

Michaël Vullers

Universal Degrees of Field Extensions

Bachelorscriptie, 06 juni 2013

Scriptiebegeleider: prof.dr. H.W. Lenstra



Mathematisch Instituut, Universiteit Leiden

CONTENTS

Introduction.....	3
1. Linear disjointness	5
2. Base extensions	8
3. The Grothendieck group of finite groups.....	12
4. Basic degrees.....	15
5. Degrees of field extensions.....	17
References	20
Index	21

INTRODUCTION

Let \mathcal{C} be the category of finite groups. Let $\text{Ob}(\mathcal{C})$ denote the class of objects of \mathcal{C} and let $\text{Ob}(\mathcal{C})/\cong = \{[G] : G \in \text{Ob}(\mathcal{C})\}$ 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 $\text{Ob}(\mathcal{C})/\cong$ subject to the relations $[G] = [H][N] \in \mathcal{G}$ if there exists a short exact sequence

$$1 \rightarrow H \rightarrow G \rightarrow N \rightarrow 1.$$

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 $D_p: \mathcal{E}_p \rightarrow \mathcal{G}$ be given by $D_p(L/K) = [\text{Aut}_K(N)][\text{Aut}_L(N)]^{-1}$, 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 $\psi: L \rightarrow L'$ 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 $d: \mathcal{E}_p \rightarrow A$ 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 $\text{Deg}(p, A)$ denote the set of all degrees $d: \mathcal{E}_p \rightarrow A$. A degree $d: \mathcal{E}_p \rightarrow A$ is called *universal* if for each abelian group B the mapping $\text{Hom}(A, B) \rightarrow \text{Deg}(p, B)$ 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 $D_0: \mathcal{E}_0 \rightarrow \mathcal{G}$ 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 $D: \mathcal{E}_p \rightarrow \mathcal{G} \times p^{\mathbb{Z}}$ 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 $\text{bdeg}(p, A)$ denote the set of all basic degrees $d: \mathcal{E}_p \rightarrow A$ and call a basic degree $d: \mathcal{E}_p \rightarrow A$ *universal* if for each abelian group B the map $\text{Hom}(A, B) \rightarrow \text{bdeg}(p, B)$ 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 $d: \mathcal{E}_0 \rightarrow (\mathbb{Q}_{>0}, \cdot)$ given by $d(L/K) = [L : K]$ is universal.

Theorem 6. Let p be prime. Then the basic degree $d: \mathcal{E}_p \rightarrow (\mathbb{Q}_{>0}, \cdot) \times p^{\mathbb{Z}}$ 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 $R \otimes_K S \rightarrow L$ 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 $x \in (R \cap S) \setminus K$. 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 $\iota: R \otimes_K S \rightarrow L$ the images of $1 \otimes x$ and $x \otimes 1$ are the same. Hence ι is not injective. \square

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 $\iota: R \otimes_K S \rightarrow L$ be the canonical ring homomorphism. Note that $R' \otimes_K S' \subset R \otimes_K S$ and the canonical ring homomorphism $\kappa: R' \otimes_K S' \rightarrow L$ 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 . \square

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 $f_j: R_j \rightarrow \varinjlim R_i$. 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 $\psi_i: R_i \rightarrow C$ such that $\psi_i = \psi_j \circ f_{ij}$ if $i \leq j$. Then there exists a unique K -algebra homomorphism $\psi: \varinjlim R_i \rightarrow C$ 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 $\{R_i \otimes_K S, f_{ij} \otimes \text{id}_S\}$ and for each $i \in I$ let $\psi_i: R_i \otimes_K S \rightarrow L$ be the canonical ring homomorphism. Note that ψ_i satisfies the condition of second property hence one obtains a unique K -algebra homomorphism $\psi: \varinjlim R_i \otimes_K S \rightarrow L$ satisfying for each $i \in I$ the equality $\psi \circ (f_i \otimes \text{id}_S) = \psi_i$. Note that $f_i \otimes \text{id}_S$ 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. \square

