Universal Degrees of Field Extensions

Vullers, M.

Michaël Vullers

Universal Degrees of Field Extensions

Bachelorscriptie, 06 juni 2013

Scriptiebegeleider: prof.dr. H.W. Lenstra

Mathematisch Instituut, Universiteit Leiden

Contents

Introduction

Let $\mathcal{C}$ be the category of finite groups. Let $\mathrm{Ob}(\mathcal{C})$ denote the class of objects of $\mathcal{C}$ and let $\mathrm{Ob}(\mathcal{C})/{\cong} = \{[G] : G \in \mathrm{Ob}(\mathcal{C})\}$ denote the set of isomorphism classes. The *Grothendieck group* $\mathcal{G}$ of $\mathcal{C}$ with respect to short exact sequences is the group generated by $\mathrm{Ob}(\mathcal{C})/{\cong}$ subject to the relations $[G] = [H][N] \in \mathcal{G}$ if there exists a short exact sequence

$$1 \to H \to G \to N \to 1.$$

Let p be zero or a prime number and let $\mathcal{E}_p$ be the collection of all pairs (K, L) where K is a field of characteristic p and L/K is a finite field extension. We call $(K, L) \in \mathcal{E}_p$ normal, Galois or separable if the field extension L/K is normal, Galois or separable. Let $D_p \colon \mathcal{E}_p \to \mathcal{G}$ be given by $D_p(L/K) = [\mathrm{Aut}_K(N)][\mathrm{Aut}_L(N)]^{-1}$, where N is a finite extension of L that is normal over K. We will call the map D_p the *Galois degree*. In Section 5 we show that the Galois degree is well-defined, as well as the following result.

Theorem 1. Suppose that $(K, L) \in \mathcal{E}_p$ and $(L, M) \in \mathcal{E}_p$. Then

$$D_p(L/K) \cdot D_p(M/L) = D_p(M/K).$$

We call a field extension L'/K' a *base extension* of a field extension L/K if there exists a field homomorphism $\psi \colon L \to L'$ with $\psi(K) \subset K'$ such that for each basis B of L as a K-vector space, $\psi(B)$ is a basis for L' as a K'-vector space. In Section 5 the following result will be shown.

Theorem 2. Assume that $(K, L) \in \mathcal{E}_p$ is normal and L'/K' is a base extension of L/K. Then $D_p(L/K) = D_p(L'/K')$.

Let A be a multiplicatively written abelian group. A map $d \colon \mathcal{E}_p \to A$ is called a *degree* with values in A if it satisfies the following two conditions:

(i) if $(K, L), (L, M) \in \mathcal{E}_p$ then $d(M/K) = d(M/L) \cdot d(L/K)$ and

(ii) if $(K, L) \in \mathcal{E}_p$ is normal and L'/K' is a base extension of L/K then $d(L/K) = d(L'/K')$.

We let $\mathrm{Deg}(p, A)$ denote the set of all degrees $d \colon \mathcal{E}_p \to A$. A degree $d \colon \mathcal{E}_p \to A$ is called *universal* if for each abelian group B the mapping $\mathrm{Hom}(A, B) \to \mathrm{Deg}(p, B)$ sending f to $f \circ d$ is a bijection.

The main results of this thesis are the following two theorems, which will be proven in Section 5.

Theorem 3. The Galois degree $D_0 \colon \mathcal{E}_0 \to \mathcal{G}$ is universal.

Theorem 4. Let p be prime and $p^{\mathbb{Z}} = \{p^n : n \in \mathbb{Z}\} \subset \mathbb{Q}_{>0}$. Then the map $D\colon \mathcal{E}_p \to \mathcal{G} \times p^{\mathbb{Z}}$ given by $D(L/K) = (D_p(L/K), [L:K]_i)$, where $[L:K]_i$ is the inseparability degree of L/K, is a universal degree.

In Section 4, a simplification of a degree, called a *basic degree* will be studied. This simplification consists of removing the condition that (K, L) is normal in (ii). In other words a basic degree is a degree that satisfies the following condition instead of (ii) above: (ii') if $(K, L) \in \mathcal{E}_p$ and L'/K' is a base extension of L/K then $d(L/K) = d(L'/K')$.
We let $\mathrm{bdeg}(p, A)$ denote the set of all basic degrees $d\colon \mathcal{E}_p \to A$ and call a basic degree $d\colon \mathcal{E}_p \to A$ *universal* if for each abelian group B the map $\mathrm{Hom}(A, B) \to \mathrm{bdeg}(p, B)$ sending f to $f \circ d$ is a bijection.

Results from Section 2 will show that D_p is not a basic degree, which gives rise to the question if there is a universal basic degree. In Section 4 this question will be answered with the following two theorems.

Theorem 5. The basic degree $d\colon \mathcal{E}_0 \to (\mathbb{Q}_{>0}, \cdot)$ given by $d(L/K) = [L:K]$ is universal.

Theorem 6. Let p be prime. Then the basic degree $d\colon \mathcal{E}_p \to (\mathbb{Q}_{>0}, \cdot) \times p^{\mathbb{Z}}$ given by $d(L/K) = ([L:K]_s, [L:K]_i)$, where $[L:K]_s$ is the separability degree of L/K, is universal.

In the first two sections we will develop, mainly using Galois theory, some theory on linear disjointness and base extensions. In Section 3 the group $\mathcal{G}$ will be studied and the following result will be proven.

Theorem 7. Let $\mathcal{S}$ be the set of isomorphism classes of finite simple groups. Then $\mathcal{G}$ is the free abelian group on $\mathcal{S}$.

1. Linear disjointness

Definition 1.1. Let L/K be a field extension and let R, S be K-subalgebras of L. Then R and S are called *K-linearly disjoint in L* if the canonical ring homomorphism $R \otimes_K S \to L$ is injective.

Proposition 1.2. Let L/K be a field extension and R, S be K-subalgebras of L. If R and S are K-linearly disjoint in L then $R \cap S = K$.

Proof. Suppose $K \subsetneq R \cap S$ and let $x \in (R \cap S) \backslash K$. Then there exists a K-basis A of R and a K-basis B of S such that $\{1, x\} \subset A \cap B$. Note that the elements $1 \otimes x$ and $x \otimes 1$ are K-linearly independent in $R \otimes_K S$. However under the canonical ring homomorphism $\iota \colon R \otimes_K S \to L$ the images of $1 \otimes x$ and $x \otimes 1$ are the same. Hence ι is not injective. □

Proposition 1.3. Let L/K be a field extension and R, S be K-linearly disjoint K-subalgebras of L. If R' (resp. S') is a K-subalgebra of R (resp. of S) then R' and S' are K-linearly disjoint in L.

Proof. Let $\iota \colon R \otimes_K S \to L$ be the canonical ring homomorphism. Note that $R' \otimes_K S' \subset R \otimes_K S$ and the canonical ring homomorphism $\kappa \colon R' \otimes_K S' \to L$ is equal to $\iota|_{R' \otimes_K S'}$. Since R and S are K-linearly disjoint ι is injective. Hence κ is injective making R' and S' linearly disjoint over K in L. □

Proposition 1.4. Let L/K be a field extension and R, S be K-subalgebras of L. Let I be a directed set. Suppose that $R = \varinjlim R_i$ is a direct limit of a directed system $\{R_i, f_{ij}\}$, where R_i is a subalgebra of R_j and f_{ij} is the inclusion of R_i in R_j if $i \leq j$, of K-subalgebras of L over I. Then R and S are K-linearly disjoint in L if and only if for all $i \in I$, the K-algebras R_i and S are K-linearly disjoint in L.

Proof. Recall that direct limits and tensor products commute, so $\varinjlim(R_i \otimes_K S) \cong (\varinjlim R_i) \otimes_K S$. Let $f_j \colon R_j \to \varinjlim R_i$. Recall that direct limits have the following universal mapping property. If C is a K-algebra with for each $i \in I$ a K-algebra homomorphism $\psi_i \colon R_i \to C$ such that $\psi_i = \psi_j \circ f_{ij}$ if $i \leq j$. Then there exists a unique K-algebra homomorphism $\psi \colon \varinjlim R_i \to C$ such that for all $i \in I$ one has $\psi \circ f_i = \psi_i$. One can find these properties of a directed system in chapter 2 of [1]. Extend the directed system $\{R_i, f_{ij}\}$ to the directed system $\{R_i \otimes_K S, f_{ij} \otimes \mathrm{id}_S\}$ and for each $i \in I$ let $\psi_i \colon R_i \otimes S \to L$ be the canonical ring homomorphism. Note that ψ_i satisfies the condition of second property hence one obtains a unique K-algebra homomorphism $\psi \colon \varinjlim R_i \otimes_K S \to L$ satisfying for each $i \in I$ the equality $\psi \circ (f_i \otimes \mathrm{id}_S) = \psi_i$. Note that $f_i \otimes \mathrm{id}_S$ is an inclusion hence injective. Therefore ψ is injective if and only if ψ_i is injective for each $i \in I$. The result now follows from applying the first property. □

Proposition 1.5. Let L/K be a field extension and R, S be K-subalgebras of L. Then R and S are K-linearly disjoint in L if and only if the subfields they generate, say E and F, are K-linearly disjoint in L.

Proof. Assume that R and S are K-linearly disjoint. It suffices to show that if $x_1, \ldots, x_n \in E$ are K-linearly independent and $y_1, \ldots, y_m \in F$ are K-linearly independent then $\{x_i y_j\}_{1 \leq i \leq n, 1 \leq j \leq m}$ are K-linearly independent in L. There exist $r_1 \ldots, r_n, r \in R$ and $s_1, \ldots, s_m, s \in S$, with $r \neq 0 \neq s$, such that $x_i = r_i/r$ and $y_j = s_j/s$ for all i and all j. Let $\alpha_{i,j} \in K$ such that $\sum_{i,j} \alpha_{i,j} r_i s_j / rs = 0$.

