Fields

Victoria Noquez

March 19, 2009

§5.1 Basics

Definition 1. A *field* K is a commutative non-zero ring ($0 \neq 1$) such that any $x \in K$, $x \neq 0$, has a unique inverse x^{-1} such that $xx^{-1} = x^{-1}x = 1$.

Definition 2. A *field homomorphism* $f : K \to K'$ is just a ring homomorphism. Note that f is necessarily injective, since if $x \in K \setminus 0$, $f(x) \cdot f(x^{-1}) = 1 \Rightarrow f(x) \neq 0$.

Remark 1. Every field K is a domain, that is, for every $a, b \in K$, if $ab = 0$, then $a = 0$ or $b = 0$. More generally, any subring of a field is a domain.

Definition 3. If R is a domain and $S = R \setminus \{0\}$, $K = S^{-1}R$ is called the *field of fractions* of R.

Definition 4. An *extension* L/K means $K \subset L$ is a subfield of the field L. A *subextension* or *intermediate extension* of L/K is a subfield M of L which contains K. We denote this $L/M/K$.

Proposition 1. *Let R be principal (PID). Let $p \in R$ be a prime element. Then R/pR is a field.*

Proof. Let $a \in R$ such that $\overline{a} \neq 0$ in R/pR. This means that p does not divide a in R, so $\gcd(a, p) = 1$. By Bézout's lemma, there are $b, c \in R$ such that $ba + cp = 1$, so in R/pR, $\overline{b} \cdot \overline{a} + 0 = 1$, which means that $\overline{b}\overline{a} = 1$, so $\overline{a} \in (R/pR)^{\times}$. Hence, since every non-zero element has a multiplicative inverse, R/pR is a field. □

Corollary 2. *Let K be a field. Let $P \in K[T]$ be an irreducible polynomial. Then $K[T]/PK[T]$ is a field.*

Proof. $R = K[T]$ is a PID, which means that P is prime. □

Definition 5. The *characteristic* of a field K, $char(K) \in \{0\} \cup \{p | p \text{ prime}\}$ is defined by $char(K) \cdot \mathbb{Z} = ker(\phi : \mathbb{Z} \to K)$ where ϕ is defined by $1 \mapsto 1$. There are two possible cases here. If $char(K) = 0$, then for every $n \in \mathbb{Z} \setminus 0$, $n \cdot 1_k \neq 0$ in K, which means that that $\mathbb{Q} \hookrightarrow K$ uniquely (for $m \neq 0$) by $\frac{n}{m} \mapsto (n \cdot 1_k) \cdot (m \cdot 1_k)^{-1}$. In this case, K is an extension of $\mathbb{Q}$. If $char(K) = p > 0$ for some prime p, then $\alpha : \mathbb{Z} \to K$ induces $\overline{\alpha} : \mathbb{Z}/p\mathbb{Z} \to K$, so this is a map from $\mathbb{F}_p \to K$.

Remark 2. If L/K, then $char(L) = char(K)$.

Corollary 3. *If $char(K) \neq char(L)$ then there is no field homomorphism from $K \to L$ (since field homomorphisms must be injective).*

Proposition 4. *For a field K, $char(K) = 0$ if and only if K is an extension of $\mathbb{Q}$. $char(K) = p > 0$ if and only if K is an extension of $\mathbb{F}_p$.*

Proof. Obvious from the above remarks. $\square$

Definition 6. The *degree* of an extension L/K is the dimension of L as a K vector space, which belongs to $\mathbb{N} \cup \{\infty\}$, denoted $[L : K]$. If $M/L/K$ is an extension, then the degree of M/K, $[M : K]$ is equal to $[M : L][L : K]$.

Definition 7. An extension L/K is *finite* if the degree $[L : K] < \infty$.

Proposition 5. *If K is a finite field then $char(K) = p > 0$ and K has p^n elements where $n = [K : \mathbb{F}_p]$.*

Proof. $char(K) = 0$ if and only if $\mathbb{Q} \hookrightarrow K$ which implies that K is infinite. So we know that if $char(K) = p$, $K/\mathbb{F}_p$. As an $\mathbb{F}_p$ vector space, $K \cong (\mathbb{F}_p)^n$ (since it is finite) for $n = dim_{\mathbb{F}_p}(K)$, so $\#(K) = p^n$. $\square$

Notation: If L/K is an extension and $E \subset L$, recall that $K[E]$ is the smallest subring of L containing K and E, which is equal to the set of all polynomials (over K) evalutaed at elements of E. We now let $K(E)$ denote the smallest subfield of L containing K and E. This is equal to the field of fractions of $K[E]$.

Definition 8. If L/K is an extension, L is a *finitely generated extension* of K if there exists a finite $E \subset L$ such that $L = K(E)$.

Note that a finitely generated extension is different than a finite extension. For example, $K(T)$ is a finitely generated extension of K, but is not a finite extension of K.

Definition 9. Let L/K be an extension. Let M_1, M_2 be two subextensions. $M_1M_2 = K(M_1 \cup M_2)$ is a subextension of L/M_i for $i = 1, 2$, and hence, of L/K.

$$
\begin{tikzcd}
& L \arrow[d, dash] \arrow[ddl, dash] \arrow[ddr, dash] & \\
& M_1M_2 \arrow[dl, dash] \arrow[dr, dash] & \\
M_1 \arrow[dr, dash] & & M_2 \arrow[dl, dash] \\
& K &
\end{tikzcd}
$$

M_1M_2 is the *composite* of M_1 and M_2.

In this definition, we could replace K with the characteristic field ($\mathbb{Q}$ if $char L = 0$ and $\mathbb{F}_p$ if $char L = p > 0$).

§5.2 Algebraic Extension

Definition 10. Let L/K be an extension. Let $x \in L$. x is *algebraic over* K if there exists $P \in K[T]$ such that $P \neq 0$ and $P(x) = 0$. WLOG, we can choose P to be monic, so this is equivalent to saying that there exists $a_1, \ldots, a_d \in K$ such that $x^d + a_1 x^{d-1} + \ldots + a_d = 0$ (in L).

Definition 11. An extension L/K is *algebraic* if every $x \in L$ is algebraic over K.

A finite extension L/K is algebraic, since for $x \in L$, $1, x, x^2, \ldots, x^n, \ldots$ cannot be linearly independent over K, so x is algebraic over K.

Definition 12. Let $x \in L$ be algebraic over K. The *minimal polynomial of x over K*, $P \in K[T]$, is the unique monic polynomial such that $Ann_{K[T]}(x) = P \cdot K[T]$, where $Ann_{K[T]}(x) = \{Q \in K[T] | Q(x) = 0\}$ is an ideal of $K[T]$. Since $K[T]$ is a PID, there is a generator of $Ann_{K[T]}(x)$ which is unique up to association, so by choosing P to be monic, it is unique. In other words, $P(x) = 0$ and for every $Q \in K[T]$ such that $Q(x) = 0$, $P|Q$ (so when P is monic, it is unique).

Proposition 6. *Let L/K be an extension. Let $x \in L$ be algebraic over K. Let $P \in K[T]$ be the minimal polynomial of X.*

1. *P is irreducible.*
2. *$K[x] = K(x) \cong K[T]/P$.*

Proof.

1. If $P_1P_2(x) = 0$ then $P_1(x)P_2(x) = 0$ in L, so since L is a field, and thus, a domain, $P_1(x) = 0$ or $P_2(x) = 0$, so $P|P_1P_2 \Rightarrow P|P_1$ or $P|P_2$. Thus, P is prime, which means that it is irreduicble since $K[T]$ is a domain.
2. The natural evaluation at x, $K[T] \to K[x]$ is surjective with kernel $Ann_{K[T]}(x) = P \cdot K[T]$. So, since ring homomorphisms from fields to rings are necessarily injective, we have an isomorphism, $K[T]/P \xrightarrow{\sim} K[x]$ (since $K[T]/P$ is a field). Thus, $K[x]$ is a field, so $K[x] = K(x)$.

□

Definition 13. If L/K is an extension, the *degree* of an algebraic element $x \in L$ (over K), $[K(x) : K]$ is the degree of the minimal polynomial of x over K.

Proposition 7. *Let L/K be an extension and let $x \in L$. x is algebraic over K if and only if there exists a subextension $L/M/K$, $M \subset L$ such that $x \in M$ and M/K is finite.*

Proof. $\Leftarrow$: Let $x \in M/K$. Since M/K is finite, x is algebraic over K.
$\Rightarrow$: Let $M = K(x)$. □

Proposition 8. *Let L/K be an extension and let $x_1, \ldots, x_n \in L$ be algebraic over K. Then $K[x_1, \ldots, x_n] = K(x_1, \ldots, x_n)$ and $K(x_1, \ldots, x_n)/K$ is an algebraic, finite extension.*

Proof. First, suppose $n = 1$. Then by Proposition 6, $K(x_1) = K[x_1]$. Clearly $K(x_1)/K$ is algebraic and finite. Now suppose the proposition holds for some fixed arbitrary $n \geq 1$. Then $K(x_1, \ldots, x_{n+1}) = K(x_1, \ldots, x_n)(x_{n+1})$. By the induction hypothesis, $K(x_1, \ldots, x_n) =$

$K[x_1, \ldots, x_n]$. Since x_{n+1} is algebraic over K, it is algebraic over $M = K(x_1, \ldots, x_n)$. Thus, $M[x_{n+1}] = M(x_{n+1})$. So $K[x_1, \ldots, x_{n+1}] = K[x_1, \ldots, x_n][x_n] = K(x_1, \ldots, x_n)(x_{n+1}) = K(x_1, \ldots, x_{n+1})$.

Finally,

$$\begin{array}{c} K[x_1, \ldots, x_{n+1}] \\ \Big| \\ K[x_1, \ldots, x_n] \\ \Big| \\ \vdots \\ \Big| \\ K[x_1] \\ \Big| \\ K \end{array}$$

is a finite tower of finite extensions, so $[K(x_1, \ldots, x_{n+1}) : K]$ is finite. Hence, by induction, the claim holds for all n. $\square$

Corollary 9. *If L/K is an extension and $x, y \in L$ are algebraic over K, then $x + y$, xy, and $\frac{x}{y}$ (if $y \neq 0$) are algebraic. Thus, $\{x \in L | x \text{ is algebraic over } K\} \subset L$ is a subfield of L.*

Proposition 10. *If L/K is an algebraic extension and M/L is an algebraic extension, then M/K is algebraic.*

Proof. Let $x \in M$ be given. x satisfies a polynomial equation with coefficients in L, so there are $y_1, \ldots, y_n \in L$ such that x is algebraic over $K(y_1, \ldots, y_n)$ (take y_i's to be the coefficients of the minimal polynomial of x in $L[T]$). Each y_i is algebraic over K, so $K(y_1, \ldots, y_n) = K[y_1, \ldots, y_n]$ is a finite extension of K, which means that $[K(y_1, \ldots, y_n, x) : K(y_1, \ldots, y_n)]$ is finite, and $[K(y_1, \ldots, y_n) : K]$ is finite, and thus, x is algebraic over K. $\square$

Definition 14. Let L/K be an extension. If $x \in L$ is not algebraic over K it is *transcendental* over K.