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 $x_1, \dots, x_n \in E$ are K -linearly independent and $y_1, \dots, y_m \in F$ 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 $r_1, \dots, r_n, r \in R$ and $s_1, \dots, s_m, s \in S$, 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 $\text{Frac}(R), \text{Frac}(S)$ 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 $\text{Frac}(R) \otimes_K \text{Frac}(S)$ 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 $T = \text{Frac}(R) \otimes_K \text{Frac}(S) \supset K$. 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 $\text{Frac}(R)$ and $\text{Frac}(S)$. Note that the induced map $\iota: T \rightarrow E$ is the quotient map $T \rightarrow T/\mathfrak{m}$. 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 $\text{Frac}(R) \otimes_K \text{Frac}(S)$ is a field. Let A be an arbitrary non-trivial ring, then any ring homomorphism $\text{Frac}(R) \otimes_K \text{Frac}(S) \rightarrow A$ is injective. Hence any ring homomorphism from $\text{Frac}(R) \otimes_K \text{Frac}(S)$ to a non-trivial K -algebra is injective. Since any field extension of K is a non-trivial K -algebra it follows that $\text{Frac}(R)$ and $\text{Frac}(S)$ 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 $\iota: E \otimes_K F \rightarrow EF$ 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 $\lambda_x: E \otimes_K F \rightarrow E \otimes_K F$ be given by $\lambda_x(y) = xy$. Since $E \otimes_K F$ is a domain λ_x is injective and since $E \otimes_K F$ is finitely generated as an F -vector space it follows that λ_x is surjective. From this it immediately follows that $E \otimes_K F$ 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 over 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 $K(X) \rightarrow K(a)$ and $K(X) \rightarrow K(b)$ be given by $X \rightarrow a$ and $X \rightarrow b$ respectively. Let $\phi: E \otimes_K F \rightarrow E \otimes_{K(X)} F$ 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 $E \rightarrow L'$ and $F \rightarrow L'$ 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 $\text{Gal}(E/(E \cap F)) \cong \text{Gal}(EF/F)$;
- (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

$$\phi: \text{Gal}(EF/F) \rightarrow \text{Gal}(E/(E \cap F)), \psi \mapsto \psi|_E.$$

Note that ϕ is well defined since each $\psi \in \text{Gal}(EF/F)$ is the identity on F and so it is the identity on $E \cap F$. By definition $\psi|_F = \text{id}_F$ hence if $\psi|_E = \text{id}_E$ then $\psi = \text{id}_{EF}$. Hence ϕ is injective. Note that $E^{\text{im}(\phi)} = E \cap F$ hence $\text{im}(\phi) = \text{Gal}(E/(E \cap F))$. 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 $\text{Ind}_G(H)$ 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 $\text{Ind}_G(H \cap I) \leq \text{Ind}_G(H) \cdot \text{Ind}_G(I)$ 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 $\text{Ind}_{HI}(I)$ is well-defined. First we show $\text{Ind}_{HI}(I) = \text{Ind}_H(H \cap I)$. Let H act on G/I by left multiplication and let $x = I/I \in G/I$. Note

that $H \cap I = \text{Stab}(x)$ 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 $\text{Ind}_{HI}(I) = \text{Ind}_H(H \cap I)$. To prove the statement observe:

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

□

Proposition 1.12. Let L/K be finite Galois with $G = \text{Gal}(L/K)$ 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 $[L^S : K] = \text{Ind}_G(S)$ for each subgroup S of G . Hence L^H and L^I are K -linearly disjoint if and only if $\text{Ind}_G(H \cap I) = \text{Ind}_G(H) \cdot \text{Ind}_G(I)$ 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 $\psi: L \rightarrow L'$ 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 $L \otimes_K K' \rightarrow L'$ 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 $\iota: L \otimes_K M \rightarrow LM$ 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 an 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 $\text{Gal}(L/K) \cong \text{Gal}(L'/K')$.