Multiplication by rs yields $\sum_{i,j} \alpha_{i,j} r_i s_j = 0$ hence $\alpha_{i,j} = 0$ for all i and all j. The converse is immediate from Proposition 1.3. $\square$

Definition 1.6. Let K be a field and R and S be K-algebras that are domains. We call R and S *somewhere K-linearly disjoint* if there exists a field extension L/K and K-algebra embeddings of R and S into L such that R and S are K-linearly disjoint in L. We call R and S *everywhere K-linearly disjoint* if for all field extensions L/K and all K-algebra embeddings of R and S into L, the embeddings of R and S are K-linearly disjoint in L.

Proposition 1.7. Let K be a field and R, S be K-algebras that are domains and let $\operatorname{Frac}(R)$, $\operatorname{Frac}(S)$ denote the fraction fields of R and S. Then the following hold:

(i) R and S are somewhere K-linearly disjoint if and only if $R \otimes_K S$ is a domain.

(ii) R and S are everywhere K-linearly disjoint if and only if $\operatorname{Frac}(R) \otimes_K \operatorname{Frac}(S)$ is a field.

Proof. (i). If R and S are somewhere K-linearly disjoint then $R \otimes_K S$ can be embedded in a field hence it is a domain. Conversely if $R \otimes_K S$ is a domain then it can be embedded in its fraction field.
(ii). Suppose R and S are everywhere K-linearly disjoint. Note that $T = \operatorname{Frac}(R) \otimes_K \operatorname{Frac}(S) \supset K$. In order to show that T is a field it suffices to show that (0) is the only maximal ideal of T. Let $\mathfrak{m} \subset T$ be a maximal ideal, then $E = T/\mathfrak{m}$ is a field containing $\operatorname{Frac}(R)$ and $\operatorname{Frac}(S)$. Note that the induced map $\iota \colon T \to E$ is the quotient map $T \to T/\mathfrak{m}$. From the assumption that R and S are everywhere K-linearly disjoint and Proposition 1.5 it follows that ι is injective hence $\mathfrak{m} = (0)$. Conversely suppose that $\operatorname{Frac}(R) \otimes_K \operatorname{Frac}(S)$ is a field. Let A be an arbitrary non-trivial ring, then any ring homomorphism $\operatorname{Frac}(R) \otimes_K \operatorname{Frac}(S) \to A$ is injective. Hence any ring homomorphism from $\operatorname{Frac}(R) \otimes_K \operatorname{Frac}(S)$ to a non-trivial K-algebra is injective. Since any field extension of K is a non-trivial K-algebra it follows that $\operatorname{Frac}(R)$ and $\operatorname{Frac}(S)$ are everywhere K-linearly disjoint and so from Proposition 1.3 it follows that R and S are everywhere K-linearly disjoint. $\square$

Proposition 1.8. Let K be a field and E, F field extensions of K that are contained in a field Ω. If E/K is finite then the following are equivalent:

(i) E and F are K-linearly disjoint in Ω;

(ii) $E \otimes_K F$ is a field;

(iii) $[E : K] = [EF : F]$.

Proof. (iii) $\Leftrightarrow$ (i). Let $\iota \colon E \otimes_K F \to EF$ be the canonical ring homomorphism. Note that ι is a surjective F-linear map between finite dimensional F-vector spaces. Hence $\dim_F \ker(\iota) = [E : K] - [EF : F]$ and so ι is injective if and only if $[E : K] = [EF : F]$.
(ii) $\Leftrightarrow$ (i). Suppose E and F are K-linearly disjoint in Ω. Then E and F are somewhere K-linearly disjoint. From Proposition 1.7 it follows that $E \otimes_K F$ is a domain. Note that $\dim_F(E \otimes_K F) \leq [E : K]$ hence $E \otimes_K F$ is a finitely generated F-vector space. Let $x \in E \otimes_K F$ be an arbitrary non-zero and let $\lambda_x \colon E \otimes_K S \to E \otimes_K S$ be given by $\lambda_x(y) = xy$. Since $E \otimes_K S$ is a domain λ_x is injective and since $E \otimes_K S$ is finitely generated as an F-vector space it follows that λ_x is surjective. From this it immediately follows that $E \otimes_K S$ is a field.
The converse is immediate from Proposition 1.7. $\square$

Theorem 1.9. Let K be a field and $K \subset E, F$ be field extensions. Then the following hold:

(i) Suppose E and F are everywhere K-linearly disjoint. Then at least one of E and F is algebraic of K.

(ii) Suppose at least one of E and F is algebraic over K. Then E and F are somewhere K-linearly disjoint if and only if E and F are everywhere K-linearly disjoint.

Proof. (i). Suppose that both E and F are not algebraic over K. Assume that E and F are everywhere K-linearly disjoint. Then it follows from Proposition 1.8 that $E \otimes_K F$ is a field. There exist transcendental subextensions $K(a) \subset E$ and $K(b) \subset F$. Let X be a variable. Let $K(X) \to K(a)$ and $K(X) \to K(b)$ be given by $X \to a$ and $X \to b$ respectively. Let $\phi\colon E \otimes_K F \to E \otimes_{K(X)} F$ be the canonical ring homomorphism. Since $E \otimes_K F$ is a field and $E \otimes_{K(X)} F \neq \{0\}$ it follows that ϕ is injective. Note that $\dim_{K(b)}(K(a) \otimes_K K(b)) = \infty$ and that $\dim_{K(b)}(K(a) \otimes_{K(X)} (K(b)) = 1$. Since $\phi(K(a) \otimes_K K(b)) = K(a) \otimes_{K(X)} K(b)$ it follows that ϕ is not injective. This is a contradiction. Hence E and F are not everywhere K-linearly disjoint.
(ii). Suppose E is algebraic over K and that E and F are K-linearly disjoint in some field L. Let L' be a field and let $E \to L'$ and $F \to L'$ be embeddings that are equal on K. It needs to be shown that E and F are K-linearly disjoint in L'. Note that every algebraic extension is a direct limit of finite extensions. Hence by Proposition 1.4 it is no loss of generality to assume that E/K is finite. From Proposition 1.8 it follows that $E \otimes_K F$ is a field and so from Proposition 1.7 it follows that E and F are everywhere K-linearly disjoint. The converse is clear. $\square$

Proposition 1.10. Let K be a field and E, F be field extensions of K that are contained in a field Ω. If E/K is finite Galois then the following hold:

(i) EF is Galois over F and $\mathrm{Gal}(E/(E \cap F)) \cong \mathrm{Gal}(EF/F)$;

(ii) E and F are K-linearly disjoint in Ω if and only if $E \cap F = K$.

Proof. (i). It is well known from basic Galois theory that EF is Galois over F. Define

$$\phi\colon \mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/(E \cap F)), \psi \mapsto \psi|_E.$$

Note that ϕ is well defined since each $\psi \in \mathrm{Gal}(EF/F)$ is the identity on F and so it is the identity on $E \cap F$. By definition $\psi|_F = \mathrm{id}_F$ hence if $\psi|_E = \mathrm{id}_E$ then $\psi = \mathrm{id}_{EF}$. Hence ϕ is injective. Note that $E^{\mathrm{im}(\phi)} = E \cap F$ hence $\mathrm{im}(\phi) = \mathrm{Gal}(E/(E \cap F))$. Therefore ϕ is surjective and thus bijective. Hence from Galois theory it follows that $[EF : F] = [E : E \cap F]$.
(ii). If $E \cap F = K$ then by part (i) one has $[E : K] = [EF : F]$ and so from Proposition 1.8 it follows that E and F are K-linearly disjoint. The converse is direct from Proposition 1.2. $\square$

Notation. Let G be a group and $H \subset G$ be a subgroup. Then $\mathrm{Ind}_G(H)$ denotes the index of H in G.

Proposition 1.11. Let G be a finite group and let $H, I \subset G$ be subgroups. Then $\mathrm{Ind}_G(H \cap I) \leq \mathrm{Ind}_G(H) \cdot \mathrm{Ind}_G(I)$ with equality if and only if $G = HI$.

Proof. Note that although HI need not be a group the number of cosets of I in HI is still well-defined hence $\mathrm{Ind}_{HI}(I)$ is well-defined. First we show $\mathrm{Ind}_{HI}(I) = \mathrm{Ind}_H(H \cap I)$. Let H act on G/I by left multiplication and let $x = I/I \in G/I$. Note that $H \cap I = \mathrm{Stab}(x)$ and HI/I is the orbit of x. Corollary 4.8 of [3] states that if a group acts on a set, then for any element of the set the index of the stabilizer is equal to the cardinality of the orbit. Hence $\#(HI/I) = \#(H/(H \cap I))$ and so $\mathrm{Ind}_{HI}(I) = \mathrm{Ind}_H(H \cap I)$. To prove the statement observe:

$$\mathrm{Ind}_G(H \cap I) = \mathrm{Ind}_G(H) \cdot \mathrm{Ind}_H(H \cap I) = \mathrm{Ind}_G(H) \cdot \mathrm{Ind}_{HI}(I) \leq \mathrm{Ind}_G(H) \cdot \mathrm{Ind}_G(I).$$

□

Proposition 1.12. Let L/K be finite Galois with $G = \mathrm{Gal}(L/K)$ and let $H, I \subset G$ be subgroups. Then L^H and L^I are K-linearly disjoint if and only if $G = HI$.

