Simple Extensions

Theorem. Let K be a finite-dimensional extension of F. Then K is a simple extension of F if and only if there are only finite number of intermediate fields.

proof. (if part) Assume that F is finite. Then K is also finite. The multiplicative group of nonzero elements of K is cyclic. Any generator of this cyclic group will generate K over F.

Suppose that F is infinite. Pick an element u in K such that $[F(u):F]$ is as large as possible. We claim that $K = F(u)$. Suppose the contrary and pick $v \in K \setminus F(u)$. Since F is infinite and there are only finitely many intermediate fields, the number of extensions of F of the form $F(u+\alpha v)$ where $\alpha \in F$ must be finite. This gives that there exist distinct $\alpha, \beta \in F$ with $F(u+\alpha v) = F(u+\beta v)$. Thus $F(u+\alpha v)$ contains both $u+\alpha v$ and $u+\beta v$, and so $(\alpha-\beta)v$, hence v and also u. It follows that $[F(u+\alpha v):F] > [F(u):F]$, a contradiction.

(Only if part) Assume that $K = F(u)$. Let f be the minimal polynomial of u over F. Let L be an interme-

diate field and let g be the minimal polynomial of u over L. Say

$$g = x^r + a_1 x^{r-1} + \cdots + a_r.$$

Since g is also minimal polynomial of u over $F(a_1, \ldots, a_r)$, we have $[K : F(a_1, \ldots, a_r)] = r$. We also know that $L \supseteq F(a_1, \ldots, a_r)$ and $[K : L] = r$. This yields $L = F(a_1, \ldots, a_r)$. Thus we may conclude that L is uniquely determined by g, which is a divisor of f. Since there are only a finite number of monic divisors of f, we have the result.

Theorem. *Any finite-dimensional separable extension E of a field F is a simple extension.*

proof. Let K be a normal closure of E over F. By the Galois correspondence, it is immediate that there are only a finite number of fields between F and K. Hence the same is true between F and E. Now the result follows from the above theorem.

Separability

Definition. Let F be a field of characteristic p. An element u is purely inseparable over F if for some k, $u^{p^k} \in F$. A field K containing F is purely inseparable over F if every element of K is purely inseparable over F.

Throughout this section, F denotes a field of characteristic p, where p is a prime number. Recall that separability comes for free over fields of characteristic zero! That's why we think of only fields of nonzero characteristic.

Theorem. If an element u is both separable and purely inseparable over F, then it lies in F.

proof. Let f be the minimal polynomial of u over F. Then f has distinct roots (in a splitting field). On the other hand, f is a divisor of a polynomial $x^{p^k} - a = (x-u)^{p^k}$ which has all its roots equal. Hence f is linear and u lies in F.

Theorem. If u is algebraic over F, then u^{p^n} is separable over F for some n.

proof. We argue by induction on the degree of u over F. If u is separable, then we are thorough. Otherwise, the minimal polynomial of u over F is actually a polynomial in x^p, whence u^p has lower degree over F than u does. By

induction, some p^k-th power of u^p is separable over F, i.e., $u^{p^{k+1}}$ is separable over F.

Theorem Let E be a finite-dimensional extension of F. Then

(1) There exists a unique largest subfield K separable over F,

(2) There exists a unique largest subfield L purely inseparable over F,

(3) $K \cap L = F$,

(4) E is purely inseparable over K,

(5) E is separable over L if and only if $KUL = E$, where KUL stands for the smallest subfield of E containing both K and L,

(6) If E is a splitting field over F, then $KUL = E$; also, E is normal over L, K is normal over F, and the Galois groups of E/L and K/F are isomorphic.

proof. (1) Take K to be the set of all elements of E that are separable over F. Then K is a subfield of E (why?) and of course it is the unique largest separable subfield.

(2) Take L to be the set of all purely inseparable elements. Then M is a subfield (why?) with the desired property.

(3) The elements of $K \cap L$ are both separable and purely inseparable over F, and so they must lie in F.

(4) Let u be any element of E. Then some u^{p^n} is separable over F, hence lies in K. This shows that E is purely inseparable over K.

(5) Suppose first that E is separable over L. Then E is separable also over KUL, and by (4) E is purely inseparable over KUL. Hence $E = KUL$.