Proof. Since L'/K' is a base extension of L/K there is an field homomorphism $\psi: L \rightarrow L'$. 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 $\phi: G \rightarrow H$ be a group homomorphism and $\psi: Y \rightarrow X$ 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 $G \subset \text{Aut}(F)$ and $S \subset \text{Aut}(E)$ be finite subgroups and let $T \subset S$ be a subgroup. Let $\phi: G \rightarrow S$ be a group homomorphism and let $\psi: E \rightarrow F$ 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 $H = \text{Stab}(T/T) \subset G$. 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 $\psi: E \rightarrow \psi(E)$ 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 .

$$\begin{array}{ccccccc}
& & T & & \phi(H) & & H \\
& & \cap & & \cap & & \cap \\
S/T \curvearrowright S & \xleftarrow{\supset} & \phi(G) & \xleftarrow{\phi} & G & \xleftarrow{\supset} & G \\
\circlearrowleft & & \circlearrowleft & & \circlearrowleft & & \circlearrowleft \\
E & \xrightarrow{\subset} & E & \xrightarrow{\psi} & \psi(E) & \xrightarrow{\subset} & F \\
| & & | & & | & & | \\
E^T & & E^{\phi(H)} & & \psi(E)^H & & F^H \\
| & & | & & | & & | \\
E^S & & E^{\phi(G)} & & \psi(E)^G & & F^G
\end{array}$$

\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 $G = \text{Gal}(M/K)$. Let $\text{Hom}_K(L, M)$ denote the set of field homomorphism $L \rightarrow M$ that are the identity on K . Note that G acts naturally on $\text{Hom}_K(L, M)$ by composition. Let $H \subset G$ be the stabilizer of the inclusion $\iota \in \text{Hom}_K(L, M)$ of L into M , then $M^H = L$. Let $\mathcal{X} = \{X_\alpha : \alpha \in \text{Hom}_K(L, M)\}$ 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 $\text{Hom}_K(L, M)$ 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 $\text{Hom}_K(L, M)$ the group G is a subgroup of S . Since G acts transitively on $\text{Hom}_K(L, M)$ 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:

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

Repeating the argument above for L'/K' yields a similar chain of base extensions of length two. Note that $n = \#\text{Hom}_K(L, M) = \#\text{Hom}_{K'}(L', M')$ 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 $\phi: S \rightarrow S'$ 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:

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

□

Definition 2.9. A base extension L'/K' of L/K is called *trivial* if there exists a field isomorphism $\psi: L \rightarrow L'$ 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 5th and an 8th 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 $\text{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong C_4$ and $\text{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong V_4$, 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 $V_4 \not\cong C_4$ it follows from Proposition 2.5 that $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is not a base extension 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 $\mathbb{Q}(\zeta_8)/\mathbb{Q}$. From 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 $V_4 \cong \text{Gal}(L/K) \cong C_4$. 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, \dots, 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 . \square

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 $K = L_n \subset L_{n-1} \subset \dots \subset L_1 \subset L_0 = L$ 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 $\phi: \mathbb{F}_p(T) \rightarrow L$ be the field homomorphism such that $\phi(T) = \alpha$ and let $\phi': \mathbb{F}_p(T) \rightarrow L'$ 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' :

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

\square

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 $\text{Gal}(L_i/K_i) \cong \text{Gal}(L_j/K_j)$ 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 $\text{Gal}(L/K) \cong \text{Gal}(L'/K')$. Then there exists a group preserving chain of base extensions of length 4 connecting L/K with L'/K' .

Proof. Set $G = \text{Gal}(L/K)$ 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 $\text{Gal}(L/\mathbb{F}) \cong C_4$. Let $\mathbb{F} \subset K \subset L$ be the fixed field of $C_2 \triangleleft C_4$. Then K/\mathbb{F} is Galois and $C_2 \cong \text{Gal}(L/K) \cong \text{Gal}(K/\mathbb{F})$. 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/\mathbb{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 $\text{Gal}(K/\mathbb{F}) \cong C_2$ 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 $\text{Hom}_{\mathbb{F}}(K, M)$ be the set of field homomorphisms $L \rightarrow M$ which are the identity on \mathbb{F} and let $\phi \in \text{Hom}_{\mathbb{F}}(K, M)$ be arbitrary. Note that $\text{Aut}_{\mathbb{F}}(M)$ acts transitively on $\text{Hom}_{\mathbb{F}}(K, M)$ by composition. It follows from the fact that K/\mathbb{F} is normal that $\sigma(\phi(K)) = \phi(K)$ for all $\sigma \in \text{Aut}_{\mathbb{F}}(M)$. Let $\psi: L \rightarrow M$ be as in the definition of a base extension. Note that $\psi|_K \in \text{Hom}_{\mathbb{F}}(K, M)$ and that $\psi(K) \subset N$. Hence it follows that $\phi(K) \subset N$ for all $\phi \in \text{Hom}_{\mathbb{F}}(K, M)$. 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

