Galois Theory - 6CCM326A

Alexandre Daoud
King's College London
alex.daoud@mac.com

March 28, 2015

Chapter 1

Ring Theory Review

Definition 1.1. *A* ***commutative ring with 1*** *is a triple* $(R, +, \times)$ *comprising of a set R equipped with two binary operations, addition + and multiplication* $\times$ *satisfying the following axioms:*

1. $(R, +)$ *is an abelian group*
2. *Multiplicaiton is associative*
3. *Multiplication distributes over addition*
4. *Multiplication is commutative*
5. *There exists* $1_R \in R$ *such that* $1_R \times r = r \times 1_R = r$ *for all* $r \in R$

Remark. *A normal ring does not require conditions 4 nor 5. We will refer to a commutative ring with 1 simply by ring henceforth.*

Proposition 1.2. *Consider an arbitrary ring R. Then there is a unique identity in R.*

Proof. Let $e_1 \neq e_2 \in R$ be two distinct identities. By definition of a ring identity, we have that $e_1 r = r e_1 = r$ and $e_2 r = r e_2 = r$ for all $r \in R$.
We thus have $e_1 e_2 = e_2 e_1 = e_1$ and $e_2 e_1 = e_2 e_1 = e_2$. But this means that $e_1 = e_2$ which is a contradiction. Hence R has a unique identity. $\square$

Example 1.3. *Typical examples of rings are* $\mathbb{Z}, \mathbb{Q}, \mathbb{C}$ *all equipped with their usual addition and multiplication.*

Example 1.4. *Let $n \in \mathbb{N}$, we define the ring $\mathbb{Z}/n\mathbb{Z}$ of* ***integers modulo n*** *as follows:*
We first define an equivalence relation $\sim$ on $\mathbb{X}$ by

$$a \sim b \text{ if } a \equiv b \ (\text{mod } n)$$

Then elements of $\mathbb{Z}/n\mathbb{Z}$ are the equivalence classes under this equivalence relation:

$$[a] = \{b \in \mathbb{Z} \,|\, a \equiv b \ (\text{mod } n) \ \}$$

Addition and multiplication is defined as $[a] + [b] = [a + b]$ and $[a][b] = [ab]$ respectively.

Definition 1.5. *Let R be a ring and X an indeterminate. We define the* ***ring of polynomials in X over R*** *$R[X]$ to be*

$$R[X] = \{c_0 + c_1X + c_2X^2 + \cdots + c_nX^n \,|\, c_i \in R \ \forall \, 0 \leq i \leq n\}$$

We define addition and multiplication on $R[X]$ as follows

$$\left(\sum_i c_iX^i\right) + \left(\sum_i c_i'X^i\right) = \sum_i (c_i + c_i')X^i$$
$$\left(\sum_i c_iX^i\right) \times \left(\sum_i c_i'X^i\right) = \sum_r \left(\sum_{i+j=r} c_ic_j'\right) X^r$$

Remark.

1. *We omit c_iX^i when $c_i = 0$*
2. *We write c_iX^i as X^i when $c_i = 1_R$*
3. *It is easily seen that R is a subset of $R[X]$ when considering the map $r \mapsto r + 0X + 0X^2 + \ldots$*
4. *If Y is any other indeterminate then we have that $(R[X])[Y] = R[X][Y] = (R[Y])[X]$*

Definition 1.6. *Let $R[X]$ be a polynomial ring and $f \in R[X]$ an arbitrary polynomial. We define the* ***degree*** *of f to be*

$$deg(f) = \begin{cases} \max\{i \,|\, c_i \neq 0\} & \text{if } \exists \, j \text{ s.t } c_j \neq 0_R \\ -\infty & \text{if otherwise} \end{cases}$$

Definition 1.7. *Let $(R, +_R, \times_R)$ and $(S, +_S, \times_S)$ be two rings. We define a **ring homomorphism** to be a function $f : R \to S$ such that for all $r_1, r_2 \in R$*

1. $f(r_1 +_R r_2) = f(r_1) +_S f(r_2)$
2. $f(r_1 \times r_2) = f(r_1) \times_S f(r_2)$
3. $f(1_R) = 1_S$

Definition 1.8. *Let $(R, +, \times)$ be a ring. We say that a ring $(S, +_S, \times_S)$ is a subring of R if*

1. $S \subseteq R$
2. $+_S|_{S\times S} = +_R$
3. $\times_S|_{S\times S} = \times_R$

Proposition 1.9. *Let R be a ring and $S \subseteq R$ a subring. Then $1_S = 1_R$.*

Proof. Consider $s \in S \subseteq R$. We have, by definition, that $s \times_S 1_S = 1_S \times_S s = s$. Since S is a subring of R, we therefore have that $s \times_R 1_S = 1_S \times_R s = s$. Now, since R is a ring, we can also see that $s \times_R 1_R = 1_R \times_R s = s$. From the two previous results, we have that $s \times_R 1_S = s \times_R 1_R$. Multiplying on the left by s^{-1} we can see that $1_S = 1_R$. □

Definition 1.10. *Let R be a ring. We say that a subset $I \subseteq R$ is an **ideal** of R if*

1. $(I, +)$ *is a subgroup of* $(R, +)$
2. $i \in I, r \in R$ *then* $ri \in I$

*We will denote an ideal by $I \lhd R$. We say that for $r \in R$, $(r) = \{xr \mid x \in R\}$ is the **ideal generated by r**.*

Definition 1.11. *Let R be a ring and $I \lhd R$ an ideal. We say that I is a **principal ideal** if there exists an element $r \in R$ such that $I = (r)$.*

Definition 1.12. *Let R be a ring and $I \triangleleft R$ an ideal. We define the* ***quotient ring*** $(R/I, +_I, \times_I)$ *as follows:*
We take the quotient of $(R, +)$ by $(I, +)$ to get the group $(R/I, +_I)$ where

$$R/I = \{\text{cosets of } I \text{ in } (R, +)\} = \{[r]_I \mid r \in R\}$$

and if $r_1, r_2 \in R$ then

$$[r_1]_I +_I [r_2]_I = [r_1 + r_2]_I$$

The multiplication in R induces a multiplicative structure on R/I. If $r_1, r_2 \in R$ then

$$[r_1]_I \times_I [r_2]_I = [r_1 \times r_2]$$

Example 1.13. *Let $n \in \mathbb{Z}$. Then the ring $\mathbb{Z}/n\mathbb{Z}$ is a quotient ring.*

Definition 1.14. *Let r_1 and r_2 be elements of a ring R. We say that $r_1 \neq 0$* ***divides*** r_2 *if there exists $r_3 \in R$ such that $r_2 = r_1 r_3$. Equivalently, r_1 divides r_2 if $(r_2) \subseteq (r_1)$. We denote this by $r_1 | r_2$.*

Definition 1.15. *Let r be an element of a ring R. We say that r is a* ***unit*** *if $r|1$. Equivalently, r is a unit if the ideal generated by r is the ring R. We also define the set*

$$R^\times = \{r \in R \mid \ r \text{ is a unit } \}$$

to be the set of units of R.

Remark. *Given a ring R, it is easy to see that $R^\times$ is a group under multiplication with identity 1_R.*

Definition 1.16. *Let r be a non-zero element of a ring R. We say that r is a* ***zero divisor*** *if there is a non-zero $s \in R$ such that $rs = 0$.*

Definition 1.17. *A ring R is called a* ***field*** *if $R^\times = R - \{0\}$*

Definition 1.18. *A ring R is called an* ***integral domain*** *if it does not contain any zero divisors.*

Definition 1.19. *Let R be a ring. We define a homomorphism from the integers to R by*

$$f_R : \mathbb{Z} \to R$$
$$f_R(n) = \begin{cases} \underbrace{1_R + \cdots + 1_R}_{n\ times} & if\ n > 0 \\ -\underbrace{(1_R + \cdots + 1_R)}_{n\ times} & if\ n < 0 \\ 0 & if\ n = 0 \end{cases}$$

This is known as the ***characteristic homomorphism****. We define the* ***characteristic of a ring*** *R to be the unique non-negative integer n such that* $ker(f_R) = (n)$*.*

Proposition 1.20. *Let R be an integral domain. Then the characteristic of R is either 0 or a prime number.*

Proof. Since R is an integral domain we have, by definition, that R has no zero-divisors. Now suppose that the characteristic n of R is composite. By definition of the characteristic of a ring we know that $f_R(n) = 0$. Now since n is composite, it must factor into some $a, b \in \mathbb{N}$. Since f_R is a ring-homomorphism (by construction) we have that

$$\begin{aligned} & f_R(n) = 0 \\ & \implies f_R(ab) = 0 \\ & \implies f_R(a) f_R(b) = 0 \end{aligned}$$

We have found zero-divisors $f_R(a), f_R(b) \in R$ which is obviously a contradiction to the assumption that R is an integral domain. Hence n cannot be composite and is either 0 or a prime. □

Definition 1.21. *Let* $I \lhd R$ *be an ideal of a ring R. We say that I is a* ***prime ideal*** *if* $I \neq R$ *and if for all* $r_1, r_2 \in R$

$$r_1 r_2 \in I \implies r_1 \in I \ or\ r_2 \in I$$

An element $r \in R$ *is called a* ***prime element*** *if the ideal* (r) *is a prime ideal.*
We can equivalently define a prime element r if $r \notin R^\times$ *and if for all* $r_1, r_2 \in R$

$$r | (r_1 r_2) \implies r | r_1 \ or\ r | r_2$$

Definition 1.22. *An element $r \notin R^\times$ of a ring R is called **irreducible** if for all $r_1 \in R$*

$$r_1 | r \implies r_1 \in R^\times$$

Proposition 1.23. *Let R be an integral domain. Then every prime element in R is irreducible.*

Proof. Suppose R is an integral domain and suppose that a prime element p is reducible. By definition we have that $p = ab$ for some $a, b \in R$. Obviously, p divides ab and since p is a prime element we know, by definition, that either p divides a or p divides b. Suppose, without loss of generality, that p divides a. By definition of divisibility we have that $a = pk$ for some $k \in R$. Inserting this into $p = ab$, we have that

$$\begin{aligned} & p = ab \\ & \implies p = pkb \\ & \implies p - pkb = 0 \\ & \implies p(1 - kb) = 0 \end{aligned}$$

Since R is an integral domain, we know that R has no zero divisors. Hence either $p = 0$ or $1 - kb = 0$.
If $p = 0$ then p is irreducible and we are done so assume that $1 - kb = 0$. It follows that $1 = kb$ and hence both k and b must be units. However this contradicts the assumption that p is reducible as we require both a and b to be non-unitary factors of p. Hence p must be irreducible. □

Definition 1.24. *A ring R is called a **unique factorisation domain** if it is an integral domain and if every non-zero element can be uniquely written as a product of irreducible elements.*

Proposition 1.25. *Let R be a unique factorisation domain. Then every irreducible element of R is a prime.*

Proof. Suppose R is a unique factorisation domain. Let $p \in R$ be an irreducible element and suppose that $ab \in (p)$ for some $a, b \in R$. We have that $ab = kp$ for some $k \in R$. Since R is a unique factorisation domain, a, b and k can be expressed as a unique product of irreducibles. Hence

$$\alpha_1 \ldots \alpha_n \beta_1 \ldots \beta_m = \gamma_1 \ldots \gamma_l p \tag{1.1}$$

for some irreducible $\alpha_i, \beta_j, \gamma_k \in R$. Since each factorisation of a, b and k must be unique, the irreducibles on the left hand side of (1.1) must match up with one on the right. Since p itself is an irreducible, it must match up with an irreducible on the left hand side. Hence p must be a factor of either a or b and thus $a \in (p)$ or $b \in (p)$ and p is a prime element. $\square$

Definition 1.26. *A ring R is called a* ***principal ideal domain*** *if it is an integral domain and every ideal of R is a principal ideal.*

Proposition 1.27. *Let R be a principal ideal domain. Then it is a unique factorisation domain.*

Definition 1.28. *Let $I \triangleleft R$ be an ideal of a ring R. We say that I is a* ***maximal ideal*** *if $I \neq R$ and if $I \subseteq J \triangleleft R$ for some ideal J then $I = J$ or $J = R$.*

Proposition 1.29. *Let R be a ring and $I \triangleleft R$ an ideal. Then*

1. *I is a prime ideal if and only if the quotient ring R/I is an integral domain*
2. *I is a maximal ideal if and only if the quotient ring R/I is a field.*
3. *Every maximal ideal is also a prime ideal*

Proof.

Part 1:

$\implies$: Let R be a ring and $I \triangleleft R$ a prime ideal. We want to show that R/I is an integral domain. We first note that from the definition of cosets, for an ideal I and an element $r \in R, r + I = I \implies r \in I$ and that I is itself the zero element of the quotient ring. Now suppose that $(r + I)(s + I) = I$ for some $r + I, s + I \in R/I$. By the definition of multiplication in a quotient ring, it follows that $rs + I = I$. From the properties of cosets mentioned before, this means that $rs \in I$. Now since I is a prime ideal, we have that either $r \in I$ or $s \in I$. But this just means that $r + I = I$ or $s + I = I$ which is exactly what it means for R/I to be an integral domain.

$\impliedby$: Now suppose that R/I is an integral domain. We need to show that I is a prime ideal. Let $a, b \in R$ be such that $ab \in I$. By the definition of the quotient ring R/I, we have that $ab + I = I$. It follows from the definition of multiplication in a quotient ring that $(a + I)(b + I) = I$. Since R/I is an integral domain, this must mean that either $a + I = I$ or $b + I = I$. Thus $a \in I$ or $b \in I$. We have shown that if $ab \in I$ then $a \in I$ or $b \in I$, hence I is a prime ideal.

Part 2:

$\Longrightarrow$: Let R be a ring and $I \triangleleft R$ a maximal ideal. We want to show that R/I is a field. In particular, we have to show that $(R/I)^{\times} = R/I - 0_{R/I} = R/I - I$. Let $a + I \in R/I$ be a non-zero element. We want to show that there exists a $b+I \in R/I$ such that $(a+I)(b+I) = 1+I$. By the definition of multiplication in a quotient ring, we have that $(a + I)(b + I) = ab + I = 1 + I$. Hence it suffices to show that there exists $b \in R$ such that $ab - 1 \in I$. Now consider the ideal

$$J = \{ar + i \,|\, i \in I\}$$

for some $r \in R$. Obviously, this ideal properly includes the ideal I. But I is a maximal ideal so J must be equal to R. Hence $ar + i = 1$ for some $r \in R$ and $i \in I$. This implies that $ar - 1 \in I$. Passing back to the quotient ring, we see that $(ar - 1) + I = I$ which implies that $ar + I = 1 + I$. By the definition of multiplication in the quotient ring, we have that $(a + I)(r + I) = 1 + I$. Hence we have found a b, namely r, for which $a + I$ has an inverse in the quotient ring. Hence the quotient ring is a field.

$\Longleftarrow$: Now suppose that R/I is a field. In particular, every non-zero element of R/I has an inverse. We want to show that I is a maximal ideal. Consider $J \supsetneq I$ an ideal of R properly containing I and let $a \in J$ such that $a \notin I$. It follows that $a + I \neq I$ and hence, since R/I is a field, $(a + I)(b + I) = 1 + I$ for some $b \in R$. By the definition of multiplication in the quotient ring, we have that $ab - 1 \in I$. Denote $i = ab - 1$. We can see that $1 = ab - m$. Since $a, m \in J$, it follows that $1 \in J$ which must mean that $J = R$. Hence I is a maximal ideal.

Part 3: Let I be a maximal ideal of R. By part 2, we have that R/I is a field. Since all fields are integral domains, we have that R/I is an integral domain. By part 1, this must mean that I is a prime ideal.

$\square$

Lemma 1.30. *Let R and S be two rings and $f : R \to S$ a homomorphism of rings. Then*

1. $ker(f) = \{r \in R \mid f(r) = 0\}$ *is an ideal of R*
2. $Im(f)$ *is a subring of S*
3. *f induces an isomorphism of rings*

$$\begin{aligned} R/ker(f) &\to Im(f) \\ [r]_{ker(f)} &\mapsto f(r) \end{aligned}$$

for all $r \in R$.

Chapter 2

Polynomial rings

Definition 2.1. *Let* $f(X) = (c_0, c_1, \dots) = \sum_i c_i X^i$ *be a non-zero polynomial. The* ***leading term*** *(leading coefficient) if* $f(X)$ *is defined to be* $c_d X^d (c_d)$*. We say that* $f(X)$ *is* ***monic*** *if the leading coefficient is 1.*

Lemma 2.2. *Let* R *be a ring and* $f_1, f_2 \in R[X]$ *two polynomials. Then*

1. $\deg(f_1 + f_2) \leq \max\{\deg(f_1), \deg(f_2)\}$
2. $\deg(f_1 f_2) \leq \deg(f_1) + \deg(f_2)$ *with equality holding if* R *is an integral domain.*

Proof. If either f_1 or f_2 are the zero polynomial then we are done hence suppose that $f_1, f_2 \neq 0$. Let $f_1(X) = \sum_i c_i X^i$ and $f_2(X) = \sum_i d_i X_i$ for some constants $c_i, d_i \in R$.

Part 1: By the definition of addition of polynomials, we have that

$$\deg\left(f_1(X) + f_2(X)\right) = \deg\left(\sum_i (c_i + d_i) X^i\right)$$

By the definition of the degree of a polynomial, it follows that

$$\begin{aligned} \deg\left(\sum_i (c_i + d_i) X^i\right) &= \max\{i \mid c_i + d_i \neq 0\} \\ &\leq \max\big\{\max\{i \mid c_i \neq 0\}, \max\{i \mid d_i \neq 0\}\big\} \\ &= \max\{\deg(f_1), \deg(f_2)\} \end{aligned}$$

Part 2: Let c_nX^n be the leading term of $f_1(X)$ and d_mX^m the leading term of $f_2(X)$. Then by the definition of polynomial multiplication, we have that $f_1(X)f_2(X) = e_{n+m}X^{n+m} + \cdots + e_0$ for some constants $e_i \in R$. Obviously, the degree of $f_1(X)f_2(X)$ can be no greater than $n+m$. Hence we have that $\deg(f_1(X)f_2(X)) \not> \deg(f_1) + \deg(f_2)$.
Since the ring R could have zero divisors, it could happen that $0 = e_{n+m} = c_nd_m$ and hence $\deg(f_1(X)f_2(X)) < \deg(f_1(X)) + \deg(f_2(X))$. Hence it follows that $\deg(f_1(X)f_2(X)) \leq \deg(f_1) + \deg(f_2)$.
In the case where R is an integral domain, it cannot have any zero divisors meaning e_{n+m} cannot be 0 hence the degree of $f_1(X)f_2(X)$ can never be less than $n+m$. We are thus left with $\deg(f_1(X)f_2(X) = \deg(f_1) + \deg(f_2)$

□

Corollary 2.3. *Let R be a ring. We have that*

1. *R is an integral domain if and only if $R[X]$ is an integral domain*
2. *$R^\times \subseteq R[X]^\times$ with equality if R is an integral domain*

Proof.

