactly one of these homomorphisms is not an injection: the homomorphism sending all elements of order p to 0.

Note that for $p = 2$ we cannot be in the latter case, since we have assumed $B[2] = C[2] = D[2]$. This means that we have (at least) two different injections ψ_1 and ψ_2 of D to $\bar{B}$. These are uniquely defined by the image of x, so $\psi_1(x) \neq \psi_2(x)$.

Because $B \subset D$ is a radical extension, the maximal radical extension $\bar{B}$ of B is also a maximal radical extension of D. Its universal property implies ψ_1 and ψ_2 can be extended to injections $\tilde{\psi}_1$, $\tilde{\psi}_2$ from C to $\bar{B}$.

We have assumed that all such injections have the same image, so $\tilde{\psi}_2$ is invertible on the image of $\tilde{\psi}_1$, and $\sigma = \tilde{\psi}_2^{-1}\tilde{\psi}_1$ gives the desired automorphism of C with $\sigma(x) \neq x$. □

Example 2.10.

Statements 1 and 2 from Theorem 2.8 are equivalent if the extra condition $B[2] = C[2]$ (i.e., statement 3) is satisfied, as the above theorems and proofs show. The necessity of this condition $B[2] = C[2]$ is illustrated by the following example where B satisfies statement 2, but not statements 1 and 3 from Theorem 2.8.

Let X be the group $(\mathbf{Q}/\mathbf{Z}) \times \mathbf{Q}$, and define C to be the subgroup generated by $x = (\frac{1}{4}, \frac{1}{2})$ and $(0, 1)$. Let B be the (infinite cyclic) subgroup of C generated by $(0, 1)$. Then $\bar{B}$ equals X.

We have that C/B is cyclic of order 4, but C has no element of order 4. We will show that all injective B-homomorphisms $\varphi : C \to \bar{B}$ have the same image.

Let φ be any injective B-homomorphism $C \to \bar{B}$. Then $4\varphi(x)$ equals $(0, 2)$, so we find

$$\varphi(x) \in \left\{(\tfrac{1}{4}, \tfrac{1}{2}), (\tfrac{1}{2}, \tfrac{1}{2}), (\tfrac{3}{4}, \tfrac{1}{2}), (0, \tfrac{1}{2})\right\}.$$

If we have $\varphi(x) \in \{(\frac{1}{2}, \frac{1}{2}), (0, \frac{1}{2})\}$, then we obtain $\varphi(2x) = 2\varphi(x) = (0, 1) = \varphi((0, 1))$ which contradicts the fact that φ is an injection. We conclude $\varphi(x) \in \{(\frac{1}{4}, \frac{1}{2}), (\frac{3}{4}, \frac{1}{2})\}$.

Since we have $(\frac{1}{4}, \frac{1}{2}) = (0, 1) - (\frac{3}{4}, \frac{1}{2})$ with $(0, 1) \in B$, this implies that $\varphi(C)$ equals C, independent of the choice of φ.

In many cases in this thesis, the base group B is the unit group of a field K. If $K \subset L$ is a field extension and C is a subgroup of L^*, then $K^*[2] = C[2]$ holds, so one of the conditions of Theorem 2.9 is automatically satisfied.

If K has characteristic zero, then $\bar{K}^*$ is a divisible abelian group containing non-trivial p-torsion for every prime p. It follows from Theorem 2.1 that the maximal radical extension $\bar{B}$ of B can then be considered a subgroup of $\bar{K}^*$, with a natural action of the absolute Galois group $\mathrm{Gal}(\bar{K}/K)$. With this action, $K^* \subset \bar{B}$ is a Galois radical extension.

Also, if we start from a Galois field extension $K \subset L$, and take $C \subset L^*$ to be the elements of L^* of which a power is in K, then C is a Galois radical group extension of K^* since C is closed under the action of $\mathrm{Gal}(L/K)$ and $K^* \subset C$ is the subgroup of invariants of the action.

Remark 2.11. If K has positive characteristic p, it is no longer true that the maximal radical extension of K^* can be considered a subgroup of $\bar{K}^*$, because $\bar{K}^*$ does not contain non-trivial p-torsion. We can adjust the definition of radical extensions to require that all finite subgroups are cyclic of order coprime to p, and likewise exclude p-torsion and extensions of degree divisible by p from the maximal radical extension. While we will not go into details, the resulting maximal radical extension will then again have the required universal properties for this restricted class of extensions, and also a natural action from the absolute Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K)$ of K.

2.4 Kummer theory of radical extensions

If $B \subset C$ is a radical extension, an automorphism of C that is the identity on B is called a B-automorphism, and we denote the group of such automorphisms by $\mathrm{Aut}_B(C)$.

Suppose that $B \subset C \subset D$ is a tower of abelian groups such that C and D are both radical groups over B, and C is a Galois radical group over B. By Theorem 2.8,

for every x in C there is a positive integer n such that $y = nx$ is in B and C has an element of order n. Any $\sigma \in \mathrm{Aut}_B(D)$ leaves y invariant, so $\sigma(x) - x$ is an n-torsion element of B, and therefore in C. So, we see that every B-automorphism of D maps C into itself. Therefore there is a well-defined restriction map $\mathrm{Aut}_B(D) \to \mathrm{Aut}_B(C)$.

As we already saw in a special case in Lemma 1.8, if D is also Galois over B, this restriction map is a surjection. This is true in general.