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

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

Definition 3.2. Let

$$\begin{aligned} (*) \quad & \{1\} = G_n \subset G_{n-1} \subset \dots \subset G_1 \subset G_0 = G \\ (**) \quad & \{1\} = H_m \subset H_{m-1} \subset \dots \subset H_1 \subset H_0 = G \end{aligned}$$

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

$$\sigma: \{0, 1, \dots, n-1\} \rightarrow \{0, 1, \dots, m-1\}$$

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

Definition 3.3. A subnormal series

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

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

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

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]. □

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

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

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 $\text{Ob}(\mathcal{C})$ denote the class of objects of \mathcal{C} and let $\text{Ob}(\mathcal{C})/\cong$ 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 $\text{Ob}(\mathcal{C})/\cong$ subject to the relations $[G] = [H][N] \in \mathcal{G}$ if there exists a short exact sequence

$$1 \rightarrow H \rightarrow G \rightarrow N \rightarrow 1.$$

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

$$1 \rightarrow H \rightarrow G \rightarrow N \rightarrow 1$$

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

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

$$1 \rightarrow H \rightarrow G \rightarrow N \rightarrow 1.$$

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

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

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

$$1 \rightarrow H \rightarrow G \rightarrow N \rightarrow 1.$$

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 $\{1\} = G_n \subset \dots \subset G_1 \subset G_0 = G$ 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:

$$1 \rightarrow G \xrightarrow{\text{id}} G \rightarrow 1 \rightarrow 1.$$

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:

$$\begin{aligned} 1 \rightarrow G &\xrightarrow{g \mapsto (g,1)} G \times H \xrightarrow{(g,h) \mapsto h} H \rightarrow 1, \\ 1 \rightarrow H &\xrightarrow{h \mapsto (1,h)} G \times H \xrightarrow{(g,h) \mapsto g} G \rightarrow 1. \end{aligned}$$

Hence it follows that $[G][H] = [G \times H] = [H][G] \in B$.

(iii). Note that for $0 < i \leq n$ the short sequence

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

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

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

\square

Theorem 3.13. Let $\mathcal{S} \subset \text{Ob}(\mathcal{C})/\cong$ 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 $\psi: (\text{Ob}(\mathcal{C})/\cong) \rightarrow \mathcal{A}$ by $\psi([G]) = \prod_{i=1}^n [Q_i]$ where Q_1, \dots, Q_n are the composition factors of G . From Remark 3.8 it follows that ψ is well-defined. Let

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

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

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

Take $Q_i = G_{i-1}/G_i$ for $0 < i \leq n$. Since $\{0\} = G_n \subset \dots \subset G_k = f(H)$ is a composition series it follows that Q_{k+1}, \dots, Q_n are the composition factors of H . Moreover Q_1, \dots, 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 $\phi: (\text{Ob}(\mathcal{C})/\cong) \rightarrow B$ a map that satisfies $\phi([G]) = \phi([H])\phi([N])$ if there exists a short exact sequence

$$1 \rightarrow H \rightarrow G \rightarrow N \rightarrow 1.$$

Define $h: \mathcal{S} \rightarrow B$ 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 $\bar{h}: \mathcal{A} \rightarrow B$. Let $[G] \in \text{Ob}(\mathcal{C})/\cong$ be arbitrary and let Q_1, \dots, 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 $d: \mathcal{E}_p \rightarrow A$ 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 $\text{bdeg}(p, A)$ denote the set of basic degrees $d: \mathcal{E}_p \rightarrow A$.

A basic degree $d: \mathcal{E}_p \rightarrow A$ is called *universal* if for each multiplicatively written abelian group B the mapping $\text{Hom}(A, B) \rightarrow \text{bdeg}(p, B)$ sending f to $f \circ d$ is a bijection.