Part 1:

$\implies$: Assume R is an integral domain and consider two polynomials $f, g \in R[X]$. Suppose that $fg = 0_R$ with $f, g \neq 0_R$. We can write $f = a_nX^n + \cdots + a_0$ and $g = b_nX^n + \cdots + b_0$ for some $a_i, b_i \in R$. We know that the leading term of fg, by definition of multiplication of polynomials is $a_nb_nX^n$. Since $fg = 0_R$, we require that $a_nb_n = 0_R$. Since R is an integral domain, either $a_n = 0_R$ or $b_n = 0_R$. Suppose, without loss of generality that $a_n = 0_R$. This is a contradiction however as we assumed that $f \neq 0 \implies a_n \neq 0_R$. Hence if $fg = 0_R$ then either $f = 0_R$ or $g = 0_R$ and $R[X]$ is an integral domain.

$\impliedby$: Assume $R[X]$ is an integral domain and consider $a, b \in R$. Now consider the two polynomials $f(X) = a$ and $g(X) = b$ in $R[X]$. Assume that $fg = 0_R$. This is equivalent to the assumption that $ab = 0_R$. Since $R[X]$ is an integral domain, this means either $f(X) = a = 0$ or $f(X) = b = 0$, meaning that R is an integral domain.

□

Theorem 2.4. *Let R be a field and $f, g \in R[X]$ two non-zero polynomials. Then there exists $q, r \in R[X]$ such that $f = qg + r$ with $\deg(r) < \deg(f)$. Furthermore, q and r are uniquely determined by f and g.*

Proof. If $\deg(f) < \deg(g)$, we can take $q = 0$ and $r = f$ and we are done so assume that $\deg(f) \geq \deg(g)$.
Now set $f(X) = a_n X^n + \cdots + a_0$ and $g(X) = b_m X^m + \cdots + b_0$ for some $a_i, b_i \in R$. We will prove the theorem by induction on the degree of f. For the base step, let $\deg(f) = 1$ and we can take $q = \frac{a_n}{b_n}$ and $r = f - qg$.
Now assume that the theorem is true for $\deg(f) = k - 1$. We want to show that it is true for $\deg(f) = k$.
Consider the polynomial

$$\begin{aligned} h &= f - \frac{a_n}{b_m} X^{n-m} g \\ &= a_n X^n + \cdots + a_0 - \frac{a_n}{b_m} X^{n-m} \left[b_m X^m + \cdots + b_0 \right] \\ &= a_n X^n + \cdots + a_0 - \left[a_n X^n + \frac{a_n b_{m-1}}{b_m} X^{n-1} + \cdots + \frac{a_n b_0}{b_m} X^{n-m} \right] \\ &= \frac{a_n b_{m-1}}{b_m} X^{n-1} + \cdots + \frac{a_n b_0}{b_m} X^{n-m} + \cdots + a_0 \end{aligned}$$

Obviously, this polynomial has degree $k-1$ and by the induction hypothesis, there exists a q_1 and r_1 such that $h = gq_1 + r_1$. Now we have that

$$\begin{aligned} & h = gq_1 + r_1 \\ \implies & f - \frac{a_n}{b_m} X^{n-m} g = gq_1 + r_1 \\ \implies & f = gq_1 + \frac{a_n}{b_m} X^{n-m} g + r_1 \\ \implies & f = g(q_1 + \frac{a_n}{b_m} X^{n-m}) + r_1 \end{aligned}$$

Hence we have found a $q = q_1 + \frac{a_n}{b_m} X^{n-m}$ and $r = r_1$ hence the theorem is true for $deg(f) = k$.
Now assume that $f = gq_1 + r_1$ and $f = gq_2 + r_2$ for distinct q_1, q_2 and r_1, r_2 with $deg(r_1) < g$ and $deg(r_2) < g$. We have that

$$\begin{aligned} & gq_1 + r_1 = gq_2 + r_2 \\ \implies & g(q_1 - q_2) = r_2 - r_1 \end{aligned}$$

Hence $g|(r_2 - r_1)$ but since $deg(r_2 - r_1) < deg(g)$, we must have that $r_2 - r_1 = 0 \implies r_2 = r_1$. Furthermore, we then have that $g(q_1 - q_2) = 0$ and since $g \neq 0$, we must have $q_1 = q_2$. □

Corollary 2.5. *Let R be a field and $f, g \in R[X]$ not both zero. Then there exists a unique $h \in R[X]$ such that*

1. *$h|f$ and $h|g$*
2. *h is monic*
3. *the degree of h is maximal among all $l \in R[X]$ such that $l|f$ and $l|g$*

Such a polynomial is called the ***greatest common divisor*** *of f and g.*

Proof. Consider the set

$$S = \{a(X)f(X) + b(X)g(X) \mid a(X), b(X) \in R[X], af + bg \neq 0\}$$

and let $h_1(X) = a_1(X)f(X) + b_1(X)g(X) \in S$ be the polynomial of least degree. If the leading coefficient is not 1_R, we can multiply though by its inverse, say a_n^{-1}, to obtain a monic polynomial $h(X) = a(X)f(X)+b(X)g(X)$ where $a(X) = a_n^{-1}a_1(X)$ and $b(X) = a_n^{-1}b_1(X)$. We claim that $h(X)|f(X)$ and $h(X)|g(X)$.
By the division algorithm for polynomials, we have that

$$\begin{aligned} f(X) = h(X)q(X) + r(X), \quad \deg(r(X)) < \deg(h(X)) \\ \implies r(X) = f(X) - h(X)q(X) \end{aligned} \tag{2.1}$$

After substituting $h(X)$ into (2.1), we are left with

$$r(X) = f(X)(1 - q(X)a(X)) - q(X)b(X)g(X)$$

Now since $deg(r(X)) < deg(h(X))$ and $h(X)$ is, by assumption, the polynomial of least degree in S, we have that $r(X) \notin S$. This implies that $r(X)$ must equal 0.
We thus have that $f(X) = h(X)q(X)$ meaning that $h(X)|g(X)$. A similar argument can be applied to $g(X)$ to arrive at $h(X)|g(X)$.
The polynomial $h(X)$ is monic by construction so it remains to show the third part.
Consider a polynomial $l(X)$ such that $l(X)|f(X)$ and $l(X)|g(X)$. Then we have that $l(X)|(a(X)f(X) + b(X)g(X))$ for all $a(X), b(X) \in R[X]$. In particular, $l(X)$ must divide $h(X)$. Hence $h(X)$ must be the polynomial of maximal degree dividing both $f(X)$ and $g(X)$. $\square$

Corollary 2.6. *If R is a field then $R[X]$ is a principal ideal domain.*

Proof. Consider an ideal $I \lhd R[X]$. If I is the zero ideal then it is principal and we are done, hence let $I \neq \{0\}$.
Now consider the set

$$S = \{f(X) \in I \mid f(X) \neq 0\}$$

and choose $h(X) \in S$ such that $h(X)$ is of minimal degree. We claim that $I = (h(X))$. It suffices to show that $f(X) = h(X)q(X)$ for some $q(X) \in R[X]$.
Since R is a filed, we can apply the division algorithm for polynomials and we have that

$$f(X) = q(X)h(X) + r(X), \quad \deg(r(X)) < \deg(h(X))$$

for some $q(X), r(X) \in R[X]$. It follows that $r(X) = f(X) - q(X)h(X)$. Since $f(X), h(X) \in I$, we can see that $r(X) \in I$. But $r(X)$ has degree strictly less than $h(X)$ and $h(X)$ is a non-zero polynomial of least degree, hence $r(X) = 0$. □

Corollary 2.7. *Let R be a field and consider a polynomial $g(X) \in R[X] \backslash R$. Then $g(X)$ is irreducible if and only if the ideal generated by $g(X)$ is maximal ideal of $R[X]$.*

Proof.

$\Longrightarrow$: Let R be a field and $g(X) \in R[X] \backslash R$ an irreducible polynomial. We want to show that $(g(X))$ is maximal. Consider a polynomial $f(X) \in R[X]$ such that $(g(X)) \subseteq (f(X)) \subsetneqq R[X]$. We therefore have that for some polynomial $h(X) \in R[X]$, $g(X) = f(X)h(X)$.
Now since $f(X)$ is irreducible, we have that either $h(X) \in R[X]^{\times}$ or $g(X) \in R[X]^{\times}$. But $(f(X))$ is a proper principal ideal and hence we cannot have that $f(X) \in R[X]^{\times}$. Hence $h(X) \in R[X]^{\times}$. Therefore $(f(X)) = (g(X))$ and the ideal generated by $g(X)$ is maximal across all proper ideals of $R[X]$.

$\Longleftarrow$: Now suppose that $(g(X))$ is maximal. We want to show that $(g(X))$ is irreducible. Assume that $(g(X))$ is reducible and hence $g(X) = f(X)h(X)$ for some non-units $f(X), h(X) \in R[X]$. Now since neither $f(X)$ and $h(X)$ are non-units, we have that $(g(X)) \subsetneqq (f(X))$ which contradicts the maximality of $(g(X))$. Hence $g(X)$ must be irreducible.

□

Definition 2.8. *Let $f(X) = \sum_{i=0}^{d} c_i X^i$ be a polynomial in $R[X]$. We define the **evaluation map at r** to be the map*

$$\begin{aligned} ev_r : R[X] &\to R \\ f(X) &\mapsto f(r) \end{aligned}$$

Lemma 2.9. *Let R be a ring and $S \subseteq R$ a subring. Consider $r \in R$. The smallest subring of R which contains both S and r is $S[R] = ev_r|_{S[X]}$.*

Lemma 2.10. *Consider a ring R and the evaluation map ev_r for some $r \in R$ and $f(X) = \sum_{i=0}^{d} c_i X^i \in R[X]$. Then the kernel of the map ev_r is the principal ideal $(X - r)$.*

Proof. By the definition of the kernel, we have that the kernel of the evaluation map is

$$\ker(ev_r) = \{f(X) \in R[X] \mid f(r) = 0\}$$

Obviously, this corresponds to all polynomials that have $r \in R$ as a root which is equivalent to all polynomials generated by the ideal $(X - r)$. $\square$

Definition 2.11. *Consider a polynomial $f \in \mathbb{Z}[X]$. We say that f is **primitive** if $\deg(f) \geq 1$ and if the greatest common divisor of the coefficients of f is 1.*

Lemma 2.12. *Consider two primitive polynomials $f = \sum_i a_i X^i, g = \sum_i b_i X^i \in \mathbb{Z}[X]$. Then their product fg is a primitive polynomial*

Proof. Let $h(X) = f(X)g(X)$. Suppose that $h(X)$ is not primitive. Then there exists a prime p that is a common divisor of all the coefficients of $h(X)$. Since $f(X)$ and $g(X)$ are primitive, p cannot be a divisor of all of the a_i or all of the b_i. Let $a_r X^r$ and $b_s S^r$ be the terms of highest degree whose coefficient p does not divide, respectively in $f(X)$ and $g(X)$. Now consider the term of degree $r + s$ in $h(X)$. By the definition of multiplication of polynomials, its coefficient is given by

$$\sum_{k+l=r+s} a_k b_l$$

This sum contains the term $a_r b_s$ which is not divisible by p. Hence the entire sum is not divisible by p. This is a contradiction to the assumption that p is a common divisor of all the coefficients of $h(X)$. Hence there does not exist a prime which divides all the coefficients of $h(X)$, thus it is primitive. $\square$

Proposition 2.13. *Consider a primitive polynomial $f \in Z[X]$. Then f is irreducible in $\mathbb{Z}[X]$ if and only if it is irreducible in $\mathbb{Q}[X]$.*

Proof.

$\Longrightarrow$: Let f be a primitive polynomial that is irreducible in $\mathbb{Z}[X]$ and let $f(X) = g(X)h(X)$ where $g(X), h(X) \in \mathbb{Q}[X]$. We can choose $\frac{a}{b}, \frac{c}{d} \in \mathbb{Q}$ such that $\frac{a}{b}f(X)$ and $\frac{c}{d}g(X)$ are primitive. Hence, by the previous lemma, $\frac{ac}{bd}f(X)$ is a primitive polynomial. But $f(X)$ is itself, by assumption, a primitive polynomial. Thus $\frac{ac}{bd} = 1$.
We therefore have that $\frac{ab}{cd}g(X)h(X) = (\frac{a}{b}g(X))(\frac{c}{d}h(X))$ is a factorisation of $f(X)$ in $\mathbb{Z}[X]$. Since $f(X)$ is irreducible, we must either have that $\frac{a}{b}g(X) \in \mathbb{Z}^\times$ or $\frac{c}{d}h(X) \in \mathbb{Z}^\times$. Hence $g(X) \in Q[X]^\times$ or $h(X) \in Q[X]^\times$.

$\Longleftarrow$: Now assume that f is a primitive polynomial that is irreducible in $\mathbb{Q}[X]$. Since $\mathbb{Z} \subseteq \mathbb{Q}$, it follows that f must be irreducible in $\mathbb{Z}[X]$.

□

Remark. *The two previous lemmas are together referred to as **Gauss' Lemma**.*

Proposition 2.14. *(Eisenstein's Criterion)*
Let $f(X) = \sum_{i=0}^{n} c_i X^i$ be a primitive polynomial of degree n in $\mathbb{Z}[X]$. If there exists a prime p such that

1. *$p|c_i$ for $0 \leq i < n$*

2. *p^2 does not divide c_0*

then $f(X)$ is irreducible in $\mathbb{Q}[X]$.

Proof. Consider a prime p satisfying the hypothesis and the image $\overline{f}(X)$ of $f(X)$ under the map

$$\begin{aligned} \mathbb{Z}[X] &\to \mathbb{F}_p[X] \\ c_i &\mapsto c_i \text{ (mod p)} \end{aligned}$$

Since $p|c_i$ for $0 \leq i < n$ and $f(X)$ is a primitive polynomial, the leading term of $\overline{f}(X)$ must be 1 while the other terms are congruent to 0 modulo p. Hence we have that $\overline{f}(X) = X^n$.
Now suppose that $f(X)$ is reducible. We have that $f(X) = g(X)h(X)$ for some $g(X), h(X) \in \mathbb{Z}[X]$ and $\deg(f) > \deg(g), \deg(h)$. Then $\overline{g}(X) = X^m$

and $\overline{h}(X) = X^{n-m}$ for some $0 < m < n$. Hence the constant term of $g(X)$ and $h(X)$ are both divisible by p. This would imply that the constant term of f is divisible by p^2 which contradicts the assumptions for the prime p. Hence f must be irreducible. $\square$

Chapter 3

Field Extensions

Definition 3.1. *Let L be a field and $K \subseteq L$ a subfield. We define the* ***field extension of L over K*** *to be the pair (K, L) and denote it by L/K.*

Remark. *We can consider a field L to be a vector space over one of its subfields K. The elements of L are the vectors and the elements of K are the scalars*

Definition 3.2. *Let L/K be a field extension. We define the* ***degree*** *of K/L to be the dimension of L as a K-vector space. It is denoted by $[L : K]$.*

Example 3.3. *Let K be a field and $f(X) \in K[X]$ an irreducible polynomial of positive degree. Then $K[X]/(f(X))$ is a field by previous results and the map*

$$\begin{aligned} i_f : K &\to K[X]/(f(X)) \\ k &\mapsto [k]_{f(X)} \end{aligned}$$

is a ring homomorphism. This gives a field extension $(K, K[X]/(f(X))$ whose degree is equal to deg(f).

Theorem 3.4. *(Tower Law)*
Consider two field extensions L/K and M/L. Then M/K is a field extension and

$$[M : K] = [M : L][L : K]$$

Proof. Let $\{m_\alpha \,|\, \alpha \in I\}$ be an L-basis of M and $\{l_\beta \,|\, \beta \in J\}$ be a K-basis of L. We will show that $\{m_\alpha l_\beta \,|\, \alpha \in I, \beta \in J\}$ is a K-basis of M.
Consider $m \in M$. Then

$$m = \sum_{i=1}^{n} x_i m_{\alpha_i}$$

for some $x_i \in L$. Now we can write each x_i as

$$x_i = \sum_{j=1}^{k} y_{ij} l_{\beta_j}$$

for some $y_{ij} \in K$. Thus

$$m = \sum_i \sum_j y_{ij} m_{\alpha_i} l_{\beta_j}$$

Hence the set $\{m_\alpha l_\beta \,|\, \alpha \in I, \beta \in J\}$ spans M as a K-vector space.
Now, if

$$\sum_{i,j} a_{ij} m_{\alpha_i} l_{\beta_j} = 0$$

with $a_i j \in K$, then

$$\sum_i \left(\sum_j a_{ij} l_{\beta_j} \right) m_{\alpha_i} = 0$$

Since $\{m_\alpha \,|\, \alpha \in I\}$ is linearly independent over L, we can see that $\sum_j a_{ij} l_{\beta_j} = 0$ for each i. Again, since $\{l_\beta \,|\, \beta \in J\}$ is linearly independent over K, we can see that $a_i j = 0$ for all i, j. Hence $\{m_\alpha l_\beta \,|\, \alpha \in I, \beta \in J\}$ is linearly independent and thus it forms a K-basis for M. The cardinality of this set is exactly equal to the product of the cardinalities of $\{m_\alpha \,|\, \alpha \in I\}$ and $\{l_\beta \,|\, \beta \in J\}$ hence it also follows that

$$[M : K] = [M : L][L : K]$$

$\square$

Chapter 4

Algebraic Extensions

Definition 4.1. *Let L/K be a field extension. An element $l \in L$ is said to be **algebraic** over K if there exists a non-zero polynomial $f \in K[X]$ such that $f(l) = 0$. If there exists no such polynomial, the element l is said to be **transcendental** over K. The extension L/K is said to be **algebraic** if every element of L is algebraic over K.*

Example 4.2. *Let L/K be a field extension and $l \in L$. Consider the evaluation at l*

$$\begin{aligned} ev_L : K[X] &\to L \\ f(X) &\mapsto f(l) \end{aligned}$$

It follows from this that l is transcendental over K if and only if ev_l is injective.