Theorem 2.12. *If $B \subset C \subset D$ is a tower of abelian groups such that C and D are both Galois radical groups over B, there is a natural exact sequence of groups*

$$0 \to \mathrm{Aut}_C(D) \to \mathrm{Aut}_B(D) \xrightarrow{\text{res}} \mathrm{Aut}_B(C) \to 0.$$

Proof. Since the proof of Lemma 1.8 doesn't use the fact that the abelian groups in question are radical groups over (the unit group of) a field specifically, the proof of that lemma applies to the present theorem unchanged. □

If C is a Galois radical extension of B, then C is the injective limit (and union) of all finite Galois radical extensions $D \subset C$ over B. This makes $\mathrm{Aut}_B(C)$ a *profinite* group, and the exact sequence given in Theorem 2.12 is an exact sequence of profinite groups.

Theorem 2.13. *Let $B \subset F$ be a radical extension of abelian groups, and C and D two subgroups of F such that $B \subset C$ and $B \subset D$ are Galois radical extensions. Then $C \cap D$ and $C + D$ are also Galois radical extensions of B and there is a natural isomorphism of profinite groups*

$$\mathrm{Aut}_B(C + D) \xrightarrow{\sim} \mathrm{Aut}_B(C) \times_{\mathrm{Aut}_B(C \cap D)} \mathrm{Aut}_B(D).$$

Proof. Since C and D are both Galois, they satisfy statements 2 and 3 from Theorem 2.8. These two statements directly transfer to $C \cap D$ and $C + D$, so by Theorem 2.9, these two groups are also Galois over B. For the second part of the theorem, we use Theorem 2.12, which gives us two restriction maps from $\mathrm{Aut}_B(C + D)$ to $\mathrm{Aut}_B(C)$ resp. $\mathrm{Aut}_B(D)$ that combine into a natural homomorphism

$$\mathrm{Aut}_B(C + D) \xrightarrow{\sim} \mathrm{Aut}_B(C) \times_{\mathrm{Aut}_B(C \cap D)} \mathrm{Aut}_B(D).$$

It is an isomorphism since an explicit inverse exists:

$$(f, g) \mapsto (c + d \mapsto f(c) + g(d)),$$

This is a well-defined map because (f, g) is in the fibered product.

□

In the general setting of a radical extension $B \subset C$ we call an element $x \in C$ a *Kummer radical* if there is a positive integer w such that wx is in B and B contains an element of order w. Generalizing the concept as it was introduced in Chapter 1, we call a radical extension generated by Kummer radicals a *Kummer radical extension*.

Every element of a Kummer radical extension is a Kummer radical, so all subextensions of a Kummer radical extension are also Kummer radical extensions. Note that by Theorem 2.9 Kummer radical extensions are Galois radical extensions.

Theorem 2.14. *Let G be a profinite group and B be an (additively written) abelian group with the discrete topology and a continuous G-action given by $f : G \to \mathrm{Aut}(B)$. Assume that all finite subgroups of B are cyclic, and that B is a Kummer radical extension of B^G. Then the image of f is $\mathrm{Aut}_{B^G}(B)$ and $\mathrm{Aut}_{B^G}(B)$ is abelian.*

We begin the proof of this theorem with the familiar Kummer pairing, for which we largely follow Lang [17], §VI.8.

Lemma 2.15. *Let $C \subset D$ be a Kummer radical extension of finite degree. Then $\mathrm{Aut}_C(D)$ is an abelian group and there is a bilinear map*

$$\begin{array}{rcl} \mathrm{Aut}_C(D) \times D & \longrightarrow & C_{\mathrm{tors}} \\ (\sigma, x) & \longmapsto & \sigma(x) - x. \end{array}$$

The kernel on the left is 1 and the kernel on the right is C.

Proof. Let x be an element of D and w a corresponding positive integer with $wx \in C$ and $\#C[w] = w$. For any element $\sigma \in \mathrm{Aut}_C(D)$ we then find $\sigma(x) - x \in D[w] \subset C_{\mathrm{tors}}$, so the map given is well-defined.

Now fix an element $x \in D$ and let $\sigma, \tau \in \mathrm{Aut}_C(D)$ be two automorphisms. Note that because σ leaves the elements of C invariant, we have the identity

$$\sigma(\tau(x) - x) = \tau(x) - x.$$

This directly implies that $\sigma\tau(x)$ equals $\tau(x)+\sigma(x)-x$. From this we see $\sigma\tau(x)-x = (\tau(x) - x) + (\sigma(x) - x)$, so the map $\mathrm{Aut}_C(D) \to C_{\mathrm{tors}}$ we get from the pairing with a fixed x is a group homomorphism.

Now define $D' = \langle C, x \rangle$. This is also a Kummer extension of C, so by the same reasoning as above, the following map defines a group homomorphism.

$$\begin{array}{rcl} \mathrm{Aut}_C(C') & \longrightarrow & C_{\mathrm{tors}} \\ \sigma & \longmapsto & \sigma(x) - x. \end{array}$$

It is injective, since if an automorphism in $\mathrm{Aut}_C(C')$ leaves x invariant, it is the identity. We see that $\mathrm{Aut}_C(C')$ is abelian. If we combine this using Theorem 2.13 for a finite set of generators of D, we see that $\mathrm{Aut}_C(D)$ is abelian.

We continue by fixing $\sigma \in \mathrm{Aut}_C(D)$ and taking $x, y \in D$. Then we can derive $\sigma(x+y)-(x+y) = \sigma(x)+\sigma(y)-(x+y) = (\sigma(x)-x))+(\sigma(y)-y)$. This means that the map $D \to C_{\mathrm{tors}}$ from the pairing with a fixed σ is also a group homomorphism, and the map $\mathrm{Aut}_C(D) \times D \to C_{\mathrm{tors}}$ is indeed bilinear.

For the kernel on the left, let $\sigma \in \mathrm{Aut}_C(D)$ be such that for all $x \in D$ we have $\sigma(x) - x = 0$. Then clearly σ is the identity.