Remark 4.2. If $d: \mathcal{E}_p \rightarrow A$ and $d': \mathcal{E}_p \rightarrow B$ are two universal basic degrees then there exists a unique group isomorphism $h: A \rightarrow B$ 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) $\mathcal{E}_p \rightarrow \{1\}, (K, L) \mapsto 1$;
- (ii) $\mathcal{E}_p \rightarrow (\mathbb{Q}_{>0}, \cdot), (K, L) \mapsto [L : K]$;
- (iii) If $d: \mathcal{E}_p \rightarrow A$ a basic degree and B is a group with a group homomorphism $f: A \rightarrow B$ 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 $\text{Char}(K) = p$ 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 $F \in \text{Aut}_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)$ 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 $[\mathbb{F}_{p^n}(X) : \mathbb{F}_p(X^p)]_i = p$. \square

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

Proof. Let B be an arbitrary multiplicatively written abelian group and $d': \mathcal{E}_0 \rightarrow B$ 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 $\phi: \mathbb{Z}_{>0} \rightarrow B$ 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 $\bar{\phi}: \mathbb{Q}_{>0} \rightarrow B$. 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. \square

Notation. Let L/K be a field extension. Then $\text{Sep}_L(K)$ 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 $d: \mathcal{E}_p \rightarrow (\mathbb{Q}_{>0}, \cdot) \times p^{\mathbb{Z}}$ given by $d(L/K) = ([L : K]_s, [L : K]_i)$ is universal.

Proof. Let B be an arbitrary multiplicatively written abelian group and $d': \mathcal{E}_0 \rightarrow B$ 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 $d'(\text{Sep}_L(K)/K) = d'(\text{Sep}_{L'}(K')/K')$. From Corollary 2.13 and Theorem 2.14 it follows that $d'(L/\text{Sep}_L(K)) = d'(L'/\text{Sep}_{L'}(K'))$. Therefore it follows that $d'(L/K) = d'(L'/K')$. Define $\phi: \mathbb{Q}_{>0} \times p^{\mathbb{Z}} \rightarrow B$ 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 $d'(L/\text{Sep}_L(K)) = d'(L'/K')^n$ where L'/K' is a purely inseparable extension of degree p . Hence the following holds:

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

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

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 $d: \mathcal{E}_p \rightarrow A$ 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 $\text{Deg}(p, A)$ denote the set of all degrees $d: \mathcal{E}_p \rightarrow A$.

A degree $d: \mathcal{E}_p \rightarrow A$ is called *universal* if for each multiplicatively written abelian group B the mapping $\text{Hom}(A, B) \rightarrow \text{Deg}(p, B)$ 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 $\text{Ins}_L(K) = \{\alpha \in L : \alpha \text{ is purely inseparable over } K\}$.

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 M/K is a normal extension and $\text{Aut}_K(M) = \text{Aut}_L(M)$.

Proof. Let \overline{M} be an algebraic closure of M and let $\text{Hom}_K(M, \overline{M})$ be the set of field homomorphism $M \rightarrow \overline{M}$ that are the identity on K . Let $\phi \in \text{Hom}_K(M, \overline{M})$ 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 $\psi \in \text{Aut}_K(M)$ is an L -homomorphism hence $\text{Aut}_K(M) = \text{Aut}_L(M)$. \square

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

- (i) $L = \text{Sep}_L(K)\text{Ins}_L(K)$ if and only if L is separable over $\text{Ins}_L(K)$.
- (ii) if L/K is normal then L is separable over $\text{Ins}_L(K)$.

Proof. (i). If $L = \text{Sep}_L(K)\text{Ins}_L(K)$ then L is obtained by adjoining to $\text{Ins}_L(K)$ roots of separable polynomials with coefficients in K , hence by polynomials with coefficients in $\text{Ins}_L(K)$. Conversely if $L/\text{Ins}_L(K)$ is separable then $L/\text{Ins}_L(K)\text{Sep}_L(K)$ is separable. Similarly since $L/\text{Sep}_L(K)$ is purely inseparable so is $L/\text{Ins}_L(K)\text{Sep}_L(K)$. Hence $L/\text{Ins}_L(K)\text{Sep}_L(K)$ is both separable and purely inseparable hence $L = \text{Sep}_L(K)\text{Ins}_L(K)$.