Proposition 4.3. *Let L/K be a finite dimensional field extension. Then L/K is algebraic.*

Proof. Let L/K be a finite extension and $l \in L$. Consider the set

$$\{1, l, l^2, \dots\}$$

If this set is finite then $l^n = 1$ for some $n \in \mathbb{N}$. This implies that l is a root of the polynomial $f(X) = X^n - 1 \in K[X]$ and hence l is algebraic over K. If the set is infinite then it cannot be linearly independent over K. Hence we have that

$$\sum_i a_i l^i = 0$$

for some $a_i \in K$. Therefore, l is a root of $f(X) = \sum_i a_i X^i \in K[X]$ and l is algebraic over K. $\square$

Proposition 4.4. *Let L/K be a field extension and $l \in L$ be algebraic over K. Then there is a unique polynomial $p(X) \in K[X]$ such that*

1. *$p(X)$ is monic*
2. *$p(l) = 0$*
3. *$\deg(p(X))$ is minimal among the polynomials $q(X) \in K[X]$ satisfying $q(l) = 0$*

Furthermore, this polynomial is irreducible and is called the ***minimal polynomial*** *of l over K. It is denoted by $\min_{l,K}(X)$.*

Proof. Consider the evaluation map

$$\begin{aligned} ev_l : L[X] &\to L \\ f(X) &\mapsto f(l) \end{aligned}$$

Let $e = ev_l|_{K[X]}$ and $I = ker(e) \subseteq K[X]$. Since l is algebraic over K, the ideal I is non-trivial. It is also not the whole ring $K[X]$ since 1_K maps to itself and is hence not in the kernel. Therefore, since a polynomial ring is a principal ideal domain, we have that $I = (p(X))$ for some non-constant polynomial $p(X) \in K[X]$.
Now assume that $p(X)$ is monic. Obviously, $p(X)$ satisfies all three conditions listed in the proposition.
To show that $p(X)$ is irreducible, assume that it is reducible. Then $p(X) = f(X)g(X)$ for some non-units $f(X), g(X) \in K[X]$ with $\deg(p) > \deg(f), \deg(g)$. Then $p(l) = f(l)g(l) = 0$. This means that either $f(l) = 0$ or $g(l) = 0$. But this contradicts the fact that $p(X)$ is the polynomial of least degree in $K[X]$ where l is a root. Therefore, $p(X)$ is irreducible in $K[X]$. $\square$

Proposition 4.5. *Let L/K be a field extension and $l \in L$ algebraic. Then there exists a unique isomorphism of rings*

$$\begin{aligned} \theta_l : K[X]/(p(X)) &\to K[l] \\ [X]_{(p(X))} &\mapsto l \\ [k]_{(p(X))} &\mapsto k, \quad \forall k \in K \end{aligned}$$

In particular, $K[l]$ is a field and the degree of the extension $K[l]/K$ is equal to $\deg(p(X))$.

Proposition 4.6. *Let L/K be a field extension and $L \in L$ transcendental. Then there exists a unique isomorphism of rings*

$$\begin{aligned} \theta_k : K[X] &\to K[l] \\ X &\mapsto l \\ k &\mapsto k, \quad \forall k \in K \end{aligned}$$

In particular, $K[l]$ is not a field and the degree of the field extension is infinite.

Definition 4.7. *Let L/K be a field extension and $l_1, l_2 \in L$. l_1 and l_2 are said to be **conjugates** if they are both algebraic over K and have the same minimal polynomial.*

Corollary 4.8. *Let K be a field, $f(X) \in K[X]$ irreducible and L_1, L_2 extensions of K. If l_1 and l_2 are roots of $f(X)$ in L_1 and L_2 respectively then there exists a unique isomorphism of fields*

$$\begin{aligned} \theta : K[l_1] &\to K[l_2] \\ l_1 &\mapsto l_2 \\ k &\mapsto k, \quad \forall k \in K \end{aligned}$$

Proof. This follows by considering the maps

$$K[L_1] \leftarrow K[X]/(p(X)) \to K[L_2]$$

□

Definition 4.9. *Let R be an integral domain and consider the set $\{\frac{r}{s} \,|\, r, s \in R, s \neq 0\}$. We define an equivalence relation $\frac{r}{s} \sim \frac{r'}{s'} \iff rs' = r's$. We then define*

$$Frac(R) = \left\{ \frac{r}{s} \,|\, r, s \in R, s \neq 0 \right\} / \sim$$

*to be the **field of fractions** of R.*

Lemma 4.10. *Let R be an integral domain. Then*

1. *$Frac(R)$ is a field*
2. *R injects into $Frac(R)$ with the map $r \to \frac{r}{1_R}$*

3. *If $\sigma : R \to K$ is an injective ring homomorphism then there is a unique ring homomorphism $\tilde{\sigma} : Frac(R) \to K$ such that the following diagram commutes*

$$\begin{tikzcd} R \arrow[r, "\sigma"] \arrow[d] & K \\ Frac(R) \arrow[ur, "\tilde{\sigma}"'] & \end{tikzcd}$$

Example 4.11. $Frac(\mathbb{Z}) \cong \mathbb{Q}$

Example 4.12. *If R is a field then $Frac(R) \cong R$*

Remark. *Let L/K be a field extension and $l_1, \ldots, l_n$ elements of L. Then we write*

$$K(l_1, \ldots, l_n) := Frac(K[l_1, \ldots, l_n])$$

Definition 4.13. *Let L/K be a field extension. We say that L is* ***generated*** *by $l_1, \ldots, l_n$ over K if $L = K(l_1, \ldots, l_n)$. The elements $l_1, \ldots, l_n$ are called* ***generators*** *of L over K.*

Definition 4.14. *Let L/K be a field extension. We say that L/K is* ***simple*** *if L is generated by a single element over K.*

Chapter 5

Embeddings of Fields

Definition 5.1. *Let K be a field and $f(X) \in K[X]$ a polynomial. We say that $f(X)$* ***splits completely*** *in K if*

$$f(X) = c(X - k_1) \dots (X - k_n)$$

for some $c, k_1, \dots, k_n \in K$.

Proposition 5.2. *Let K be a field and $f(X) \in K[X]$ a polynomial. Then there exists a field extension L/K of finite degree such that $f(X)$ splits completely in $L[X]$.*

Proof. We prove the theorem by induction on $\deg(f)$. For the basis case, assume $deg(f) = 1$. By definition, $f(X)$ splits completely in $K[X]$. Now assume that the proposition is true for any polynomial $f(X) \in K[X]$ with $\deg(f(X)) \leq n$. Hence there exists a field extension L of K in which $f(X)$ splits completely.
We now consider a polynomial $f(X)$ where $\deg(f(X)) = n + 1$. If $f(X)$ is reducible then we can write $f(X) = g(X)h(X)$ where $\deg(g), \deg(h) \leq n$. By the induction hypothesis, we can find a field extension L_1 of K in which $g(X)$ splits completely. We can again apply the induction hypothesis to L_1 and $h(X)$ to obtain a field L_2 in which $h(X)$ splits completely. Hence $f(X)$ splits completely in L_2 and we are done.
On the other hand, if $f(X)$ is irreducible over $K[X]$ then we can take the finite extension $L_1 = K[X]/(f(X))$. Then L_1 contains a root of $f(X)$. Hence $f(X)$ is reducible over L_1 and by the previous case, we can construct a finite extension of L_1 containg all roots of $f(X)$. $\square$

Definition 5.3. *Let K be a field and $f(X) \in K[X]$ a polynomial. Consider an extension L/K such that $f(X)$ splits completely in $L[X]$, say $f(X) = c(X - l_1)\dots(X - l_n)$ where $c, l_1, \dots, l_n \in L$. The subfield of L generated by $l_1, \dots, l_n$ over K is called a* ***splitting field*** *of $f(X)$ over K.*

Definition 5.4. *Let L_1/K and L_2/K be two field extensions. A* ***K-embedding*** *(**K-isomorphism**) from L_1 to L_2 is an injective (bijective) ring homomorphism that fixes all elements of K:*

$$\theta : L_1 \to L_2$$

such that $\theta|_k$ is the identity map.

Remark. *Let $\theta : L_1 \to L_2$ be a ring homomorphism. It extends uniquely to a ring homomorphism*

$$\begin{aligned} \overline{\theta} : L_1[X] &\to L_2[X] \\ \sum_i c_i X^i &\mapsto \sum_i \theta(c_i) X^i \end{aligned}$$

We note that

1. *If θ is injective then $\overline{\theta}$ is injective*
2. *Let $f(X) \in L_1[X]$. An element $l_1 \in L_1$ is a root of $f(X)$ if and only if $\theta(l_1)$ is a root of $\theta(f(X))$*
3. *Assume that θ is bijective. The polynomial $f(X)$ is irreducible in $L_1[X]$ if and only if $\overline{\theta}(f(X))$ is irreducible in $L_2[X]$*

Definition 5.5. *Let L/K be a field extension and $\sigma : LtoL$ an automorphism. We say that σ is a K-automorphism if σ fixes every element of K.*

Proposition 5.6. *Let L/K be an algebraic field extension. Then every K-embedding of L into itself is necessarily a K-automorphism.*

Proof. Since every ring homomorphism is injective, it suffices to show that any K-endomorphism of L is surjective. Let σ be a K-embedding of L. Since σ is a K-embedding, we have that for all $f[X] \in K[X], \sigma(f(X)) = f(X)$. Hence l is a root of $f(X)$ if and only if $\sigma(l)$ is a root of $f(X)$.
Consider $l \in L$. We want to show that there exists $l_1 \in L$ such that $\sigma(l_1) = l$.

Since L/K is an algebraic extension, there exists a polynomial $f(X) \in K[X]$ of minimal degree such that $f(l) = 0$. Let $\{l_1, \ldots, l_r\}$ be all the roots of the polynomial $f(X)$ in L. Then σ induces an injective map from $\{l_1, \ldots, l_r\}$ to itself. Since this is a finite set, the induced map must also be surjective. Hence l must be in the image of σ. $\square$

Definition 5.7. *Let L/K be a field extension. We write $\mathbf{Aut_K(L)}$ for the group of K-automorphisms of L.*

Theorem 5.8. *(Artin's Extension Theorem)*
Let K_1 and K_2 be two fields, $\sigma : K_1 \to K_2$ a field isomorphism and $f \in K_1[X]$ an irreducible polynomial. Furthermore, let α be a root of $f(X)$ in an extension L_1 of K_1 and β a root of $\overline{\sigma}(f(X))$ in an extension L_2 of K_2. Then there exists a unique isomorphism of fields

$$\tau : K_1(\alpha) \to K_2(\beta)$$

such that $\tau(\alpha) = \beta$ and $\tau|_{K_1} = \sigma$. This is shown by the following diagram

$$\begin{tikzcd}
L_1 \arrow[d, dash] & L_2 \arrow[d, dash] \\
K_1(\alpha) \arrow[r, dashed, "\tau", "\sim"'] \arrow[d, dash] & K_2(\beta) \arrow[d, dash] \\
K_1 \arrow[r, "\sigma", "\sim"'] & K_2
\end{tikzcd}$$

Proof. We note that $\overline{\sigma}$ induces an isomorphism, which we again denote by $\overline{\sigma}$:

$$\overline{\sigma} : K_1[X]/(f(X)) \to K_2[X]/(\overline{\sigma}(f(X)))$$

Then the proposition follows directly from Proposition 4.5 and the following diagram

$$\begin{tikzcd}
L_1 \arrow[d, dash] & & & L_2 \arrow[d, dash] \\
K_1(\alpha) \arrow[r, "\sim"] \arrow[d, dash] & K_1[X]/(f) \arrow[r, "\overline{\sigma}", "\sim"'] & K_2[X]/(\overline{\sigma}(f)) \arrow[r, "\sim"] & K_2(\beta) \arrow[d, dash] \\
K_1 \arrow[rrr, "\sigma", "\sim"'] & & & K_2
\end{tikzcd}$$

□

Corollary 5.9. *Let K_1 and K_2 be two fields and $\sigma : K_1 \to K_2$ an isomorphism of fields. Consider a polynomial $f \in K_1[X]$ and choose splitting fields L_1 for f over K_1 and L_2 for $\overline{\sigma}(f)$ over K_2. Then there exists an isomorphism*

$$\tau : L_1 \to L_2$$

such that $\tau_{K_1} = \sigma$. In particular, if $K_1 = K_2 = K$ and $\sigma = id_K$, we have that any two splitting fields for f over K are K-isomorphic.

Proof. We prove the corollary by induction on $\deg(f)$. If $\deg(f) = 1$ then $L_1 = K_1$ and $L_2 = K_2$ and there is nothing to prove. Now assume that the corollary is true for $\deg(f) < n$.
Let f be a polynomial of degree n. If f is reducible then take an irreducible factor p of f in $K_1[X]$. Then $\overline{\sigma}(p)$ is an irreducible factor of $\overline{\sigma}(f)$ in $K_2[X]$. Now let $M_1 \subseteq L_1$ be the splitting field of p and $M_2 \subseteq$ the splitting field of $\overline{\sigma}(p)$. Then by the induction hypothesis, there is an isomorphism

$$\tau' : M_1 \to M_2$$

such that $\tau'|_{K_1} = \sigma$. Next we can apply the induction hypothesis to M_1, M_2 and τ' to get an isomorphism

$$\tau : L_1 \to L_2$$

such that $\tau|_{M_1} = \tau' \implies \tau|_{K_1} = \sigma$.
Now we consider the case where f is irreducible. Let α be a root of f in L_1 and β a root of $\overline{\sigma}(f)$ in L_2. Then by Artin's Extension Theorem, we have that there is an isomorphism

$$\tau' : K_1(\alpha) \to K_2(\beta)$$

such that $\tau'|_{K_1} = \sigma$. Over the field $K_1(\alpha)$, the polynomial f is reducible and hence we are done by the previous case. □

Theorem 5.10. *Let $\sigma : K_1 \to K_2$ be a field embedding and let L_1/K_1 be a finite extension. Then for any given extension M/K_2 there are at most $[L_1 : K_1]$ distinct embeddings*

$$\tau : L_1 \to M$$

such that $\tau|_{K_1} = \sigma$

Proof. We prove the theorem by induction. Let $L_1 = K_1(\alpha_1, \dots, \alpha_r)$ for some $\alpha_1, \dots, \alpha_r \in L_1$. We first prove the result for $K_1(\alpha_1)/K_1$.
Let $f_1(X) \in K_1[X]$ be the minimal polynomial of α_1 over K_1. Let $\overline{\sigma}(f_1) = f_2(X) \in K_2[X]$. If f_2 has no roots in M then there is no embedding of $K_1(\alpha_1)$ in M. More generally, if $\{\beta_1, \dots, \beta_m\}$ are the roots of f_2 in M, then there are m embeddings $\tau_1, \dots, \tau_m$

$$\tau_i : K_1(\alpha_1) \to M$$

such that $\tau_i|_{K_1} = \sigma$ and $\tau_i(a_1) = \beta_i$. Moreover, these are all the embeddings since α_1 has to map to a root of f_2 and the image of α_1 determines τ. Since $m \leq \deg(f_1) = [K_1(\alpha_1) : K_1]$, the theorem is true for $K_1(\alpha_1)/K_1$.
Now assume that the theorem is true for $K_1(\alpha_1, \dots, \alpha_s)/K_1$ for some $1 \leq s < r$. Let $L_0 = K_1(\alpha_1, \dots, \alpha_s)$ and fix an embedding $\tau : L_0 \to M$ such that $\tau|_{K_1} = \sigma$. Then by what we have just proven, we have that the number of embeddings

$$\tau' : L_0(\alpha_{s+1}) \to M$$

such that $\tau'|_{L_0} = \tau$ is less than or equal to $[L_0(\alpha_{s+1}) : L_0]$. Hence the number of embeddings

$$\tau : L_0(\alpha_{s+1}) \to M$$

such that $\tau|_{K_1} = \sigma$ is less than or equal to $[L_0(\alpha_{s+1}) : L_0][L_0 : K_1] = [L_0(\alpha_{s+1}) : K_1)]$. □

Chapter 6

Separable Extensions

Definition 6.1. *Let $f(X) \in K[X]$ be a polynomial. We say that $f(X)$ is* ***separable*** *if it has $\deg(f(X))$ distinct roots in every splitting field over K. If L/K is a field extension, we say that an element $l \in L$ is* ***separable over*** *K if it is algebraic over K and its minimal polynomial $p(X)$ is separable. We say that an extension L/K is* ***separable*** *if it is algebraic and every element of L is separable over K.*

Definition 6.2. *Let $f(X) = c_nX^n + \cdots + c_0$ be a polynomial. We define its* ***derivative*** *$f'(X)$ to be*

$$f'(X) = nc_nX^{n-1} + (n-1)c_{n-1}X^{n-2} + \cdots + c_1$$

Lemma 6.3. *Consider a field K, an element $a \in K$ and a polynomial $p(X) \in K[X]$. Then a is a multiple root of $p(X)$ if and only if $p(a) = 0$ and $p'(a) = 0$.*

Proof.

$\Longrightarrow:$ Let a be a multiple root of $p(X)$. Then $p(X) = (X-a)^n f(X)$ for some $f(X) \in K[X]$ and $n \geq 2$. Obviously, $p(a) = 0$.
Now, by the product rule and chain rule, we see that $p'(X) = n(X-a)^{n-1}f(X) + (X-a)^n f'(X)$. Hence $p'(a) = 0$.

$\Longleftarrow:$ Now assume that $p(a) = 0$ and $p'(a) = 0$ and assume that the a is not a multiple root of $p(X)$. Then we have that $p(X) = (X-a)f(X)$ for some $f(X) \in K[X]$ where a is not a root of $f(X)$. By the product rule, we have that $p'(X) = f(X) + (X-a)f'(X)$. Now, $p'(a) = f(a)$. But a is not a root of $f(X)$ hence $f(X) \neq 0$ which is a contradiction to the assumption that $p'(a) = 0$. Hence a must be a multiple root of $p(X)$.

∎

Definition 6.4. *Let K be a field. We say that K is **perfect** if either $char(K) = 0$ or $char(K) = p$ for some prime p and the map*

$$\begin{aligned}\sigma : K &\to K \\ x &\mapsto x^p\end{aligned}$$

is an isomorphism.