On the right, let x be an element of D. Then by definition x is in the kernel on the right if and only if for all $\sigma \in \mathrm{Aut}_C(D)$ we have $\sigma(x) - x = 0$. This is equivalent with x being invariant under $\mathrm{Aut}_C(D)$. Since $C \subset D$ is a Galois radical extension, the invariants of $\mathrm{Aut}_C(D)$ are exactly C. We conclude that the kernel on the right is C. □

Corollary 2.16. *Let $C \subset D$ be a Kummer radical extension of finite degree. Then the automorphism group $\mathrm{Aut}_C(D)$ is abelian of order $\#(D/C)$.*

Proof. We can invoke duality (specifically, Theorem 9.2 in Chapter 1 of [17]) to see that the following map induced by the pairing is a group isomorphism.

$$\begin{array}{rcl} \mathrm{Aut}_C(D) & \xrightarrow{\sim} & \mathrm{Hom}(D/C, C_{\mathrm{tors}}) \\ \sigma & \longmapsto & (x \mapsto \sigma(x) - x) \end{array}$$

This directly shows that $\mathrm{Aut}_C(D)$ is an abelian group of order $\#(D/C)$. □

Proof of Theorem 2.14. Abusing notation, we will write $\sigma(x)$ for $f(\sigma)(x)$, for $\sigma \in G$ and $x \in B$.

We start by proving the theorem in the case that G is finite. The lemma shows that $G/\ker f$ is abelian, and a similar construction to the one in the lemma gives a bilinear map of abelian groups

$$\begin{array}{rcl} (G/\ker f) \times B & \longrightarrow & B^G_{\mathrm{tors}} \\ (\sigma, x) & \longmapsto & \sigma(x) - x. \end{array}$$

The kernel on the left is 1 since we have already divided by $\ker f$. The kernel on the right is B^G by definition.

Since B^G_{tors} is finite and cyclic, by duality the following map is an isomorphism.

$$\begin{array}{rcl} G/\ker f & \longrightarrow & \mathrm{Hom}(B/B^G, B^G_{\mathrm{tors}}) \\ \sigma & \longmapsto & (x \mapsto \sigma(x) - x) \end{array}$$

Using duality as in the proof of Corollary 2.16 now proves the theorem in the finite case.

In the general profinite case, note that B is the union of all C with $B^G \subset C \subset B$ and $B^G \subset C$ a finite Galois radical extension. This implies that $\mathrm{Aut}_{B^G}(B)$ is the projective limit of $\mathrm{Aut}_{B^G}(C)$, and in particular we give it the corresponding profinite topology.

For every C with $B^G \subset C \subset B$, the induced map $\varphi_C : G \to \mathrm{Aut}_{B^G}(C)$ is surjective and it factors via $G/\ker(\varphi_C)$, which is finite since $\mathrm{Aut}_{B^G}(C)$ is finite. That means the finite case of the present theorem applies to the action $G/\ker(\varphi_C) \to \mathrm{Aut}_{B^G}(C)$.

As G maps surjectively to each $\mathrm{Aut}_{B^G}(C)$, the image of G is dense in $\mathrm{Aut}_{B^G}(B)$.

The group G is profinite and therefore compact, and its image under the continuous map to $\mathrm{Aut}_{B^G}(B)$ is therefore also compact. Since $\mathrm{Aut}_{B^G}(B)$ is Hausdorff because it is also profinite, this compact image is closed. We have already shown it is dense, so it is equal to the full group, proving that $f : G \to \mathrm{Aut}_{B^G}(B)$ is surjective. Since additionally $\mathrm{Aut}_{B^G}(B)$ is the projective limit of the abelian groups $\mathrm{Aut}_{B^G}(C)$, it is itself abelian.

This concludes the proof of Theorem 2.14.

□

To compute an automorphism group of a Galois radical extension of abelian groups $B \subset C$, it is often useful to consider the tower $B \subset B + C_{\text{tors}} \subset C$. By Theorem 2.12 there is an exact sequence

$$0 \to \text{Aut}_{(B+C_{\text{tors}})}(C) \to \text{Aut}_B(C) \xrightarrow{\text{res}} \text{Aut}_B(B + C_{\text{tors}}) \to 0.$$

Since the restriction map $\text{Aut}_B(B + C_{\text{tors}}) \to \text{Aut}_{B_{\text{tors}}}(C_{\text{tors}})$ is an isomorphism, we in fact have an exact sequence

$$0 \to \text{Aut}_{(B+C_{\text{tors}})}(C) \to \text{Aut}_B(C) \xrightarrow{\text{res}} \text{Aut}_{B_{\text{tors}}}(C_{\text{tors}}) \to 0. \tag{2.17}$$

This sequence does not necessarily split, as illustrated by the following example.

Example 2.18.

Let C be the abelian group $\mathbf{Z}/8\mathbf{Z} \times \mathbf{Z}$ and B the subgroup generated by $(4, 0)$ and $(1, 2)$. Note that this is a radical extension since $8C$ is a subgroup of B. The torsion of C is of order 8, so $\text{Aut}(C_{\text{tors}})$ is isomorphic to V_4. Since B_{tors} is of order 2 and C has only one element of order 2 (as required), every automorphism of C_{tors} automatically leaves the elements of B_{tors} invariant. We find that $\text{Aut}_{B_{\text{tors}}}(C_{\text{tors}}) \cong V_4$.

For the step from $B + C_{\text{tors}}$ to C, we see that C is generated by $(0, 1)$ as an extension of $B + C_{\text{tors}}$, and that $2 \cdot (0, 1)$ is in $B + C_{\text{tors}}$. We conclude that $\text{Aut}_{B+C_{\text{tors}}}(C)$ is of order 2.