Conversely, suppose $E = KUL$. If $u_1, \ldots, u_n$ are any generators of K over F, then $E = L(u_1, \ldots, u_n)$ and E is separable over L. (see exercise 3)

(6) Let L_0 be the fixed subfield of E under automorphisms of E/F. We claim that $L_0 = L$. First suppose $u \in L$. Then u satisfies a polynomial equation over F of the form $x^{p^n} - a$ which has all its roots equal. Hence u cannot be moved by an automorphism and $u \in L_0$. Suppose $u \in L_0$ and let f be the minimal polynomial of u over F. If v is another root of f, then $v \in E$ (since E is a splitting field over F, by assumption), and there is an automorphism of E/F sending u into v. It follows that all the roots of f are equal and then that u is purely inseparable over F (see Exercise 4 below!)

We have thus proved $L = L_0$, i.e., E is normal over L. By (5), $KUL = E$. Let τ be any automorphism of E/L. τ must send K onto itself for separable elements go into separable elements. By

restricting τ to K, we get an automorphism of K/F. The resulting homomorphism from the Galois group of E/L to the Galois group of K/F is onto (since E is a splitting field also over K) and one-to-one for if τ is in the kernel it leaves both K and L elementwise fixed and hence also $E = K \cup L$. Finally, K is normal over F, since $K \cap L = F$ and only elements of L are fixed under all automorphisms of E/F. This completes the proof of the theorem.

Exercise 3. (i) Show that if $u_1, \ldots, u_n$ are separable over F, then $F(u_1, \ldots, u_n)$ is separable over F.
(ii) Let E/F be an extension of fields. Then show that the subset K of E consisting of all elements which are separable over F is a subfield of E containing F.
(iii) For an extension E/F, show that the subset L of E consisting of all elements which are purely inseparable over F is a subfield of E containing F.

Exercise 4. Let f be an irreducible polynomial over F and suppose that (in a splitting field) f has all its roots equal. Show that the characteristic of F must be $p \neq 0$, and f must have the form $x^{p^n} - a$.

Theorem. (Transitivity of separability) If $F \subset E \subset K$, E is separable over F, and K is separable over E,

(all extensions finite-dimensional), then K is separable over F.

proof. Let P denote the maximal separable subfield of K, regarded as an extension field of F. Of course $P \supseteq E$. By (4) of the above theorem K is purely inseparable over P. But K is also separable over P, since it is separable over E. Hence $K = P$.

Question. When does the field F have the property that every finite-dimensional extension of F is separable?

We give an answer to this question in the next theorem. But, before, we need to make a definition.

Definition. A field F of characteristic $p \neq 0$ is perfect if every element of F is a p-th power in F.

Theorem. F is perfect if and only if every finite-dimensional extension of F is separable over F.

proof. Suppose that the extensions of F are separable. If an element $a \in F$ has no p-th root in F we form $F(u)$ with u a root of $x^p - a$. Then the minimal polynomial of u over F (which is, in fact, $x^p - a$) has all its roots equal. So, u is not separable, a contradiction.

Conversely, suppose that F is perfect. Let u be algebraic

over F and f its minimal polynomial. If u is not separable, then f is actually a polynomial in x^p. By extracting the p-th root of each coefficient of f, we can write f itself as a p-th power, contradicting the irreducibility of f.

Algebraically Closed Fields and Algebraic Closure

A field K is said to be algebraically closed if every polynomial over K of degree ≥ 1 has a root in K.

Theorem. Let F be a field. Then there exists an algebraically closed field containing F (as a subfield).

proof. We first construct an extension K of F in which every polynomial over F of degree ≥ 1 has a root. One can proceed as follows (Artin):

To each polynomial $f \in F[x]$ of degree ≥ 1 we associate a letter X_f and let S be the set of all such letters X_f. We form the polynomial ring $F[S]$, and claim that the ideal generated by all the polynomials $f(X_f)$ in $F[S]$ is not the unit ideal. If it is, then there is a finite combination of elements in our ideal which is equal to 1:

$$g_1 f_1(X_{f_1}) + \cdots + g_n f_n(X_{f_n}) = 1$$

with $g_i \in F[S]$. For simplicity, write X_i instead of X_{f_i}. The polynomials g_i will involve actually only a finite number of variables, say $X_1, \ldots, X_N$ (with $N \geq n$). Our relation then reads

$$\sum_{i=1}^{n} g_i(X_1, \ldots, X_N) f_i(X_i) = 1.$$

Let E be a finite extension in which each polynomial $f_1, \ldots, f_n$ has a root, say α_i is a root of f_i in E, for $i = 1, \ldots, n$. Let $\alpha_i = 0$ for $i > n$. Substitute α_i for X_i in our relation. We get $0 = 1$, contradiction.

Let $\mathfrak{M}$ be a maximal ideal containing the ideal generated by all the polynomials $f(X_f)$ in $F[S]$. Then $F[S]/\mathfrak{M}$ is a field containing a copy of F, in which every polynomial $f \in F[X]$ has a root.