Example 6.5. *$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a perfect field.*

Example 6.6. *Let $\mathbb{F}_p(t)$ be the field of fractions of the polynomial ring $\mathbb{F}_p[t]$. Then $\mathbb{F}_p(t)$ is not a perfect field.*

Proposition 6.7. *Let K be a perfect field and L/K a field extension. If $l \in L$ is algebraic over K then all the roots of the minimal polynomial of l over K are simple.*

Proof. Let $f(X) \in K[X]$ be the minimal polynomial of l over K. Then $f(X)$ is irreducible over K. We also note that $\deg(f) > \deg(f')$. Now let a be a root of f. By the previous lemma, we have that a is a multiple root if and only if $f'(a) = 0$. Since f is irreducible over K, f must also be the minimal polynomial of a over K. If $f'(a) = 0$, then $f(X)|f'(X)$. But as $\deg(f) > \deg(f')$, we must have that $f'(X) = 0$. This is not possible in a characteristic 0 field. Hence if $char(K) = 0, f'(a) \neq 0$ and all roots of f are simple roots.
If $char(K) = p$ and $f'(a) = 0$ then $f'(X) = 0$. In this case, we can see that $f(X) = h(X^p)$ for some $h(X) \in K[X]$. Let $h(X) = a_nX^n + \cdots + a_0$. Since K is a perfect field of characteristic p there exists $b_i \in K$ such that $a_i = b_i^p$ for all $0 \leq i \leq n$. Hence

$$\begin{aligned}f(X) = h(X^p) &= a_nX^{np} + \cdots + a_0 \\ &= b_n^pX^{np} + \cdots + b_0^p \\ &= (b_nX^n + \cdots + b_0)^p\end{aligned}$$

□

But this cannot happen since $f(X)$ is irreducible. Hence $f'(a) \neq 0$ and all the roots of f are simple roots.

Corollary 6.8. *Every algebraic extension of a perfect field is separable.*

Proof. Let L/K be an algebraic extension and K a perfect field. Then every $l \in L$ is algebraic over K. By the previous proposition, we have that the minimal polynomial of l over K has no repeated roots. Hence every element of L is separable over K and L/K is a separable extension. □

Theorem 6.9. *Let $L = K(\alpha_1, \ldots, \alpha_n)$ be a finite extension of K. Let f_i be the minimal polynomial of α_i over K. Let $\sigma : K \to K_1$ be an isomorphism of fields and M an extension of K_1. Assume that $\overline{\sigma}(f_i)$ splits completely in M for every $1 \leq i \leq n$. Then L/K is separable if and only if the number of embeddings $\tau : L \to M$ such that $\tau|_K = \sigma$ is equal to $[L : K]$.*

Proof.

$\Longrightarrow$: Assume that L/K is separable. By Theorem 5.10, we know that the number of embeddings τ such that $\tau|_K = \sigma$ is less than or equal to $[L : K]$. We must show equality. We first show the result for $K(\alpha_1)/K$. As L/K is separable, the minimal polynomial f_1 of α_1 has simple roots. Hence $\overline{\sigma}(f_1)$, which we denote by g_1, has simple roots in M. Let $\{\beta_1, \ldots, \beta_m\}$ be the roots of g_1 in M. Then $r = deg(g_1) = deg(f_1)$. For every $1 \leq j \leq r$, there is an embedding

$$\tau_j = K(\alpha_1) \to M$$

such that $\tau_j|_K = \sigma$ and $\tau_j(\alpha_1) = \beta_i$. Moreover, $\tau_j \neq \tau_j'$ if $j \neq j'$. Hence we have $[K(\alpha_1) : K] = \deg(f_1) = r$ embeddings of $K(\alpha_1)$ in M whose restriction to K is σ.
Now assume that the result is true for $K(\alpha_1, \ldots, \alpha_s)/K$ for some $1 \leq s < n$. Denote $L_0 = K(\alpha_1, \ldots, \alpha_n)$. Now fix an embedding $\tau : L_0 \to M$ such that $\tau|_K = \sigma$. Let $p(X)$ be the minimal polynomial of α_{s+1} over L_0. Then $p(X)|f_{s+1}(X)$. Since $f_{s+1}(X)$ has simple roots, $p(X)$ must also have simple roots. Hence $\overline{\tau}(p)$ must have simple roots. As all the roots of $\overline{\tau}(f_{s+1}) = \overline{\sigma}(f_{s+1})$ are in M, all the roots of $\overline{\tau}(p)$ are also in M. Hence by the first part, the number of embeddings $\tau' : L_0(\alpha_{s+1}) \to M$ such that $\tau'|_{L_0} = \tau$ is equal to $[L_0(\alpha_{s+1}) : L_0] = deg(p)$. Hence the number of embeddings $\tau' : L_0 \to M$ such that $\tau'|_K = \sigma$ is equal to $[L_0(\alpha_{s+1}) : L_0][L_0 : K] = [L_0(\alpha_{s+1}) : K]$.

$\Longleftarrow$: Now assume that the number of embeddings $\tau : L \to M$ such that $\tau|_K = \sigma$ is equal to $[L : K]$. We want to show that L/K is separable.
Consider $l \in L$ and let $f(X) \in K[X]$ be the minimal polynomial of l over K.

Let $g = \overline{\sigma}(f) \in M[X]$. f has simple roots if and only if g has simple roots. By Theorem 5.10, the number of embeddings

$$\tau' : K(l) \to M$$

such that $\tau'|_K = \sigma$ is less than or equal to $[K(l) : K]$. Once we fix such a τ' and apply Theorem 5.10 again, we get that the number of embeddings

$$\tau : L \to M$$

such that $\tau|_{K(l)} = \tau'$ is less than or equal to $[L : K(l)]$. Hence the number of

$$\tau : L \to M$$

such that $\tau|_K = \sigma$ is less than or equal to $[L : K(l)][K(l) : K] = [L : K]$. But by hypithesis, this number is equal to $[L : K]$. Hence the number of τ's as above should be equal to $[K(l) : K] = \deg(f) = \deg(g)$. As each map τ' maps l to a root of g and different τ's maps l to distinct roots of g, we have that g has $\deg(g)$ distinct roots in M. Hence all the roots of g are simple which implies that all the roots of f are simple and hence l is separable over K.

$\square$

Corollary 6.10. *Let L/K be a field extension and $l \in L$ separable over K. Then $K(l)/K$ is a separable extension.*

Corollary 6.11. *Let L/K be a field extension. Then*

$$M = \{l \in L \mid \ l \text{ is separable over } K\ \}$$

is a field.

Proposition 6.12. *Let $K \subseteq L \subseteq M$ be fields. Then L/K and M/L are separable if and only if M/K is separable.*

Proof. $\implies$: Assume that L/K and M/L are separable. Let $m \in M$. We want to show that m is separable over K. Let $p(X) = \sum_{i=0}^{n} l_i X^i \in L[X]$ be the minimal polynomial of m over L. Let $L_0 = K(l_1, \dots, l_n)$. Then L_0/K is a separable finite extension. Let $M_0 = L_0(m)$. The minimal polynomial of m over L_0 is $p(X)$. Hence M_0/L_0 is a separable finite extension. Let E be an extension of K which contains all the conjugates of each l_i and m. Then by Theorem 6.9, the number of embeddings

$$\tau : L_0 \to E$$

such that $\tau|_K = id_K$ is equal to $[L_0 : K]$. Once we fix such an embedding τ, the nunber of embeddings

$$\tau' : M_0 \to E$$

such that $\tau'|_{L_0} = \tau$ is equal to $[M_0 : L_0]$. Hence the number of embeddings

$$\tau' : M_0 \to E$$

such that $\tau'_K = id_K$ is equal to $[M_0 : L_0][L_0 : K] = [M_0 : K]$. Hence by Theorem 6.9, we have that M_0/K is separable.

$\Longleftarrow$: Let M/K be separable. We want to show that L/K and M/L are separable. Since every $l \in L$ is also an element of M, l is separable over K by assumption, hence L/K is separable. Now since every $m \in L$ is separable over K, it must also be separable over L.

$\square$

Chapter 7

Algebraic Closure and Primitive Element Theorem

Definition 7.1. *A field K is called **algebraically closed** if every polynomial $f(X) \in K[X]$ of degree greater than or equal to 1 has a root in K.*

Definition 7.2. *Let L/K be a field extension. If L is algebraic over K and is algebraically closed, we say that L is an **algebraic closure** of K. An algebraic closure of K is denoted by $\overline{K}$.*

Proposition 7.3. *Let K be a field. Then there exists a field extension E/K such that E is algebraically closed.*

Proof. Let $S = \{f \in K[X] \mid \text{f is irreducible over K}\}$. Let X_f be an indeterminant indexed by $f \in S$. Denote $K[S] = K[X_f : f \in S]$ the polynomial ring with infinitely many variables. Now let I be an ideal of $K[S]$ generated by each $f(X_f)$. We claim that I is not the whole ring. Suppose that I is the whole ring. Then $1 \in I$. We therefore have that

$$1 = \sum_{i=1}^{n} g_i f_i(X_{f_i})$$

Rename, for efficiency, X_{f_i} to X_i and assume that only $X_1, \ldots, X_n$ appear in the equation. Now let L be a splitting field of $f_1(X_1), \ldots, f_n(X_n)$ and $\alpha_i \in L$ a root of $f_i(X_i)$. Setting $X_i = \alpha_i$ in the equation above, we see that $1 = 0$, an obvious contradiction. Hence I cannot equal the whole ring.
Now consider $\mathfrak{m}$ a maximal ideal of $K[S]$ containing I. Let $E_1 = K[S]/\mathfrak{m}$.

Then E_1 is an extension of K and it contains all roots of any non-constant polynomial in $K[X]$. We can apply the same process to E_1 to obtain an extension E_2/E_1 wich contains all roots of any non-constant polynomial in $E_1[X]$ and so on. We get a sequence of fields

$$K \subseteq E_1 \subseteq E_2 \subseteq \dots$$

Letting $E = \bigcup_{i \geq 1} E_i$, we see that E has the structure of a field. Consider any non-constant polynomial $f(X) \in E[X]$. Then $f(X) \in E_n[X]$ for some n. Hence $f(X)$ has a root in $E_{n+1} \subseteq E$. Thus, E is algebraically closed. $\square$

Theorem 7.4. *Let K be a field. Then the algebraic closure $\overline{K}$ of K exists.*

Proof. Let E/K be the extension constructed in the previous proposition and let $\overline{K} = \{a \in E \,|\, \text{a is algebraic over K}\}$. Then $\overline{K}/K$ is algebraic. Let $a \in E$ be algebraic over $\overline{K}$ and $f(X) = \min_{a,\overline{K}}(X)$. Let L be a finite extension of K containing $f(X)$ (for example, take L to be the field generated by the coefficients of f). Then a is algebraic over L. Hence $L(a)$ is a finite extension of L and therefore a finite extension of K. Hence a is algebraic over K i.e $a \in \overline{K}$. Therefore, $\overline{K}$ is algebraically closed. $\square$

Definition 7.5. *Let L/K be a finite extension. Then L/K is called a* ***simple extension*** *if $L = K(\alpha)$ for some $\alpha \in L$. In this case, we say that α is a* ***primitive element****.*

Proposition 7.6. *Let L/K be a finite extension. Then L is simple if and only if there are only finitely many fields F_i such that $K \subseteq F_1 \subseteq \dots \subseteq F_n \subseteq L$ for some $n \in \mathbb{N}$.*

Proof. If K is a finite field then since L/K is a finite extension, we see that L is also finite. But then it is obvious that there are only finitely many fields between K and L.
Now since L is finite, it follows that $L^\times$ is a finite abelian group. Let m be the lowest common multiple of all elements in $L^\times$. Then $l^m = 1$ for all $l \in L^\times$. Hence all elements of $L^\times$ are roots of the polynomial $X^m - 1$. This polynomial can have at most m roots hence $m \geq |L^\times|$. Now consider the subgroup of $L^\times$ generated by some element of order m. By Lagrange's theorem, we have that m divides $|L^\times|$. Hence $m = n$. This implies that $L^\times$ is cyclic. Therefore L is generated by a single element which is exactly what it means for L to be simple.
We now assume that K is an infinite field.

$\Longrightarrow$: Assume that L is simple i.e $L = K(\alpha)$. Let $f(X)$ be the minimal polynomial of α over K. Now let $K \subseteq F \subseteq L$ and $g(X)$ be the minimal polynomial of α over F. Then $g(X)|f(X)$. Let F_0 be the subfield of F generated over K by the coefficients of $g(X)$. Then $L = K(\alpha) = F(\alpha) = F_0(\alpha)$ and $g(X)$ is irreducible over F_0. Therefore we have that $g(X) = min_{\alpha,F_0}(X)$. Hence $[L : F_0] = [L : F] = \deg(g(X))$ which implies that $F = F_0$. We therefore have an injective map between the subfields of L containing K into the set of monic divisors of $f(X)$. Since the latter set is finite, we have that the former set is also finite.

$\Longleftarrow$: Now suppose that there are only finitely many fields between L and K. We want to show that given any a, b in L, there exists a $\alpha \in L$ such that $K(a, b) = K(\alpha)$. We shall show this by induction.
Assume that $L = K(a, b)$ and consider all fields of the form $K(a + cb)$ for all $c \in K$. Since there are infinitely many elements of L and only finitely many intermediate fields, there must exist distinct elements $c, c' \in K$ such that $K(a + cb) = K(a + c'b)$. Let $\alpha_1 = a + cb$ and $\alpha_2 = a + c'b$. Then $K(\alpha_1) = K(\alpha_2)$ so $\alpha_2 \in K(\alpha_1)$. Hence $\alpha_1 - \alpha_2 = (c - c')b \in K(\alpha_1)$. Therefore $b \in K(\alpha_1)$ and $\alpha_1 - cb = \alpha \in K(\alpha_1)$. Thus, $L = K(a + cb)$.
Now assume that the proposition is true for extensions $L = K(a_1, \dots, a_n$.
Consider $L = K(a_1, \dots, a_{n+1})$Then $L = K(a_1, \dots, a_{n+1}) = K(a_1, \dots, a_n)(a_{n+1})$.
By the induction hypothesis, we can show that there is an $a \in K(a_1, \dots, a_n)$ such that $K(a_1, \dots, a_n) = K(a)$. Hence we have that $L = K(a)(a_{n+1}) = K(a, a_{n+1})$. By the basis case, we can find a $b \in K(a, a_{n+1})$ such that $K(a, a_{n+1}) = K(b)$. hence $L = K(b)$ and L is a simple extension.

□

Theorem 7.7. *(Primitive Element Theorem)*
Let L/K be a finite separable extension. Then L is a simple extension of K.

Proof. If K is finite then, from the previous proposition, we have that L/K is simple and we are done. Hence assume that K is infinite. It suffices to consider the case when $L = K(a, b)$ and the generalisation will follow from induction.
Let $n = [L : K]$. Then since L/K is a separable extension, we have that there exists n distinct K-embeddings of L into $\overline{K}$. Now suppose that there exists $c \in L$ such that $L = (a + cb)$. Then $a + cb$ must have n distinct conjugates which are exactly the images of $a + cb$ under the action of the n K-embeddings of L. We denote these embeddings by $\sigma_1, \dots, \sigma_n$. These

embeddings map $a + cb$ to the roots of the polynomial $p(x) = min_{a+cb,K}(X)$ in $\overline{K}$. Hence $a + cb$ is a primitive element if and only if there exists n K-embeddings of L such that $\sigma_i(a + cb) \neq \sigma_j(a + cb)$ for all $i \neq j$. This is equivalent to saying that

$$\prod_{i \neq j}^{n} (\sigma_i(a) - \sigma_j(a) - c(\sigma_i(b) - \sigma_j(b)) \neq 0$$

Now this is equivalent to saying that c is not a root of the following polynomial

$$f(X) = \prod_{i \neq j}^{n} (\sigma_i(a) - \sigma_j(a) - X(\sigma_i(b) - \sigma_j(b))$$

Since K is infinite and $f(X)$ has finitely man roots, we can easily find such a c. Hence $a + cb$ is a primitive element and thus $L = (a + cb)$. $\square$

Chapter 8

Normal Extensions

Definition 8.1. *Let L/K be a field extension. Then L/K is called* ***normal*** *if it is algebraic and for every $l \in L$, the minimal polynomial of l over K splits completely over L.*

Example 8.2. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ *is normal.*

Proposition 8.3. *Let K be a field and $f(X) \in K[X]$. Then a splitting field of f is a normal extension of K.*

Proof. Let L be a splitting field of f and $\alpha_1, \dots, \alpha_r$ the roots of f. Hence $L = K(\alpha_1, \dots, \alpha_r)$. Let $l \in L$ and $p(X)$ be the minimal polynomial of l over K. Let M be a splitting field of $p(X)$ over L. Let $l' \in M$ be a root of $p(X)$. We must show that $l' \in L$. There is a unique isomorphism

$$\tau : K(l) \to K(l')$$

such that $\tau(l) = l'$ and $\tau|_K = id_K$. By Artin's Extension Theorem, we may extend τ to $\tau' : L \to M$ such that $\tau'|_{K(l)} = \tau$. We can find such an extension as follows.
Assume that we have an extension $\tau' : K(l, \alpha_1, \dots, \alpha_n) \to M$ for some $1 \leq s < r$. Let $g(X)$ be the minimal polynomial of α_{s+1} over $K(l, \alpha_1, \dots, \alpha_s)$. Then $g(X)|f(X)$ and hence $\overline{\tau}'(g)|\overline{\tau}'(f) = f$. Since f splits completely in L, so does $\overline{\tau}(g)$. Let α'_{s+1} be a root of $\overline{\tau}(g)$ in M. Then there is an extension

$$\tau'' : K(l, \alpha_1, \dots, \alpha_{s+1}) \to M$$

such that $\tau''|_{K(l,\alpha_1,\dots,\alpha_{s+1})} = \tau'$ and $\tau''(\alpha_{s+1}) = \alpha'_{s+1}$.
We therefore have an embedding $\tau' : L \to M$ such that $\tau'|_K = id_K$ and

$\tau'(l) = l'$. We now claim that $\tau'(L) = L$. Noote that τ' is determined by where it sends α_i's. $\tau'(\alpha_i)$ must be a root of $\overline{\tau}'(f) = f$. Hence $\tau'(\alpha_i) \in \{\alpha_1, \ldots, \alpha_r\}$ for each i. Hence $\tau'(L) \subseteq L$ and by Proposition 5.6 $\tau'(L) = L$. Hence $l' \in L$ and $p(X)$ splits completely in L. $\square$

Theorem 8.4. *Let L/K be an algebraic extension. Then L/K is normal if and only if for any extension M of L and for any K-embedding, $\tau : L \to M$ maps L to itself.*

Proof.

$\implies$: Assume that L/K is normal and let $\tau : L \to M$ be an embedding. Let $l \in L$ and $f(X) \in K[X]$ be the minimal polynomial of l over K. Then L contains all the roots of $f(X)$. Also note that $\tau(l)$ is a root of $\overline{\tau}(f) = f$. Hence $\tau(l) \in L$. Now by Proposition 5.6, $\tau(L) = L$.