Finally, consider the isomorphism σ of C sending $(1, 0)$ to $(3, 0)$ and $(0, 1)$ to $(3, 1)$. This leaves the elements of B invariant since it satisfies $\sigma(4, 0) = (4, 0)$ and $\sigma(1, 2) = (1, 2)$. Its order is 4 because $\sigma(0, 1) = (3, 1)$, and $\sigma^2(0, 1) = (4, 1)$. This means the exact sequence does not split.

Using the exact sequence 2.17, we can count the number of automorphisms of a Galois radical extension of finite degree.

Theorem 2.19. *If $B \subset C$ is a Galois radical extension of finite degree, then the order of the automorphism group $\text{Aut}_B(C)$ equals*

$$\#(C/B) \prod_{\substack{p \text{ prime} \\ C[p] \neq B[p]}} \frac{p-1}{p}.$$

Proof. The automorphism group $\text{Aut}_{(B+C_{\text{tors}})}(C)$ on the left side of (2.17) corresponds to a Kummer extension, so the cardinality of the automorphism group is equal to $\#C/(B + C_{\text{tors}})$.

On the right side of (2.17), the automorphism group $\text{Aut}_{B_{\text{tors}}}(C_{\text{tors}})$ is a subgroup of $\text{Aut}(C_{\text{tors}})$. If we write $n = \#C_{\text{tors}}$ and $w = \#B_{\text{tors}}$, we see that $\text{Aut}(C_{\text{tors}})$ is canonically isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$. Under that isomorphism, $\text{Aut}_{B_{\text{tors}}}(C_{\text{tors}})$ corresponds to the subgroup of elements that are 1 modulo w, of which there are

exactly $\varphi(n)/\varphi(w)$. So, the order of $\mathrm{Aut}_{B_{\mathrm{tors}}}(C_{\mathrm{tors}})$ is equal to

$$\frac{n}{w}\prod_{\substack{p \text{ prime}\\ p|n}}\frac{p-1}{p}\prod_{\substack{p \text{ prime}\\ p|w}}\frac{p}{p-1}=\#(C_{\mathrm{tors}}/B_{\mathrm{tors}})\prod_{\substack{p \text{ prime}\\ C[p]\neq B[p]}}\frac{p-1}{p}.$$

Multiplying the orders on the left and right sides of the exact sequence 2.17 concludes the proof of the theorem. □

2.5 Abelian radical extensions and Schinzel's theorem

Let G be a profinite group and B be an abelian group with the discrete topology and a continuous G-action. In this section we will give an explicit criterion for when the image of G in $\mathrm{Aut}(B)$ is abelian, as a generalization of Schinzel's Theorem 1.7. We will then use it to identify the maximal abelian sub-extension of a Galois radical extension.

Theorem 2.20. *Let G be a profinite group and B be an (additively written) discrete abelian group with a continuous G-action given by $f : G \to \mathrm{Aut}(B)$. Assume B/B^G is a Galois radical extension.*

Then, the image of f is abelian if and only if the following holds:

$$\forall x \in B : \exists w \in \mathbf{Z}_{>0} : wx \in B_{\mathrm{tors}} + B^G \text{ and } B^G \text{ has an element of order } w.$$

Proof. First assume that the image of f is abelian. Let x be an element of B. We will explicitly give an integer w that satisfies the condition from the theorem.

Let $I \subset \mathbf{Z}[G]$ again be the augmentation ideal, and denote Ix by T. The group T is finite and cyclic by Proposition 2.6. Let τ be a generator and n its order.

The $\mathbf{Z}[G]$-module T has an annihilator $J \subset \mathbf{Z}[G]$, which is a two-sided ideal. As J is also the annihilator of τ, this gives an isomorphism of $\mathbf{Z}[G]$-modules

$$\mathbf{Z}[G]/J \cong_{\mathbf{Z}[G]} T = \langle\tau\rangle,$$

and since T is cyclic of order n, a unique isomorphism of rings

$$\mathbf{Z}[G]/J \cong \mathbf{Z}/n\mathbf{Z}.$$

Under this isomorphism, the ideal $(I+J)/J$ corresponds to an ideal $\bar{I}$ in $\mathbf{Z}/n\mathbf{Z}$. Now define $w \mid n$ by $\bar{I} = w\mathbf{Z}/n\mathbf{Z}$.

Then the w-torsion of the $\mathbf{Z}/n\mathbf{Z}$-module T is cyclic of order w and equal to the $(I+J)/J$-torsion of T as a $\mathbf{Z}[G]/J$-module. This is in turn equal to the I-torsion of T as a $\mathbf{Z}[G]$-module, which is T^G. So $T^G \subset B^G$ contains an element of order w, and the condition that B^G contains an element of order w is satisfied.

We have defined w to be in $I+J$, so $wx \in Ix + Jx$. Since the image of G in $\mathrm{Aut}(B)$ is abelian, we have $IJx = JIx = 0$. So, the $\mathbf{Z}[G]$-module Jx is annihilated

by I and therefore contained in B^G. Moreover, Ix is contained in B_{tors}, so we conclude $wx \in B_{\text{tors}} + B^G$ holds, as required. This proves the first implication.

For the converse, assume that for every $x \in B$ there exists $w \in \mathbf{Z}_{>0}$ such that wx is in $B_{\text{tors}} + B^G$ and B^G has an element of order w.