Inductively, we can form a sequence of fields

$$K_1 \subset K_2 \subset \ldots \subset K_n \subset \ldots$$

such that every polynomial over K_n of degree ≥ 1 has a root in K_{n+1}. Let K be the union of all fields K_n, $n = 1, 2, \ldots$. Then K is naturally a field and every polynomial in $K[X]$ of degree ≥ 1 has a root in K, as desired.

Corollary. Let F be a field. There exists an extension which is algebraic over F and algebraically closed.

proof. Let K be an extension of F which is algebraically closed and let C be the union of all subextensions of K, which are algebraic over F. Clearly C is a field, (Why?) which is algebraic over F. Let $f \in C[X]$. Since $C[X] \subseteq K[X]$ and K is algebraically closed, f has a root $\alpha \in K$. Since α is algebraic over C and C is algebraic over F. It follows that

$\alpha \in C$, and so C is algebraically closed.

Exercise. Let K/F be an extension of fields. Show that the union of all subextensions of K, which are algebraic over F, is also a field which is algebraic over F.

Remarks.

(1) Observe that if K is an algebraically closed field and $f \in K[X]$ has degree ≥ 1, then there exists $c \in K$ and $\alpha_1, \ldots, \alpha_n \in K$ such that $f(X) = c(X - \alpha_1) \ldots (X - \alpha_n)$. [Use induction!]

(2) If L is a field algebraic over an algebraically closed field F, then $L = F$.

Exercise. Prove part (2) of above remarks.

Theorem. Let F be a field, K an algebraic extension of F, and $\sigma : F \longrightarrow L$ an embedding of F into an algebraically closed field L. Then there exists an extension of σ to an embedding of K into L. If K is algebraically closed and L is algebraic over σF, then any such extension of σ is an isomorphism of K onto L.

proof. Let $\mathcal{S}$ be the set of all pairs (E, τ) where E

is a subfield of K containing F, and τ is an extension of σ to an embedding of E into L. If (E, τ) and (E', τ') are such pairs, we write $(E, \tau) \leq (E', \tau')$ if $E \subseteq E'$ and $\tau'|_E = \tau$. Note that S is not empty [it contains (F, σ)], and contains a maximal element, say (M, λ), by Zorn's Lemma. We claim that $M = K$. Otherwise, there exists $\alpha \in K \setminus M$. Since α is algebraic over F (and hence over M) λ has an extension to $M(\alpha)$, thereby contradicting the maximality of (M, λ). This proves that there exists an extension of σ to K. We denote this extension again by σ.

If K is algebraically closed, and L is algebraic over σF, then σK is algebraically closed and L is algebraic over σK, hence $L = \sigma K$.

Corollary. Let F be a field and let C, C' be algebraic extensions of F. Assume that C, C' are algebraically closed. Then there exists an isomorphism $\tau : C \longrightarrow C'$ of C onto C' that leaves F fixed elementwise.

We see that an algebraically closed and algebraic extension of F is determined up to an isomorphism. Such an extension will be called an algebraic closure of F, and we frequently denote it by $\bar{F}$.

In the following exercise we give some alternative ways for probing the existence and uniqueness of the algebraic closure.

Exercise.

(1) Prove that if K is an algebraic extension of F with the property that every polynomial with coefficients in F factors completely in K, then K is algebraically closed.

(2) Let $\{f_\lambda\}$ be a well-ordering of the irreducible polynomials over a field F. Define

$$K_\lambda := \begin{cases} \text{a splitting field of } K_\alpha, & \text{if } \lambda = \alpha + 1 \\ \bigcup_{\alpha<\lambda} K_\alpha & \text{, if } \lambda \text{ is a limit ordinal} \end{cases}$$

Prove that $\bigcup K_\lambda$ is an algebraic closure of F.

(3) Let F be a field, $\{f_\alpha\}$ a set of polynomials with coefficients in F. A field $K \supseteq F$ is said to be a splitting field of $\{f_\alpha\}$ over F if each f_α factors completely in K and K can be obtained from F by adjoining the roots of the f_α's. Prove that K is a splitting field of any set of polynomials over F if and only if whenever an irreducible polynomial over F has a root in K, it factors

completely in K. (In other words, generalize the corresponding theorem given for the characterization of finite-dimensional splitting fields.)

(4) Prove that if K is an algebraic closure of F, then it is a splitting field over F of all polynomials over F, or of all irreducible polynomials over F.

(5) Let F and F_0 be fields and $\sigma : F \longrightarrow F_0$ an isomorphism. Show that σ extends to an isomorphism of any algebraic closure of F onto any algebraic closure of F_0.