Proof. From Proposition 1.8 it follows that L^H and L^I are K-linearly disjoint if and only if $[L^H : K] = [L^H L^I : L^I]$ which is equivalent to $[L^H L^I : K] = [L^H : K][L^I : K]$ since L/K is finite. From Galois theory one has $L^H L^I = L^{H \cap I}$ and $[L^S : K] = \mathrm{Ind}_G(S)$ for each subgroup S of G. Hence L^H and L^I are K-linearly disjoint if and only if $\mathrm{Ind}_G(H \cap I) = \mathrm{Ind}_G(H) \cdot \mathrm{Ind}_G(I)$ and so from Proposition 1.11 one obtains that L^H and L^I are K-linearly disjoint if and only if $G = HI$. □

2. Base extensions

Definition 2.1. A field extension L'/K' is called a *base extension* of a field extension L/K if there exists a field homomorphism $\psi \colon L \to L'$ with $\psi(K) \subset K'$ satisfying the following two equivalent conditions:

(i) for every basis B of L as a K-vector space, $\psi(B)$ is a basis of L' as a K'-vector space;

(ii) the canonical map $L \otimes_K K' \to L'$ is an isomorphism.

Remark 2.2 (Transitive property of base extensions)**.** If L'/K' is a base extension of L/K and L''/K'' is a base extension of L'/K' then L''/K'' is a base extension of L/K.

Definition 2.3. A set $\{L_i/K_i\}_{i=0}^n$ of field extension is called a *chain of base extensions* if L_{i+1}/K_{i+1} is a base extension of L_i/K_i or L_i/K_i is a base extension of L_{i+1}/K_{i+1} for each $0 \leq i < n$.
The number n of base extensions in a chain (of base extensions) is called the *length* of the chain.
Two field extension L/K and L'/K' are called *connected* if there exists a chain of base extensions containing L/K and L'/K'.

Proposition 2.4. Let K be a field and $K \subset L, M$ be two field extensions that are everywhere K-linearly disjoint. Then $L \otimes_K M/M$ is a base extension of L/K. Moreover if L and M are contained in a larger field Ω then LM/M is a base extension of L/K.

Proof. From Proposition 1.7 it follows that $L \otimes_K M$ is a field. It is immediate from the definition that $L \otimes_K M/M$ is a base extension of L/K. Suppose L and M are contained in a larger field Ω. Let $\iota \colon L \otimes_K M \to LM$ be the canonical homomorphism. Note that ι is surjective. Moreover since $L \otimes_K M$ is a field and $LM \neq \{0\}$ it follows that ι is injective. Hence ι is a isomorphism and thus LM/M is a base extension of L/K. □

Proposition 2.5. Let L/K be a finite Galois extension and let L'/K' be a base extension of L/K. Then L'/K' is finite Galois and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L'/K')$.

Proof. Since L'/K' is a base extension of L/K there is an field homomorphism $\psi\colon L \to L'$. Identify L and K with their images under ψ and take $\Omega = L'$. Note that L and K' are K-linearly disjoint in L'. Hence from Proposition 1.2 it follows that $L \cap K' = K$. From Proposition 1.8 it follows that $[L : K] = [LK' : K']$ hence it follows that $LK' = L'$. The result follows from Proposition 1.10. $\square$

Definition 2.6. Let G and H be groups, let X be a G-set and Y be a H-set. Let $\phi\colon G \to H$ be a group homomorphism and $\psi\colon Y \to X$ be a map. The actions of G and H are called *compatible* through ϕ and ψ if for all $g \in G$ and all $y \in Y$ the equality $\psi({}^{\phi(g)}y) = {}^{g}(\psi(y))$ holds.

Theorem 2.7. Let E and F be fields with the same characteristic. Let $G \subset \mathrm{Aut}(F)$ and $S \subset \mathrm{Aut}(E)$ be finite subgroups and let $T \subset S$ be a subgroup. Let $\phi\colon G \to S$ be a group homomorphism and let $\psi\colon E \to F$ be an field homomorphism. Suppose that the actions of G and S are compatible through ϕ and ψ and that G acts transitively on S/T through ϕ, and let $H = \mathrm{Stab}(T/T) \subset G$. Then F^H/F^G is a base extension of E^T/E^S.

Proof. Since the actions of G and S are compatible so are the actions of $\phi(G)$ and S. Since G acts transitively on S/T so does $\phi(G)$, which is equivalent to $S = T\phi(G)$. Hence from Proposition 1.12 it follows that E^T and $E^{\phi(G)}$ are linearly disjoint over E^S. From the definition of H one has $\phi(H) = T \cap \phi(G)$ and from Galois theory it follows that $E^T E^{\phi(G)} = E^{\phi(H)}$. Applying Proposition 2.4 with $K = E^S$, $L = E^T$ and $M = E^{\phi(G)}$ yields that $E^{\phi(H)}/E^{\phi(G)}$ is a base extension of E^T/E^S. Note that $\psi\colon E \to \psi(E)$ is an isomorphism and that the composition of an isomorphism with a base extension is again a base extension. With the compatibility of the actions it follows that $\psi(E)^H/\psi(E)^G$ is a base extension of E^T/E^S. Since $\psi(E)/\psi(E)^G$ is Galois one obtains from Proposition 1.10 that $\psi(E)$ and F^G are linearly disjoint over $\psi(E) \cap F^G = \psi(E)^G$. From Proposition 1.3 it follows that $\psi(E)^H$ and F^G are $\psi(E)^G$-linearly disjoint. Note $\psi(E)^H F^G \subset F^H$ and by Proposition 1.8 and the assumption that G acts transitively on S/T one has

$$[\psi(E)^H F^G : F^G] = [\psi(E)^H : \psi(E)^G] = [G : H] = [F^H : F^G].$$

Hence $\psi(E)^H F^G = F^H$. By the transitive property of base extensions F^H/F^G is a base extension of E^T/E^S.

$$\begin{tikzcd}
T & \phi(H) & & H \\
\cap & \cap & & \cap \\
S/T \circlearrowleft S & \phi(G) \arrow[l, "\supset"'] & G \arrow[l, "\phi"'] & G \arrow[l, "\supset"'] \\
\circlearrowleft & \circlearrowleft & \circlearrowleft & \circlearrowleft \\
E \arrow[r, "\subset"] & E \arrow[r, "\psi"] & \psi(E) \arrow[r, "\subset"] & F \\
E^T \arrow[u, dash] & E^{\phi(H)} \arrow[u, dash] & \psi(E)^H \arrow[u, dash] & F^H \arrow[u, dash] \\
E^S \arrow[u, dash] & E^{\phi(G)} \arrow[u, dash] & \psi(E)^G \arrow[u, dash] & F^G \arrow[u, dash]
\end{tikzcd}$$

$\square$

Notation. Let K be a field and let $\mathcal{X} = \{X_i : i \in I\}$ be a set of independent variables. Then $K(\mathcal{X})$ denotes the field of rational functions in the variables $X_i \in \mathcal{X}$ over K.

Theorem 2.8. Let K, K' be fields with the same characteristic and let $n \in \mathbb{Z}_{>0}$. Suppose L/K, L'/K' are finite separable field extensions of degree n. Then there exists a chain of base extensions of length 4 connecting L/K with L'/K'.

Proof. Let M be a Galois closure of L and let $G = \mathrm{Gal}(M/K)$. Let $\mathrm{Hom}_K(L, M)$ denote the set of field homomorphism $L \to M$ that are the identity on K. Note that G acts naturally on $\mathrm{Hom}_K(L, M)$ by composition. Let $H \subset G$ be the stabilizer of the inclusion $\iota \in \mathrm{Hom}_K(L, M)$ of L into M, then $M^H = L$. Let $\mathcal{X} = \{X_\alpha : \alpha \in \mathrm{Hom}_K(L, M)\}$ be a set of independent variables. The group G acts on $M(\mathcal{X})$ by its action on M and its action on $\mathcal{X}$. Note that this action is compatible with the action of G on M. Hence from Theorem 2.7 it follows that $M(\mathcal{X})^H/M(\mathcal{X})^G$ is a base extension of $M^H/M^G = L/K$. Let S be the symmetric group of the set $\mathrm{Hom}_K(L, M)$ and let $T \subset S$ be the stabilizer of ι. Let $\mathbb{F}$ be the prime field of K and let S act on $\mathbb{F}(\mathcal{X})$ by its action on $\mathcal{X}$. Note that the action of G on $M(\mathcal{X})$ is compatible with the action of S on $\mathbb{F}(\mathcal{X})$. Through its action on $\mathrm{Hom}_K(L, M)$ the group G is a subgroup of S. Since G acts transitively on $\mathrm{Hom}_K(L, M)$ and T is a stabilizer it follows that $S = GT$ which is equivalent to G acting transitively on S/T. Hence from Theorem 2.7 it follows that $M(\mathcal{X})^H/M(\mathcal{X})^G$ is a base extension of $\mathbb{F}(\mathcal{X})^T/\mathbb{F}(\mathcal{X})^S$, hence one obtains the following chain of base extensions of length two:

$$\left\{L/K, M(\mathcal{X})^H/M(\mathcal{X})^G, \mathbb{F}(\mathcal{X})^T/\mathbb{F}(\mathcal{X})^S\right\}.$$

Repeating the argument above for L'/K' yields a similar chain of base extensions of length two. Note that $n = \#\mathrm{Hom}_K(L, M) = \#\mathrm{Hom}_{K'}(L', M')$ hence the symmetric groups are isomorphic. It is clear that by identifying the inclusion of L in M with the inclusion of L' in M' one obtains a group isomorphism $\phi\colon S \to S'$ such that $\phi(T) = T'$. Hence $M'(\mathcal{X}')^{H'}/M'(\mathcal{X}')^{G'}$ is a base extension of $\mathbb{F}(\mathcal{X})^T/\mathbb{F}(\mathcal{X})^S$. Therefore one obtains the following chain of base extensions connecting L/K to L'/K' of length four:

$$\left\{L/K, M(\mathcal{X})^H/M(\mathcal{X})^G, \mathbb{F}(\mathcal{X})^T/\mathbb{F}(\mathcal{X})^S, M'(\mathcal{X}')^{H'}/M'(\mathcal{X}')^{G'}, L'/K'\right\}.$$

□

Definition 2.9. A base extension L'/K' of L/K is called *trivial* if there exists a field isomorphism $\psi\colon L \to L'$ that satisfies the conditions of Definition 2.1.