The group B is a radical group over B^G, so there is a maximal B^G-radical extension $\bar{B}$. Since all elements of a Kummer radical extension are Kummer radicals, the subgroup of $\bar{B}$ consisting of all Kummer radicals is the maximal Kummer radical extension of B. We call this $\bar{B}_{\text{Kum}}$:

$$\bar{B}_{\text{Kum}} = \{x \in \bar{B} : \exists w \in \mathbf{Z}_{>0} : wx \in B^G \text{ and } B^G \text{ has an element of order } w\},$$

Then from the assumption, it follows that B is a subset of $C = \bar{B}_{\text{Kum}} + \bar{B}_{\text{tors}}$. Since both $\bar{B}_{\text{Kum}}$ and $B^G + \bar{B}_{\text{tors}}$ are Galois radical groups over B^G (by Theorem 2.9), the automorphism group $\text{Aut}_{B^G}(C)$ is a subgroup of the product $\text{Aut}_{B^G}(\bar{B}_{\text{Kum}}) \times \text{Aut}_{B^G}(B^G + \bar{B}_{\text{tors}})$ due to Theorem 2.13. The extension $B^G \subset B^G + \bar{B}_{\text{tors}}$ is generated by torsion elements so $\text{Aut}_{B^G}(B^G + \bar{B}_{\text{tors}})$ is abelian, and $\text{Aut}_{B^G}(\bar{B}_{\text{Kum}})$ is abelian by Theorem 2.14, so this product of automorphism groups is abelian. This implies that $\text{Aut}_{B^G}(B)$, which is a quotient of $\text{Aut}_{B^G}(C)$ by Theorem 2.12, is also abelian, proving the theorem. □

Schinzel's Theorem 1.7 is a corollary of this theorem:

Corollary 2.21 (Schinzel)**.** *Let F be a field, $a \in F$, and n a positive integer not divisible by* $\operatorname{char} K$*. Let w be the number of n-th roots of unity in F. Then, the splitting field Ω of $X^n - a$ is abelian over F if and only if there exists $b \in F$ with $a^w = b^n$.*

Proof. Define B as $\langle F^*, \zeta_n, \sqrt[n]{a}\rangle$ and apply the theorem to the natural action given by the map $\text{Gal}(\Omega/F) \to \text{Aut}(B)$. Since this action is faithful, we only need to verify that there exists $b \in F$ with $a^w = b^n$ if and only if the following condition from the theorem holds:

$$\forall x \in B : \exists w \in \mathbf{Z}_{>0} : wx \in B_{\text{tors}} + B^G \text{ and } B^G \text{ has an element of order } w.$$

Suppose there is an element $b \in F$ with $a^w = b^n$. To show that the theorem applies, it is sufficient to prove the condition for a set of generators of B over F^*, such as ζ_n and a choice of $\sqrt[n]{a}$. For the root of unity this is immediate.

For $x \in B$ with $x^n = a$, we use that we have $a^w = b^n$. This implies that $x^w = \zeta b$ for some $\zeta \in \mu_n$. Since μ_n is contained in B, this shows that x^w is in $B_{\text{tors}} B^G$.

For the other implication, suppose that the condition from the theorem holds. We will show $a^w \in F^{*n}$.

Let $x \in B$ be such that $x^n = a$. Then by assumption there is a positive integer v such that F^* has an element of order v and $x^v \in B_{\text{tors}} F^*$. Since both x^v and x^n are elements of $B_{\text{tors}} F^*$, we in fact have $x^w \in B_{\text{tors}} F^*$, since w is a multiple of $\gcd(n, v)$. So, we can choose $\zeta \in B_{\text{tors}}$ such that we have $x^w \in \zeta F^*$, and we have that ζ^n is an element of F^{*w}.

Let m be any common multiple of n and the order of ζ. Then because we have $F^*[n] = F^*[w]$, the orders of $(F^*[m])^n$ and $(F^*[m])^w$ are equal, and therefore these two subgroups of F^* are equal. Since we have $\zeta^n \in F^*[m]^w$, we then also have $\zeta^n \in F^*[m]^n \subset F^{*n}$. We now conclude that $a^w = x^{nw} \in F^{*n}$. □

Theorem 2.20 gives a condition for when a group acts in an abelian way on a radical group extension. This can also be used to characterize the maximal G-submodule B_{ab} on which a group G acts in an abelian way, shown by the following definition and accompanying theorem.

Define B_{ab} as follows:

$$B_{\mathrm{ab}} = \{x \in B : \exists w \in \mathbf{Z}_{>0} : wx \in B_{\mathrm{tors}} + B^G \text{ and } B^G \text{ has an element of order } w\}.$$

Note that this definition does not depend on the choice of G, but only on its invariants B^G.

Theorem 2.22. *Let G be a profinite group and B be a discrete abelian group with a continuous G-action. Assume that B/B^G is torsion and all finite subgroups of B are cyclic.*

1. *For a G-module C with $B^G \subset C \subset B$, the image of G in $\mathrm{Aut}(C)$ is abelian if and only if C is a subgroup of B_{ab}.*
2. *Write $[G, G]$ for the closed subgroup of G generated by the commutators of G. Then B_{ab} equals $B^{[G,G]}$.*

We will use the following proposition in the proof of this theorem.

Proposition 2.23. *Let C be a G-module with $B^G \subset C \subset B$. Then we have $C_{\mathrm{ab}} = B_{\mathrm{ab}} \cap C$.*

Proof. Since B^G equals C^G and $(B_{\mathrm{tors}} + B^G) \cap C$ equals $C_{\mathrm{tors}} + C^G$, we can derive the following expressions for C_{ab}.

$$\begin{aligned}
C_{\mathrm{ab}} &= \{x \in C : \exists w \in \mathbf{Z}_{>0} : wx \in C_{\mathrm{tors}} + C^G \text{ and} \\
&\qquad\qquad C^G \text{ has an element of order } w\} \\
&= \{x \in C : \exists w \in \mathbf{Z}_{>0} : wx \in (B_{\mathrm{tors}} + B^G) \cap C \text{ and} \\
&\qquad\qquad B^G \text{ has an element of order } w\} \\
&= C \cap \{x \in B : \exists w \in \mathbf{Z}_{>0} : wx \in B_{\mathrm{tors}} + B^G \text{ and} \\
&\qquad\qquad B^G \text{ has an element of order } w\} \\
&= B_{\mathrm{ab}} \cap C.
\end{aligned}$$

□

Proof of Theorem 2.22. Let C be a G-module with $B^G \subset C \subset B$. By Theorem 2.20, the group G acts in an abelian way on C if and only if C equals C_{ab}. Because C_{ab} is the intersection of B_{ab} and C (Prop. 2.23), the first part of the theorem follows.