Proposition 11. *If L/K is an extension and $x \in L$ is transcendental over K, then if $Q \in K[T]$ is such that $Q(x) = 0$, then $Q = 0$. This is equivalent to saying that $K \subset K(T) \cong K(x) \subset L$ where $K(T) \cong K(x)$ is a K-isomorphism.*

§5.3 Remarks on ruler and compass constructions

The idea here is to take a set of "known" points in $\mathbb{R}^2$, typically we begin with $\mathbb{Z}^2$, from which we can get $\mathbb{Q}^2$, and then try to construct new points with an (unmarked) ruler and a compass.

With the ruler we are able to draw a line through two known points and with the compass we can draw a circle with a known center through a known point (or with a known radius).

Definition 15. The points of intersection of any two distinct lines or circles drawn using the ruler and compass are said to be *constructible.* A point $r \in \mathbb{R}^2$ is said to be constructible from an initial set of points P_0 if there is a finite sequence $r_1, \ldots, r_n = r$ of points of $\mathbb{R}^2$ such that for each $j = 1, \ldots, n$, the point r_j is constructible in one step from the set $P_0 \cup \{r_0, \ldots, r_{j-1}\}$.

To formalize this idea in terms of field extensions, we begin with $K_0 \subset \mathbb{R}$ to be the field generated by the x and y coordinates of each of the points in P_0, then for $j > 0$, $K_j = K_{j-1}(x_j, y_j)$ where r_j is the point (x_j, y_j). Note that we are not adjoining the point $(x_j, y_j) \in \mathbb{R}^2$, we are adjoining each of the elements of $\mathbb{R}$, x_j and y_j.

Thus, we have a tower of subfields $K_0 \subset K_1 \subset \ldots \subset K_n \subset \mathbb{R}$.

Lemma 12. *x_j and y_j are zeros in K_j of a quadratic polynomial in K_{j-1}.*

Proof. There are three cases to consider: when a line meets a circle, when a line meets a line, and when a circle meets a circle. Let $A = (p, q)$, $B = (r, s)$ and $C = (t, u)$ be points in K_{j-1} and draw the line AB and the circle with center C and radius w where $w^2 \in K_{j-1}$ (since we can construct this distance using the coordinates of the center and a point on the circle which are in K_{j-1} using Pythagoras). The equation of the line AB is $\frac{x-p}{r-p} = \frac{y-q}{s-q}$ and the equation of the cirle is $(x-t)^2 + (y-u)^2 = w^2$. Combining these equations gives us

$(x-t)^2 + (\frac{(s-q)}{(r-p)}(x-p) + q - u)^2 = w^2$

so the x-coordinates of the intersection points X and Y are zeros of quadratic polynomials over K_{j-1}, as are the y-coordinates.

Now let $D = (v, z)$. The equation of the line CD is $\frac{x-t}{v-t} = \frac{y-u}{z-u}$, so combining this with the equation of the line AB gives us x and y in terms of $p, q, r, s, t, u, v, z \in K_{j-1}$, and thus, $x, y \in K_{j-1}$. So, x and y are solutions of the quadratic equations $(T-x)^2$ and $(T-y)^2$ in $K_{j-1}[T]$ respectively.

Finally, let $A = (a, b)$, $C = (c, d)$ and consider the circles $(x-a)^2 + (y-b)^2 = r^2$ and $(x-c)^2 + (y-d)^2 = s^2$ where $a, b, c, d, s^2, r^2 \in K_{j-1}$. Combining these equations gives us the line $(-2a-2c)x + (-2b-2d)y = r^2 - s^2$, so intersecting this line with either of the circles gives us the points of intersection. Hence, by the first case the x and y coordinates of each of the points of intersection are solutions of quadratic polynomials over K_{j-1}. □

Theorem 13. *If $r = (x, y)$ is constructible from a subset P_0 of $\mathbb{R}^2$, and K_0 is the subfield of $\mathbb{R}$ generated by the coordinates of the points of P_0, then $[K_0(x) : K_0]$ and $[K_0(y) : K_0]$ are powers of 2.*

Proof. We have seen that for each step in the construction, if $r_j = (x_j, y_j)$, then $[K_{j-1}(x_j) : K_{j-1}]$ and $[K_{j-1}(y_j) : K_{j-1}]$ must be either 1 or 2, since x_j and y_j are the solutions of quadratic polynomials, which are either irreducible, in which case the degree is 2, or can be written as the product of linear factors, in which case the degree is 1. Thus, $[K_{j-1}(x_j, y_j) :$

$K_{j-1}] = [K_{j-1}(x_j, y_j) : K_{j-1}(x_j)][K_{j-1}(x_j) : K_{j-1}]$ which is 1, 2, or 4, so it is a power of 2. Thus, $[K_j : K_{j-1}]$ is a power of 2.

So, since $[K_n : K_0] = [K_n : K_{n-1}] \dots [K_1 : K_0]$, this is also a power of 2.

Thus, since $[K_n : K_0(x)][K_0(x) : K_0] = [K_n : K_0]$, we must have that $[K_0(x) : K_0]$ is a power of 2, since it divides $[K_n : K_0]$. Similarly, $[K_0(y) : K_0]$ is also a power of 2.

$\square$

Corollary 14. *If $x \in \mathbb{C}$ is such that $[\mathbb{Q}(x) : \mathbb{Q}]$ is not a power of 2, then x is not constructible with a ruler and compass.*

§5.4 Splitting Fields and Algebraic Closures

Definition 16. Let K be a field and $P \in K[T]$ a non-constant polynomial. A *splitting field* of P is an extension L/K in which P decomposes into degree 1 factors, that is, $P(T) = c(T-\alpha_1)\dots(T-\alpha_n)$ in $L[T]$ where $\alpha_1, \dots, \alpha_n \in L$ and $c \in K$. L is generated by the roots of P, that is, $L = K(\alpha_1, \dots, \alpha_n)$. Note that the α_i's are algebraic over K, so $K(\alpha_1, \dots, \alpha_n) = k[\alpha_1, \dots, \alpha_n]$ is a finite, and thus, algebraic extension of K.

Proposition 15. *Any non-constant polynomial $P \in K[T]$ (where K is a field) admits a splitting field.*

Proof. It is enough to show that there exists an extension M/K in which the given $P \in K[T]$ decomposes completely. First suppose P is irreducible. Let $M_0 = K[T]/P$, and note that this is a field since P is irreducible. This is an extension, M_0/K, in which P has a root, namely, $\alpha = \overline{T} = T + PK[T]$, the class of T. This is because $P(\alpha) = P(\overline{T}) = \overline{P(T)} = 0$, since $P \in PK[T]$. Then, choose an irreduicble factor of P in $M_0[T]$ and construct M_1 in the same way such that P decomposes further in M_1. Continue this process, and by induction on the maximal degree of polynomials which are irreduicble and divide P, in some M_n with $n >> 0$, P will be the product of linear factors. □

Corollary 16. *Let $p_1, \dots, p_s \in K[T]$ be non-constant polynomials over the field K. There exists an extension L/K in which all $p_1, \dots, p_s$ decompose into degree 1 factors.*

Proof. Apply the above to $P = p_1 \cdot \dots \cdot p_s$. □

Definition 17. A field E is called *algebraically closed* if it admits no algebraic extension except itself. That is, L/E is algebraic $\Rightarrow L = E$.

Proposition 17. *E is algebraically closed if and only if every polynomial in E decomposes as a product of degree 1 factors.*

Proof. $\Rightarrow$: Let $P \in E[T]$ and let L/E be the splitting field of P (note that L/E is algebraic). Then $L = E$, so P decomposes as a product of degree 1 factors in $E[T]$.

$\Leftarrow$: Suppose L/E is an algebraic extension. The minimal polynomial of any $\alpha \in L$ must be of degree $1 \Rightarrow \alpha \in E$. □

Fact 1. (From Chapter 6) If R is a non-zero commutative ring, there exists a ring homomorphism from $R \to K$ where K is a field (take m to be a maximal ideal in R and $K = R/m$).

Theorem 18. *Let K be a field. There exists an extension E/K ($K \hookrightarrow E$) with E algebraically closed.*

Proof. Let $A = K[x_p]_{p \in K[T] \setminus K}$. A is a big polynomial ring with infinitely many variables over K, one variable for each non-constant polynomial $p \in K[T]$. Consider the ideal $I \subset A$ defined by $I = \langle P(x_P) \rangle_{p \in K[T]/K} \subset K[x_p]_{p \in K[T] \setminus K} = A$. Let $Q = \displaystyle\sum_{i=1}^{n} Q_i P_i(x_{P_i}) \in I$ where $Q_i \in A$ for $1 \le i \le n$. Consider that $P_1, \dots, P_n \in K[T]$. By the last corollary, there exists L/K in which the P_i's all decompose completely. In particular, there are $\alpha_1, \dots, \alpha_n \in L$ such that $P_i(\alpha_i) = 0$ for $1 \le i \le n$. Evaluate $Q = Q(x_{p_1}, x_{p_2}, \dots, x_{p_n}, \text{other } x_p\text{'s})$ at $x_{p_i} = \alpha_i$

and set the other x_p's all to 0. This gives us 0 in L. Thus, Q cannot be equal to 1 in A. Hence, since $Q \in I$ was arbitrary, $1 \notin I$, so $I \neq A$.

Consider $R = A/I$, a commutative, non-zero (since $I \neq A$) ring. By the above fact, there is a field E_1 and a ring homomorphism $\overline{f} : R \to E_1$. This is just a ring homomorphism $f : A \to E_1$ such that $f(I) = 0$. Since $A = K[x_P]_{P \in K[T] \setminus K}$, this E_1 is an extension of K. So we have:

$$\begin{tikzcd}
K \arrow[r, hook, "\phi"] \arrow[ddr] & E_1 & \\
& & R = A/I \arrow[ul, "\overline{f}"'] \\
& K[x_p]_{p \in K[T] \setminus K} = A \arrow[uu, "f"] \arrow[ur, "\pi"'] &
\end{tikzcd}$$

Where ϕ is the composition of ring homomorphisms into a field, and thus, is injective.

Consider $p \in K[T]$ non-constant. Let $\alpha_p = f(x_p) \in E_1$. $p(\alpha_p) = p(f(x_p)) = f(p(x_p)) = 0$, since f is a homomorphism. Thus, every polynomial of K has a root in E_1.

Thus, repeat this process by induction, and get $K \hookrightarrow E_1 \hookrightarrow E_2 \hookrightarrow \ldots \hookrightarrow E_n \hookrightarrow E_{n+1} \hookrightarrow \ldots$ such that every non-constant polynomial in E_n has a root in E_{n+1}. Let $E = \operatorname{colim}_{n \to \infty} E_n = \bigcup_{n \geq 1} E_n$ (and since the category of fields is closed under colimits, this is a field). This E is algebraically closed, since $E(T) = \bigcup_{n \geq 1} E_n[T]$, so any non-constant polynomial in T exists in E_n for some n, and thus, has a root in $E_{n+1} \subset E$. $\square$

Definition 18. Let K be a field. An *algebraic closure* is an algebraic extension E/K with E algebraically closed.