$\impliedby$: Assume that for any extension M of L and any K-embedding, $\tau : L \to M$ maps L to itself. We take M to be an algebraic closure of K. Let l in L and $f(X) \in K[X]$ be the minimal polynomial of l over K. We must show that $f(X)$ splits completely in L. Let $l' \in \overline{K}$ be a root of $f(X)$. Then by Artin's Extension Theorem, there is a unique ismorphism $\tau : K(l) \to K(l')$ such that $\tau|_K = id_K$ and $\tau(l) = l'$. We claim that we can extend τ to an embedding $\tau' : L \to M$. Let E be the maximal subfield of L containing $K(l)$ such that τ can be extended to an embedding $\tau' : E \to \overline{K}$. If $E \neq L$, take $\alpha \in L - E$ and let $p(X)$ be the minimal polynomial of α over K. Then $p(X)$ splits completely in $\overline{K}$. Let $g(X)$ be the minimal polynomial of α over E. Then $\overline{\tau}'(g)$ splits completely in $\overline{K}$. Let $\alpha' \in \overline{K}$ be a root in $\overline{\tau}'(g)$. Then by Artin's Extension Theorem, we get

$$\tau'' : E(\alpha) \to \tau'(E)(\alpha') \subseteq \overline{K}$$

such that $\tau''|_E = \tau'$ i.e we get an extension of τ to $E(\alpha)$. By maximality of E, $\alpha \in E$ which is a contradiction. Hence $E = L$. As $\tau(L) = L$ by hypothesis, we get $\tau(l) = l' \in L$.

$\square$

Proposition 8.5. *Let $K \subseteq L \subseteq M$ be fields. If M/K is normal then so is M/L. Let $f(X) \in L[X]$ be an irreducible polynomial with a root $l \in M$. Let $g(X) \in K[X]$ be the minimal polynomial of l over K. Then $f(X)|g(X)$. As M/K is normal, g splits completely in $M[X]$. Hence $f(X)$ splits completely in $M[X]/$*

Chapter 9

Galois Extensions

Definition 9.1. *A field extension L/K is called* ***Galois*** *if it is normal and separable. The group $Aut_K(L)$ of K-automorphisms of L is called the* ***Galois group*** *of L/K and is denoted by* $\mathbf{Gal(L/K)}$.

Proposition 9.2. *Let $K \subseteq L \subseteq M$ be fields. If M/K is a Galois extension then so is M/L.*

Definition 9.3. *Let L/K be an extension and let H a subgroup of $Gal(L/K)$. Then the* ***fixed field*** *of H in L is defined to be*

$$L^H := \{l \in L \mid h(l) = l \; \forall \, h \in H\}$$

Remark. *Clearly, L^H is an intermediate extension of L/K and L/L^H is a galois extension.*

Chapter 10

Fundamental Theorem of Galois Theory

Lemma 10.1. *(Zorn's Lemma)*
Let S be a non-empty partially ordered set. Assume that every chain in S has an upper bound i.e if $s_1 \leq s_2 \leq \ldots$ is a chain in S then there exists $s \in S$ such that $s_i \leq s$ for all i. Then S has a maximal element, say s, such that there is no $s' \in S$ with $s < s'$.

Proposition 10.2. *Let L/K be a normal extension. Let $K \subseteq M \subseteq L$ be an intermediate extension. Then any K-embedding $\tau : M \to L$ can be extended to a K-automorphism of L.*

Proof. Assume that E is the maximal extension of M contained in L such that τ extends to an embedding of $\tau' : E \to L$. The existence of such an extension is guaranteed by Zorn's Lemma as follows.
Let S be the set of all pairs (E, τ') such that $M \subseteq E \subseteq L$ is an intermediate extension and $\tau' : E \to L$ is an embedding such that $\tau'|_M = \tau$. Then S is non-empty because $(M, \tau) \in S$. The partial ordering on S is given as follows

$$(E_1, \tau_1') \leq (E_2, \tau_2')$$

if

$$E_1 \subseteq E_2,\ \tau_2'|_{E_1} = \tau_1'$$

Let $\{(E_i, \tau_i')\}$ be a chain in S. Let $E = \bigcup_i E_i$. There is an embedding $\tau' : E \to L$, defined as $\tau'(e) = \tau_i'(e)$ if $e \in E_i$. With this definition, (E, τ') is

an upper bound of the chain. Hence S has a maximal element.
We now claim that $E = L$. Let $\alpha \in L$ and consider $E(\alpha)$. Let $p(X) \in K[X]$ be the minimal polynomial of α in K and let $f(X) \in E[X]$ be the minimal polynomial of α over E. Since L/K is normal, L/E is also normal and hence both $p(X)$ and $f(X)$ split completely over L. We note that $\overline{\tau}'(f)|p(X)$ and hence $\overline{\tau}'(f)$ splits completely in L. Let $\alpha' \in L$ be any root of $\overline{\tau}'(f)$. By Artin's Extension Theorem, τ' extends to an isomorphism

$$\tau'' : E(\alpha) \to \tau'(E)(\alpha') \subseteq L$$

As $\tau''|_M = \tau'|M = \tau$, by maximality of E, $E = E(\alpha)$. Hence $\alpha \in L$. Since α was an arbitrary element of L, $L \subseteq E$. Hence $L = E$ and we are done. $\square$

Proposition 10.3. *Let L be a field and G the group of automorphisms of L. Consider the fixed field $K = L^G$. Then L/K is Galois with $Gal(L/K) = G$ and thus $[L : K] = |G|$*

Proof. Let $\alpha \in L$. We find a seperable polynomial in $K[X]$ with α as one of its roots. Let $\{\sigma_1, \dots, \sigma_r\}$ be a maximal set of elements of G such that $\sigma_1(\alpha), \dots, \sigma_r(\alpha)$ are all distinct. Then for any $\tau \in G$

$$(\tau\sigma_1(\alpha), \dots, \tau\sigma_r(\alpha))$$

is a permutation of

$$(\sigma_1(\alpha), \dots, \sigma_r(\alpha))$$

Indeed, if it is not a permutation then the maximality of $\{\sigma_1, \dots, \sigma_r\}$ is contradicted.
Now consider the polynomial

$$f(X) = \prod_{i=1}^{r}(X - \sigma_i(\alpha))$$

It is obviously seperable as each $\sigma_i(\alpha)$ is distinct and has α as a root since G is a group and hence one of the σ_i must be the identity mapping. We can also see that given any $\tau \in G, \overline{\tau}(f) = f$. Therefore $f(X) \in K[X]$. Hence every $\alpha \in L$ is a root of a seperable polynomial of degree less than or equal to $|G|$ over K meaning that L is seperable. Moreover, these polynomials obviously split completely over L and hence L is a normal extension. Therefore, L/K

is a Galois extension.
We now show that $[L : K] = |G|$. Let $n = |G|$ and $G = \{\sigma_1, \ldots, \sigma_r\}$. Assume that $\{l_1, \ldots, l_{n+1}\} \subseteq L$ is linearly independent over K. Now consider the system of equations

$$\begin{aligned} \sigma_1(l_1)X_1 + \cdots + \sigma_1(l_{n+1})X_{n+1} &= 0 \\ \vdots \\ \sigma_n(l_1)X_1 + \cdots + \sigma_n(l_{n+1})X_{n+1} &= 0 \end{aligned} \tag{10.1}$$

Assume that $\vec{\alpha} = (\alpha_1, \ldots, \alpha_r, 0, \ldots, 0)$ is a solution of these equations with minimal r and fix $\sigma \in G$. $(\sigma\sigma_1, \ldots, \sigma\sigma_n)$ is just a permutation of $(\sigma_1, \ldots, \sigma_n)$. Therefore the system of equations

$$\begin{aligned} \sigma\sigma_1(l_1)\sigma(\alpha_1) + \cdots + \sigma\sigma_1(l_r)\sigma(\sigma_r) &= 0 \\ \vdots \\ \sigma\sigma_n(l_1)\sigma(\alpha_1) + \cdots + \sigma\sigma_n(l_r)\sigma(\alpha_r) &= 0 \end{aligned}$$

can be written, up to permutation of the equations, as

$$\begin{aligned} \sigma_1(l_1)\sigma(\alpha_1) + \cdots + \sigma_1(l_r)\sigma(\sigma_r) &= 0 \\ \vdots \\ \sigma_n(l_1)\sigma(\alpha_1) + \cdots + \sigma_n(l_r)\sigma(\alpha_r) &= 0 \end{aligned} \tag{10.2}$$

Let $(10.1)(\vec{\alpha})$ denote the equations in (10.1) evaluated at $\vec{\alpha}$ then taking $\alpha_r(10.2) - \sigma(\alpha_r)(1)(\vec{\alpha})$

$$\begin{aligned} \sigma_1(l_1)(\alpha_r\sigma(\alpha_1) - \alpha_1\sigma(\alpha_r)) + \cdots + \sigma_1(l_{r-1})(\alpha_r\sigma(\alpha_{r-1}) - \alpha_{r-1}\sigma(\alpha_r)) &= 0 \\ \vdots \\ \sigma_n(l_1)(\alpha_r\sigma(\alpha_1) - \alpha_1\sigma(\alpha_r)) + \cdots + \sigma_n(l_{r-1})(\alpha_r\sigma(\alpha_{r-1}) - \alpha_{r-1}\sigma(\alpha_r)) &= 0 \end{aligned}$$

This is a solution of (10.1) with fewer non-zero terms. Therefore, all the terms must be zero. We thus have that $\alpha_r\sigma(\alpha_i) = \alpha_i\sigma(\alpha_r)$ for all $i \leq r-1$. This is equivalent to having $\sigma(\alpha_i\alpha_r^{-1}) = \alpha_i\alpha_r^{-1}$ for all $i \leq r-1$.
Now since σ is an arbitrary K-automorphism in G, we must have that $m_i := \alpha_i\alpha_r^{-1} \in K$ for all $i \leq r-1$. Hence $\alpha_i = m_i\alpha_r$ for all $i \leq r$. Then equation

(10.1), evaluated at $\vec{\alpha}$ gives

$$\begin{aligned} 0 &= \sigma_1(l_1)\alpha_1 + \cdots + \sigma_1(l_r)\alpha_r \\ &= (\sigma(l_1)m_1 + \cdots + \sigma_1(l_r)m_r)\alpha_r \\ &= \sigma_1(l_1m_1 + \cdots + l_rm_r)\alpha_r \end{aligned}$$

Since α_r is not 0 by construction, we must have that $\sigma_1(l_1m_1+\cdots+l_rm_r) = 0$. Now since σ is an isomorphism, its kernel is trivial hence $l_1m_1+\cdots+l_rm_r = 0$. But this is a contradiction to the assumption that $\{l_1, \ldots, l_r\}$ are linearly independent over K. Hence $[L : K] \leq n$.
Now Theorem 5.10 implies that $[L : K] \geq n$. Thus we must have that $[L : K] = n$. □

Theorem 10.4. *(Fundamental Theorem of Galois Theory for Finite Extensions)*
Let L/K be a finite Galois extension, H a subgroup of $Gal(L/K)$ and E and intermediate field of L/K. Then

1. *the maps*

$$\begin{aligned} H &\mapsto L^H \\ E &\mapsto Gal(L/E) \end{aligned}$$

   are mutually inverse, inclusion reversing bijections between the subgroups of $Gal(L/K)$ and the intermediate fields of L/K.

2. *L^H/K is Galois if and only if H is a normal subgroup of $Gal(L/K)$. In this case, the restriction map*

$$\begin{aligned} Gal(L/K) &\to Gal(L^H/K) \\ \sigma &\mapsto \sigma|_{L^H} \end{aligned}$$

   induces an isomorphism of groups $Gal(L/K)/H \to Gal(L^H/K)$.

Proof. Part 1: We first show that the mappings are inclusion reversing. Let $K \subseteq F_1 \subseteq F_2 \subseteq L$ and $G_i = Gal(L/F_i)$. If $\sigma \in G_2$ then σ fixes F_2. Since $F_1 \subseteq F_2$, we have that σ fixes F_1 and hence $\sigma \in G_1$.
Now let $H_1 \subseteq H_2 \subseteq Gal(L/K)$ and $F_i = L^{H_i}$. If $x \in F_2$ then $\sigma(x) = x$ for all $\sigma \in H_2$. Since $H_1 \subseteq$, we have that $\sigma(x) = x$ for all $x \in H_1$. Hence $x \in F_1$. Therefore the maps are inclusion reversing.

We now show that the map $E \mapsto Gal(L/E)$ is injective. Let $G = Gal(L/K)$. We shall first prove that $L^G = K$. It is clear that $K \subseteq L^G$. Let $\alpha \in L^G$ and consider the extension $K(\alpha)/K$. Let $f(X) \in K[X]$ be the minimal polynomial of α over K. Since L is normal, $f(X)$ splits completely in $L[X]$ and since it is also seperable, all the roots of f are simple roots. If $deg(f) > 1$ then let $\alpha' \neq \alpha$ be another root of $f(X)$. Then there is a K-isomorphism

$$\tau : K(\alpha) \to K(\alpha')$$

Since L is a normal extension of K containing both $K(\alpha)$ and $K(\alpha')$, this isomorphism τ can be etended to a K-automorphism, say τ', of L. Hence τ' is an element of G. Since $\alpha \in L^G, \alpha = \tau'(\alpha) = \tau(\alpha)$. But $\tau(\alpha) = \alpha'$ by construction. By asssumption, $\alpha \neq \alpha'$ hence this is a contradiction and $deg(f) = 1$ and $a \in K$. Hence $L^G = K$. Now let E and E' be two intermediate fields of L/K such that $H := Gal(L/E) = Gal(L/E') =: H'$. By the result we have just shown, we have that $E = L^H = L^{H'} = E'$. Therefore $E \mapsto Gal(L/E)$ is an injective mapping.
We now show that $E \mapsto Gal(L/E)$ is a surjective mapping. We have to prove that for every subgroup of the Galois group of L/K, there exists a fixed field of L/K that maps to it. Let $H \subseteq G$ be a subgroup of the Galois group of L/K. Then by Proposition 10.4, L/L^H is a Galois extension with Galois group H. Hence the mapping $E \mapsto Gal(L/E)$ is surjective.

Part 2:

$\Longrightarrow$: Now assume that L^H/K is a Galois extension. Then the restriction map

$$\phi : Gal(L/K) \to Gal(L^H/K)$$
$$\sigma \mapsto \sigma|_{L^H}$$

induces a group homomorphism.
Since L is a normal extension, any automorphism of L^H can be extended to an automorphism of L. This implies that the map is surjective. Now

$$\ker(\phi) = \{\sigma \in Gal(L/K) \mid \sigma|_{L^H} = id\}$$

Hence the kernel is comprised of all those automorphisms that, when restricted to L^H are just the identity automorphism. Bu this is exactly H.

Since H is the kernel of a group homomorphism on $Gal(L/K)$, H must be a normal subgroup.

$\Longleftarrow$: Now assume that L^H is not Galois over K. Then there exists an automorphism of L, say σ, such that $\sigma(L^H) \neq L^H$. Indeed, if there did not exist such an automorphism, then Theorem 8.4 would imply that L^H is normal over K and hence Galois.
We claim that $\sigma H \sigma^{-1} \neq H$. To show this, we need to prove that $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$.
Let $Z = \sigma(L^H)$ and $x \in Z$. Then $x = \sigma(y)$ for some $y \in L^H$. Now

$$\begin{aligned}(\sigma\phi\sigma^{-1})(x) &= \sigma\phi(y)\\ &= \sigma(y)\\ &= x\end{aligned}$$

for all $\phi \in H$. Hence x is also fixed by $\sigma\phi\sigma^{-1}$ and therefore $x \in L^{\sigma H \sigma^{-1}}$. Thus we have that $\sigma(L^H) \subseteq L^{\sigma H \sigma^{-1}}$.
Now let $x \in L^H$. We have that $x = \sigma^{-1}(y)$ for some $y \in Z$. Therefore

$$\begin{aligned}(\sigma^{-1}\phi'\sigma)(x) &= \sigma^{-1}\phi'(y)\\ &= \sigma^{-1}(y)\\ &= x\end{aligned}$$

for all ϕ' in H', the Galois group of Z. Therefore $H \subseteq \sigma H' \sigma^{-1}$ and thus $\sigma H \sigma^{-1} \subseteq H'$. It hence follows that $L^{\sigma H \sigma^{-1}} \subseteq L^{H'} = \sigma(L^H)$. We can now see that $\sigma(L^H) = L^{\sigma H \sigma^{-1}}$.
Now assume that H is normal so that $\sigma H \sigma^{-1} = H$. By what we have just proved, this implies that $\sigma(L^H) = L^H$. But this is a contradiction and we hence see that H is not a normal subgroup.

$\square$

Definition 10.5. *Let $f(X) \in K[X]$. We define the* ***Galois group*** *of $f(X)$ over K to be*

$$Gal(f/K) = Gal(K_f/K)$$

where K_f is a splitting field of $f(X)$ over K.

Definition 10.6. *Let $r > 0$. We denote the group of permutations on r elements by S_r. We say that a subgroup of S_r is* ***transitive*** *if it acts transitively on the set of r elements.*

Example 10.7. $\{(1),(1,2)(3,4),(1,3)(2,4),(1,4),(2,3)\}$ *is a transitive subgroup of* S_4*.*

Proposition 10.8. *Let* $f(X) \in K[X]$ *be a polynomial with* r *distinct roots. Then* $Gal(f/K)$ *is isomorphic to a subgroup of of* S_r *and hence the order of* $Gal(f/K)$ *divides* $r!$*. Moreover, if* f *is irreducible over* K *then* $Gal(f/K)$ *is a transitive subgroup of* S_r*.*

Proof. Let L be a splitting field of f over K and $l_1, \dots, l_r$ be roots of f. Then $L = K(l_1, \dots, l_r)$. A K-automorphism of L is determined by the images of the l_i's. Such an automorphism must map a root of f to a root. Hence a K-automorphism of L permutes elements of the set $l_1, \dots, l_r$. Hence we get an injection of $Gal(f/K)$ into S_r.
Now assume that f is irreducible over K. Then for any $1 \le i \le r$, there is a K-isomorphism

$$K(l_1) \to K(l_i)$$

By Proposition 10.2, this can be extended to an automorphism of L and hence to an element of $Gal(f/K)$. Therefore, $Gal(f/K)$ is a transitive subgroup of S_r. □

Chapter 11

Cubic Polynomials

Let $f(X) \in K[X]$ be a cubic polynomial. Then $Gal(f/K)$ is a subgroup of S_3. S_3 has 6 subgroups, namely

- $\{(1)\}$
- $\{(1), (1,2)\}$
- $\{(1), (1,3)\}$
- $\{(1), (2,3)\}$
- $\{(1), (1,2,3), (1,3,2)\}$
- $\{(1), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$

If $f(X)$ splits completely over K then $Gal(f/K) = \{(1)\}$. If $f(X)$ is reducible over K but does not split completely then $Gal(f/K)$ is isomorphic to the cyclic group of order 2.
If $Gal(f/K) \cong S_3$ then by the fundamental theorem of Galois Theory, there exists a field extension M such that $K \subseteq M \subseteq L$ and $Gal(M/K) \cong C_3$. We have that $M = K(\delta)$ where $\delta \in L$. Even permutations of S_3 fix δ and odd permutations send δ to $-\delta$. If $\alpha_1, \alpha_2, \alpha_3$ are the roots of f then

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1)$$

If f is irreducible over K then $Gal(f/K)$ is S_3 if and only if $\delta \notin K$.