Example 2.10. Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and let $\zeta_5, \zeta_8 \in \overline{\mathbb{Q}}$ be a 5^{th} and an 8^{th} primitive root of unity. Then it follows from Galois theory that $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ and $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ are finite Galois extensions with $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong C_4$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong V_4$, where C_4 is the cyclic group of order 4 and V_4 is the Klein four-group. From the above theorem it follows that there exists a chain of base extensions of length 4 connecting $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ with $\mathbb{Q}(\zeta_8)/\mathbb{Q}$. In this example we show that there does not exist a shorter such chain. Since $V_4 \ncong C_4$ it follows from Proposition 2.5 that $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is not a base extension of of $\mathbb{Q}(\zeta_8)/\mathbb{Q}$. Hence there is no chain of length equal to one. Suppose that $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is a base extension of L/K. Then it immediately follows that $K = \mathbb{Q}$ and $L \cong \mathbb{Q}(\zeta_5)$. Hence $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is not a non-trivial base extension of a field extension L/K. It is clear that this argument also applies to $\mathbb{Q}(\zeta_8)/\mathbb{Q}$. Form this it follows that a chain of length 3 can be shortened using the transitive property of base extensions to a chain of length equal to 2 or 1. It remains to show that there is no chain of length two. Suppose that there is such a chain. Then there exists a field extension L/K such that L/K is a base extension both of $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ and of $\mathbb{Q}(\zeta_8)/\mathbb{Q}$. From Proposition 2.5 it follows that L/K is Galois and that $V_4 \cong \mathrm{Gal}(L/K) \cong C_4$. This is a contradiction hence there is no chain of length two. Hence there is no chain of base extensions connecting $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ with $\mathbb{Q}(\zeta_8)/\mathbb{Q}$ of length shorter than four.

Proposition 2.11. Let p be prime and K a field of characteristic p and let $f \in K[X]$ be irreducible. Write $f(X) = g(X^{p^m})$ with $m \geq 0$ maximal. Then g is irreducible and separable over K and each root of f has multiplicity equal to p^m.

Proof. Since $\deg f = p^m \deg g$ there is a largest possible m that can be used. Note that since $f(X) = g(X^{p^m})$, any non-trivial factorisation of g gives a non-trivial factorisation of f hence g is irreducible in $K[X]$. Since g is irreducible it follows that g is separable if and only if its derivative is non-zero. By the maximality of m it follows that g is not a polynomial in X^p, hence its derivative is non-zero. Let M/K be a splitting field of g and factor g over M as

$$g(X) = c(X - a_1)(X - a_2)\cdots(X - a_n).$$

Note that the a_i are distinct since g is separable. Take $b_1, \ldots, b_n$ in a sufficiently large field extension of M such that $a_i = b_i^{p^m}$. It follows from the distinctness of the a_i that the b_i are distinct. From this it follows that

$$f(X) = g(X^{p^m}) = c(X^{p^m} - a_1)\cdots(X^{p^m} - a_n) = c(X - b_1)^{p^m}\cdots(X - b_n)^{p^m},$$

which shows that the roots of f have multiplicity equal to p^m. □

Corollary 2.12. Let p be prime and K a field of characteristic p. Suppose that $f \in K[X]$ is irreducible with exactly one root in a splitting field over K. Then f is of the form $X^{p^m} - a$ for some $m \geq 0$.

Corollary 2.13. Let p be prime, K a field of characteristic p and L/K a finite purely inseparable field extension. Then $[L : K] = p^n$ for some $n \geq 0$ and there exists a tower of field extensions $K = L_n \subset L_{n-1} \subset \ldots L_1 \subset L_0 = L$ such that L_i/L_{i+1} is purely inseparable of degree p.

Theorem 2.14. Let p be prime and let K, K' be fields of characteristic p. Suppose that L/K and L'/K' are purely inseparable field extensions such that $[L : K]_i = [L' : K']_i = p$. Then there exists a chain of base extensions of length 2 connecting L/K with L'/K'.

Proof. Since $[L : K]_i = p$ there exists $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^p \in K$. Similarly there exists $\alpha' \in L'$ such that $L' = K'(\alpha')$ and $(\alpha')^p \in K'$. Note that α and α' are transcendental over $\mathbb{F}_p$. Let T be a variable. Let $\phi\colon \mathbb{F}_p(T) \to L$ be the field homomorphism such that $\phi(T) = \alpha$ and let $\phi'\colon \mathbb{F}_p(T) \to L'$ be the field homomorphism such that $\phi'(T) = \alpha'$. It is clear that ϕ and ϕ' make L/K and L'/K' into base extensions of $\mathbb{F}_p(T)/\mathbb{F}_p(T^p)$. Hence one obtains the following chain of base extensions of length 2 connecting L/K with L'/K':

$$\{L/K, \mathbb{F}_p(T)/\mathbb{F}_p(T^p), L'/K'\}.$$

□

Definition 2.15. A chain of base extensions $\{L_i/K_i\}_{i=0}^n$ is called *group preserving* if each L_i/K_i is finite Galois.

Remark 2.16. Let $\{L_i/K_i\}_{i=0}^n$ be a group preserving chain of base extensions. Then it follows from Proposition 2.5 that $\mathrm{Gal}(L_i/K_i) \cong \mathrm{Gal}(L_j/K_j)$ for $0 \leq i, j \leq n$.

Theorem 2.17. Let K, K' be fields with the same characteristic. Suppose L/K, L'/K' are finite Galois extensions such that $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L'/K')$. Then there exists a group preserving chain of base extensions of length 4 connecting L/K with L'/K'.

Proof. Set $G = \mathrm{Gal}(L/K)$ and let $\mathcal{X} = \{X_\sigma : \sigma \in G\}$ be a set of independent variables. Let G act on $L(\mathcal{X})$ by its action on L and its action on $\mathcal{X}$. The action of G on $L(\mathcal{X})$ is compatible with the action of G on L. Hence from Theorem 2.7 it follows that $L(\mathcal{X})/L(\mathcal{X})^G$ is a base extension of L/K. Let $\mathbb{F}$ be the prime field of K and let G act on $\mathbb{F}(\mathcal{X})$ by its action on $\mathcal{X}$. The action of G on $L(\mathcal{X})$ is compatible with the action of G on $\mathbb{F}(\mathcal{X})$. Hence Theorem 2.7 shows that $L(\mathcal{X})/L(\mathcal{X})^G$ is a base extension of $\mathbb{F}(\mathcal{X})/\mathbb{F}(\mathcal{X})^G$. Let G act on $L'(\mathcal{X})$ by its action on L' and its action on $\mathcal{X}$. Applying the arguments above to $L'(\mathcal{X})$ one obtains, using Proposition 2.5, the following group preserving chain of base extensions of length 4:

$$\{L/K, L(\mathcal{X})/L(\mathcal{X})^G, \mathbb{F}(\mathcal{X})/\mathbb{F}(\mathcal{X})^G, L'(\mathcal{X})/L'(\mathcal{X})^G, L'/K'\}.$$

□

Example 2.18. Let $\mathbb{F}$ be a prime field and let $L/\mathbb{F}$ be a Galois extension such that $\mathrm{Gal}(L/\mathbb{F}) \cong C_4$. Let $\mathbb{F} \subset K \subset L$ be the fixed field of $C_2 \triangleleft C_4$. Then is $K/\mathbb{F}$ is Galois and $C_2 \cong \mathrm{Gal}(L/K) \cong \mathrm{Gal}(K/\mathbb{F})$. From the theorem above it follows that there exists a group preserving chain of base extensions connecting $K/\mathbb{F}$ with L/K of length four. In this example we show that there does not exist a shorter such chain. First note that L/K is not a base extension of K/F hence there does not exist a chain of length one. Using similar arguments as in Example 2.10 it follows that $K/\mathbb{F}$ is not a non-trivial base extension. Suppose that L/K is a base extension of M/N. From $\mathrm{Gal}(K/\mathbb{F}) \cong C_2$ it follows that either L/K is a trivial base extension of M/N or $N = \mathbb{F}$ and $M \cong K$. Since L/K is not a base extension of $K/\mathbb{F}$ it follows that L/K is not a non-trivial base extension of M/N. It follows from this that a chain of length 3 can be shortened using the transitive property of base extensions to a chain of length equal to 2 or 1. Hence to show that there does not exist a chain of length shorter than 4 it suffices to show that there is no chain of length 2. Suppose that M/N is a base extension of L/K and of $K/\mathbb{F}$. Let $\mathrm{Hom}_{\mathbb{F}}(K, M)$ be the set of field homomorphisms $L \to M$ which are the identity on $\mathbb{F}$ and let $\phi \in \mathrm{Hom}_{\mathbb{F}}(K, M)$ be arbitrary. Note that $\mathrm{Aut}_{\mathbb{F}}(M)$ acts transitively on $\mathrm{Hom}_{\mathbb{F}}(K, M)$ by composition. It follows from the fact that $K/\mathbb{F}$ is normal that $\sigma(\phi(K)) = \phi(K)$ for all $\sigma \in \mathrm{Aut}_{\mathbb{F}}(M)$. Let $\psi\colon L \to M$ be as in the definition of a base extension. Note that $\psi|_K \in \mathrm{Hom}_{\mathbb{F}}(K, M)$ and that $\psi(K) \subset N$. Hence it follows that $\phi(K) \subset N$ for all $\phi \in \mathrm{Hom}_{\mathbb{F}}(K, M)$. Therefore M/N cannot be a base extension of $K/\mathbb{F}$. Hence there does not exist a group preserving chain of base extensions connecting $K/\mathbb{F}$ with L/K of length shorter than 4.