Proposition 19. *Any field admits an algebraic closure.*

Proof. Let K be a field. By the previous theorem, there exists $K \hookrightarrow L$ with L algebraically closed. Take E to be the set of elements in L which are algebraic over K. $E = \{x \in L | x$ is algebraic over $K\}$. Then E/K is algebraic. Let $p \in E[T]$. p decomposes completely in L, $P(T) = c(T - \alpha_1) \ldots (T - \alpha_n)$ for $c \in E$ and $\alpha_1, \ldots, \alpha_n \in L$. Now, each α_i is algebraic over E since $p(\alpha_i) = 0 \Rightarrow E(\alpha_i)$ is algebraic over E, and E is algebraic over $K \Rightarrow E(\alpha_i)$ is algebraic over $K \Rightarrow \alpha_i$ is algebraic over $K \Rightarrow \alpha_i \in E$ by definition of E. Hence, the above complete decomposition holds in $E[T]$. Since $p \in E[T]$ was arbitrary, E is algebraically closed. $\square$

Theorem 20. *Let E be algebraically closed and let $\sigma_0 : K \hookrightarrow E$ be a homomorphism. Let L/K be an algebraic extension. Then there is $\sigma : L \to E$ such that σ is K-linear, i.e., $\sigma|_K = \sigma_0$.*

$$\begin{tikzcd}
L \arrow[r, hook, dashed, "\sigma"] & E \\
K \arrow[u, dash] \arrow[ur, hook, "\sigma_0"'] &
\end{tikzcd}$$

Proof. Consider $S = \{(M,\tau) | K \subset M \subset L, \tau : M \to E, \tau|_K = \sigma_0\}$ with an ordering $(M,\tau) \le (M',\tau')$ if $M \subset M'$ and $\tau'|_M = \tau$. This is a partial ordering, so by Zorn's lemma, there is a maximal element, (M,σ). This means that if there is (M',σ') such that $M \subset M'$ and $\sigma'|_M = \sigma$, then $M = M'$.

We claim that $M = L$. Let $\sigma_0 : K \hookrightarrow E$ be a homomorphism with E algebraically closed and let L/K be an algebraic extension. Let $x \in L$ be given. Then there exists a homomorphism $\sigma : K(x) \to E$ such that $\sigma|_K = \sigma_0$, since if P is the minimal polynomial of x over K, then $K[T]/P \xrightarrow{\sim} K[x] \cong K(x) \subset L$, so $\sigma_0(P)$ is a polynomial in $E[T]$ and E is algebraically closed $\Rightarrow \exists \alpha \in E$ a root of $\sigma_0(P) \Rightarrow \sigma_0 K \hookrightarrow E$ and $T \mapsto \alpha$ define the homomorphism $\tau : K[T] \to E$ by $Q \mapsto (\sigma_0(Q))(\alpha)$ and $\tau(P) = (\sigma_0(P))(\alpha) = 0$ (by choice). Hence, τ induces a field homomorphism $\overline{\tau} : K[T]/P \hookrightarrow E$, so we have

$$\begin{tikzcd}
K(x) \arrow[rr, "\sigma"] & & E \\
& K[T]/P \arrow[ul, "\cong"] \arrow[ur, hook, "\overline{\tau}"'] & \\
& K[T] \arrow[u, two heads] \arrow[uul, two heads] \arrow[uur, "\tau"'] & \\
& K \arrow[u, hook] \arrow[uuul, hook] \arrow[uuur, "\sigma_0"'] &
\end{tikzcd}$$

where $K[T]/P \hookrightarrow E$ is defined by $T \mapsto$ the root of P^n.

By the commutativity of the diagram, $\sigma|_K = \sigma_0$. □

Corollary 21. *Let E/K be an algebraic closure of K. Let $M/L/K$ be an algebraic extension and let $\sigma_0 : L \to E$ be a K-linear homomorphism. Then there exists a K-linear homomorphism $\sigma : M \to E$ such that $\sigma|_L = \sigma_0$.*

Proof. Apply the theorem to

$$\begin{tikzcd}
M \arrow[r, dashed, "\exists\sigma"] & E \\
L \arrow[u, dash] \arrow[ur, hook, "\sigma_0"'] &
\end{tikzcd}$$

σ is automatically K-linear since $\sigma|_K = \sigma_0|_K$ which is the inclusion map $K \hookrightarrow E$, and thus, fixes K). □

Thus, algebraic closures are unique up to (non-unique) isomorphism of fields. So when we refer to "the" algebraic closure of a field K, we are referring to some choice of algebraic closure, and we denote this $\overline{K}/K$.

Definition 19. Let $\mathcal{F}$ be a family of non-constant polynomials in $K[T]$. A *splitting field* for $\mathcal{F}$ is an extension L/K such that every $p \in \mathcal{F}$

1. decomposes completely in $L[T]$
2. $L = K(A)$ if $A = \{\alpha \in L | \alpha \text{ is a root of some } p \in \mathcal{F}\}$.

Proposition 22. *Let K be a field and $\mathcal{F} \subset K[T]$ be a family of non-constant polynomials*

1. *A splitting field for $\mathcal{F}$ exists: In $\overline{K}$, the algebraic closure of K, we can and must take $L = K(A) \subset \overline{K}$ where A is the set of roots of polynomials of $\mathcal{F}$.*

2. *The splitting field is unique up to K-isomorphism.*

Proof.

1. In L, any $p \in \mathcal{F}$ decomposes completely and L, by construction, is generated by the roots.

2. This follows from the fact that L must be $K(A)$ where A is the set of roots of polynomials in $\mathcal{F}$. If L'/K is some other splitting field, by the previous theorem there is $\sigma : L \to \overline{K}$ which is a K-homomorphism so $\sigma|_L : L \xrightarrow{\cong} \sigma(L) \subset \overline{K}$, and $\sigma(L)$ is a splitting field in $\overline{K}$, which must be unique because of the first part.

□

§5.5 Normal Extensions

Definition 20. Let L/K be an algebraic extension. We say that this is *normal* if for any irreducible polynomial $P \in K[T]$, if P has a root in L, then it has all roots in L. That is, $P \in K[T]$ irreducible with $\alpha \in L$ such that $P(\alpha) = 0 \Rightarrow P = c(x-\alpha_1)\dots(x-\alpha_n)$ in $L[T]$.

$\mathbb{Q}(2^{\frac{1}{4}}) \subset \mathbb{R}$ is not a normal extension of $\mathbb{Q}$, since $T^4 - 2$ does not decompose completely in $\mathbb{Q}(2^{\frac{1}{4}} \subset \mathbb{R}$ (since $\pm 2^{\frac{1}{4}} i$ are also roots and $i \notin \mathbb{Q}(2^{\frac{1}{4}}) \subset \mathbb{R}$).

Recall that if L_1/K and L_2/K are extensions of K, a K-homomorphism $\sigma : L_1 \to L_2$ is just a ring homomorphism which is the identity on K. This is equivalent to saying σ is K-linear.

Proposition 23. *Let L/K be an algebraic extension. Let $\overline{K}/L$ be an algebraic closure of K and L (they have the same closure since L/K is algebraic). TFAE:*

1. *L/K is normal.*

2. *For any K-homomorphism, $L \overset{\sigma}{\hookrightarrow} \overline{K}$, we have $\sigma(L) \subset L$.*

3. *For any K-homomorphism $\overline{K} \overset{\sigma}{\hookrightarrow} \overline{K}$, we have $\sigma(L) \subset L$.*

Proof. 1. $\Rightarrow$ 2.: Let $x \in L$. let $P \in K[T]$ be the minimal polynomial of x. By assumption, P decomposes completely in L. For any $\sigma : L \to \overline{K}$ K-homomorphism, $0 = \sigma(0) = \sigma(P(x))$ since $P(x) = 0$, which is equal to $P(\sigma(x))$ since σ is a K-homomorphism, so it fixes the coefficients in P. Thus, $\sigma(x)$ is also a root of P, but all of the roots are in L, so $\sigma(x) \in L$. Thus, since $x \in L$ was arbitrary, $\sigma(L) \subset L$.

2. $\Rightarrow$ 3.: Obvious: If $\sigma : \overline{K} \to \overline{K}$ then $\sigma|_L : L \to \overline{K}$ is a K-homomorphism, so by assumption, $\sigma|_L(L) \subset L$, which means that $\sigma(L) \subset L$.

3. $\Rightarrow$ 1.: Let $P \in K[T]$ be an irreducible polynomial which has a root $\alpha \in L$. Let $\beta \in \overline{K}$ be another root. We have a K-isomorphism

$$\begin{tikzcd}
L \supset K(\alpha) \arrow[dr, dash, "\supset"'] & K[T]/P \arrow[l, "\sim"'] \arrow[r, "\sim"] & K(\beta) \subset \overline{K} \arrow[dl, dash, "\subset"] \\
& K &
\end{tikzcd}$$

So by Theorem 20, there is $\sigma : \overline{K} \to \overline{K}$ which extends $K(\alpha) \xrightarrow{\sim} K(\beta) \hookrightarrow \overline{K}$. Thus, we have this:

$$\begin{tikzcd}
\overline{K} \arrow[rr, hook, "\sigma"] \arrow[d, dash] & & \overline{K} \arrow[dd, dash] \\
L \arrow[d, dash] & & \\
K(\alpha) \arrow[rr, "\sim"] \arrow[dr, dash] & & K(\beta) \arrow[dl, dash] \\
& K &
\end{tikzcd}$$

By hypothesis, $\sigma(L) \subset L$, and hence, $\beta = \sigma(\alpha) \in \sigma(L) \subset L$, so $\beta \in L$. $\square$

Theorem 24. *Let L/K be an algebraic extension. Then L/K is normal if and only if L is the splitting field of some family of polynomials in K.*

Proof. $\Rightarrow$: If L/K is normal, take $\mathcal{F}$ to be the set of $p \in K[T]$ such that p is the minimal polynomial of some $x \in L$ (for all $x \in L$). Let A be the set of $\alpha \in L$ such that α is the root of some $p \in \mathcal{F}$. By Proposition 22, $L = K(A)$, and any $p \in \mathcal{F}$ decomposes completely in $L[T]$ since L is normal. Hence, L is the splitting field of $\mathcal{F}$.

$\Leftarrow$: Suppose $\mathcal{F} \subset K[T]$ is a family of polynomials and let L/K be the splitting field of $\mathcal{F}$. Let $\sigma : \overline{K} \to \overline{K}$ be a K-homomorphism. Let A be the set of roots of $P \in \mathcal{F}$. By assumption, $L = K(A)$. For every $\alpha \in A$, there is $P \in \mathcal{F}$ such that $P(\alpha) = 0$, so $0 = \sigma(0) = \sigma(P(\alpha)) = P(\sigma(\alpha))$ (as in the previous proposition) since σ is K-linear and $P \in K[T]$. Thus, $\sigma(\alpha)$ is a root of P, so $\sigma(\alpha) \in A \subset K(A)$. Hence, by the previous proposition, L/K is normal. $\square$

Corollary 25. *Finite normal extensions are just splitting fields of finite families of polynomials, which are the same as splitting fields of one polynomial.*

Remark 3. Let $M/L/K$ be an algebraic extension.

1. If M/K is normal, then M/L is normal. This is obvious from the theorem, since if $\mathcal{F} \subset K[T]$ is such that M is the splitting field of $\mathcal{F}$ over K, then M is also the splitting field of $\mathcal{F}$ over L.