Since the image of G in $\mathrm{Aut}(B_{\mathrm{ab}})$ is abelian, B_{ab} is pointwise invariant under the action of the commutator subgroup $[G,G]$, and so B_{ab} is a subgroup of $B^{[G,G]}$.

For the opposite inclusion, the abelian group $G/[G,G]$ acts on $B^{[G,G]}$ since $[G,G]$ is a normal subgroup of G. We conclude that G itself acts on $B^{[G,G]}$ in an abelian way, so by the first part of the theorem, $B^{[G,G]}$ is contained in B_{ab}. □

Corollary 2.24. *The action of G on B induces a surjection $[G,G] \to \mathrm{Aut}_{B_{\mathrm{ab}}}(B)$.*

Proof. The (closed) commutator subgroup $[G,G]$ acts on B, and the extension of radical groups B over $B^{[G,G]} = B_{\mathrm{ab}}$ is a Kummer radical extension. Therefore, by Theorem 2.14 the induced map $[G,G] \to \mathrm{Aut}_{B_{\mathrm{ab}}}(B)$ is a surjection. □

2.6 The entanglement group

As before, let G be a profinite group, and let B be a discrete (additively written) abelian group with a continuous G-action given by $f : G \to \mathrm{Aut}(B)$. Assume B/B^G is a Galois radical extension.

In this section we will prove the following main theorem.

Theorem 2.25. *With B and G as above, $f(G)$ is a normal subgroup of $\mathrm{Aut}_{B^G}(B)$ and $\mathrm{Aut}_{B^G}(B)/f(G)$ is an abelian profinite group.*

Definition 2.26. This cokernel $\mathrm{Aut}_{B^G}(B)/f(G)$ is called the *entanglement group* of B, and written $E(G,B)$, or $E(B)$ if the group G is clear from the context.

The term reflects how in the case of radical group extensions of the unit group of a field, certain multiplicatively independent radicals are *entangled* in the additive field structure. For example, the radical extensions $\mathbf{Q}^* \subset \langle \mathbf{Q}^*, \zeta_5, \sqrt{5} \rangle$ and $\mathbf{Q}^* \subset \langle \mathbf{Q}^*, \zeta_5, \sqrt{-5} \rangle$ have the same group structure and hence have isomorphic automorphism groups. However, when considering them with the natural action of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, the corresponding field extensions are $\mathbf{Q}(\zeta_5, \sqrt{5})/\mathbf{Q}$ and $\mathbf{Q}(\zeta_5, \sqrt{-5})/\mathbf{Q}$. These have different degrees due to the additive relation $\sqrt{5} = \zeta_5 + \zeta_5^{-1} - \zeta_5^2 - \zeta_5^{-2}$, which has no equivalent for $\sqrt{-5}$. Informally, we say that the radicals $\sqrt{5}$ and ζ_5 are entangled. This lower degree of $\mathbf{Q}(\zeta_5, \sqrt{5})$ is reflected in a smaller image of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$ in the automorphism group, and leads to an entanglement group of order 2.

The map from the automorphism group $\mathrm{Aut}_{\mathbf{Q}^*}(\langle \mathbf{Q}^*, \zeta_5, \sqrt{5} \rangle)$ to the entanglement group can be used to determine if a group automorphism extends to a field automorphism. In this example, this map checks if the action on ζ_5 and that on $\sqrt{5}$ are compatible with respect to the additive relation between the two radicals.

For the radical extension $\mathbf{Q}^* \subset \langle \mathbf{Q}^*, \zeta_5, \sqrt{-5} \rangle$, with the action of the absolute Galois group of $\mathbf{Q}$, the entanglement group is trivial.

Another example of non-trivial entanglement is the radical group extension $\mathbf{Q}^* \subset \langle \mathbf{Q}^*, \sqrt[4]{-4} \rangle$. Note that the square of $\sqrt[4]{-4}$ is $2\sqrt{-1}$, so this extension contains 4th roots of unity and is therefore a Galois radical extension. The automorphism group $\mathrm{Aut}_{\mathbf{Q}^*}(\langle \mathbf{Q}^*, \sqrt[4]{-4} \rangle)$ is non-cyclic of order 4.

On the field side, the extension $\mathbf{Q}(\sqrt[4]{-4})/\mathbf{Q}$ has degree 2, which can be seen by writing $\sqrt[4]{-4}$ as $\zeta_8\sqrt{2} = 1 + i$, with corresponding Galois group isomorphic to C_2, and an entanglement group of order 2.

Replacing $\sqrt[4]{-4}$ by $\sqrt[4]{-9}$ in this example leaves the abelian group structure unchanged, but removes the additive relation and leads to a trivial entanglement group.

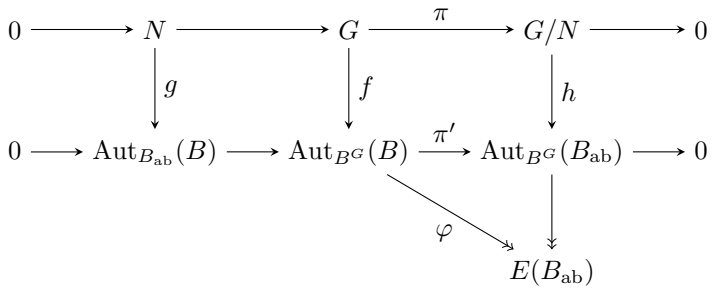
We proceed with the proof of the main theorem.