3. The Grothendieck group of finite groups

Definition 3.1. Let G be a group. A series

$$\{1\} = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G$$

of subgroups of G is called *subnormal* if $G_i \triangleleft G_{i-1}$ for $0 < i \leq n$.

Definition 3.2. Let

$$(*) \qquad \{1\} = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G$$
$$(**) \qquad \{1\} = H_m \subset H_{m-1} \subset \ldots \subset H_1 \subset H_0 = G$$

be two subnormal series of a group G. The subnormal series $(**)$ is called a *refinement* of $(*)$ if $(**) = (*)$ or $(**)$ is obtained from $(*)$ by insertion of subgroups. The subnormal series $(*)$ and $(**)$ are called *equivalent* if there exists a bijection

$$\sigma\colon \{0, 1, \ldots, n-1\} \to \{0, 1, \ldots, m-1\}$$

such that $G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}$ for each i.

Definition 3.3. A subnormal series

$$\{1\} = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G$$

of a group G is called a *composition series* if each G_{i+1} is a maximal normal subgroup in G_i.

Remark 3.4. A subnormal series

$$\{1\} = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G$$

of a group G is a composition series if and only if G_i/G_{i+1} is simple for all i.

Remark 3.5. Let G be a finite group. Then G has a composition series.

Theorem 3.6 (Jordan-Hölder-Schreier)**.** Let G be a group. Then any two subnormal series of G have refinements that are equivalent. Moreover any two composition series of G are equivalent.

Proof. See [2]. $\square$

Definition 3.7. Let G be a group with a composition series

$$\{1\} = G_n \subset G_{n-1} \subset \ldots \subset G_1 \subset G_0 = G.$$

The factor groups G_i/G_{i+1} are called the *composition factors* of G.

Remark 3.8. From Theorem 3.6 it follows that two composition series of a group G are equivalent. Therefore the composition factors of a group are well-defined.

Definition 3.9. Let $\mathcal{C}$ be the category of finite groups. Let $\mathrm{Ob}(\mathcal{C})$ denote the class of objects of $\mathcal{C}$ and let $\mathrm{Ob}(\mathcal{C})/\cong$ denote the set of isomorphism classes. The *Grothendieck group* $\mathcal{G}$ on $\mathcal{C}$ with respect to short exact sequences is the group generated by $\mathrm{Ob}(\mathcal{C})/\cong$ subject to the relations $[G] = [H][N] \in \mathcal{G}$ if there exists a short exact sequence

$$1 \to H \to G \to N \to 1.$$

Remark 3.10. The Grothendieck group $\mathcal{G}$ satisfies the following universal mapping property. For each group B and each map $\phi\colon \mathrm{Ob}(\mathcal{C})/\cong \to B$ which satisfies $\phi([G]) = \phi([H])\phi([N])$ if there exists as short exact sequence

$$1 \to H \to G \to N \to 1$$

there exists a unique group homomorphism $h\colon \mathcal{G} \to B$ such that $h \circ \mathrm{id}_{\mathrm{Ob}(\mathcal{C})/\cong} = \phi$.

Proposition 3.11. Let B be a group with a map $\psi\colon \mathrm{Ob}(\mathcal{C})/\cong \to B$ that satisfies $\psi([G]) = \psi([H])\psi([N])$ if there exists a short exact sequence

$$1 \to H \to G \to N \to 1.$$

Suppose that B and ψ satisfy the universal mapping property of $\mathcal{G}$. Then there exists a unique group isomorphism $h\colon \mathcal{G} \to B$ such that $h \circ \mathrm{id}_{\mathrm{Ob}(\mathcal{C})/\cong} = \psi$. Moreover h satisfies $h^{-1} \circ \psi = \mathrm{id}_{\mathrm{Ob}(\mathcal{C})/\cong}$.

Proof. Since $\mathcal{G}$ satisfies the universal mapping property there exists a unique group homomorphism $h\colon \mathcal{G} \to B$ such that $h \circ \mathrm{id}_{\mathrm{Ob}(\mathcal{C})/\cong} = \psi$. Furthermore since B and ψ satisfy the universal mapping property there exists a unique group homomorphism $h'\colon B \to \mathcal{G}$ such that $h' \circ \psi = \mathrm{id}_{\mathrm{Ob}(\mathcal{C})/\cong}$. From this it follows that $\psi = h \circ \mathrm{id}_{\mathrm{Ob}(\mathcal{C})/\cong} = (h \circ h') \circ \psi$ hence $h \circ h' = \mathrm{id}_{\mathcal{G}}$ and similarly $h' \circ h = \mathrm{id}_B$. Hence $h' = h^{-1}$. □

Proposition 3.12. Let B be an arbitrary group with a map $\phi\colon (\mathrm{Ob}(\mathcal{C})/\cong) \to B$ such that $\phi([G]) = \phi([H])\phi([N])$ if there exists a short exact sequence

$$1 \to H \to G \to N \to 1.$$

Then the following hold:

(i) $\phi([\{1\}]) = 1 \in B$;

(ii) the image of ϕ generates an abelian subgroup of B;

(iii) let G be a finite group with a subnormal series $\{1\} = G_n \subset \ldots \subset G_1 \subset G_0 = G$ and let $Q_i = G_{i-1}/G_i$. Then the equality $\phi([G]) = \prod_{i=1}^{n} \phi([Q_i])$ holds in B.

Proof. (i). Let G be an arbitrary finite group. Then the following short sequence is exact:

$$1 \to G \xrightarrow{\mathrm{id}} G \to 1 \to 1.$$

Therefore $\phi([G]) = \phi([G])\phi([\{1\}])$ hence $\phi([\{1\}]) = 1 \in B$.
(ii). Let G and H be finite groups. Note that the following short sequences are exact:

$$1 \to G \xrightarrow{g \mapsto (g,1)} G \times H \xrightarrow{(g,h) \mapsto h} H \to 1,$$

$$1 \to H \xrightarrow{h \mapsto (1,h)} G \times H \xrightarrow{(g,h) \mapsto g} G \to 1.$$

Hence it follows that $[G][H] = [G \times H] = [H][G] \in B$.
(iii). Note that for $0 < i \leq n$ the short sequence

$$1 \to G_i \to G_{i-1} \to Q_i \to 1$$

is exact, hence $\phi([Q_i]) = \phi([G_{i-1}])\phi([G_i])^{-1}$ in B. From part (i) and part (ii) it follows that

$$\prod_{i=1}^{n} \phi([Q_i]) = \prod_{i=1}^{n} \left(\phi([G_{i-1}])\phi([G_i])^{-1}\right) = \phi([G_0])\phi([G_n])^{-1} = \phi([G]).$$

□

Theorem 3.13. Let $\mathcal{S} \subset \mathrm{Ob}(\mathcal{C})/\cong$ be the set of isomorphism classes of simple groups. Then $\mathcal{G}$ is the free abelian group on $\mathcal{S}$.

Proof. Let $\mathcal{A}$ be the free abelian group on $\mathcal{S}$. Define the map $\psi\colon (\mathrm{Ob}(\mathcal{C})/\cong) \to \mathcal{A}$ by $\psi([G]) = \prod_{i=1}^{n} [Q_i]$ where $Q_1, \ldots, Q_n$ are the composition factors of G. From Remark 3.8 it follows that ψ is well-defined. Let

$$1 \to H \xrightarrow{f} G \xrightarrow{g} N \to 1$$

be a short exact sequence of finite groups. Then $H \cong f(H) \triangleleft G$ and $N \cong G/f(H)$. Hence $\{1\} \triangleleft H \triangleleft G$ is a subnormal series which can be extended to a composition series

$$\{1\} = G_n \subset G_{n-1} \subset \ldots \subset G_k = f(H) \subset \ldots \subset G_0 = G.$$

Take $Q_i = G_{i-1}/G_i$ for $0 < i \leq n$. Since $\{0\} = G_n \subset \ldots \subset G_k = f(H)$ is a composition series it follows that $Q_{k+1}, \ldots Q_n$ are the composition factors of H. Moreover $Q_1, \ldots, Q_k$ are the composition factors of N. Hence it follows that

$$\psi([G]) = \prod_{i=1}^{n}[Q_i] = \left(\prod_{i=k+1}^{n}[Q_i]\right)\left(\prod_{i=1}^{k}[Q_i]\right) = \psi([H])\psi([N]).$$

Let B be a group and $\phi\colon (\mathrm{Ob}(\mathcal{C})/\cong) \to B$ a map that satisfies $\phi([G]) = \phi([H])\phi([N])$ if there exists a short exact sequence

$$1 \to H \to G \to N \to 1.$$

Define $h\colon \mathcal{S} \to B$ by $h([S]) = \phi([S])$. From Proposition 3.12 it follows that without loss of generality it can be assumed that B is abelian. By the universal mapping property of a free abelian group it follows that h can be extended uniquely to a group homomorphism $\bar{h}\colon \mathcal{A} \to B$. Let $[G] \in \mathrm{Ob}(\mathcal{C})/\cong$ be arbitrary and let $Q_1 \ldots, Q_n$ be the composition factors of G. Then from Proposition 3.12 it follows that

$$\phi([G]) = \prod_{i=1}^{n}\phi([Q_i]) = \prod_{i=1}^{n}\bar{h}([Q_i]) = (\bar{h} \circ \psi)([G]).$$

□

4. Basic degrees

Definition 4.1. Let p be zero or a prime number and let $\mathcal{E}_p$ be the collection of all pairs (K, L) with K a field of characteristic p and L a finite field extension of K. Let A be a multiplicatively written abelian group. A *basic degree* with values in A is a map $d\colon \mathcal{E}_p \to A$ such that:

(i) if $(K, L) \in \mathcal{E}_p$ and $(L, M) \in \mathcal{E}_p$ then $d(M/K) = d(M/L) \cdot d(L/K)$,

(ii) if $(K, L) \in \mathcal{E}_p$ and (K', L') is a base extension of (K, L) then $d(L/K) = d(L'/K')$.