2. If M/K is normal it does not imply that L/K is normal. For example, $\mathbb{Q}(2^{\frac{1}{4}})/\mathbb{Q}$ is not normal, but $\mathbb{Q}(2^{\frac{1}{4}}, i)/\mathbb{Q}$ is.

Proposition 26. *Let L/K be algebraic. There exists N/L algebraic such that N/K is normal (hence, N/L is as well) and which is minimal by extension. This N is unique up to K-isomorphism. Finally, if L/K is finite, so is N/L.*

Proof. It is enough to produce $N \subset \overline{K} = \overline{L}$ a (fixed) algebraic extension and prove uniqueness of N in $\overline{K}$ (since algebraic closures are isomorphic). Let $A \subset L$ be such that $L = K(A)$ and note that A is finite if L/K is finite. Let $\mathcal{F} \subset K[T]$ be the collection of minimal polynomials of $\alpha \in A$ ($\mathcal{F}$ is finite if A is finite). Then, let N be the splitting field of $\mathcal{F}$ in $\overline{K}$. We have that A is a subset of the set of roots of polynomials in $\mathcal{F}$ which is a subset of N, so $L = K(A) \subset N$, which means that N/K is normal. Any normal M/L must contain all of the roots of $\mathcal{F}$, and hence, must contain N. $\square$

§5.6 Separable Extensions

Definition 21. Let L/K be an extension.

1. $x \in L/K$ is *separable* over K if it is algebraic over K and its minimal polynomial over K has only simple roots in $\overline{K}$.

2. An irreduicble polynomial $p \in K[T]$ is *separable* if it has only simple roots in $\overline{K}$, that is, $p = c(T-\alpha_1)\ldots(T-\alpha_n)$ and $\alpha_i \neq \alpha_j$ for $i \neq j$.

3. A general polynomial in $K[T]$ is *separable* if its irreducible factors are separable.

4. An algebraic extension L/K is *separable* if every $x \in L$ is separable.

Proposition 27. *Let $P \in K[T]$ be irreduicble. P has multiple roots (is not separable) if and only if $P' = 0$. This can only happen in positive characeristic, say, $char(K) = p > 0$, in which case, $P = Q(T^p)$ with $Q \in K[T]$ irreducible.*

Proof. Suppose P has a multiple root α. Then $P(T) = (T-\alpha)^2 R(T)$, so $P'(T) = 2(T-\alpha)R(T) + (T-\alpha)^2 R'(T)$. Thus, $P'(\alpha) = 0$.

So $P' \in K[T]$ has α as a root, but P is the minimal polynomial of α over K, because P is irreduicble. Thus, $P|P'$, but $degP' \leq degP - 1$, so $P' = 0$.

Now suppose $P \in K[T]$ such that $P' = 0$. $P = a_d T^d + \ldots + a_1 T + a_0$, so $P' = da_d T^{d-1} + \ldots + 2a_2 T + a_1$. Thus, $P' = 0 \Rightarrow ia_i = 0$ for $1 \leq i \leq d \Rightarrow i = 0$ or $a_i = 0$ since K is a field, and thus a domain, and since $i \neq 0$, $a_i = 0$ for each $1 \leq i \leq d$. Thus, $P = a_0$ is constant, but this is not an irreduicble polynomial (it is a unit or 0), so this is a contradiction. Hence, $char(K) = p > 0$. So, the equation $ia_i = 0$ implies that $a_i = 0$ for i such that p does not divide i, for $1 \leq i \leq d$. Thus, $P = a_0 + a_p T^p + a_{2p} T^{2p} + \ldots + a_{rp} T^{rp} = Q(T^p)$ for $Q(T) = a_0 + a_p T + \ldots + a_{rp} T^r$. If P is irreducible, then Q is (otherwise a factorization of Q would give a factorization of P). Finally, if P is irreduicble, $P' = 0 \Rightarrow P = Q(T^p)$, Q irreducible. Factor $Q(T) = c(T-\beta_1)\ldots(T-\beta_r)$ in $\overline{K}$. Then $P(T) = Q(T^p) = c(T^p - \beta_1)\ldots(T^p - \beta_r)$ in $\overline{K}$. In $\overline{K}$, there exists α_i such that $\alpha_i^p = \beta_i$ for each $1 \leq i \leq r$ (solutions to $y^p - \beta_i$), so $P(T) = c(T^p - \alpha_1^p)\ldots(T^p - \alpha_r^p) = c(T-\alpha_1)^p \ldots (T-\alpha_n)^p$ (since in characteristic p, $(a^p \pm b^p) = (a \pm b)^p$). Thus, P has multiple roots. ☐

Definition 22. If $char(K) = p > 0$, $x \mapsto x^p$ defines a homomorphisms from $K \to K$. This is called the *Frobenius Homomorphism.*

Corollary 28. *In characteristic 0, all (irreduicble) polynomials are separable and all algebraic elements are separable. Hence, all algebraic extensions are separable.*

Proposition 29. *If $char(K) = p > 0$ and $a \in K$ but $a \notin K^p = \{b^p | b \in K\}$, then $P(T) = T^p - a \in K[T]$ is irreducible and non-separable (in fact, P only has one root).*

Proof. Let $K = \mathbb{F}_p(x)$. Consider $a = x$ in K. Note that a does not have a p^{th} root in K, so $P(T) = T^p - a \in K[T]$ is irreduicble. Indeed: use $P(t) = (T-\beta)^p$ for β any p^{th} root of a in $\overline{K}$, hence, a factorization of P in $K[T]$ must be $(T-\beta)^i (T-\beta)^{p-i} = (T^i - \beta^i)(T^{p-i} - \beta^{p-i})$ which means β^i or β^{p-i} is in K. If $i \neq 0, p$, then $i \in \mathbb{Z}/p$ is invertible $\Rightarrow \exists k$ such that $p| - ik + 1$, so $\beta = \beta^{ik}\beta^{1-ik} \in K$ since $\beta^{ik}, \beta^{1-ik} \in K$, which is a contradiction.

Hence, P is irreducible, and $P' = pT^{p-1} = 0$, so by the previous proposition, P is not separable. ☐

Proposition 30. *Let L/K be an algebraic extension. The extension is separable if and only if for every $x \in L$ we have $x \in K(x^p) \subset L$.*

Proof. Suppose L/K is separable. Let $x \in L$ and $M = K(x^p)$. Then the extension L/M is still separable (since the minimal polynomial over K divides the minimal polynomial over M, so if that has only simple roots, the other only has simple roots). So, x is separable over M. But, x is a root of $P(T) = T^p - x^p \in M[T]$. Since P is not separable, P cannot be the minimal polynomial of $x \Rightarrow P$ is irreduicble $\Rightarrow$ (by the previous proposition) $x^p \in M \Rightarrow$ since the p^{th} root is unique, $x \in M$.

Conversely, suppose $x \in K(x^p)$ for every $x \in L$. Let $x \in L$. Suppose for the sake of contradiction that x is not separable over K. Then, let P be the minimal polynomial of x, it has the form $P(T) = Q(T^p)$ with Q irreduicble. Then Q is the minimal polynomial of x^p, since $Q(x^p) = P(x) = 0$ and Q is irreducible. So, $K(x^p)/K$ has degree equal to the degree of Q, which is strictly less than the degreep of P (specifically, it is $\frac{deg(P)}{p}$), but $x \in K(x^p)$, so the degree of the minimal polynomial of x is less than or equal to $[K(x^p) : K] < deg(P)$ which is a contradiction. ☐

Remark 4. In this proof we used the fact that if L/K is separable and $L/M/K$ is an intermediate extension, then L/M and M/K are separable. This is because for $x \in L$, if $p \in K[T]$ is the minimal polynomial of x over K, and $Q \in M[T]$ is the minimal polynomial of x over M, then $Q|P$ in $M[T]$ since $P(x) = 0$, so if P is separable, Q must be separable. And since $x \in M \subset L$ has a separable polynomial in $K[T]$. This is Corollary 35.

Definition 23. Let L/K be an algebraic extension and let $\overline{K}/K$ be a given algebraic closure. The *separable degree* is $[L : K]_S := \#(Hom_K(L, \overline{K}))$. This could be ∞. Note that it is enough to have $\sigma_0 : K \hookrightarrow \overline{K}$ and define $Hom_K(L, \overline{K}) = \{\sigma : L \to \overline{K} | \sigma|_K = \sigma_0\}$. This does not depend on σ_0.

If E_1/L and E_2/L are algebraic extensions of L, and thus, of K, and E_1, E_2 are both algebraically closed, then $\#(Hom_K(L, E_1)) = \#(Hom_K(L, E_2))$ where $Hom_K(L, E)$ is the set of K homomorpshisms from $L \hookrightarrow E$. To see this it is enough to show that $\#(Hom_K(L, E_1)) = \#(Hom_K(L, \overline{K}))$ for any algebraic closure $\overline{K}$ of K. By Theorem 20 there is $\tau : \overline{K} \hookrightarrow E_1$ which is K-linear and since $\tau(\overline{K})$ is algebraic over K, it is contained in the algebraic closure of K in E_1, so $\tau(\overline{K})$ is an algebraic closed algebraic extension of K in E (so it is an algebraic closure of K in E). Thus, $Hom_K(L, E_1) \xrightarrow{\cong} Hom_K(L, \overline{K})$ via $\sigma \mapsto \tau^{-1} \circ \sigma$ and $\sigma' \mapsto \tau \circ \sigma'$.

$$\begin{tikzcd}
 & E_1 \arrow[d, dash] & \\
L \arrow[ur, "\sigma"] \arrow[r, dashed, "\exists!\sigma"] \arrow[dr, dash, "\text{alg}"'] & \tau\overline{K} \arrow[d, dash] & \overline{K} \arrow[l, "\sim", "\tau"'] \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Proposition 31. *If $M/L/K$ is algebraic, then $[M : L]_S[L : K]_S = [M : K]_S$.*

Proof. Suppose $M/L/K$ is algebraic and let $\overline{K}$ be an algebraic closure of K. Note that $\overline{K} = \overline{M} = \overline{L}$. Fix $\sigma_0 : K \hookrightarrow \overline{K}$. It admits $[L : K]_S$ extensions, that is, $\sigma_1 : L \to \overline{K}$ such that

$\sigma_1|_K = \sigma_0$. Each $\sigma_1 : L \to \overline{K}$ admits $[M : L]_S$ extensions $\sigma_2 : M \to \overline{K}$ such that $\sigma_2|_L = \sigma_1$. We have a partition (just by restricting from M to L),

$$\{\sigma_2 : M \to \overline{K} | \sigma_2|_K = \sigma_0\} = \bigsqcup_{\substack{\sigma_i : L \to \overline{K} \\ s.t.\ \sigma_1|_K = \sigma_0}} \{\sigma_2 : M \to \overline{K} | \sigma_2|_L = \sigma_i\}.$$

Since there are $[L : K]_S$ many $\sigma_i : L \to \overline{K}$ such that $\sigma_i|_K = \sigma_0$ and for each such σ_i there are $[M : L]_S$ many $\sigma_2 : M \to \overline{K} | \sigma_2|_L = \sigma_i$, we see that $[M : K]_S = \#\{\sigma_2 : M \to \overline{K} | \sigma_2|_K = \sigma_0\} = [M : L]_S [L : K]_S$.