Proof of Theorem 2.25. A main ingredient in the proof is restricting to the maximal subgroup $B_{\mathrm{ab}} \subset B$ for which $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ is abelian, as defined in the previous section.

Consider the following exact sequence of automorphism groups.

$$0 \to \mathrm{Aut}_{B_{\mathrm{ab}}}(B) \to \mathrm{Aut}_{B^G}(B) \xrightarrow{\mathrm{res}} \mathrm{Aut}_{B^G}(B_{\mathrm{ab}}) \to 0$$

For brevity, we will write N for the commutator subgroup $[G, G]$ in this proof. As we have seen, the action of G on B induces an action of G/N on B_{ab} with invariants B^G. It also induces an action of N on B with invariants B_{ab}. Adding those actions (as vertical maps) to the exact sequence above, we get the rows of the following diagram. These rows are exact, and the squares commute by definition of the vertical maps.



We proceed analogously to the proof of Theorem 1.6.

On the right side of the diagram, the group $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ is abelian by definition of B_{ab} and Theorem 2.20, so the image of h is a normal subgroup with abelian cokernel $E(B_{\mathrm{ab}})$. Let φ be the composite homomorphism from $\mathrm{Aut}_{B^G}(B)$ through $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ to $E(B_{\mathrm{ab}})$. We have to show that φ is surjective with kernel $f(G)$.

The image of f is contained in $\ker(\varphi)$ because of the commutativity of the right square of the diagram. To show the other inclusion, take $x \in \ker(\varphi)$. Then $\pi'(x)$ maps to 0 in $E(B_{\mathrm{ab}})$, so it is the image of h. The map π is surjective, so there is an element $y \in G$ with $h\pi(y) = \pi'(x)$. We then have $\pi' f(y) = \pi'(x)$, so $xf(y)^{-1}$ is in the kernel of π', which equals $\mathrm{Aut}_{B_{\mathrm{ab}}}(B)$. Because g is a surjection (Corollary 2.24), there is an element $z \in N \subset G$ with $g(z) = xf(y)^{-1}$. It follows that $f(zy) = x$ and $x \in f(G)$.

Surjectivity of φ follows immediately from its being composed from two surjective maps. This shows that $f(G)$ is a normal subgroup of $\mathrm{Aut}_{B^G}(B)$ with an abelian cokernel and concludes the proof of Theorem 2.25. □

If C is a G-submodule of B containing B^G, then by Theorem 2.12 the restriction map from $\mathrm{Aut}_{B^G}(B)$ to $\mathrm{Aut}_{B^G}(C)$ is a surjection, so there is a natural surjection $E(G,B) \twoheadrightarrow E(G,C)$. The proof of the theorem shows that this surjection is an isomorphism if we take $C = B_{\mathrm{ab}}$:

Corollary 2.27. *With B and G as in the theorem, $E(G, B_{\mathrm{ab}})$ is equal to $E(G,B)$.*

To derive more tangible expressions for the entanglement group, we study how $E(G,B) = E(G,B_{\mathrm{ab}})$ behaves when B_{ab} is the sum of two smaller G-modules.

Theorem 2.28. *Let B, G and B_{ab} be as before, and suppose $B_{\mathrm{ab}} = C + D$ with C, D two G-submodules of B_{ab}. Then the entanglement group $E(G,B) = E(G, C+D)$ is a part of the following short exact sequence.*

$$0 \to \mathrm{Aut}_{D\cap(B^G+C)}(D)/\mathrm{im}(G_C) \to E(G, C+D) \to E(G,C) \to 0,$$

where G_C is the kernel of the map $G \to \mathrm{Aut}(C)$ induced by the action of G on B.

Proof. We build up a diagram around the short exact sequence

$$0 \to \mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}}) \to \mathrm{Aut}_{B^G}(B_{\mathrm{ab}}) \to \mathrm{Aut}_{B^G}(B^G + C) \to 0$$

and the G-action on B_{ab}.

First of all, note that we can replace G by its image in $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$. This group is abelian, so we assume without loss of generality that G is abelian in this proof. Because C is a G-submodule of B_{ab}, there is an induced map $G \to \mathrm{Aut}_{B^G}(B^G + C)$, and this factors faithfully via G/G_C, by definition of G_C. On the left side of the sequence, the subgroup G_C acts on B_{ab} and leaves B^G and C pointwise invariant, so the image of G_C inside $\mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ ends up inside $\mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}})$.

This leads to the following commutative diagram of abelian groups.

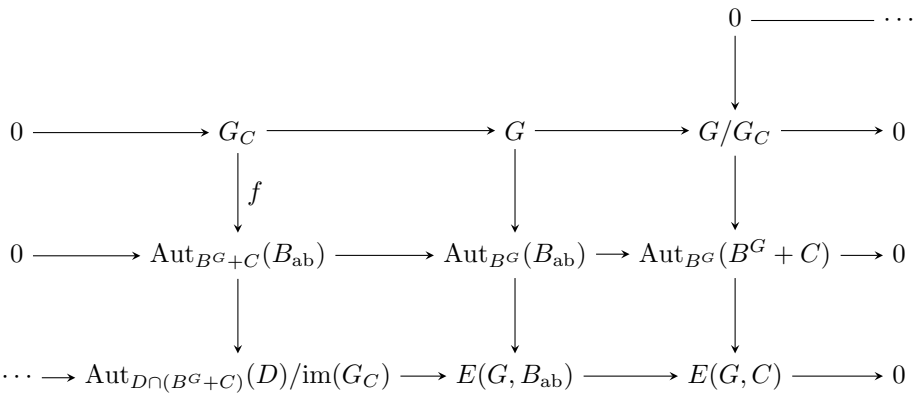
$$\begin{array}{ccccccccc}
 & & & & & & 0 & & \\
 & & & & & & \downarrow & & \\
0 & \longrightarrow & G_C & \longrightarrow & G & \longrightarrow & G/G_C & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle f} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}}) & \longrightarrow & \mathrm{Aut}_{B^G}(B_{\mathrm{ab}}) & \longrightarrow & \mathrm{Aut}_{B^G}(B^G+C) & \longrightarrow & 0
\end{array}$$