Let $\mathrm{bdeg}(p, A)$ denote the set of basic degrees $d\colon \mathcal{E}_p \to A$.
A basic degree $d\colon \mathcal{E}_p \to A$ is called *universal* if for each multiplicatively written abelian group B the mapping $\mathrm{Hom}(A, B) \to \mathrm{bdeg}(p, B)$ sending f to $f \circ d$ is a bijection.

Remark 4.2. If $d\colon \mathcal{E}_p \to A$ and $d'\colon \mathcal{E}_p \to B$ are two universal basic degrees then there exists a unique group isomorphism $h\colon A \to B$ such that $h \circ d = d'$. Moreover h satisfies $h^{-1} \circ d' = d$.

Example 4.3. Let p be zero or a prime number. Then the following are examples of basic degrees:

(i) $\mathcal{E}_p \to \{1\}, (K, L) \mapsto 1$;

(ii) $\mathcal{E}_p \to (\mathbb{Q}_{>0}, \cdot), (K, L) \mapsto [L : K]$;

(iii) If $d\colon \mathcal{E}_p \to A$ a basic degree and B is a group with a group homomorphism $f\colon A \to B$ then $f \circ d$ is a basic degree.

Proposition 4.4. Let p be zero or a prime number. Then for all $n, m \in \mathbb{Z}_{>0}$ there exists a tower of field extensions $K \subset L \subset M$ such that $\mathrm{Char}\,(K) = p$ and $([L : K]_s, [M : L]_s) = (n, m)$. Moreover if p is prime then for all $n \in \mathbb{Z}_{>0}$ there exists a field extension L/K such that $[L : K]_s = n$ and $[L : K]_i = p$.

Proof. Let $n, m \in \mathbb{Z}_{>0}$ be arbitrary and let X be a variable. Note that $\mathbb{Q}(X^{nm}) \subset \mathbb{Q}(X^m) \subset \mathbb{Q}(X)$ is a tower of separable field extensions such that $[\mathbb{Q}(X^m) : \mathbb{Q}(X^{nm})]_s = n$ and $[\mathbb{Q}(X) : \mathbb{Q}(X^m)]_s = m$. Assume that p is prime. Let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$ and let $F \in \mathrm{Aut}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ be the Frobenius map. From Galois theory it follows that $\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}}_p : F^n(\alpha) = \alpha\}$ is a separable field extension of $\mathbb{F}_p$ of degree n. Hence it follows that $\mathbb{F}_p \subset \mathbb{F}_{p^n} \subset \mathbb{F}_{p^{nm}}$ is a tower of separable field extensions such that $[\mathbb{F}_{p^n} : \mathbb{F}_p]_s = n$ and $[\mathbb{F}_{p^{nm}} : \mathbb{F}_{p^n}]_s = m$. Note that $\mathbb{F}_{p^n}(X^p)/\mathbb{F}_p(X^p)$ is a base extension of $\mathbb{F}_{p^n}/\mathbb{F}_p$ hence $\mathbb{F}_{p^n}(X^p)/\mathbb{F}_p(X^p)$ is a separable extension of degree n. It is clear that $\mathbb{F}_{p^n}(X)/\mathbb{F}_{p^n}(X^p)$ is a purely inseparable field extension such that $[\mathbb{F}_{p^n}(X) : \mathbb{F}_{p^n}(X^p)]_i = p$. Hence it follows that $\mathbb{F}_{p^n}(X)/\mathbb{F}_p(X^p)$ is a field extension such that $[\mathbb{F}_{p^n}(X) : \mathbb{F}_p(X^p)]_s = n$ and $[\mathbb{F}_{p^n}(X) : \mathbb{F}_p(X^p)]_i = p$. □

Theorem 4.5. The basic degree $d\colon \mathcal{E}_0 \to (\mathbb{Q}_{>0}, \cdot)$ given by $d(K, L) \mapsto [L : K]$ is universal.

Proof. Let B be an arbitrary multiplicatively written abelian group and $d' : \mathcal{E}_0 \to B$ an arbitrary basic degree with values in B. Let $(K, L), (K', L') \in \mathcal{E}_0$ be such that $[L : K] = [L' : K']$. Then from Theorem 2.8 it follows that $d'(L/K) = d'(L'/K')$. Define the map $\phi\colon \mathbb{Z}_{>0} \to B$ by $\phi(n) = d'(L/K)$ where $[L : K] = n$. From Proposition 4.4 and the above it follows that ϕ is well-defined and multiplicative hence ϕ can be extended to a group homomorphism $\bar{\phi}\colon \mathbb{Q}_{>0} \to B$. Note that $\bar{\phi}$ is unique since every group homomorphism on $\mathbb{Q}_{>0}$ is uniquely determined by its values on $\mathbb{Z}_{>0}$. Moreover it follows in a straightforward way from the definition of ϕ that $\bar{\phi} \circ d = d'$. This proves that d is universal. □

Notation. Let L/K be a field extension. Then $\mathrm{Sep}_L(K)$ denotes the separable closure of K in L.

Theorem 4.6. Let $p > 0$ be prime and $p^{\mathbb{Z}} = \{p^n : n \in \mathbb{Z}\} \subset \mathbb{Q}_{>0}$. Then the basic degree $d\colon \mathcal{E}_p \to (\mathbb{Q}_{>0}, \cdot) \times p^{\mathbb{Z}}$ given by $d(L/K) = ([L : K]_s, [L : K]_i)$ is universal.

Proof. Let B be an arbitrary multiplicatively written abelian group and $d' : \mathcal{E}_0 \to B$ an arbitrary basic degree with values in B. Let $(K, L), (K', L') \in \mathcal{E}_p$ be such that $[L : K]_s = [L' : K']_s$ and $[L : K]_i = [L' : K']_i$. Then from Theorem 2.8 it follows that $d'(\mathrm{Sep}_L(K)/K) = d'(\mathrm{Sep}_{L'}(K')/K')$. From Corollary 2.13 and Theorem 2.14 it follows that $d'(L/\mathrm{Sep}_L(K)) = d'(L'/\mathrm{Sep}_{L'}(K'))$. Therefore it follows that $d'(L/K) = d'(L'/K')$. Define $\phi\colon \mathbb{Q}_{>0} \times p^{\mathbb{Z}} \to B$ by

$$\phi\,(a/b, p^n) = d'(L_a/K_a)(d'(L_b/K_b))^{-1}(d'(L'/K'))^n$$

where L_a/K_a (resp. L_b/K_b) is a separable field extension of degree a (resp. degree b) and L'/K' is a purely inseparable field extension of degree p. It follows from Proposition 4.4 that ϕ is a well-defined group homomorphism. Let $(K, L) \in \mathcal{E}_p$ be arbitrary. Then from Theorem 2.14 and Corollary 2.13 it follows that if $[L : K]_i = p^n$ then $d'(L/\mathrm{Sep}_L(K)) = d'(L'/K')^n$ where L'/K' is a purely inseparable extension of degree p. Hence the following holds:

$$d'(L/K) = d'(\mathrm{Sep}_L(K)/K)d'(L/\mathrm{Sep}_L(K)) = \phi([L : K]_s, [L : K]_i) = (\phi \circ d)(K, L).$$

Hence ϕ satisfies $\phi \circ d = d'$. It is clear that ϕ is unique. This shows that d is a universal basic degree. □

5. Degrees of field extensions

Definition 5.1. Let p be zero or prime and A be a multiplicatively written abelian group. A *degree* with values in A is a map $d\colon \mathcal{E}_p \to A$ such that:

(i) if $(K,L),(L,M) \in \mathcal{E}_p$ then $d(M/K) = d(M/L) \cdot d(L/K)$;

(ii) if $(K,L) \in \mathcal{E}_p$ is normal and L'/K' is a base extension of L/K then $d(L/K) = d(L'/K')$.

Let $\mathrm{Deg}(p,A)$ denote the set of all degrees $d\colon \mathcal{E}_p \to A$.
A degree $d\colon \mathcal{E}_p \to A$ is called *universal* if for each multiplicatively written abelian group B the mapping $\mathrm{Hom}(A,B) \to \mathrm{Deg}(p,B)$ sending f to $f \circ d$ is a bijection.

Definition 5.2. Let K be a field of characteristic $p > 0$ and let L/K be a field extension. Let $\alpha \in L$. If $\alpha^{p^n} \in K$ for some $n \in \mathbb{Z}_{\geq 0}$ then α is called *purely inseparable*. The *inseparable closure* of K in L is $\mathrm{Ins}_L(K) = \{\alpha \in L : \alpha \text{ is purely inseparable over } K\}$.