(ii). Let $\alpha \in L \setminus \text{Ins}_L(K)$. 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 $\sigma \in \text{Aut}_K(L)$ such that $\sigma(\alpha) = \beta$. Let g be the minimal polynomial of α over $\text{Ins}_L(K)$ and let $\alpha_1, \dots, \alpha_r$ 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 $\text{Aut}_{\text{Ins}_L(K)}(L)$. Hence $r \in \text{Ins}_L(K)[X]$ and thus $L/\text{Ins}_L(K)$ is obtained by adjoining roots of separable polynomials and therefore is $L/\text{Ins}_L(K)$ separable. \square

Theorem 5.5. Let p be zero or a prime number. The map $D_p: \mathcal{E}_p \rightarrow \mathcal{G}$ given by $D_p(L/K) = [\text{Aut}_K(N)][\text{Aut}_L(N)]^{-1}$, 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 $\text{Ins}_L(K)$. 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

$$\begin{aligned} 1 \rightarrow \text{Aut}_M(N_i) \rightarrow \text{Aut}_L(N_i) \xrightarrow{\sigma \mapsto \sigma|_M} \text{Aut}_L(M) \rightarrow 1 \\ 1 \rightarrow \text{Aut}_M(N_i) \rightarrow \text{Aut}_K(N_i) \xrightarrow{\sigma \mapsto \sigma|_M} \text{Aut}_K(M) \rightarrow 1 \end{aligned}$$

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

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

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:

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

Suppose that L/K is normal and that L'/K' is a base extension of L/K . From Proposition 5.4 it follows that $L/\text{Ins}_L(K)$ is separable. Let $\psi: L \rightarrow L'$ be as in the definition of a base extension. It is clear that $\psi(\text{Ins}_L(K)) \subset \text{Ins}_{L'}(K')$. Hence $L'/\text{Ins}_{L'}(K')$ is a base extension of $L/\text{Ins}_L(K)$. 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 $d: \mathcal{E}_p \rightarrow A$ is a degree;
- (ii) The Galois degree D_p ;
- (iii) Assume p is prime. Then the map $D: \mathcal{E}_p \rightarrow \mathcal{G} \times p^{\mathbb{Z}}$ 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 $\text{Char}(K) = p$ and $\text{Gal}(M/L) \cong G$, $\text{Gal}(L/K) \cong H$ and $\text{Gal}(M/K) \cong G \times H$.
- (ii) Let G be a finite group with composition factors Q_1, \dots, Q_n . Then there exists a tower of Galois extensions $L_0 \subset L_1 \subset \dots \subset L_{n-1} \subset L_n$ and a permutation $\sigma \in S_n$ such that $\text{Char}(L_0) = p$ and $\text{Gal}(L_n/L_0) = G$ and $\text{Gal}(L_i/L_{i-1}) \cong Q_{\sigma(i)}$.
- (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 $\text{Aut}_K(L) \cong H$, $\text{Aut}_M(L) \cong G$, $[L:K]_i = p^n$, $[M:L]_i = p^m$ and $\text{Aut}_K(M) \cong G \times H$.

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 through 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

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

(ii). Let $\{1\} = G_n \subset \dots \subset G_1 \subset G_0 = G$ 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 $\text{Char}(K) = p$ and $\text{Gal}(L/K) \cong G$. For $0 \leq i \leq n$ 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 $\text{Gal}(L'/K') \cong H$, $\text{Gal}(M'/L') \cong G$ and $\text{Gal}(M'/K') \cong G \times H$. The existence of such a tower follows from part (i). Let X and Y be two independent variables. Define $K = K'(X^{p^n}, Y^{p^m})$, $L = L'(X, Y^{p^m})$ 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 $\text{Gal}(L/K(X, Y^{p^m})) \cong \text{Gal}(L'/K')$. Note that $K(X, Y^{p^m}) = \text{Ins}_L(K)$. Hence from Proposition 5.4 it follows that L/K is normal. Therefore $\text{Aut}_K(L) = \text{Aut}_{\text{Ins}_L(K)}(L) \cong H$. Applying the same arguments to M/L and M/K yields $\text{Aut}_L(M) = \text{Aut}_{\text{Ins}_M(L)}(M) \cong G$ and $\text{Aut}_K(M) = \text{Aut}_{\text{Ins}_M(K)}(M) \cong G \times H$. \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 $\text{Gal}(L/K) \cong A_5$ and $\text{Gal}(L'/K') \cong G$. 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 $n \geq 5$. From this and Theorem 3.13 it follows that $[A_5] \neq [G] = [C_3][C_4][C_5] \in \mathcal{G}$ hence $D_p(L/K) \neq D_p(L'/K')$ contradicting D_p being a basic degree.