□

Definition 24. An algebraic extension L/K is *simple* if there exists $x \in L$ such that $L = K(x)$. Such an x is called a *primitive element*. In this case, $L \cong K[T]/p$ where $p \in K[T]$ is the minimal polynomial of x, via $T \mapsto x$.

Proposition 32. *Let $P \in K[T]$ be irreducible and let $L = K[T]/P$. Then the separable degree of $[L : K]_S$ is the number of distinct roots of P in $\overline{K}$. Hence, $[L : K]_S \leq deg(P) = [L : K]$.*

Proof. $Hom_K(K[T]/P, \bar{[}K])$ is in bijective correspondence with the set of roots of P via $\alpha \mapsto (\phi : K[T]/P \to \overline{K})$ defined by $\overline{Q} \mapsto \overline{Q}(\alpha)$ and $f \mapsto f(t)$ where $t = \overline{T} \in L$. □

Proposition 33. *If L/K is finite then $[L : K]_S \leq [L : K]$.*

Proof. This follows from induction from the previous proposition, since we know that $[L : K]_S \leq [L : K]$ when $L = K(x)$, and thus, is also true when $L = K(x_1, \ldots, x_{n+1}) = K(x_1, \ldots, x_n)(x_{n+1})$ and since $[L : K]_S$ and $[L : K]$ are both multiplicative. □

Remark 5.

1. If $L = K(x)$ is a simple extension with x separable, then $[L : K]_S = [L : K]$ since both are equal to the degree of the minimal polynomial of x over K.

2. If $char K = p > 0$, $L = K(x)$ with $x^p \in L$ (not separable), if $a := x^p \in L$, if $x \in K$, then $L = K$. So if $x \notin K$, $L \neq K$, so the minimal polynomial of x is $T^P - a \in K[T]$ which is equal to $(T - x)^p \in L[T]$ where $x^p = a$. We have seen previously that this is irreducible, so $[L : K]_S$ is equal to the number of roots of P, which is 1 (P has only one root).

Theorem 34. *Let L/K be a finite extension. Then L/K is separable if and only if $[L : K]_S = [L : K]$. That is, for every $\sigma_0 : K \hookrightarrow \overline{K}$, there is exactly $[L : K]$ many $\sigma_1 : L \to K$ such that $\sigma_1|_K = \sigma_0$.*

Proof. $\Rightarrow$: By induction on $[L : K]$: Let $x \in L$ and M be such that $L = M(x)$, $x \notin M$. Then by the first remark, $[L : M(x)]_S = [L : M(x)]$. Then, we will assume that $[M : K]_S = [M : K]$ for $L/M/K$ and we see that $[L : K]_S = [L : M]_S [M : K]_S = [L : M][M : K] = [L : K]$.

$\Leftarrow$: Suppose L/K is not separable. By Proposition 30 there exists $x \in L$ such that $x \notin K(x^p)$ where $p = char(K) > 0$. Consider

$$
\begin{array}{c}
L \\
| \\
K(x) = M(x) \\
|\ \neq \\
M := K(x^p) \\
| \\
K
\end{array}
$$

The middle extension $(K(x)/K)$ is like the extension in teh second remark, so $[K(x) : K]_S = 1 < [K(x) : K]$.

$[L : K]_S = [L : K(x)]_S[K(x) : K(x^p)]_S[K(x^p) : K]_S < [L : K(x)][K(x) : K(x^p)][K(x^p) : K] = [L : K]$. $\square$

Corollary 35. *Suppose $M/L/K$ is algebraic. M/L and L/K are both separable if and only if M/K is separable.*

Proof. $\Rightarrow$: If M/L and L/K are both separable, then $[M : L]_S = [M : L]$ and $[L : K]_S = [L : K]$, so $[M : K]_S = [M : L]_S[L : K]_S = [M : L][L : K] = [M : K]$.

$\Leftarrow$: $[M : K]_S = [M : K] = [M : L][L : K] \geq [M : L]_S[L : K]_S = [M : K]_S$. Thus, we must have $[M : L]_S = [M : L]$ and $[L : K]_S = [L : K]$, so they are both separable.

$\square$

Theorem 36. *Let L/K be an extension. Let $x_i \in L$, $i \in I$, be a collectoin of (algebraic and) separable elements. Then the K-field generated by $K(\{x_i\}_{i \in I}) \subset L$ is a separable extension of K.*

Proof. It is enough to show that $K(x_1, \ldots, x_n)/K$ is separable if $x_1, \ldots, x_n$ are separable (since the infinite case is just a union of these). Then, it is enough to show that $K(x)/K$ is separable if x is separable over K, then the rest follows by induction on n. We have seen though (Remark 5.1) that if $[K(x) : K]_S$ is the degree of the minimal polynomial of x, which is $[K(x) : K]$, then $K(x)/K$ is separable. $\square$

Definition 25. If L/K is an algebraic extension, $M = \{x \in K | x \text{ is separable over } K\}$ is called the *separable closure* of K in L. If L is not specified, we mean in $\overline{K}$. We use $K^{sep} \subset \overline{K}$ to denote hte separable closure of K in $\overline{K}$.

Corollary 37. *Let L/K be algebraic. Then, $M = \{x \in K | x$ is separable over $K\}$ is a subfield of L and M/K is separable.*

Proof. Pick $x, y \in M$. By the previous theorem, $K(x, y)$ is separable over K, and this contains $x + y$, xy and x^{-1} if $x \neq 0$. $\square$

Theorem 38. *Let L/K be a finite extension. There exists an element $\alpha \in L$ such that $L = K(\alpha)$ (that is, L is a simple extension of K) if and only if there exist only a finite number of fields M such that $K \subset M \subset L$.*

Proof. Let L/K be a finite extension. If K is finite, the multiplicative group of L is cyclic, and thus, is generated by one element α. So, since $0 \in K$, $L = K(\alpha)$.

Also, there can only be finitely many fields between K and L, if $char(K) = p > 0$, there can only be as many $K \subset M \subset L$ as there are powers of p between $|K|$ and $|L|$.

Hence, the claim holds for finite fields. Assume K is infinite.

$\Leftarrow$: Suppose there are onyl finitely many fields M such that $K \subset M \subset L$. Let $\alpha, \beta \in L$ be givein. Since there are onyl finitely many fields between K and L, there are finitely many $c \in K$ such that $K(\alpha + c\beta)$ are distinct. Thus, since K is infinite, we can choose $c_1, c_2 \in K$, $c_1 \neq c_2$, such that $K(\alpha + c_1\beta) = K(\alpha + c_2\beta) =: M$. So, since $\alpha + c_1\beta$ and $\alpha + c_2\beta$ are both in M, $(c_2 - c_1)\beta \in M$, and since $c_2 - c_1 \neq 0$, $\beta \in M$. Thus, $c_1\beta \in M$, so $\alpha \in M$.

Hence, $K(\alpha, \beta)$ can be generated by one element. So, by induction, if $M = K(\alpha_1, \ldots, \alpha_n)$, there is $z \in M$ such that $M = K(z)$. Thus, since L/K is finite, there is $\alpha \in L$ such that $L = K(\alpha)$.

$\Rightarrow$: Now assume $L = K(\alpha)$ for some $\alpha \in L$. Let f be the minimal polynomial of α over K. Let $\overline{L}$ be a fixed algebraic closure of L (and thus, of K). We see that since f is monic, it factors uniquely into linear terms in $\overline{L}[T]$. Thus, since any $g \in L[T]$ which divides f will also factor into linear terms in $\overline{L}[T]$, and these must be among the terms in the factorization of f. Hence, there are only finitely many monic polynomials in $L[T]$ which divide f.

Let M be a field between K and L. Then there is a monic polynomial $g \in M[T] \subset L[T]$ which is the minimal polynomial of α over M. This clearly divides f. So in this way we can associate each intermediate field of L/K with a polynomial in $L[T]$ which divides f.

Now let $K \subset M \subset L$ be given and let g be the corresponding divisor of f. Let N be the subfield of M generated by the coefficients of g over K. Thus, $g \in M[T]$, and since g is irreducible in $M \supset N$, g is irreducible in $N[T]$, and since $g(\alpha) = 0$, g must be the minimal polynomial of α over N. But then, we know that $[M : N] = \frac{[L:N]}{[L:M]} = 1$ since the degree of the minimal polynomial of α over M and N is the same. Thus, $M = N$. So, for any field E with the same minimal polynomial over α as that in M, $E = N = M$.

Hence, we see that associating each intermediate field of L/K with a polynomial in $L[T]$ in this way gives us a bijective correspondence, and thus, since there are only finitely many such polynomials, there can only be finitely many intermediate fields.

$\square$

Theorem 39 (Primitive Element Theorem)**.** *Let L/K be finite and separable. Then L is simple.*

Proof. First suppose K (and hence, L) is finite. Then, by Corollary 45, $L^\times$ is a cyclic group, so $L^\times = \langle x \rangle$ for some $x \in L$, and thus, since $0 \in K$ and $L \setminus \{0\} = L^\times$, $L = K(x)$.

Now suppose K is infinite (note that this does not imply $char(K) = 0$, for example, $\overline{\mathbb{F}_p(T)}$ is infinite and has characteristic $p > 0$).

Suppose $L = K(x, y)$ is separable over K. Let $n = [K(x, y) : K] = [K(x, y) : K]_S$ (by assumption). Thus, there are n distinct K-homomorphisms $\sigma_1, \ldots, \sigma_n : K(x, y) \to \overline{K}$ (where $\overline{K}$ is a fixed algebraic closure of K, and thus, of $K(x, y)$). Consider $P(T) \in \overline{K}[T]$ defined by $P(T) = \prod_{i \neq j}((\sigma_i(x) + T\sigma_i(y)) - (\sigma_j(x) + T\sigma_j(y)))$. This $P(T)$ is non-zero, or else there would be $i \neq j$ such that $\sigma_i(x) = \sigma_j(x)$ and $\sigma_i(y) = \sigma_j(y)$, but since $\sigma_i|_K = \sigma_j|_K = id_K$, this implies that $\sigma_i = \sigma_j$, which contradicts our assumption that $\sigma_1, \ldots, \sigma_n$ are distinct.

P has finitely many roots, which means that since K is infinite, we can choose $t \in K$ such that $P(t) \neq 0$. Let $z = x + ty \in K(x,y)$. Then, for each $1 \leq i \leq n$, $\sigma_i(z) = \sigma_i(x+ty) = \sigma_i(x) + t\sigma_i(y)$ since $t \in K$. Thus, since $P(t) \neq 0$, we know that for every $i \neq j$, $\sigma_i(x) + t\sigma_i(y) \neq \sigma_j(x) + t\sigma_j(y)$, and hence, $\sigma_i(z) \neq \sigma_j(z)$. Thus, for each $i \neq j$, $\sigma_i|_{K(z)} \neq \sigma_j|_{K(z)}$ and $\{\sigma_1|_{K(z)}, \ldots, \sigma_n|_{K(z)}\} \subset Hom_K(K(z), \overline{K})$, so $\#Hom_K(K(z), \overline{K}) \geq n$.