Definition 11.1. *Let $f(X) \in K[X]$ be a cubic polynomial and $\alpha_1, \alpha_2, \alpha_3$ its roots in a splitting field over K. Then we define the* ***descriminant*** *D of f as*

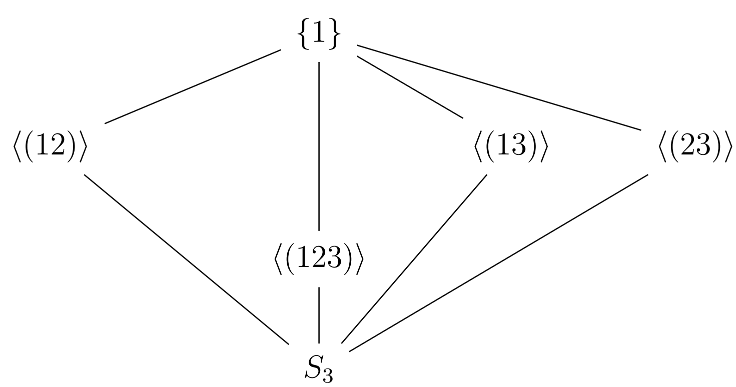
$$D = \delta^2 = (\alpha_1 - \alpha_2)^2(\alpha_2 - \alpha^3)(\alpha_3 - \alpha_1)^2$$

Suppose that $\sqrt{D} \in K$. Then any element of $Gal(f/K)$ must fix $\sqrt{D}$. But a transposition of two roots does not fix $\sqrt{D}$. S_3 contains exactly 3 such permutations (namely the cyclic groups of order 2). Therefore $Gal(f/K) \cong S_3$ if and only if D is not a square in K. If $f(X) = X^3 + aX + b$ then

$$D = -4a^3 - 27b^2$$

If $f(X) = X^3 + a_2X^2 + a_1X + a_0$ and $char(K) \neq 3$ then we can eliminate the quadratic term with the change of variable $Y = X - \frac{a_2}{3}$.

Example 11.2. *Consider the polynomial $f(X) = X^3 + 2 \in \mathbb{Q}[X]$. By Eisenstein's Criterion, we have that the prime number 2 divies every coefficient except the leading one and $2^2 = 4 \not| a_0 = 2$ hence $f(X)$ is irreducible over $\mathbb{Q}$. It's Galois group $Gal(f/\mathbb{Q})$ is hence either S_3 or C_3. The descriminant of $f(X)$ is $D = -27 \cdot 2^2$. This is not a square in $\mathbb{Q}$ and hence the Galois group is S_3.*
We shall now describe all intermediate extensions of $\mathbb{Q}$ and the splitting field of f.
Let L be a splitting field of f over $\mathbb{Q}$. Since $Gal(L/\mathbb{Q}) = S_3$, we have that there are 3 intermediate extensions of degree 3 and one of degree 2.
The intermediate field of degree 2 is fixed by $C_3 \subseteq S_3$. Since C_3 is a normal subgroup of S_3, we have that the intermediate field L^{C_3} is Galois over $\mathbb{Q}$. The other extensions are not normal subgroups of S_3 and hence none of their corresponding fixed fields are Galois over $\mathbb{Q}$. We obtain the following lattice diagrams



$$
\begin{tikzcd}
 & & L \arrow[dll, dash] \arrow[dd, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
\mathbb{Q}(\alpha_3) = L^{\langle (12) \rangle} \arrow[ddrr, dash] & & & \mathbb{Q}(\alpha_2) = L^{\langle (13) \rangle} \arrow[ddl, dash] & \mathbb{Q}(\alpha_1) = L^{\langle (23) \rangle} \arrow[ddll, dash] \\
 & & \mathbb{Q}(\sqrt{D}) = L^{\langle (123) \rangle} \arrow[d, dash] & & \\
 & & S_3 & &
\end{tikzcd}
$$

We can write α_2 *and* α_3 *in terms of* $\sqrt{D}$ *and* α_1*. Note that*

$$f(X) = (X - \alpha_1)g(X)$$

where

$$g(X) = X^2 + \alpha_1 X + \alpha_1^2 + a$$

We thus see that $\alpha_2, \alpha_3 = \frac{-\alpha_1 \pm \sqrt{disc(g)}}{2}$*. It is easily shown that* $disc(g) = (\alpha_2 - \alpha_3)^2$*. Another calculation shows that* $D = disc(f) = g(\alpha_1)^2 disc(g)$*.*

Example 11.3. *Consider the polynomial* $f(X) = X^3 + X + 1$ *over the rational numbers. The image of* $f(X)$ *under the map*

$$\begin{aligned} \sigma : \mathbb{Q}[X] &\to \mathbb{F}_2[X] \\ f(X) &\mapsto f(X) \quad (mod\ 2) \end{aligned}$$

has no roots in $\mathbb{F}_2$ *and is hence irreducible over this field. We therefore have that* $f(X)$ *is irreducible over the* $\mathbb{Z}$ *and, by Gauss' Lemma, irreducible over* $\mathbb{Q}$*.*
The discriminant of $f(X)$ *is given by*

$$D = -4 - 27 = -31$$

This is not a square in the rational numbers. Hence $Gal(f/\mathbb{Q}) = S_3$*.*

Example 11.4. *Consider the polynomial* $f(X) = X^3 - X^2 - 2X + 1$ *over the rational numbers. By argumentation similar to the previous example, we can see that* $f(X)$ *is irreducible over* $\mathbb{F}_2$ *and thus over* $\mathbb{Z}$*. By Gauss' Lemma,*

$f(X)$ is irreducible over $\mathbb{Q}$.
By making the linear change of variable $X = X + \frac{1}{3}$ to get the polynomial $g(X) = X^3 - \frac{7}{3}X + \frac{7}{27}$, we can see that the discriminant is

$$\begin{aligned} D &= -4 \cdot \left(\frac{-7}{3}\right)^3 - 27 \cdot \left(\frac{7}{27}\right)^2 \\ &= 4 \cdot \frac{7^3}{27} - \frac{7^2}{27} \\ &= 7^2 \left(\frac{28/27}{-}\frac{1}{27}\right) \\ &= 7^2 \end{aligned}$$

Hence D is a square in $\mathbb{Q}$ and $Gal(f/\mathbb{Q}) \cong A_3$.

Chapter 12

Symmetric Polynomials

Definition 12.1. *Let $X_1, \dots X_n$ be variables. We define the **elementary symmetric functions** in X_i to be*

$$\begin{aligned}
s_1 &= X_1 + X_2 \dots + X_n \\
s_2 &= X_1X_2 + X_1X_3 + \dots + X_{n-1}X_n = \sum_{i<j} X_iX_j \\
s_3 &= \sum_{i<j<k} X_iX_jX_k \\
&\vdots \\
s_n &= X_1X_2 \dots X_n
\end{aligned}$$

Obviously S_n acts on $X_1, \dots, X_n$. This action can be extended to an action on the polynomial ring $R[X_1, \dots, X_n]$ for any ring R. Let $f \in R[X_1, \dots, X_n]$ and $\sigma \in S_n$. Then

$$\sigma(f)(X_1, \dots, X_n) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$$

Example 12.2. *Let $f(X_1, X_2, X_3) = X_1X_2 + X_2^2X_3^2$ and $\sigma = (123) \in S_3$. Then $\sigma(f)(X_1, X_2, X_3) = X_2X_3 + X_3^2X_1^2$.*

Definition 12.3. *We say that a polynomial $f(X_1, \dots, X_n) \in R[X_1, \dots, X_n]$ is a **symmetric polynomial** if $\sigma(f) = f$ for all $\sigma \in S_n$.*

Definition 12.4. *We say that a polynomial $f(X_1, \dots, X_n) \in R[X_1, \dots, X_n]$ is a **partially symmetric polynomial** with respect to H if $\sigma(f) = f$ for all $\sigma \in H$ for some $H \subseteq S_n$.*

Example 12.5.

$$f(X_1, \ldots, X_n) = \prod_{1 \leq i \leq j \leq n} (X_i - X_j)$$

is partially symmetric with respect to the subgroup $A_n \subseteq S_n$*.*

Example 12.6.

$$f(X_1, X_2, X_3, X_4) = X_1X_3 + X_2X_4$$

is partially symmetric with respect to the subgroup $D_4 \subseteq S_4$*.*

Theorem 12.7. *Any symmetric polynomial in* $X_1, \ldots, X_n$ *can be uniquely expressed in terms of elementary symmetric polynomials.*

Example 12.8. $X_1^2 + X_2^2 + X_3^2 = s_1^2 - 2s_2$

Corollary 12.9. *The ring* $R[s_1, \ldots, s_n]$ *is isomorphic to the polynomial ring in* n *variables over* R*.*

Definition 12.10. *A rational function* $f \in K(X_1, \ldots, X_n)$ *is **symmetric** if* $\sigma(f) = f$ *for all* $\sigma \in S_n$*.*

Corollary 12.11. *A symmetric rational function can be uniquely expressed as a rational function in* $s_1, \ldots, s_n$*.*

Corollary 12.12. *Let* K *be a field,* $M = K(X_1, \ldots, X_n)$ *and* $L = K(s_1, \ldots, s_n)$*. Then* M/L *is Galois with* $Gal(M/L) \cong S_n$*.*

Definition 12.13. *Let* $f \in K[X]$ *be a polynomial of degree* n *with roots* $\alpha_1, \ldots, \alpha_n$*. Then we define the **descriminant** of* f *by*

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

Remark. *The polynomial* $\prod_{i<j}(X_i - X_j)^2$ *is symmetric meaning* D *is fixed by all* $\sigma \in S_n$*. It is clear that* D *is non-zero if and only if* f *is a seperable polynomial. We can also see that* $D \in K$*.*

Chapter 13

Quartic equation

Let $f(X) \in K[X]$ be a quartic polynomial. Then $Gal(f/K)$ is a subgroup of S_4. S_4 has 24 subgroups, namely

- Isomorphic to C_1: $\{(1)\}$
- Isomorphic to C_2: six subgroups generated by the six transpositions and three subgroups generated by the products of two distinct transpositions
- Isomorphic to C_3: four subgroups generated by three cycles
- Isomorphic to $V_4 := C_2 \times C_2$: one transitive subgroup

  $$V = \{(1), (12)(34), (13)(24), (14)(23)\}$$

  and three non-transitive subgroups from products of C_2's above.
- Isomorphic to C_4: three transitive subgroups generated by $(1234), (1324), (1243)$
- Isomorphic to S_3: four non-transitive subgroups obtained as stabilisers of each element of the finite set.
- Isomorphic to D_4: three transitive subgroups generated by the three C_4's above and one by the non-transitive V_4's above.
- The alternating subgroup A_4
- S_4

We shall only consider the cases where f is an irreducible quartic polynomial over K so that the Galois group is one of V, C_4, D_4, A_4, S_4.

Proposition 13.1. *Let $f(X) = X^4 + bX^2 + c \in K[X]$ be an irreducible seperable polynomial. Then $Gal(f/K) = V$ if and only if c is a square in K.*

Proof. The roots of $f(X)$ are given by $\pm\sqrt{r \pm s\sqrt{t}}$ where $b = -2r$ and $c = r^2 - s^2t$. Letting $\alpha = \sqrt{r + s\sqrt{t}}$ and $\alpha' = \sqrt{r - s\sqrt{t}}$ then the roots of f are $\alpha, -\alpha, \alpha', -\alpha'$. The splitting field for f over K is therefore $L = K(\sqrt{t}, \alpha, \alpha')$. Therefore $|Gal(f/K)|$ divides 8. We hence have that $Gal(f/K)$ is either C_4, D_4 or V.
The discriminant of f is given by

$$D = \delta^2 = 2^4(b^2 - 4c)^2c = 2^8s^4t^2(r^2 - s^2t)$$

If c is a square in K then so is D. Hence $Gal(f/K) \subseteq A_4$. Since the order of the Galois group must divide 8, the only choice is that $Gal(f/K) = V$. □

Remark. *We also see from the above proof that $\sqrt{r + s\sqrt{t}}$ can be written as $\sqrt{a} + \sqrt{b}$ if and only if $r^2 - s^2t$ is a square in K.*

Remark. *To check if a polynomial of the form $f(X) = X^4 + aX^2 + b$ is irreducible over K, we first consider the quadratic polyomial $g(Y) = Y^2 + aY + b$. If the roots of f are $\pm\alpha$ and $\pm\alpha'$ then the roots of g are α^2 and α'^2. If $g(X)$ is reducible then α^2 and α'^2 lie in K and hence $f(X)$ factorises into $(X^2 - \alpha^2)(X^2 - \alpha'^2)$.*
Conversely, if $g(X)$ is irreducible then we just have to check if $f(X)$ factorises over $K[X]$ into two quadratic polynomials. Writing

$$f(X) = (X^2 + aX + b)(X^2 + cX + d)$$

we can check if there exist solutions of $a, b, c, d \in K$ with a and c non-zero. If such no such solution exists thatn $f(X)$ is irreducible over K.

Example 13.2. *Consider the polynomial $f(X) = X^4 - 10X^2 + 1$ over $\mathbb{Q}$. By the remark above, we can show that f is irreducible over $\mathbb{Q}$. The quadratic polynomial $Y^2 - 10Y + 1$ has no roots in $\mathbb{Q}$. Hence if $f(X)$ is reducible, it should factorise as*

$$\begin{aligned} f(X) = X^4 - 10X^2 + 1 &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a + c)X^3 + (b + d + ac)X^2 + (bc + ad)X + bd \end{aligned}$$

Hence, $a = -c, b + d - a^2 = -10, a(d - b) = 0$ *and* $bd = 1$. *We see that* $b = d = \pm 1$. *Therefore* $a^2 = \pm 2 + 10$ *which has no rational solutions. Hence* $f(X)$ *is irreducible over* $\mathbb{Q}$.
By the proposition, since $c = 1$ *is a square in* $\mathbb{Q}$, *we have that* $Gal(f/\mathbb{Q}) \cong V$. *By the fundamental theorem, there are three intermediate extensions of degree 2 over* $\mathbb{Q}$. *The roots of the polynomial are* $\pm\sqrt{5 \pm 2\sqrt{6}}$. *Let* $\alpha_1 = -\alpha_2 = \sqrt{5 + 2\sqrt{6}}$ *and* $\alpha_3 = -\alpha_4 = \sqrt{5 - 2\sqrt{6}}$.

The orbit of α_1 *under the group generated by* $\sigma_1 := (12)(34)$ *is* $\{\alpha_1, \alpha_2\}$. *Therefore the field fixed by* σ_1 *contains* $\alpha_1 + \alpha_2 = 0$ *and* $\alpha_1\alpha_2 = -(5 + 2\sqrt{6})$. *The fixed field is thus* $L^{\langle \sigma_1 \rangle} = \mathbb{Q}(\sqrt{6})$. *Furthermore, the group generated by* σ_1 *is a normal subgroup of* V. *Therefore* $\mathbb{Q}(\sqrt{6})$ *is Galois over* $\mathbb{Q}$.

The orbit of α_1 *under the group generated by* $\sigma_2 := (13)(24)$ *is* $\{\alpha_1, \alpha_3\}$. *Therefore the field fixed by* σ_2 *contains* $\alpha_1 + \alpha_3$ *and* $\alpha_1\alpha_3 = 1$. $(\alpha_1 + \alpha_3)^2 = 5 + 2\sqrt{6} + 5 - 2\sqrt{6} + 2\alpha_1\alpha_3 = 12$. *Hence* $\alpha_1 + \alpha_3 = \sqrt{12} = 2\sqrt{3}$. *The fixed field is thus* $L^{\langle \sigma_2 \rangle} = \mathbb{Q}(\sqrt{3})$. *Furthermore, the group generated by* σ_2 *is a normal subgroup of* V. *Therefore* $\mathbb{Q}(\sqrt{3})$ *is Galois over* $\mathbb{Q}$.

The orbit of α_1 *under the group generated by* $\sigma_3 := (14)(23)$ *is* $\{\alpha_1, \alpha_4\}$. *Therefore the field fixed by* σ_3 *contains* $\sigma_1 + \sigma_4$ *and* $\sigma_1\sigma_4 = -1$. $(\sigma_1 + \sigma_4)^2 = 5 + 2\sqrt{6} + 5 - 2\sqrt{6} + 2\alpha_1\alpha_4 = 8$. *Hence* $\alpha_1 + \alpha_4 = \sqrt{8} = 2\sqrt{2}$. *The fixed field is thus* $L^{\langle \sigma_3 \rangle} = \mathbb{Q}(\sqrt{2})$. *Furthermore, the group generated by* σ_3 *is a normal subgroup of* V. *Therefore* $\mathbb{Q}(\sqrt{3})$ *is Galois over* $\mathbb{Q}$.

The lattice diagrams of the subgroups of $Gal(f/\mathbb{Q})$ *and the intermediate fields of* L *and* $\mathbb{Q}$ *are*

$$\begin{tikzcd}[arrows=dash]
 & \{1\} \arrow[dl] \arrow[d] \arrow[dr] & \\
\langle\sigma_1\rangle \arrow[dr] & \langle\sigma_2\rangle \arrow[d] & \langle\sigma_3\rangle \arrow[dl] \\
 & V &
\end{tikzcd}
\qquad
\begin{tikzcd}[arrows=dash]
 & L \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathbb{Q}(\sqrt{6}) \arrow[dr] & \mathbb{Q}(\sqrt{3}) \arrow[d] & \mathbb{Q}(\sqrt{2}) \arrow[dl] \\
 & \mathbb{Q} &
\end{tikzcd}$$

From the above computations, we can obtain an explicit expression of the form $\sqrt{a} + \sqrt{b}$ *for the roots of* f. $\alpha_1 + \alpha_3 = 2\sqrt{3}$ *and* $\alpha_1 + \alpha_4 = \alpha_1 - \alpha_3 = 2\sqrt{2}$. *Hence* $\alpha_1 = \sqrt{2} + \sqrt{3}$ *and* $\alpha_3 = \sqrt{3} - \sqrt{2}$.