Because D is a Galois radical extension of D^G, we have that D is a Galois radical extension over $D \cap (B^G + C)$, by statement 1 of Theorem 2.8 and Theorem 2.9. Therefore, there is a well-defined restriction homomorphism

$$\mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}}) \xrightarrow{\sim} \mathrm{Aut}_{D\cap(B^G+C)}(D).$$

By the fibered sum structure $B_{\mathrm{ab}} = (B^G+C) \oplus_{D\cap(B^G+C)} D$, and the same reasoning as in the proof of Theorem 2.13, this restriction map is an isomorphism.

The cokernel of f is then given by $\mathrm{Aut}_{D\cap(B^G+C)}(D)/\mathrm{im}(G_C)$. The cokernels of the middle and right vertical maps are $E(G, B_{\mathrm{ab}})$ and $E(G, C)$ respectively, by definition. The snake lemma then gives us the desired sequence:



□

Corollary 2.29. *Let B, G and B_{ab} be as in the theorem, and again suppose we have $B_{\mathrm{ab}} = C + D$ with C, D two G-submodules of B_{ab}. Define G_C to be the kernel of the induced map $G \to \mathrm{Aut}(C)$.*

If we have $E(G, C) = 1$, then there is an isomorphism

$$E(G, B) \xrightarrow{\sim} \mathrm{Aut}_{D\cap(B^G+C)}(D)/\mathrm{im}(G_C)$$

that, for each $\sigma \in \mathrm{Aut}_{B^G}(B)$ and $g \in G$ with $\sigma|_C = g|_C$, sends $\bar{\sigma} \in E(G, B)$ to $\sigma|_D(g|_D)^{-1}$.

Proof. Note that the existence of an isomorphism follows directly from the theorem since $E(G, C)$ is trivial. To get the explicit expression for the isomorphism, consider an element $\sigma \in \mathrm{Aut}_{B^G}(B)$. We proceed by diagram chasing in the diagram from the proof of the theorem. Since $E(G, C)$ is trivial, the vertical map $G/G_C \to \mathrm{Aut}_{B^G}(B^G + C)$ on the right side is a surjection, which implies there exists $g \in G$ satisfying $g|_C = \sigma|_C$. By multiplying σ with the inverse of g, we get $\tau = \sigma g^{-1} \in \mathrm{Aut}_{B^G}(B_{\mathrm{ab}})$ which acts as the identity on C by construction. This implies that τ is an element of the subgroup $\mathrm{Aut}_{B^G+C}(B_{\mathrm{ab}})$, on the left side of the diagram, and by mapping it down to $\mathrm{Aut}_{D\cap(B^G+C)}(D)/\mathrm{im}(G_C)$ we find the unique residue class there that maps to $\bar{\tau} \in E(B_{\mathrm{ab}})$, by commutativity. Because τ and σ differ by an element of G, we see that $\bar{\tau} = \bar{\sigma} \in E(B_{\mathrm{ab}})$, concluding the proof of this corollary. □

In the case that D is a Kummer radical extension of B^G, we can simplify the quotient we obtained here. First of all, since in that case D contains B^G, we can rewrite $D \cap (B^G + C)$ to the more symmetric $B^G + (C \cap D)$. Then, it follows from Theorem 2.14 (applied on G_C acting on W) that the image of G_C in $\mathrm{Aut}(D)$ is

$\mathrm{Aut}_{W^{G_C}}(W)$, and the following natural restriction map of the quotient is therefore an isomorphism:

$$\mathrm{Aut}_{B^G+(C\cap D)}(D)/\mathrm{im}(G_C) \xrightarrow{\sim} \mathrm{Aut}_{B^G+(C\cap D)}(D^{G_C}). \tag{2.30}$$

Going one step further, we can conclude the following if additionally there is no cyclotomic entanglement. This is a generalization of Theorem 1.10.

Corollary 2.31. *Let B, G and B_{ab} be as in the theorem, and suppose we have $B_{\mathrm{ab}} = \mu + W$ with μ a subgroup of B_{tors} and $W \subset B$ a Kummer radical extension of B^G. Define G_μ as the kernel of the restriction map $G \to \mathrm{Aut}(\mu)$.*

If we have $E(G, \mu) = 1$, then there is an isomorphism

$$E(G, B) \xrightarrow{\sim} \mathrm{Aut}_{B^G+(\mu\cap W)}(W^{G_\mu})$$

that, for each $\sigma \in \mathrm{Aut}_{B^G}(B)$ and $g \in G$ with $\sigma|_\mu = g|_\mu$, sends $\bar{\sigma} \in E(G, B)$ to $\sigma|_{W^{G_\mu}}(g|_{W^{G_\mu}})^{-1}$.

Proof. We start from the previous corollary (2.29), take $C = \mu$ and $D = W$ and apply Equation 2.30. □

This description of the entanglement group assumes that B_{ab} can be generated by roots of unity and Kummer roots. This condition is often fulfilled, in particular in the case of maximal radical extension which we study in Chapter 3, but we shall encounter situations where this is not the case later. In those cases, it is possible to extend B and B_{ab} with extra roots of unity to handle this. We describe this approach in Propositions 4.9 and 5.6.