Proposition 5.3. Let $K \subset L \subset M$ be a tower of field extensions such that L/K is purely inseparable and M/L is normal. Then is M/K a normal extension and $\mathrm{Aut}_K(M) = \mathrm{Aut}_L(M)$.

Proof. Let $\overline{M}$ be an algebraic closure of M and let $\mathrm{Hom}_K(M,\overline{M})$ be the set of field homomorphism $M \to \overline{M}$ that are the identity on K. Let $\phi \in \mathrm{Hom}_K(M,\overline{M})$ be arbitrary. Let $\alpha \in L$ arbitrary and let $f \in K[X]$ be irreducible such that $f(\alpha) = 0$. Then $f(\phi(\alpha)) = 0$ and since L/K is purely inseparable it follows that $\phi(\alpha) = \alpha$. Hence ϕ is a L-homomorphism and since M/L is normal it follows that $\phi(M) = M$ making M/K normal. Similar argumentation shows that each $\psi \in \mathrm{Aut}_K(M)$ is an L-homomorphism hence $\mathrm{Aut}_K(M) = \mathrm{Aut}_L(M)$. □

Proposition 5.4. Let L/K be an algebraic extension. Then the following hold:

(i) $L = \mathrm{Sep}_L(K)\mathrm{Ins}_L(K)$ if and only if L is separable over $\mathrm{Ins}_L(K)$.

(ii) if L/K is normal then L is separable over $\mathrm{Ins}_L(K)$.

Proof. (i). If $L = \mathrm{Sep}_L(K)\mathrm{Ins}_L(K)$ then L is obtained by adjoining to $\mathrm{Ins}_L(K)$ roots of separable polynomials with coefficients in K, hence by polynomials with coefficients in $\mathrm{Ins}_L(K)$. Conversely if $L/\mathrm{Ins}_L(K)$ is separable then $L/\mathrm{Ins}_L(K)\mathrm{Sep}_L(K)$ is separable. Similarly since $L/\mathrm{Sep}_L(K)$ is purely inseparable so is $L/\mathrm{Ins}_L(K)\mathrm{Sep}_L(K)$. Hence $L/\mathrm{Ins}_L(K)\mathrm{Sep}_L(K)$ is both separable and purely inseparable hence $L = \mathrm{Sep}_L(K)\mathrm{Ins}_L(K)$.
(ii). Let $\alpha \in L\backslash \mathrm{Ins}_L(K)$. Then α is not inseparable over K. Hence the minimal polynomial f of α over K has at least one other distinct root β in an algebraic closure. Since L/K is normal it follows that $\beta \in L$. Note that there exists $\sigma \in \mathrm{Aut}_K(L)$ such that $\sigma(\alpha) = \beta$. Let g be the minimal polynomial of α over $\mathrm{Ins}_L(K)$ and let $\alpha_1, \ldots, \alpha_r$ be the distinct roots of g in an algebraic closure. Note that $r = \prod_{i=1}^{r}(X - \alpha_i)$ is separable and invariant under the action of $\mathrm{Aut}_{\mathrm{Ins}_L(K)}(L)$. Hence $r \in \mathrm{Ins}_L(K)[X]$ and thus $K/\mathrm{Ins}_L(K)$ is obtained by adjoining roots of separable polynomials and therefore is $L/\mathrm{Ins}_L(K)$ separable. □

Theorem 5.5. Let p be zero or a prime number. The map $D_p\colon \mathcal{E}_p \to \mathcal{G}$ given by $D_p(L/K) = [\mathrm{Aut}_K(N)][\mathrm{Aut}_L(N)]^{-1}$, where N is a finite extension of L that is normal over K, is a degree.

Proof. It first needs to be shown that D_p is well-defined. Let $(K, L) \in \mathcal{E}_p$ arbitrary. Let N_1, N_2 be two finite extensions of L that are normal over $\mathrm{Ins}_L(K)$. It follows from Proposition 5.3 that N_1/K and N_2/K are normal hence $M = N_1 \cap N_2$ is normal over K. From the normality of N_i/K, where $i = 1, 2$, and M/K it follows that the short sequences

$$1 \to \mathrm{Aut}_M(N_i) \to \mathrm{Aut}_L(N_i) \xrightarrow{\sigma \mapsto \sigma|_M} \mathrm{Aut}_L(M) \to 1$$
$$1 \to \mathrm{Aut}_M(N_i) \to \mathrm{Aut}_K(N_i) \xrightarrow{\sigma \mapsto \sigma|_M} \mathrm{Aut}_K(M) \to 1$$

are exact. Hence from Proposition 3.12 it follows that for $i = 1, 2$

$$\begin{aligned}[\mathrm{Aut}_K(N_i)][\mathrm{Aut}_L(N_i)]^{-1} &= [\mathrm{Aut}_M(N_i)][\mathrm{Aut}_K(M)][\mathrm{Aut}_L(M)]^{-1}[\mathrm{Aut}_M(N_i)]^{-1} \\ &= [\mathrm{Aut}_K(M)][\mathrm{Aut}_L(M)]^{-1}.\end{aligned}$$

From Proposition 5.3 it follows that D_p is well defined.
Let $(K, L), (L, M) \in \mathcal{E}_p$ be arbitrary and let N be a finite extension of M that is normal over K. Then from the above it follows that:

$$\begin{aligned}D_p(L/K) \cdot D_p(M/L) &= [\mathrm{Aut}_K(N)][\mathrm{Aut}_L(N)]^{-1} \cdot [\mathrm{Aut}_L(N)][\mathrm{Aut}_M(N)]^{-1} \\ &= [\mathrm{Aut}_K(N)][\mathrm{Aut}_M(N)]^{-1} = D_p(M/K).\end{aligned}$$

Suppose that L/K is normal and that L'/K' is a base extension of L/K. From Proposition 5.4 it follows that $L/\mathrm{Ins}_L(K)$ is separable. Let $\psi \colon L \to L'$ be as in the definition of a base extension. It is clear that $\psi(\mathrm{Ins}_L(K)) \subset \mathrm{Ins}_{L'}(K')$. Hence $L'/\mathrm{Ins}_{L'}(K')$ is a base extension of $L/\mathrm{Ins}_L(K)$. Therefore it follows from proposition 5.3 that it is no loss of generality to assume that L/K is separable. Hence L/K is Galois and from Proposition 2.5 it follows that $D_p(L/K) = D_p(L'/K')$. Hence D_p is a degree. $\square$

Definition 5.6. Let p be zero or a prime number. We call the degree D_p given in Theorem 5.5 the *Galois degree*.

Example 5.7. Let p be zero or prime. Then the following are degrees:

(i) Every basic degree $d \colon \mathcal{E}_p \to A$ is a degree;

(ii) The Galois degree D_p;

(iii) Assume p is prime. Then the map $D \colon \mathcal{E}_p \to \mathcal{G} \times p^{\mathbb{Z}}$ given by $D(L/K) = (D_p(L/K), [L : K]_i)$ is a degree.

The second statement is proven below.

Proposition 5.8. Let p be prime or zero. Then the following hold:

(i) For all finite groups G and H there exists a tower of Galois extensions $K \subset L \subset M$ such that $\mathrm{Char}\,(K) = p$ and $\mathrm{Gal}(M/L) \cong G$, $\mathrm{Gal}(L/K) \cong H$ and $\mathrm{Gal}(M/K) \cong G \times H$.

(ii) Let G be a finite group with composition factors $Q_1, \ldots, Q_n$. Then there exists a tower of Galois extensions $L_0 \subset L_1 \subset \ldots \subset L_{n-1} \subset L_n$ and a permutation $\sigma \in S_n$ such that $\mathrm{Char}\,(L_0) = p$ and $\mathrm{Gal}(L_n/L_0) = G$ and $\mathrm{Gal}(L_i/L_{i-1}) \cong Q_{\sigma(i)}$.

(iii) If p is prime, G, H are finite groups and $n, m \in \mathbb{Z}_{\geq 0}$. Then there exists a tower of field extensions $K \subset L \subset M$ such that $\mathrm{Aut}_K(L) \cong H$, $\mathrm{Aut}_M(L) \cong G$, $[L : K]_i = p^n$, $[M : L]_i = p^m$ and $\mathrm{Aut}_K(M) \cong G \times H$.