Example 13.3. *Consider the polynomial* $f(X) = X^4 - 4X^2 + 2$*. By Eisenstein's criterion with the prime number 2, we have that* $f(X)$ *is irreducible over the rational numbers. The roots of this polynomial are* $\pm\sqrt{2 \pm \sqrt{2}}$*. Denote* $\alpha_1 = -\alpha_2 = \sqrt{2+\sqrt{2}}$ *and* $\alpha_3 = -\alpha_4 = \sqrt{2-\sqrt{2}}$*. Since* $c = 2$ *is not a square in* $\mathbb{Q}$*,* $Gal(f/\mathbb{Q})$ *is either* C_4 *or* D_4*.*
Consider the extension $L = \mathbb{Q}(\alpha_1)$*. Trivially,* $\alpha_1, \alpha_2 = L$*. We can see that* $\alpha_1\alpha_2 = \sqrt{2} \in L$ *and* $\alpha_1 + \alpha_3 = \sqrt{2}\alpha$*. Hence all roots of* $f(X)$ *are in* L*.* L *must therefore be a splitting field and hence is a normal extension of* $\mathbb{Q}$*. Thus* $|Gal(f/K)| = [L : K] = 4$*. We must therefore have that* $Gal(f/K) = C_4$ *as* D_4 *has order 8.* C_4 *has two proper subgroups, namely the trivial subgroup and the cyclic group of order 2.*

The orbit of α_1 *under the permutation* $\sigma := (12) \subseteq C_2$ *is* $\{\alpha_1, \alpha_2\}$*. Therefore the field fixed by* σ *contains* $\alpha_1 + \alpha_2$ *and* $\alpha_1\alpha_2 = -\sqrt{2}$*.* $(\alpha_1 + \alpha_2)^2 = 2 + \sqrt{2} - 2(2+\sqrt{2}) + 2 + \sqrt{2} = 0$*. Hence we see that* $L^{\langle\sigma\rangle} = \mathbb{Q}(\sqrt{2})$*. Furthermore,* $C_2 \triangleleft C_4$ *hence* $L^{\langle\sigma\rangle}$ *is Galois over* $\mathbb{Q}$*.*
The lattice diagrams are

$$\begin{array}{cc} \{1\} & L \\ | & | \\ C_2 & \mathbb{Q}(\sqrt{2}) \\ | & | \\ C_4 & \mathbb{Q} \end{array}$$

Example 13.4. *Consider the polynomial* $f(X) = X^4 - 6X^2 + 7$ *over the rational numbers. The quadratic polynomual* $Y^2 - 6Y + 7$ *has no rational roots. Hence if* $f(X)$ *is reducible then it should factorise as*

$$\begin{aligned} X^4 - 6X^2 + 7 &= (X^2 + aX + b)(X^2 + cX + d) \\ &= X^4 + (a+c)X^3 + (b+d+ac)X^2 + (bc+ad)X + bd \end{aligned}$$

We have that $b = d$ *and thus* $b^2 = 7$*. This has no rational solutions hence* $f(X)$ *is irreducible over* $\mathbb{Q}$*.*
Now, $c = 7$ *is not a square in* $\mathbb{Q}$*. Therefore* $Gal(f/\mathbb{Q})$ *is either* C_4 *or* D_4*. The roots of* $f(X)$ *are* $\pm\sqrt{3 \pm \sqrt{2}}$*. Denote* $\alpha_1 = -\alpha_2 = \sqrt{3+\sqrt{2}}$ *and* $\alpha_3 = -\alpha_4 = \sqrt{3-\sqrt{2}}$*.* $\alpha_1\alpha_2 = \sqrt{7}$ *and* $\alpha_1^2 - 3 = \sqrt{2}$*. Hence any*

splitting field L of $f(X)$ must have two quadratic intermediate fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{7})$. This is only possible if $Gal(f/K) = D_4$. By the definition of D_4, we have that $Gal(f/\mathbb{Q}) = \langle x = (1324), y = (13)(24)\rangle$. The following table shows whether or not each subgroup of D_4 fixes the roots and combinations of roots that are present in L. An element is designated fixed by $\square$.

	$\langle x\rangle$	$\langle x^2\rangle$	$\langle y\rangle$	$\langle xy\rangle$	$\langle x^2y\rangle$	$\langle x^3y\rangle$	$\{e\}$	D_4
α_1	$\times$	$\times$	$\times$	$\times$	$\times$	$\square$	$\square$	$\times$
α_3	$\times$	$\times$	$\times$	$\square$	$\times$	$\times$	$\square$	$\times$
$\sqrt{2}$	$\times$	$\square$	$\times$	$\square$	$\times$	$\square$	$\square$	$\times$
$\sqrt{7}$	$\times$	$\square$	$\times$	$\times$	$\square$	$\times$	$\square$	$\times$
$\sqrt{2}, \sqrt{7}$	$\times$	$\square$	$\times$	$\times$	$\times$	$\times$	$\square$	$\times$
$\alpha_1 + \alpha_3$	$\times$	$\times$	$\square$	$\times$	$\times$	$\times$	$\square$	$\times$
$\alpha_1 - \alpha_3$	$\times$	$\times$	$\times$	$\times$	$\square$	$\times$	$\square$	$\times$
$\sqrt{14}$	$\square$	$\times$	$\times$	$\times$	$\times$	$\times$	$\square$	$\times$

We therefore obtain the following lattices

$$\begin{tikzcd}
 & & \{1\} \arrow[dll, no head] \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] \arrow[drr, no head] & & \\
\langle xy\rangle \arrow[dr, no head] & \langle x^3y\rangle \arrow[d, no head] & \langle x^2\rangle \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \langle y\rangle \arrow[d, no head] & \langle x^2y\rangle \arrow[dl, no head] \\
 & \langle x^2, xy\rangle \arrow[dr, no head] & \langle x\rangle \arrow[d, no head] & \langle x^2, y\rangle \arrow[dl, no head] & \\
 & & D_4 & &
\end{tikzcd}$$

$$\begin{tikzcd}
 & & L \arrow[dll, no head] \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] \arrow[drr, no head] & & \\
\mathbb{Q}(\alpha_3) \arrow[dr, no head] & \mathbb{Q}(\alpha_1) \arrow[d, no head] & \mathbb{Q}(\sqrt{2}, \sqrt{7}) \arrow[dl, no head] \arrow[d, no head] \arrow[dr, no head] & \mathbb{Q}(\alpha_1 + \alpha_3) \arrow[d, no head] & \mathbb{Q}(\alpha_1 - \alpha_3) \arrow[dl, no head] \\
 & \mathbb{Q}(\sqrt{2}) \arrow[dr, no head] & \mathbb{Q}(\sqrt{14}) \arrow[d, no head] & \mathbb{Q}(\sqrt{7}) \arrow[dl, no head] & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

Example 13.5. *Consider the polynomial* $f(X) = X^4 - 6x^2 + 6$ *over the rational numbers. By Eisenstein's criterion with the prime number 3,* $f(X)$ *is irreducible over* $\mathbb{Q}$*. Since* $c = 6$ *is not a square in* $\mathbb{Q}$*, we have that* $Gal(f/\mathbb{Q})$ *is either* C_4 *or* D_4*. The roots of the polynomial are* $\pm\sqrt{3 \pm \sqrt{3}}$*. Denote* $\alpha_1 = -\alpha_2 = \sqrt{3+\sqrt{3}}$ *and* $\alpha_3 = -\alpha_4 = \sqrt{3-\sqrt{3}}$*. Now* $\alpha_1\alpha_3 = \sqrt{6}$ *and* $\alpha_1^2 - 3 = \sqrt{3}$*. Hence any splitting field L of f contains two quadratic intermediate extensions, namely* $\mathbb{Q}(\sqrt{6})$ *and* $\mathbb{Q}(\sqrt{3})$ *hence* $Gal(f/K) \cong D_4$*.*

Definition 13.6. *Let* $f(X)$ *be a quartic polynomial with roots* $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ *and consider the partially symmetric functions*

$$\begin{aligned}\beta_1 &= \alpha_1\alpha_3 + \alpha_2\alpha_4\\ \beta_2 &= \alpha_1\alpha_2 + \alpha_3\alpha_4\\ \beta_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_3\end{aligned}$$

then the polynomial

$$g(X) = (X - \beta_1)(X - \beta_2)(X - \beta_3)$$

lies in $K[X]$ *and is called the* ***cubic resolvent*** *of* $f(X)$*.*

If the cubic resolvent of a quartic polynomial is reducible in $K[X]$ then $Gal(f/K)$ is a subgroup of D_4. Hence we can apply the above analysis with the discriminant D to determine whether the Galois group is V, C_4 or D_4. If $g(X)$ is irreducible in $K[X]$ then the Galois group is either A_4 or S_4. We can then determine which one it is by checking if the discriminant is a square in K. If it is then the $Gal(f/K) = A_4$. If not then $Gal(f/K) = S_4$.
For a quartic polynomial of the form $f(X) = X^4 + aX + b$, the discriminant is $D = -27a^4 + 256b^3$ and the cubic resolvent is $g(X) = X^3 - 4bX - a^2$.

Example 13.7. *Let* $f(X) = X^4 + X + 1$ *be a polynomial over the rationals.* $f(X)$ *is irreducible modulo 2 hence f is irreducible over* $\mathbb{Z}$*. By Gauss' Lemma, it is hence irreducible over* $\mathbb{Q}$*. The discriminant of f is* $D = -27 + 256 = 229$ *which is not a square in the rational numbers. The cubic resolvent of f is* $g(X) = X^3 - 4X - 1$*.* $g(X)$ *is irreducible modulo 2 and is therefore irreducible over* $\mathbb{Z}$ *by Gauss' Lemma. Hence* $Gal(f/\mathbb{Q}) = S_4$*.*

Example 13.8. *Consider the polynomial* $f(X) = X^4 + 8X + 12$ *over the rational numbers. This function is always positive at integers and thus has*

no roots in $\mathbb{Z}$. Therefore it has no roots in $\mathbb{Q}$. This rules out factorisations into 4 linear factors or one linear factor and one cubic factor. However, the polynomial could still have a factorisation of two quadratics.
If $f(X)$ factorises into two irreducible quadratic factors over $\mathbb{Z}$ then it should do so modulo p for any prime p. But

$$f(X) = (X-4)(X^3 + 4X^4 + X + 2) \quad (mod\ 5)$$

and $X^3 + 4X^2 + X + 2$ is irreducible modulo 5. Hence $f(X)$ cannot factor into two irreducible quadratic polynomials over $\mathbb{Z}$. Therefore f is irreducible over $\mathbb{Z}$ and by Gauss' lemma, over $\mathbb{Q}$.
The discriminant of f is $-3^3 \cdot 2^1 2 + 2^8 \cdot 2^6 \cdot 3^3 = 3^3 \cdot 2^1 2(4-1) = 2^1 2 \cdot 3^4$. This is a square in $\mathbb{Q}$ hence the Galois group is either V or A_4. The cubic resolvent of f is $g(X) = X^3 - 48X - 64$. This is irreducible mod 5 and hence over $\mathbb{Q}$. Therefore $Gal(f/K) = A_4$.

Chapter 14

Finite Fields

Lemma 14.1. *Let F be a finite field of characteristic p. Then $|F| = p^s$ for some $s \in \mathbb{N}$.*

Proof. The characteristic homomorphism from $\mathbb{Z}$ to F has kernel (p) for some prime p. Therefore $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is contained in F. We can then consider F as a finite dimensional vector space over $\mathbb{F}_p$. Therefore F has a basis $b_1, \ldots, b_s$ of s elements, say. Then any $f \in F$ can be represented in the form $f = a_1b_1 + \cdots + a_sb_s$ for some $a_i \in \mathbb{F}_p$. Since each a_i can take p different values, we have that there must be p^s different elements in F for some $s \geq 1$. $\square$

Lemma 14.2. *If a field of order p^s exists for some $s \in \mathbb{N}$ then it is unique up to isomorphism.*

Proof. Let F be a finite field of order p^s. Then $F^\times$ is a finite abelian group of order $p^s - 1$. Therefore $\alpha^{p^s-1} = 1$ for all $\alpha \in \mathbb{F}^{\approx}\sqsupset\gtrdot\sim$. Hence $\alpha^{p^s} = \alpha$ for all $\alpha \in F$. Now let $f(X) = X^{p^s} - X$. Then $f(\alpha) = 0$ for all $\alpha \in F$. Since F has characteristic p, we see that $f'(X) = -1$ so $f(X)$ is seperable. Hence f has p^s different roots. We can thus see that F is a splitting field of $f(X)$ over $\mathbb{F}_p$. Since any two splitting fields for a polynomial over the same base field are isomorphic, we have that any two fields of order p^s must be isomorphic. $\square$

Proposition 14.3. *Let p be a prime and $s \in \mathbb{N}$. Then the field of order p^s exists.*

Proof. Consider the polynomial $f(X) = X^{p^s} - X \in \mathbb{F}_p[X]$. Let F be the splitting field of $f(X)$ over $\mathbb{F}_p[X]$. Then $\mathbb{F}$ is a finite field and $|F| \geq p^s$.
Now let S be the set of roots of $f(X)$ in F. We claim that $S = F$. It suffices

to show that S is a field. Since $f(0) = f(1) = 0$, S contains 0 and 1. Now let $\alpha, \beta \in S$. It is easy to see that $\alpha + \beta, \alpha\beta, \alpha, \alpha^{-1}$ are all in S. Hence S is a field. □

Remark. *We denote the field of order p^s by $\mathbb{F}_{p^s}$. Note, however, that $\mathbb{F}_{p^s}$ is never $\mathbb{Z}/p^s\mathbb{Z}$. Since $\mathbb{F}_{p^s}$ is a seperable splitting field over $\mathbb{F}_p$, it follows that $\mathbb{F}_{p^s}$ is Galois over $\mathbb{F}_p$. Moreover, since $[\mathbb{F}_{p^s} : \mathbb{F}_p] = s$, we get that $|Gal(\mathbb{F}_{p^s}/\mathbb{F}_p)| = s$.*

Definition 14.4. *Let **Frob** be the automorphism of $\mathbb{F}_{p^s}$ given by*

$$Frob(x) = x^p$$

*Frob is an $\mathbb{F}_p$-automorphism of $\mathbb{F}_{p^s}$. It is called the **Frobenius** automorphism.*

Proposition 14.5. *$\mathbb{F}_{p^s}^\times$ is a cyclic group of order $p^s - 1$.*

Proof. Let $n = p^s - 1$. For all $0 < d|n$, denote

$$\Omega_d := \{\alpha \in \mathbb{F}_{p^s}^\times \,|\, \text{order of } \alpha \text{ is } d\}$$

We claim that $|\Omega_d| \leq \varphi(d)$. If Ω_d is empty then $|\Omega_d| = 0$ and we are done. Hence assume that $|\Omega_d|$ is non-empty and $\alpha \in \Omega_d$. The polynomial $X^d - 1$ has at most d roots in $\mathbb{F}_{p^s}$ and hence $1, \alpha, \alpha^2, \ldots, \alpha^{d-1}$ are all the roots of $X^d - 1$ in $\mathbb{F}_{p^s}$. Furthermore, $\alpha^i \in \Omega_d$ if and only if $\gcd(i, d) = 1$. Hence Ω_d has $\varphi(d)$ elements.
Now we observe that any element of $\mathbb{F}_{p^s}^\times$ has order d for some $0 < d|n$. Therefore,

$$\mathbb{F}_{p^s}^\times = \bigcup_{0<d|n} \Omega_d$$

and the union is disjoint. Therefore

$$n = |\mathbb{F}_{p^s}^\times| = \sum_{0<d|n} |\Omega_d| \leq \sum_{0<d|n} \varphi(d) = n$$

Hence we have an equality and each Ω_d is in fact non-empty and has exactly $\varphi(d)$ elements. Therefore $\mathbb{F}_{p^s}^\times$ has an element of order n and is thus cyclic. □

Corollary 14.6. *The order of the Frobenius automorphism of $\mathbb{F}_{p^s}$ is s. Therefore $Gal(\mathbb{F}_{p^s}/\mathbb{F})$ is a cyclic group generated by Frob.*

Proof. Let m be the order of Frob of $\mathbb{F}_{p^s}$. Then $\alpha^{p^m} = \alpha$ for all $\alpha \in \mathbb{F}_{p^s}$. This is equivalent to having $\alpha^{p^m-1} = 1$ for all $\alpha \in \mathbb{F}_{p^s}^{\times}$. The least such m is s by the previous proposition. Hence the order of the Frobenius automorphism of $\mathbb{F}_{p^s}$ is s. □

Theorem 14.7. *The field $\mathbb{F}_{p^s}$ injects in $\mathbb{F}_{p^{s'}}$ if and only if $s|s'$.*

Proof.

$\Longrightarrow:$ Assume that $\mathbb{F}_{p^s}$ injects in $\mathbb{F}_{p^{s'}}$. Then the group $Gal(\mathbb{F}_{p^s}/\mathbb{F})$ can be obtained through a quotient of the group $Gal(\mathbb{F}_{p^{s'}}/\mathbb{F})$. Hence $s|s'$.

$\Longleftarrow:$ Conversely, if $s|s'$ then $(X^{p^s} - X)|(X^{p^{s'}} - X)$. Therefore, a splitting field of $X^{p^{s'}} - X$ over $\mathbb{F}_p$ contains a splitting field of $X^{p^s} - X$ over $\mathbb{F}_p$.