Since $K(z) \subset K(x,y)$, $[K(z) : K] \leq [K(x,y) : K]$, so $n \leq [K(z) : K]_S \leq [K(z) : K] \leq [K(x,y) : K] = [K(x,y) : K]_S = n$. Thus, $[K(z) : K] = [K(x,y) : K] = n \Rightarrow [K(x,y) : K(z)] = \frac{n}{n} = 1 \Rightarrow K(z) = K(x,y)$.

Then, assume that for some fixed arbitrary $n \geq 2$, if $m \leq n$ and $L = K(x_1, \ldots, x_m)/K$ is separable, then there is $z \in L$ such that $L = K(z)$.

Let $L = K(x_1, \ldots, x_n, x_{n+1})/K$ be a separable extension. Then, $K(x_1, \ldots, x_n)/K$ is separable, so by the induction hypothesis, $\exists y \in K(x_1, \ldots, x_n)$ such that $K(x_1, \ldots, x_n) = K(y)$. So, since $K(x_1, \ldots, x_n)(x_{n+1})/K$ is separable, that is, $K(y, x_{n+1})/K$ is separable, there is $z \in K(y, x_{n+1})$ such that $K(z) = K(y, x_{n+1}) = K(x_1, \ldots, x_n, x_{n+1})$.

Thus, by induction, we see that for any finite separable extension L/K, there is $z \in L$ such that $L = K(z)$. □

Corollary 40. *In characteristic* 0*, any finite extension is simple.*

Proof. In characteristic 0, all extensions are separable. □

Remark 6. If L/K is separable and finite, then $L \cong K[T]/P$ for some $P \in K[T]$ which is irreducible and separable.

Definition 26. A field is *perfect* if any algebraic extension is separable. So all fields of characteristic 0 are perfect.

Proposition 41. *Any algebraic extension of a perfect field is perfect.*

Proof. Let K be perfect and let L/K be algebraic. Let M/L be an algebraic extension of L. Then M/K is lagebraic, so since K is perfect, M/K is separable. Thus, since $M/L/K$, M/L is separable by Corollary 35. Hence, since the algebraic extension M/L was arbitrary, L is perfect. □

Definition 27. In characteristic $p > 0$, if E/F is a finite extension, $a \in E$ is *purely inseparable* over F if $a^{p^n} \in F$ for some $n \geq 0$. E/F is purely inseparable if every element in E is purely inseparable over F.

Proposition 42. *If E/F is a finite extension and L is the separable closure of F in E, then L/F is separable and E/L is purely inseparable.*

Proof. Let L be the separable closure of F in E. We have seen that L/F is separable (by definition). Since E/F is finite, it is algebraic. Let $x \in E$ be given and let $G \in F[T]$ be the minimal polynomial of x over F. If x is separable over F, then $x^{p^0} = x \in L$ (by definition). If not, then $G(T) = H_1(T^p)$ for some irreducible $H_1 \in F[T]$, so $g = deg(G) = pn_1$ where $n_1 = deg(H_1)$, so $n_1 = \frac{g}{p}$. Then, since H_1 is irreducible (and monic, since G is monic), it is the minimal polynomial of x^p. So, if H_1 is separable, $x^p \in L$ (by definition). If not, there is $H_2 \in F[T]$ irreducible (and monic) such that $H_1(T) = H_2(T^P)$, so $G(T) = H_1(T^p) = H_2(T^{p^2})$. Thus, $n_2 = deg(H_2) = \frac{n_1}{p} = \frac{g}{p^2}$. Again, if $H - 2$ is separable, then since it is the minimal polynomial of x^{p^2}, $x^{p^2} \in L$. If not, we repeat this process.

Let m be such that $p^{m+1} \geq g$ (such an m exists since g is finite). So, for $i < m$, if H_i is separable, $x^{p^i} \in L$. If not, choose $H_{i+1} \in F[T]$ irreducible (and monic) such that $H_i(T) = H_{i+1}(T^P)$, so $G(T) = H_i(T^{p^i}) = H_{i+1}(T^{p^{i+1}})$. Thus, $deg(H_{i+1}) = \frac{deg(H_i)}{p} = \frac{\frac{g}{p_i}}{p} = \frac{g}{p^i}$.

Then, suppose we have continued this process until we get a monic irreducibile polynomial $H_m \in F[T]$ with degree $\frac{g}{p^m}$ which is not separable. $deg(H_m) \leq p$ since $g \leq p^{m+1}$. Again, we see that H_m is the minimal polynomial of x^{p^m}. Then, we see that for any irreducible $Q \in F[T]$, $deg(Q(T^p)) = deg(Q)p \geq p \geq \frac{g}{p^m} = deg(H_m)$ and equality can only hold if $deg(Q) = 1$ and $deg(H_m) = p$, in which case $H_m(T) = T^p - a$ for some $a \in F$, so $0 = H_m(x^{p^m}) = x^{p^{m+1}} - a \Rightarrow x^{p^{m+1}} = a \in F \subset L$.

Otherwise, there is no irreducible Q such that $Q(T^p) = H_m(T)$, and thus, H_m is separable, which means that $x^{p^m} \in L$.

Thus, since $x \in E$ was arbitrary, E/L is purely inseparable. □

Proposition 43. *If $char(K) = p > 0$, K is perfect if and only if for every $a \in K$, there is $x \in K$ such that $x^p = a$.*

Proof. $\Rightarrow$: Suppose K is perfect. Let $a \in K$ be given and let L/K be the splitting field of $T^p - a \in K[T]$. Let $x \in L$ be a zero of $T^p - a$. Then, $x^p - a = 0 \Rightarrow x^p = a$, so we can write this as $T^p - x^p = (T - x)^p$ (since $char(L) = p$). Since K is perfect and L/K is algebraic, the minimal polynomial of x has simple roots and divides $(T - x)^p$, so it must be $T - x \Rightarrow x \in K$.

$\Leftarrow$: First of all, from Proposition 27, a polynomial f is separable if and only if $f' \neq 0$. Let $f \in K[T]$ be irreducible. Since we have assumed $K = K^p$ and $char(K) = p$, $f' = 0$ if and only if f is a power of p. To see this, if $f(T) = (g(T))^p$, $f'(T) = p(g(T))^{p-1} - 0$, and if $f' = 0$, then for $f = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $a_i i = 0$ for every a_i, which, if $f \neq 0$, is only possible if each i is a multiple of p. Thus, $f(T) = g(T^p)$, and hence, since $K^p = K$, $f(T) = (g(T))^p$. But if this is the case, then f is not irreducible. Thus, every irreducible polynomial over K must be separable.

Let L/K be an algebraic extension and let $x \in L$. Then the minimal polynomial of x over K is irreducible, and thus separable, and hence, x is separable. Thus, since this is true for every $x \in L$, L/K is separable, and since L was arbitrary, K is perfect. □

§5.7 Finite Fields

We have seen that a finite field K must have p^n elements where $p = char(K)$ is prime and $n \geq 1$. Conversely, for any $q \in \mathbb{N}$ of the form $q = p^n$ for p-prime and $n \geq 1$, there exists *exactly one* field with q elements denoted by $\mathbb{F}_q$. Explicitly, it is $\{x \in \overline{\mathbb{F}_p} | x^q = x\}$ where $\overline{\mathbb{F}_p}$ is any algebraic closure of $\mathbb{F}_p = \mathbb{Z}/p$.

Recall that if K is a field and $char(K) = p > 0$, the *Frobenius Homomorphism* $F_p : K \to K$ is given by $x \mapsto x^p$. It is additive since $\binom{p}{j} = \frac{p!}{j!(p-j)!}$ is divisible by p for every $0 < j < p$, so $(x+y)^p = \displaystyle\sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j} = x^p + y^p$ (since all of the terms are 0 except when $j = 0$ and $j = p$).

Theorem 44 (Kronecker)**.** *Let K be a field and let $G \subset K^\times$ be a finite subgroup of the units of K (with respect to multiplication). Then G is cyclic.*

Proof. G is a finite abelian group, so by the results on finitely generated modules over PIDs, we know that $G \cong \mathbb{Z}/a_1 \oplus \ldots \oplus \mathbb{Z}/a_s$ with $a_1 | a_2 | \ldots | a_s$. We will write this as $G \cong C_{a_1} \times \ldots C_{a_s}$ where $C_r = \langle \sigma | \sigma^r = 0 \rangle$ is the cyclic gorup with r elements. For any $x \in G$, we have $x^{a_s} = 1$(since a_s is the lowest common multiple of the a_i's). In K, $G \subset \{x \in K | x^{a_s} = 1\}$ which is the set of roots of $T^{a_s} - 1$, and there are at most a_s many elements. SO, $|G| \leq a_s$, but $|G| = a_1 \ldots a_s \Rightarrow a_1 = \ldots a_{n-1} = 1$, so $s = 1 \Rightarrow G$ is cyclic. Specifically, $G = C_{a_s}$. □

Corollary 45. *If K is finite with q elements, then $x^q = x$ for every $x \in K$.*

Proof. $K^\times$ is a finite subgroup of itself, and thus, is cyclic with $q - 1$ elements, so for every $x \neq 0$, $x^{q-1} = 1$. □

Proposition 46. *There is exactly one finite field with q elements where $q = p^n$ for some prime p and some $n \geq 1$.*

Proof. Let $\mathbb{F}_q$ be the set of roots of $T^q - T$ in $\overline{\mathbb{F}_p}$

The derivative of $T^q - T$ is $qT^{q-1} - 1 = -1 \neq 0$, so this polynomial is separable over $\mathbb{F}_p$. Thus, it has q distinct roots, so $|\mathbb{F}_q| = q$.

Then, for $x, y \in \mathbb{F}_q$, $(x+y)^{p^n} - (x+y) = x^{p^n} + y^{p^n} - (x+y)$ since the characteristic is p, which is equal to $(x^{p^n} - x) + (y^{p^n} - y) = 0$ since x, y are solutions of $T^{p^n} - T$.

Let F_p denote the Frobenius homomorphism. Then, since $x^{p^n} = x$ for all $x \in \mathbb{F}_q$, $x = F_p^n(x)$, where F^n denotes n applications of the homomorphism. So, $F^n(xy) = F^n(x)F^n(y) = xy$, and since $F^n(xy) = (xy)^{p^n}$, $(xy)^{p^n} - (xy) = 0$, so $xy \in \mathbb{F}_q$.

Let $x \neq 0$. Then, $x^{p^n} - x = 0$, so $x(x^{q-1} - 1) = 0$, and since $x \neq 0$, $x^{q-1} - 1 = 0$, so $x^{q-1} = 1$. So, since $q \geq 2$, x^{q-2} is x^{-1}. Then, $(x^{q-2})^q = F^n(x^{q-2}) = (F^n(x))^{q-2} = x^{q-2}$, so $x^{q-2} \in \mathbb{F}_q$.

And clearly, $\mathbb{F}_q \subset \overline{\mathbb{F}_p}$ since each element of q is the solution of $T^q - T \in \mathbb{F}_p[T]$. Thus, $\mathbb{F}_q$ is a subfield of $\overline{\mathbb{F}_p}$.