Proof. (i). Let $\mathbb{F}$ be the prime field of characteristic p and let $\mathcal{X} = \{X_\sigma : \sigma \in G \times H\}$ be a set of independent variables and let $G \times H$ act on $\mathcal{X}$ by ${}^\tau X_\sigma = X_{\tau\sigma}$ for all $\tau, \sigma \in G \times H$. Take $M = \mathbb{F}(\mathcal{X})$ and let $G \times H$ act on M trough its action on $\mathcal{X}$. Note that $G \times \{1\} \triangleleft G \times H$ hence from Galois theory it follows that

$$M^{G\times H} \subset M^{G\times\{1\}} \subset M$$

is a tower of Galois extensions with

$$\mathrm{Gal}(M/M^{G\times\{1\}}) \cong G \quad \text{and} \quad \mathrm{Gal}(M^{G\times\{1\}}/M^{G\times H}) \cong H.$$

(ii). Let $\{1\} = G_n \subset \ldots \subset G_1 \subset G_0 = G$ be a composition series of G. Then by Theorem 3.6 there exists a permutation $\sigma \in S_n$ such that $G_i/G_{i+1} \cong Q_{\sigma(i)}$. From part (i) it follows that there exists a Galois extension L/K such that $\mathrm{Char}\,(K) = p$ and $\mathrm{Gal}(L/K) \cong G$. For $0 \le i \le n$ define $L_i = L^{G_i}$, then $L_0 = K$ and $L_n = L$. Since G_i is normal in G_{i-1} it follows from Galois theory that L_i/L_{i-1} is Galois with Galois group isomorphic to G_i/G_{i-1}.
(iii). Let $K' \subset L' \subset M'$ be a tower of Galois extensions such that $\mathrm{Gal}(L'/K') \cong H$, $\mathrm{Gal}(M'/L') \cong G$ and $\mathrm{Gal}(M'/K') \cong G \times H$. The exists of such a tower follows from part (i). Let X and Y be two independent variables. Define $K = K'(X^{p^n}, Y^{pm})$, $L = L'(X, Y^{p^m})$ and $M = M'(X, Y)$. Then $[M : L]_i = p^m$ and $[L : K]_i = p^n$. Note that $L/K'(X, Y^{p^m})$ is a base extension of M'/K'. Hence from Proposition 2.5 it follows that $L/K(X, Y^{p^m})$ is Galois with $\mathrm{Gal}(L/K(X, Y^{p^m}) \cong \mathrm{Gal}(L'/K')$. Note that $K(X, Y^{p^m}) = \mathrm{Ins}_L(K)$. Hence from Proposition 5.4 it follows that L/K is normal. Therefore $\mathrm{Aut}_K(L) = \mathrm{Aut}_{\mathrm{Ins}_L(K)}(L) \cong H$. Applying the same arguments to M/L and M/K yields $\mathrm{Aut}_L(M) = \mathrm{Aut}_{\mathrm{Ins}_M(L)}(M) \cong G$ and $\mathrm{Aut}_K(M) = \mathrm{Aut}_{\mathrm{Ins}_M(K)}(M) \cong G \times H$. $\square$

Example 5.9. In this example it will be shown that the Galois degree D_p, where p is zero or a prime number, is not a basic degree. Hence it will be shown that not every degree is a basic degree. Consider the groups A_5 and $G = C_3 \times C_4 \times C_5$ and note that $\#A_5 = \#G = 60$. Let $(K, L), (K', L') \in \mathcal{E}_p$ be Galois extensions such that $\mathrm{Gal}(L/K) \cong A_5$ and $\mathrm{Gal}(L'/K') \cong G$. Proposition 5.8 shows that such L/K and L'/K' exist. Suppose that D_p is a basic degree. Then from Theorem 2.8 it follows that $D_p(L/K) = D_p(L'/K')$. Theorem 4.33 of [3] states that A_n is simple for $n \ge 5$. From this and Theorem 3.13 it follows that $[A_5] \ne [G] = [C_3][C_4][C_5] \in \mathcal{G}$ hence $D_p(L/K) \ne D_p(L'/K')$ contradicting D_p being a basic degree.

Definition 5.10. A Galois extension L/K is called *simple* if $\mathrm{Gal}(L/K)$ is simple.

Notation. Let L/K be a finite separable extension. Then $\mathrm{GCl}_K(L)$ denotes a Galois closure of L/K.

Theorem 5.11. The Galois degree D_0 is universal.

Proof. Let B be an arbitrary abelian group and let $d' \colon \mathcal{E}_0 \to B$ be an arbitrary degree. Let $(K, L), (K', L') \in \mathcal{E}_0$ such that $\mathrm{Gal}(\mathrm{GCl}_K(L)/K) \cong \mathrm{Gal}(\mathrm{GCl}_{K'}(L')/K')$ and $\mathrm{Gal}(\mathrm{GCl}_K(L)/L) \cong \mathrm{Gal}(\mathrm{GCl}_{K'}(L')/L')$. Then it follows from Theorem 2.17 that $d'(L/K) = d'(L'/K')$. Let $Q_1, \ldots, Q_n$ be the composition factors of $\mathrm{Gal}(\mathrm{GCl}_K(L)/K)$ and let $(K_i, L_i) \in \mathcal{E}_0$ be Galois such that $\mathrm{Gal}(L_i/K_i) \cong Q_i$. Then from Proposition 5.8 and Theorem 2.17 one obtains that $d'(\mathrm{GCl}_K(L)/K) = \prod_{i=1}^n d'(L_i/K_i)$. From this it follows that d' is uniquely determined by its restriction to

$$\mathcal{S}_0 = \{(K, L) \in \mathcal{E}_0 : L/K \text{ is simple Galois}\} \subset \mathcal{E}_0.$$

Hence it suffices to show that there exists a unique group homomorphism $\phi \colon \mathcal{G} \to B$ such that $\phi \circ D_0|_{\mathcal{S}_0} = d'|_{\mathcal{S}_0}$. Define $\psi \colon \mathcal{S} \to B$ by $\psi([S]) = d'(L/K)$ where $(K, L) \in$

$\mathcal{S}_0$ such that $\mathrm{Gal}(L/K) \in [S]$. From Theorem 2.17 it follows that ψ is well-defined. Note that the following diagram commutes.

$$\begin{tikzcd} & \mathcal{S} \arrow[dr, "\psi"] & \\ \mathcal{S}_0 \arrow[ur, "(K,L)\mapsto[\mathrm{Gal}(L/K)]"] \arrow[rr, "d'|_{\mathcal{S}_0}"'] & & B \end{tikzcd}$$

From the universal mapping property of free abelian groups follows that ψ uniquely extends to a group homomorphism $\phi\colon \mathcal{G} \to B$ that satisfies $\phi \circ D_0|_{\mathcal{S}_0} = d'|_{\mathcal{S}_0}$. This shows that the Galois degree D_0 is universal. $\square$

Theorem 5.12. Let p be prime. Then the degree $D\colon \mathcal{E}_p \to \mathcal{G} \times p^{\mathbb{Z}}$ given by $D(L/K) = (D_p(L/K), [L:K]_i)$ is universal.

Proof. Let B be an arbitrary multiplicatively written abelian group and let $d' : \mathcal{E}_p \to B$ be an arbitrary degree. Let $(K,L), (K',L') \in \mathcal{E}_p$. If $[L:K]_i = [L':K']_i$ then it follows from Theorem 2.14 and Corollary 2.13 and the fact that purely inseparable extensions are normal that $d'(L/\mathrm{Sep}_L(K)) = d'(L'/\mathrm{Sep}_{L'}(K'))$. If

$$\mathrm{Gal}(\mathrm{GCl}_K(\mathrm{Sep}_L(K))/K) \cong \mathrm{Gal}(\mathrm{GCl}_{K'}(\mathrm{Sep}_{L'}(K'))/K') \text{ and}$$
$$\mathrm{Gal}(\mathrm{GCl}_K(\mathrm{Sep}_L(K))/\mathrm{Sep}_L(K)) \cong \mathrm{Gal}(\mathrm{GCl}_{K'}(\mathrm{Sep}_{L'}(K'))/\mathrm{Sep}_{L'}(K'))$$

then it follows from Theorem 2.17 that $d'(\mathrm{Sep}_L(K)/K) = d'(\mathrm{Sep}_{L'}(K')/K')$. Hence if (K,L) and (K',L') satisfy both the above conditions then $d'(L/K) = d'(L'/K')$. Define $\phi\colon \mathrm{Ob}(\mathcal{C})/{\cong} \times \{p^n : n \in \mathbb{Z}_{\geq 0}\} \to B$ by $\phi([G], p^n) = d'(L/K)$ where L/K is a field extension such that $[L:K]_i = p^n$ and $\mathrm{Sep}_L(K)/K$ is Galois with $\mathrm{Gal}(\mathrm{Sep}_L(K)/K) \in [G]$. It follows from the above and Proposition 5.8 that ϕ is well-defined and multiplicative. Hence it follows that ϕ extends to a group homomorphism $\bar{\phi}\colon \mathcal{G} \times p^{\mathbb{Z}} \to B$. Note that $\bar{\phi}$ is unique since $\mathrm{Ob}(\mathcal{C})/{\cong} \times \{p^n : n \in \mathbb{Z}_{\geq 0}\}$ generates $\mathcal{G} \times p^{\mathbb{Z}}$. It remains to show that $\bar{\phi}$ satisfies $\bar{\phi} \circ D = d'$. Let $(F,E) \in \mathcal{E}_p$ be arbitrary. Then the following holds

$$\begin{aligned} d'(E/F) &= d'(\mathrm{Sep}_E(F)/F) \cdot d'(E/\mathrm{Sep}_E(F)) \\ &= d'(\mathrm{GCl}_F(\mathrm{Sep}_E(F))/F)(d'(\mathrm{GCl}_F(\mathrm{Sep}_E(F))/\mathrm{Sep}_E(F)))^{-1} d'(E/\mathrm{Sep}_E(F)) \\ &= \bar{\phi}([\mathrm{Gal}(\mathrm{GCl}_F(\mathrm{Sep}_E(F))/F)][\mathrm{Gal}(\mathrm{GCl}_F(\mathrm{Sep}_F(E))/\mathrm{Sep}_F(E))]^{-1}, \\ &\qquad [E:F]_i) \\ &= \bar{\phi}(D_p(E/F), [E:F]_i) = (\bar{\phi} \circ D)(E/F). \end{aligned}$$

This shows that the degree D is universal. $\square$

References

[1] M. F. Atiyah and I. G. MacDonald. *Introduction To Commutative Algebra.* Addison-Wesley series in mathematics. Westview Press, 1994. First published in 1969.

[2] B. Baumslag. *A Simple Way of Proving the Jordan-Hölder-Schreier Theorem.* The American Mathematical Monthly, Vol. 113, No. 10, Dec. 2006.

[3] James S. Milne. Group theory (v3.13), 2013.
Available at www.jmilne.org/math/.

Index