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

Notation. Let L/K be a finite separable extension. Then $\text{GCl}_K(L)$ 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 $d' : \mathcal{E}_0 \rightarrow B$ be an arbitrary degree. Let $(K, L), (K', L') \in \mathcal{E}_0$ such that $\text{Gal}(\text{GCl}_K(L)/K) \cong \text{Gal}(\text{GCl}_{K'}(L')/K')$ and $\text{Gal}(\text{GCl}_K(L)/L) \cong \text{Gal}(\text{GCl}_{K'}(L')/L')$. Then it follows from Theorem 2.17 that $d'(L/K) = d'(L'/K')$. Let Q_1, \dots, Q_n be the composition factors of $\text{Gal}(\text{GCl}_K(L)/K)$ and let $(K_i, L_i) \in \mathcal{E}_0$ be Galois such that $\text{Gal}(L_i/K_i) \cong Q_i$. Then from Proposition 5.8 and Theorem 2.17 one obtains that $d'(\text{GCl}_K(L)/K) = \prod_{i=1}^n d'(L_i/K_i)$. 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 $\phi : \mathcal{G} \rightarrow B$ such that $\phi \circ D_0|_{\mathcal{S}_0} = d'|_{\mathcal{S}_0}$. Define $\psi : \mathcal{S} \rightarrow B$ by $\psi([S]) = d'(L/K)$ where $(K, L) \in$

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

$$\begin{array}{ccc} & \mathcal{S} & \\ \begin{array}{c} \nearrow \\ (K, L) \mapsto [\text{Gal}(L/K)] \end{array} & & \searrow \psi \\ \mathcal{S}_0 & \xrightarrow{d'|_{\mathcal{S}_0}} & B \end{array}$$

From the universal mapping property of free abelian groups follows that ψ uniquely extends to a group homomorphism $\phi: \mathcal{G} \rightarrow B$ 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 $D: \mathcal{E}_p \rightarrow \mathcal{G} \times p^{\mathbb{Z}}$ 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 $d': \mathcal{E}_p \rightarrow B$ 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 $d'(L/\text{Sep}_L(K)) = d'(L'/\text{Sep}_{L'}(K'))$. If

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

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

then it follows from Theorem 2.17 that $d'(\text{Sep}_L(K)/K) = d'(\text{Sep}_{L'}(K')/K')$. Hence if (K, L) and (K', L') satisfy both the above conditions then $d'(L/K) = d'(L'/K')$. Define $\phi: \text{Ob}(\mathcal{C})/\cong \times \{p^n : n \in \mathbb{Z}_{\geq 0}\} \rightarrow B$ by $\phi([G], p^n) = d'(L/K)$ where L/K is a field extension such that $[L : K]_i = p^n$ and $\text{Sep}_L(K)/K$ is Galois with $\text{Gal}(\text{Sep}_L(K)/K) \in [G]$. 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 $\bar{\phi}: \mathcal{G} \times p^{\mathbb{Z}} \rightarrow B$. Note that $\bar{\phi}$ is unique since $\text{Ob}(\mathcal{C})/\cong \times \{p^n : n \in \mathbb{Z}_{\geq 0}\}$ 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

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

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

- C_4 , 10
- D_p , 3
- $K(\mathcal{X})$, 9
- V_4 , 10
- $\text{GCl}_K(L)$, 19
- $\text{Ind}_G(H)$, 7
- $\text{Ins}_L(K)$, 17
- $\text{Sep}_L(K)$, 16

- base extension, 3, 8
 - chain of, 8
 - connected, 8
 - group preserving, 11
 - length, 8
 - trivial, 10

- compatible action, 9
- composition factors, 13
- composition series, 13

- degree, 3, 17
 - basic degree, 4, 15
 - universal, 4, 15
 - Galois, 3
 - universal, 3, 17

- Galois degree, 18
- Grothendieck group \mathcal{G} , 3, 13

- inseparable closure, 17

- linearly disjoint, 5
 - everywhere, 6
 - somewhere, 6

- purely inseparable, 17

- simple Galois, 19
- subnormal series, 12
 - equivalent, 13
 - refinement, 13