Finally, let K be a field of order $q = p^n$. Then, let $x \in K$ be such that $K^\times = \langle x \rangle$ (this exists by Corollary 45). Then, we can define an isomorphism to $\mathbb{Z}/p^n$ via $0 \mapsto 0$ and 1 mapping to the generator of $(\mathbb{Z}/q)^\times$ (which is a cyclic group). Hence, since this is clearly an isomorphism (since $0 \mapsto 0$, the generator of K^x maps to the generator of $(\mathbb{Z}/q)^\times$, and $|K^\times| = |(\mathbb{Z}/p)^\times|$), we see that fields with q elements are unique up to isomorphism. □

Proposition 47. *Any finite extension of a finite field is normal.*

Proof. First note that it is enough to show that for any prime p, if $q = p^n$ for some $n \geq 1$, then $\mathbb{F}_q/\mathbb{F}_p$ is normal since for $v = p^m$ with $m \leq n$, this implies that $\mathbb{F}_q/\mathbb{F}_v$ is normal.

Let $\sigma : \mathbb{F}_q \to \overline{\mathbb{F}_p}$ which is $\mathbb{F}_p$-linear be given. Let $x \in \mathbb{F}_q$. Then x is a solution to $T^q - T$ (from the previous problem).

$0 = \sigma(x^q - x) = (\sigma(x))^q - (\sigma(x))$, and thus, $\sigma(x) \in \mathbb{F}_q$. Hence, since $x \in \mathbb{F}_q$ was arbitrary, $\sigma(\mathbb{F}_q) \subset \mathbb{F}_q$. Thus, the extension is normal. □

Proposition 48. *Any finite extension of a finite field is separable.*

Proof. Again, we need only consider the case $\mathbb{F}_q/\mathbb{F}_p$ where $q = p^n$ for some $n \geq 1$ and p is prime, since this being separable implies that $\mathbb{F}_q/\mathbb{F}_v$ where $v = p^m$ for $m \leq n$ is separable.

Let $x \in \mathbb{F}_q$ be given. Then, by definition we know that $x = x^q = x^{p^n}$. And we know that $x^{p^n} \in \mathbb{F}_p(x^p)$, since $(x^{p^n}) = (x^p)^{p^{n-1}}$ (and $n \geq 1$). Thus, $x \in \mathbb{F}_p(x^p)$ for all $x \in \mathbb{F}_q$, so $\mathbb{F}_q/\mathbb{F}_p$ is separable. □

§5.8 Galois Theory

Definition 28. An algebraic extension L/K is *Galois* if it is normal and separable. The *Galois Group* of the extension $Gal(L/K) = Gal_K(L) = Aut_K(L)$ is the group of K-automorphisms of L, i.e., the group (for composition) of $\sigma : L \xrightarrow{\sim} L$ which are isomorphisms of rings (or fields) such that $\sigma|_K = id_K$ (that is, σ is K-linear).

For example, K/K is Galois, with $Gal(K/K) = 1$. $\mathbb{C}/\mathbb{R}$ is galois since it is normal (and separable since the characteristic is 0), and $Gal(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2 = \{1, \sigma\}$ where $\sigma : \mathbb{C} \to \mathbb{C}$ is defined by conjugation, $z \mapsto \overline{z}$. In general, in characteristic 0, $\overline{K}/K$ is Galois. Even more generally, K^{sep}/K is Galois. In fact, K^{sep} is the union of all L/K with $K \subset L \subset \overline{K}$ and L/K Galois.

Definition 29. The *absolute Galois group* of K refers to $Gal(\overline{K}^{sep}/K)$. If K is perfect, this is just $Gal(\overline{K}/K)$ (this is the case when $char(K) = 0$).

Theorem 49. *Any extension of a finite field is Galois.*

Proof. By Proposition 47, any finite extension of a finite field is normal and by Proposition 48, any finite extension of a finite field is separable. Thus, any finite extension of a finite field is Galois.

Let L/K be an extension of a finite field K, and let $\overline{K}$ be a fixed algebraic closure of K. Then, $L = \displaystyle\bigcup_{\substack{L \subset M \subset \overline{K} \\ M \text{ finite}}} M$. As we have seen, each M/K is both separable and normal, and thus, L/K is separable and normal, and hence, is Galois. □

Theorem 50. *Let L/K be finite (and thus, algebraic). The following are equivalent:*

1. *L/K is Galois.*
2. *L is the splitting field of some irreducible $P \in K[T]$ such that P is separable (and hence, $L \cong K[T]/P$ with P separable (and thus, simple)).*
3. *The group $Aut_K(L)$ has exactly $[L : K]$ elements.*

Proof. 1. ⇒ 2.: By Theorem 39, $L = K(x)$ since L/K is separable and finite. let P be the minimal polynomial of x over K. Since L/K is normal, P decomposes completely in L, so since x is a root of P and $x \in L$, L is the splitting field of P (which is separable since x is), so $L \cong K[T]/P$.
2. ⇒ 1.: If L is the splitting field of a separable polynomial P, then $L = K(\alpha_1, \ldots, \alpha_n)$ where the α_i's are the roots of P, which are separable. Thus, L/K is separable, since $K(\alpha_1, \ldots, \alpha_n) \subset K^{sep}$ and K^{sep}/K is seaprable, so by Corollary 35, $K(\alpha_1, \ldots, \alpha_n)/K$ is separable. Since L is a splitting field, it is normal. Hence, L/K is Galois.
1. ⇒ 3.: Fix $\sigma L \hookrightarrow \overline{K}$. Then, $Gal(L/K) = Aut_K(L) \hookrightarrow Hom_K(L, \overline{K})$ via $\tau \mapsto \sigma \circ \tau$. By definition, $Hom_K(L, \overline{K})$ has $[L : K]_S$ elements, so $|Aut_K(L)| \leq [L : K]_S = [L : K]$ since L/K is separable.

Conversely, for any $\rho \in Hom_K(L, \overline{K})$, $\rho(L) \subset L$ since L is normal (by Proposition 23). That is, $\rho|_L : L \to L$ is an automorphism of L. In other words, the inclusion $Aut_K(L) \subset Hom_K(L, \overline{K})$ is an equality. Hence, $|Aut_K(L)| = [L : K]$.

3. $\Rightarrow$ 1.: Fix $\sigma : L \hookrightarrow \overline{K}$, and consider $Aut_K(L) \subset Hom_K(L, \overline{K})$. By hypothesis, $[L : K] = |Aut_K(L)| \leq |Hom_K(L, \overline{K})| := [L : K]_S \leq [L : K]$. Thus, $[L : K]_S = [L : K]$, so L/K is separable, and $Hom_K(L, \overline{K}) = Aut_K(L)$, so for every $\rho : L \to \overline{K}$ which is K-linear, $\rho \in Aut_K(L)$, so $\rho(L) \subset L$, which by Proposition 23 means that L/K is normal. Hence, L/K is Galois.

□

Corollary 51. *If L/K is finite and Galois, then $|Gal(L/K)| = [L : K]$.*

Theorem 52. *Let L be a field, let G be a finite subgroupe of the group of field automorphisms of L. Then let $L^G = \{x \in L | \sigma(x) = x \forall \sigma \in G\} \subset L$. The extension L/L^G is finite and Galois with Galois group G.*

Proof. Let G be a finite subgroup of the group of field automorphisms of L and let $K = L^G$.

Let $x \in L$ be given and consider the finite set $Gx = \{\sigma(x) | \sigma \in G\}$, that is, the orbit of x under G.

Let $P_x = \prod_{y \in Gx} (T - y) \in L[T]$. By construction, P_X has only simple roots, and $P_x(X) = 0$ since $x \in G_x$ (because $x = id(x)$). Since G acts on L, it acts on $L[T]$ by coefficients. The action of G on $L[T]$ is by ring homomorphisms.

Then, for every $\sigma \in G$, $\sigma P_x = \prod_{y \in Gx} (T - \sigma y) = P_x$ since $y \in Gx$, thus the coefficients fo P_x are fixed by σ for every $\sigma \in G$, which means that $P_x \in L^G[T] = K[T]$.

Since $P_x(x) = 0$, the minimal polynomial of x over K divides P_x, so sinc eP_x has only simple roots, the minimal polynomail of x can only have simple roots, and thus is separable. Hence, x is separable over K, and since $x \in L$ was arbitrary, L/K is separable.

Also, L is the splitting field of the family $\{P_x | x \in L\}$, which means that L is normal.

Hence, L/K is Galois.

Now let $n = |G|$, and for the sake of contradiction, suppose there are m linearly indepdent (over K) elements $x_1, \ldots, x_m \in L$ with $m > n$. Let $G = \{\sigma_1, \ldots, \sigma_n\}$. Consider the matrix $A = (\sigma_i(x_j))_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \in M_{n \times n}(L)$.

Thus, we have a linear map from $L^m \xrightarrow{A} L^n$.

Since $m > n$, $ker(A) \neq 0$. Let λ be

$$\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix}$$

.

in $ker(A) \setminus 0$ with the least number of non-zero entries.

We may assume without loss of generality that $\lambda_1 \neq 0$, so $\lambda_1^{-1}\lambda$ is

$$\begin{pmatrix} 1 \\ \lambda_2/\lambda_1 \\ \vdots \\ \lambda_m/\lambda_1 \end{pmatrix}$$

and this has the same properties as λ, so without loss of generality we may assume $\lambda_1 = 1$.

We have $A \cdot \lambda = 0$, so for every $1 \leq i \leq n$, $(A \cdot \lambda)_i = \sum_{j=1}^{m} \sigma_i(x_j)\lambda_j = 0$.

Suppose that $\lambda_j \in K = L^G$ for all j. Then $0 = \sum_{j=1}^{m} \sigma_i(x_j)\lambda_j = \sum_{j=1}^{m} \sigma_i(x_j)\sigma_i(\lambda_j) = \sigma_i(\sum_{j=1}^{m} x_j\lambda_j) \Rightarrow \sum_{j=1}^{m} x_j\lambda_j = 0$, which would contradict the hypothesis that the x_j's are linearly independent.

So one of the λ_j's must be in $L \setminus K$. Without loss of generality, we may assume that it is λ_2. $\lambda_2 \notin K = L^G$ means that for some $1 \leq k \leq n$, $\sigma_k(\lambda_2) \neq \lambda_2$. Consider $\sigma_k(\lambda)$. This is just

$$\begin{pmatrix} \sigma_k(1) = 1 \\ \sigma_k(\lambda_2) \\ \vdots \\ \sigma_k(\lambda_m) \end{pmatrix}$$

Then, for $1 \leq i \leq n$, to compute $\sum_{j=1}^{m} \sigma_i(x_i) \cdot \sigma_k(\lambda_j)$, not that for some l, $\sigma_i = \sigma_k\sigma_l$ (in particular, $\sigma_l = \sigma_k^{-1}\sigma_i$), so this sum is just $\sum_{j=1}^{m} \sigma_k\sigma_l(x_i) \cdot \sigma_k(\lambda_j) = \sigma_k(\sum_{j=1}^{m} \sigma_l(x_i)\lambda_j) = 0$ since $\sum_{j=1}^{m} \sigma_l(x_i)\lambda_j = 0$. Thus, $\sigma_k(\lambda) \in ker(A)$.