□

Theorem 14.8. *Let p be a prime and $f(X) \in \mathbb{F}_p[X]$ a irreducible polynomial of degree d over $\mathbb{F}_p$. Then $Gal(f/\mathbb{F})$ is a cyclic group of order d. More generally, if f is not irreducible but nreaks into r irreducible factors of degree $d_1, d_2, \ldots, d_r$ then $Gal(f/\mathbb{F}_p)$ is a cyclic group of order $lcm(d_1, d_2, \ldots, d_r)$.*

Proof. Let $f(X) \in \mathbb{F}_p[X]$ be an irreducible polynomial of degree d and $F = \mathbb{F}[X]/(f(X))$. Then F is a field and the extension $F/\mathbb{F}_p$ has degree d. Therefore $F \cong \mathbb{F}_{p^d}$. But we know that $\mathbb{F}_{p^d}/\mathbb{F}$ is a Galois extension. It contains a root of $f(X)$ and hence $f(X)$ must split completely in $\mathbb{F}_{p^s}[X]$. In particular, $\mathbb{F}_{p^d}$ contains the splitting field of f. Since $\deg(f) = d = [\mathbb{F}_{p^d} : \mathbb{F}_p]$, we must have that $\mathbb{F}_{p^d}$ is a splitting field of f over $\mathbb{F}_p$. Therefore $Gal(f/\mathbb{F}_p)$ is a cyclic group of order d. □

Chapter 15

Inverse Limits, Profinite Groups and Topology

Definition 15.1. *Let $\mathcal{F}$ be a set with a binary relation $\leq$ that is reflexive, antisymmetric and transitive. Then we say that $\mathcal{F}$ is a* ***partially ordered set****.*

Definition 15.2. *Let $\mathcal{F}$ be a partially ordered set and $i, j \in \mathcal{F}$. We say that $\mathcal{F}$ is* ***directed*** *if there exists $k \in \mathcal{F}$ such that $i \leq K$ and $j \leq K$.*

Definition 15.3. *Let $\mathcal{F}$ be a directed partially ordered set and for every $i \in \mathcal{F}$ let G_i be a finite group. Consider a pair $i, j \in \mathcal{F}$ such that $i \leq j$ and $\varphi_{i,j} : G_j \to G_i$ a mapping satisfying $\varphi_{i,i} = id_{G_i}$ and if $i \leq j \leq k$ then $\varphi_{i,j} \circ \varphi_{j,k} = \varphi_{i,k}$.*
We define the ***inverse limit*** *$\varprojlim_{i \in \mathcal{F}} G_i$ to be the subset of $\prod_{i \in \mathcal{F}} G_i$ containing all $(x_i)_{i \in \mathcal{F}}$ such that $\varphi_{i,j}(x_j) = x_i$ for all $i \leq j$. This is a subgroup of $\prod_{i \in \mathcal{F}} G_i$. A group of the form $\varprojlim_{i \in \mathcal{F}} G_i$ is called a* ***profinite group****.*

Example 15.4. *Any finite group G is a profinite group. Indeed, we may take $\mathcal{F}$ to be $\{1\}$ and $G_1 = G$.*

Example 15.5. *The set of natural numbers with usual ordering is a directed partially ordered set. Let p be a prime number and for every $n \in \mathbb{N}$, denote $G_n = \mathbb{Z}/p^n\mathbb{Z}$. The maps from $G_n \to G_m$ for any $m \leq n$ is the natural projection. Then the inverse limit $\varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$ is called the group of* ***p-adic*** *integers.*

Example 15.6. *We may consider another ordering on* $\mathbb{N}$. *Let* $m \leq n$ *if* m *divides* n. *Then, with this ordering,* $\mathbb{N}$ *is a directed partially ordered set. For every* $n \in \mathbb{N}$, *denote* $G_n = \mathbb{Z}/n\mathbb{Z}$. *We again take the map from* $G_n \to G_m$ *to be the natural projection for any* $m|n$. *The inverse limit* $\varprojlim_n \mathbb{Z}/n\mathbb{Z}$ *is denoted by* $\hat{\mathbb{Z}}$.

Example 15.7. *We again consider* $\mathbb{N}$ *with its usual ordering and let* $G_n = \mathbb{Z}/p^n\mathbb{Z}$. *This time, consider the map* $\varphi_n : G_n \to G_{n-1}$ *to be multiplication by* p. *Then* $\varprojlim_n G_n = 0$.

Example 15.8. *Let* K/F *be a Galois extension (not necessarily finite) and* $G = Gal(K/F)$. *Consider the set*

$$\mathcal{F} = \{L \,|\, L/F \text{ is a finite Galois extension contained in } K\}$$

We have the natural directed partial ordering on $\mathcal{F}$ *where* $L \leq L'$ *if* $L \subseteq L'$. *For every* $L \in \mathcal{F}$, *we have the group* $G_L = Gal(L/F)$. *For* $L \subseteq L'$, *there is the obvious resstriction map* $G_{L'} \to G_L$. *Then* $\mathcal{F}$ *is non-empty and* $G \cong \varprojlim_L Gal(L/K)$.

Definition 15.9. *Let* X *be a set and* $\mathcal{P}(X)$ *be the set of all subsets of* X. *Then a* ***topology*** *on* X *is a subset* $\mathcal{T}(X)$ *of* $\mathcal{P}(X)$ *such that*

1. *X and the empty set $\varnothing$ are in $\mathcal{T}(X)$*

2. *Arbitrary unions of sets in $\mathcal{T}(X)$ are in $\mathcal{T}(X)$*

3. *Finite intersections of sets in $\mathcal{T}(X)$ are in $\mathcal{T}(X)$ A topological space is a pair $(X, \mathcal{T}(X))$ where X is a set and $\mathcal{T}(X)$ is a topology on X. The subsets of X contained in $\mathcal{T}(X)$ are called* ***open*** *subsets of X. A subset of X is called* ***closed*** *if its complement in X is open.*

Definition 15.10. *A basis of a topological space* X *is a collection* $\mathcal{B}$ *of open subsets of* X *such that every open subset can be writen as the union of sets in* $\mathcal{B}$.

Definition 15.11. *Let* G *be a profinite group. Then the* ***Krull Topology*** *on* G *is the topology with basis given by cosets of finite order subgroups of* G. *Let* K/F *be a Galois extension. Then the* ***Krull Topology*** *on* $Gal(K/F)$ *is the one with the basis given by all cosets of* $Gal(K/L)$ *where* L *is a finite extension of* K.

Theorem 15.12. *Let K/F be a Galois extension and $G = Gal(K/F)$. Let G be endowed with the Krull topology. Then there is a bijection between the closed subgroups H of G and the intermediate fields of K/F given by $H \mapsto K^H$ and $L \mapsto Gal(K/L)$.*
For any subgroup H of G, we have that $Gal(K/K^H) = \overline{H}$.
A field L such that $F \subseteq L \subseteq K$ is a Galois extension of F if and only if $Gal(K/L)$ is a normal subgroup of G. Moreover, the restriction map $G \to Gal(L/F)$ induces a continuous isomorphism

$$Gal(K/F)/Gal(K/L) \to Gal(L/F)$$

Chapter 16

Cyclotomic Extensions

Definition 16.1. *We say that ζ_n is an n^{th} **root of unity** if $\zeta_n^n = 1$. If $\zeta_n = 1$ but $\zeta_n^m \neq 1$ for all $1 \leq m \leq n-1$, we say that ζ_n is the **primitive** $n^t h$ root of unity.*

Definition 16.2. *Let K be a subfield of $\mathbb{C}$. We say that the extension $K(\zeta_n)$ is the n^{th} cyclotomic extension of K.*

Remark. *The n^{th} cyclotomic extension of K is the splitting field of $X^n - 1$ over K. Hence $K(\zeta_n)/K$ is Galois.*

Lemma 16.3. *Let n be a prime number. Then the minimal polynomial of ζ_n over $\mathbb{Q}$ is $\Phi_n(X) := X^{n-1} + X^{n-2} + \cdots + 1$.*

Proof. We note that

$$\Phi_n(X) = X^{n-1} + X^{n-2} + \cdots + 1 = \frac{X^n - 1}{X - 1}$$

Hence $\Phi_n(\zeta_n) = 0$. $\square$

Lemma 16.4. *Let $n \in \mathbb{N}$. Then the minimal polynomial $\Phi_n(X)$ of ζ_n over $\mathbb{Q}$ is*

$$\Phi_n(X) = \frac{X^n - 1}{\prod_{0<d<n, d|n} \Phi_d(X)}$$

Proof. Let $f(X)$ be the minimal polynomial over $\mathbb{Q}$. We prove that if p is a prime nnumber not dividing n then ζ_n^p is a root of $f(X)$. Obviously,

$f(X)|(X^n-1)$. Let $X^n-1 = f(X)h(X)$. By Gauss' lemma, both f and h have integer coefficients. Since X^n-1 is a seperable polynomial, ζ_n^p is either a root of $f(X)$ or $h(X)$ but not both. Assume that ζ_n^p is a root of $h(X)$. Then $f(X)|h(X^p)$. Let $h(X^p) = f(X)g(X)$ for some monic $g(X) \in \mathbb{Z}[X]$. Now $a^p \equiv a \pmod p$ for all $a \in \mathbb{Z}$ implies that

$$f(X)g(X) = h(X^p) \equiv h(X)^p \pmod p$$

Hence $f(X)$ and $g(X)$ have common factors modulo p and therefore X^n-1 has multiple roots modulo p. But as p does not divide n and 0 is not a root of X^n-1, the polynomial X^n-1 cannot have multiple roots modulo p. Therefore ζ_n^p must be a root of $f(X)$. Hence $f(X)$ is also the minimal polynomial of ζ_n^p over $\mathbb{Q}$. Therefore, ζ_n^m is also a root of $f(X)$ for any m coprime to n. Hence $\deg(f) \geq \varphi(n)$.
Now we denote the minimal polynomial of ζ_n by $\Phi_n(X)$. Then we claim that

$$\prod_{0<d|n} \Phi_d(X) = X^n - 1$$

Note that $\Phi_d(X) \neq \Phi_{d'}$ if $d \neq d'$ as $\Phi_d(X)|X^d-1$ and $\Phi_{d'}(X)$ does not divide X^d-1 if $d' > d$. Hence $\Phi_d(X)$ are all pairwise coprime. Since $\Phi_d(X)|X^n-1$ for every $d|n$, we have that $\prod_{0<d|n}\Phi_d(X)|X^n-1$. Using the results from the previous claim, we have that $\deg(\Phi_d) \geq \varphi(d)$ whence $\deg(\prod_{0<d|n}\Phi_d(X)) \geq \sum_{0<d|n}\varphi(d) = n$. Hence we see that $\prod_{0<d|n}\Phi_d(X) = X^n-1$. □

Remark. *Using the above lemma, we can recursively find the n^{th} **cyclotomic polynomial**.*

Corollary 16.5. $[\mathbb{Q}(\zeta_n):\mathbb{Q}] = \varphi(n)$. *More generally,* $[K(\zeta_n):K] \leq \varphi(n)$.

Proof. Since the degree of $\Phi_n(X)$ is $\varphi(n)$, the assertion about $\mathbb{Q}$ is clear. Now we observe that $\Phi_n(X)$ is a monic polynomial with coefficients in $\mathbb{Z}$. We can therefore consider $\Phi_n(X)$ over any field and ζ_n is its root over such a field. Hence the minimal polynomial of ζ_n over K divides $\Phi_n(X)$ and thus $[K(\zeta_n):K] \leq \deg(\Phi_n(X)) = \varphi(n)$. □

Proposition 16.6. *$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$. More generally, $Gal(K(\zeta_n)/K)$ injects in $(\mathbb{Z}/n\mathbb{Z})^\times$.*

Proof. We first observe that

$$\Phi_n(X) = \prod_{0 \leq i \leq n, \gcd(n,i)=1} (X - \zeta_n^i)$$

The elements of $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ are determined by the images of ζ_n. Hence

$$Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \{\sigma_i \,|\, 0 \leq i \leq n, \gcd(n,i) = 1\}$$

where $\sigma_i(\zeta_n) = \zeta_n^i$. It obviously follows that the map

$$\begin{aligned} Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) &\to (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma_i &\mapsto i \end{aligned}$$

is an isomorphism.
For a general field K, the minimal polynomial of ζ_n over K is a divisor of $\Phi_n(X)$. Hence only those σ_i's lie om $Gal(K(\zeta_n)/K)$ for which ζ_n^i is a root of the minimal polynomial. Hence the above map forms an injection from $Gal(K(\zeta_n)/K)$ in $(\mathbb{Z}/n\mathbb{Z})^\times$. $\square$

Chapter 17

The equation $X^n - a$

Let $K \subseteq \mathbb{C}$ be a subfield and $a \in K$. Consider the polynomial $X^n - a \in K[X]$. If α is a root of $X^n - a$ then all the roots are of the form $\{\zeta_n^i \alpha \,|\, 0 \leq i \leq n\}$. Hence the splitting field of $X^n - a$ over K is $K(\zeta_n, \alpha)$. The extension $K(\zeta_n, \alpha_)/K$ is normal since it is the splitting field of a polynomial. It is seperable as K as a subfield of $\mathbb{C}$ has characteristic 0.

To find $Gal(K(\zeta_n, \alpha)/K)$, we first consider the subgroup $Gal(K(\zeta_n, \alpha)/K(\zeta_n))$.

Proposition 17.1. *$Gal(K(\zeta_n, \alpha)/K(\zeta_n)$ is a cyclic group of order dividing n.*

Proof. The conjugates of α over $K(\zeta_n)$ is a subset of

$$\{\zeta_n^i \,|\, 0 \leq i \leq n\}$$

Now we define a map

$$\chi : Gal(K(\zeta_n, \alpha)/K(\zeta_n)) \to \mathbb{Z}/n\mathbb{Z}\lambda \qquad \mapsto i$$

if $\lambda(\alpha) = \zeta_n^i \alpha$. Then this mapping is a homomorphism and, since the image of α determines elements of the Galois Group, the map is injective. It is not necessarily surjective and is only so if $X^n - a$ is irreducible over $K(\zeta_n)$. Since the subgroups of any cyclic group are again cyclic groups, it follows that $Gal(K(\zeta_n, \alpha)/K(\zeta_n))$ is isomorphic to a cyclic group. $\square$

Corollary 17.2. *$Gal(K(\zeta_n, \alpha)/K)$ contains $Gal(K(\zeta_n, \alpha)/K(\zeta_n))$ as a normal subgroup and the quotient is abelian.*

Proof. Using the fundamental theorem of Galois theory, since $K(\zeta_n)/K$ is a Galois extension, the subgroup $Gal(K(\zeta_n, \alpha)/K(\zeta_n))$ is a normal subgroup of $Gal(K(\zeta_n, \alpha)/K)$ and the quotient is isomorphic to $Gal(K(\zeta_n)/K)$ which is cyclic and hence abelian by the previous proposition. □

Proposition 17.3. *Let K be a field containing ζ_n and L a Galois extension of K such that $Gal(L/K)$ is a cyclic group of order n. Then there exists an element $l \in L$ such that $L = K(l)$ and $l^n \in K$.*

Proof. Let σ be the generator of $Gal(L/K)$. Then σ induces a K-linear transformation of the K-vector space L. Since σ is a finite order linear transformation, it is diagonalisable. Since σ^n is the identity, the eigenvalues of σ are the n^{th} roots of 1. Since σ^m is not the identity for all $) < m < n$ then there must be an eigenvalue which is a primitive n^{th} root of 1. Let $l \in L$ be the corresponding eigevectro. We hence have that

$$\sigma(l) = \zeta l$$

where ζ is the primitive n^{th} root of 1. Note that $\sigma(\zeta) = \zeta$ as $\zeta \in K$. Hence $\sigma^i(l) = \zeta^i$. Therefore l has n conjugates over K. Therefore $[K(l) : K] = n$ and so $K(l) = L$. Furthermore, $\sigma(l^n) = \sigma(l)^n = (\zeta l)^n = l^n$. Hence $l^n \in L^{\langle\sigma\rangle} = K$. □

Chapter 18

Solvability

Definition 18.1. *A group G is called **solvable** if there exists a finite chain of subgroups*

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

such that each G_{i-1} is normal in G_i and the quotient group G_i/G_{i-1} is cyclic for $1 \le i \le n$.

Lemma 18.2.

1. *Let G be solvable and $H \subseteq G$ a subgroup. Then H is solvable.*
2. *Let $H \lhd G$ be a normal subgroup. Then G is solvable if and only if both H and G/H are solvable.*
3. *Any abelian group is solvable*

Proof.

Part 1: Let G be a solvable group with a finite chain of subgroups

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

such that G_{i-1} is normal in G_i and the quotient group G_i/G_{i-1} is cyclic for $1 \le i \le n$. Let H be a subgroup of G and define $H_i = G_i \cap H$ for all $0 \le i \le n$. Hence we get the chain

$$\{e\} = H_0 \lhd H_1 \lhd \cdots \lhd H_{n-1} \lhd H_n = H$$

Each H_{i-1} is normal in H_i. Indeed, let $h \in H_i$, then

$$\begin{aligned} hH_{i-1} &= h\left(G_{i-1} \cap H\right) \\ &= \left(hG_{i-1}\right) \cap \left(hH\right) \end{aligned}$$

We have that $h \in H_i \iff h \in G_i \cap H_i \implies h \in G_i$. It is also clear that $h \in H$. Now since G_{i-1} is normal in G_i and H is trivially normal with respect to itself, we see that

$$\begin{aligned} hH_{i-1} &= h\left(G_{i-1} \cap H\right) \\ &= \left(hG_{i-1}\right) \cap \left(hH\right) \\ &= \left(G_{i-1}h\right) \cap \left(Hh\right) \\ &= \left(G_{i-1} \cap H\right) h \\ &= H_{i-1}h \end{aligned}$$

The quotient group H_i/H_{i-1} injects in G_i/G_{i-1} and must hence be cyclic. Therefore H is solvable.

□

Proposition 18.3. *Let K be a field and $n \in \mathbb{N}$. If the char(K) is positive, we assume that n is coprime to char(K). Let $a \in K$. Then the Galois group of $X^n - a$ is solvable.*

Proof. By Corollary 17.2, we can see that $Gal(K(\zeta_n, \alpha)/K$ contains $Gal(K(\zeta_n, \alpha)/K(\zeta_n))$ as a normal subgroup and the quotient is abelian. Hence by the previous lemma, $Gal(K(\zeta_n, \alpha)/K$ is solvable. □

Definition 18.4. *Let L/K be a field extension. We say that L/K is a **radical** extension if there exists an element $l \in L$ such that $L = K(l)$ and $l^n \in K$ for some $n \in \mathbb{N}$.*

Definition 18.5. *Let L/K be a field extension. We say that L/K is **solvable by radicals** if there exists a chain of subfields*

$$K = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_{n-1} \subseteq L_n \supseteq L$$

such that L_n/K is Galois and each extension L_i/L_{i-1} is a radical extension for $1 \leq i \leq n$.

Definition 18.6. *Let α be an algebraic element over K. Then we say that α is **solvable by radicals** if $K(\alpha)/K$ is solvable by radicals.*

Lemma 18.7. *Let $f(X) \in K[X]$ be an irreducible polynomial and α a root of $f(X)$. If α is solvable by radicals then so is any other root of $f(X)$.*

Proof. Let $L = K(\alpha)$ and each L_i subfields fitting the definition of a solvable by radical extension. Then L_n/K is Galois and contains α. Hence $f(X)$ splits completely in L_n. Let β be another root of $f(X)$. Then $K(\beta) \subseteq L_n$. Therefore $K(\beta)/K$ is solvable by radicals. $\square$

Definition 18.8. *We say that L/K is **solvable** if there exists a finite degree Galois extension M/K such that $L \subseteq M$ and $Gal(L/K)$ is a solvable group.*

Theorem 18.9. *Let L/K be a field extension. Then L/K is solvable if and only if L/K is solvable by radicals.*