Hence, $\lambda - \sigma_k(\lambda) \in ker(A)$ (since $ker(A)$ is a subspace), and we can write $\lambda - \sigma_k(\lambda)$ as

$$\begin{pmatrix} 1 - 1 = 0 \\ \lambda_2 - \sigma_k(\lambda_2) \neq 0 \\ \vdots \\ \lambda_m - \sigma_k(\lambda_m) \end{pmatrix}$$

Then, for every $1 \leq j \leq m$ such that $\lambda_j = 0$, we have $\lambda_j - \sigma_k(\lambda_j) = 0$. Thus, $\lambda - \sigma_k(\lambda_j) \in ker(A)$ and has strictly fewer non-zero entries than λ, which contradicts our selection of λ.

Thus, we must have that $[L : K] \leq |G|$.

Then, since $G \subset Aut_K(L)$, $|G| \leq |Aut_K(L)| = |Gal(L/K)| = [L : K]$.

Thus, $|G| = [L : K]$, and since $G \subset Gal(L/K)$, and they have the same number of elements, $G = Gal(L/K)$.

□

Corollary 53. *If L/K is Galois and finite with $Gal(L/K) = G$, then $K = L^G$.*

Proof. We have $K \subset L^G$ and $[L : L^G] = |G| = [L : K] \Rightarrow [L^G : K] = 1$. □

Definition 30. For $G \subset Aut(L)$, the subfield $L^G = \{x \in L | \sigma(x) = x \forall \sigma \in G\}$ is called the *fixed field* of G.

Theorem 54 (Fundamental Theorem for Finite Galois Extensions)**.** *Let L/K be a finite Galois extension. Let $G = Gal(L/K) = Aut_K(L)$. Then, there is a bijection of sets between*

$\{M|L/M/K\}$ and $\{H|H \leq G\}$. That is, between intermediate extension of L/K and subgroups of G, defined by $M \mapsto Gal(L/M) \leq G$ and $H \leq G \mapsto L^H$. Note that this bijection reverses inclusions.

Also, M/K is Galois if and only if M/K is normal and separable, and M/K is normal if and only if $H = Gal(L/M)$ is normal is G. Thus, there is a natural isomorphism $Gal(M/K) \cong G/H$.

Proof. Let M be an intermediate extension of L/K. We konw that L/M is Galois and $H = Gal(L/M) \leq Gal(L/K) = G$ since $\sigma|_M = id_M \to \sigma|_K = id_K$. By the previous corollary applied to L/M, we have $L = M$.

Let $H \leq G$. By the previous theorem, applied to L and the group H, we have L/L^H is Galois and $Gal(L/L^H) = H$. Of course, $K \subset L^H$ since $H \leq G = Aut_K(L)$.

Hence, we have the required bijection. Reversing inclusion is obvious, since if $H \leq H'$, then $L^{H'} \subset L^H$.

Let $L/M/K$ be given. We will show that M/K is normal if and only if $H \triangleleft G$. Note that $Hom_K(L, \overline{K}) \cong Aut_K(L)$ (using the fact that L is normal), and moreover, that any $\sigma \in Hom_K(M, \overline{K})$ is the restriction of some $\sigma \in Hom_K(L, \overline{K})$, and hence, of $\sigma \in Gal(L/K) = G$. Thus, we have $\sigma(M) \subset L$. By the bijection, $\sigma(M)$ corresponds to some subgroup. We see that this must be $\sigma H \sigma^{-1}$. Thus, M is normal if and only if $\sigma(M) \subset M$ for every $\sigma \Leftrightarrow \sigma(M) = M$ for every $\sigma \Leftrightarrow \sigma H \sigma^{-1} = H$ for every $\sigma \Leftrightarrow H \triangleleft G$.

The restriction $G = Gal(L/K) \to Gal(M/K)$ is surjective by the discussion above and has kernel $Gal(L/M) = H$. Hence, $G/H \xrightarrow{\cong} Gal(M/K)$.

□

Thus, we see that Galois theory connects fields to groups, and thus we have the following terminology.

Definition 31. An extension L/K is called *abelian* if it is Galois with an abelian Galois group, $G = Gal(L/K)$. It is called *cyclic* if G is cyclic.

§5.9 Galois Groups and Polynomials

Definition 32. Let $P \in K[T]$ be a polynomial of degree d and $\alpha_1, \dots, \alpha_d$ be the roots of P is $\overline{K}$ (repitition in roots is okay). Then the *discriminant* of P is the following number:

$$\Delta(P) = \Delta = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

P has multiple roots if and only if $\Delta P = 0$.

Consider $\delta = \prod_{i<j} (\alpha_i - \alpha_j)$. If $\sigma \in S_d$, σ acts on δ by permuting the α_i's, so $\sigma(\delta) = sgn(\sigma)\delta$.

Hence, $\sigma(\Delta) = sgn(\sigma)^2 \Delta = \Delta$. So Δ does not depend on the order of the roots.

Since Δ is a symmetric polynomial in the roots of P, it must be a polynomial of the coefficients of P.

Definition 33. Let $P \in K[T]$ be a *separable polynomial* (a product of irreducible separable polynomials). Its *Galois group* is $Gal(L/K)$ where L is the splitting field of P over K (which is a Galois extension).

Remark 7. If $P = (T - \alpha_1) \dots (T - \alpha_n) \in \overline{K}$, then for any $\sigma \in G = Gal(L/K)$ (where L is the splitting field of P), $\sigma(\alpha_i) = \alpha_j$ for some j. That is, σ permutes the roots, so $G \hookrightarrow S_n$. This is a monomorphism of groups, injectivity comes from the fact that $L = K(\alpha_1, \dots, \alpha_n)$ In particular, $[L : K] = |G|$, and $|G|$ divides $|S_n| = n!$. If P is also irreducible, $K(\alpha_i) = K[T]/P$ is a subfield of L of degree n, so $n | [L : K] | n!$.

Remark 8. Since $\sigma(\Delta) = \Delta$ for all $\sigma \in G \subset S_n$, $\Delta \in L^G = K$. Also, $K(\delta) \subset L$ corresponds to the subgroup $G \cap A_n$ of G (with $G \hookrightarrow S_n$ as above), since if $\sigma \in A_n$, $sgn(\sigma) = 1$, so $\sigma(\delta) = sgn(\sigma)\delta = \delta$.

Corollary 55. *If $P \in K[T]$, $char(K) \neq 2$, P is degree 3, irreducible, and separable, and L is the splitting field of P, then $[L : K] = 3$ if and only if $\Delta \in K^2$ (i.e., $\delta \in K$), in which case $Gal(L/K) = \mathbb{Z}/3\mathbb{Z}$. Otherwise, if $\Delta \notin K^2$, then $[L : K] = 6$ and $Gal(L/K) = S_3$.*

Remark 9. Let $P \in K[T]$ be separable and irreducible. Let $L = Split_K(P)$. The extension L/K is Galois. Let $\alpha_1, \dots, \alpha_n \in L$ be the roots of P. The α_i's are called conjugates, i.e., the conjugate of α means another root of $m_\alpha(x)$. The point is that the α_i's are permuted by $Gal(L/K)$, in fact, they are permuted transitively.

§5.10 Cyclotomic Extensions and Cyclic Extensions

Definition 34. Let $n \in \mathbb{N}$. An n^{th} root of unity in a field K is an $x \in K$ such that $x^n = 1$. By Kronecker, they form a cyclic subgroup of $K^\times$. A primitive n^{th} root of unity is an $x \in K$ such that $x^n = 1$ and $x^m \neq 1$ for every $m < n$.

For example, if $char(K) = p > 0$, then $T^p - 1 = (T-1)^p$, so there is only one p^{th} root of unity, namely, 1.

As such, when considered n^{th} roots of unity, we usually assume $char(K)$ does not divide n. In this case there are exactly n n^{th} roots of unity in $\overline{K}$. These roots form a subgroup of K^{times}, generated by any primitive n^{th} root.

In $\mathbb{Q}$, $\zeta = e^{2\pi i/n} \in \overline{\mathbb{Q}} \subset \mathbb{C}$ is a primitive n^{th} root of unity.

Definition 35. The polynomial $\Phi_n(T)$ given by $\Phi_n(T) := \prod_{gcd(j,n)=1} (T - \zeta^i)$ is the n^{th} *cyclotomic polynomial.* $\Phi_n \in \mathbb{Z}[T]$ is irreducible, and $T^n - 1 := \prod_{d|n} \Phi_d(T)$.

For a prime p, $\Phi_p(T) = \frac{T^p-1}{T-1} = T^{p-1} + \ldots + T + 1$. This is irreducible.

Remark 10. For any $n \in \mathbb{N}$, $deg(\Phi_n) = \#(\mathbb{Z}/n\mathbb{Z})^\times = \phi(n)$ where $\phi(mn) = \phi(m)\phi(n)$ if $(m,n) = 1$ and $\phi(p^l) = (p-1)p^{l-1}$.

Theorem 56. *The so-called cyclotomic extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ where $\zeta = e^{\frac{2\pi i}{n}}$ (or any primitive n^{th} root of unity) is Galois of degree $\phi(n)$. Moreover, $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \xrightarrow{\cong} (\mathbb{Z}/n\mathbb{Z})^\times$ via $\sigma \mapsto j$ such that $\sigma(\zeta) = \zeta^j$ and $j \mapsto (\zeta \mapsto \zeta^j)$.*

Proof. Let $L = \mathbb{Q}(\zeta)$. This containes ζ^j for every j, and thus, it is the splitting field of $\Phi_n(x)$ which has degree $\phi(n)$. For $\sigma \in Gal(L/\mathbb{Q})$, $\sigma(\zeta)$ is another primitive n^{th} root of unity, and hence, $\sigma(\zeta) = \zeta^j$ for some $j \in (\mathbb{Z}/n\mathbb{Z})^\times$. Thus, the map $Gal(L/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ which is clearly injcetive (since $L = \mathbb{Q}(\zeta)$) is a group homomorphism. Hence, it is an isomorphism since they have the same number of elements.

□

Theorem 57. *Let K be a field and $n \in \mathbb{Z}$ such that $char(K)$ does not divide n and K contains all n^th roots of unity (i.e., contains a primitive n^{th} root). Let $a \in K$ and consider $T^n - a \in K[T]$, $a \neq 0$. Let L' be a splitting field of $T^n - a$. Let $\alpha \in L'$ such that $\alpha^n = a$. Now, let $L = K(\alpha)$. Then, L is cyclic of order $d|n$, and $\alpha^d \in K$.*

Proof. First we have the decomposition $T^n - a = \prod_{0 \leq j \leq n-1} (T - \zeta^i \alpha)$. For $\sigma \in Gal(L/K)$, we have $\sigma(\alpha)$ is some othe rroot of $T^n - a$, hence, $\sigma(\alpha) = \zeta^j \alpha$ for $j \in \mathbb{Z}/n\mathbb{Z}$. As before, this gives an embedding of $Gal(L/k) \hookrightarrow \mathbb{Z}_n$. Then, $G := Gal(L/K)$ is a subgroup of $\mathbb{Z}_n$, which implies $G \cong (\mathbb{Z}/d\mathbb{Z})$ for some $d|n$. Finally, $N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$ is fixed by G, hence, belongs in K. So, $\alpha^d \zeta^k \in K$, which implies that $\alpha^d \in K$. □