Galois Theory, IIB

By Dr. P.M.H. Wilson, LaTeXed by Matt Daws, Michaelmas 1999
Email: matt.daws@cantab.net

0.1 Introduction

These notes are based upon the lectures given by Dr. P.M.H. Wilson in Michaelmas 1999. These typed notes are pretty much verbatim what was lectured by Dr. Wilson. However, some explanations have been added, mainly to help gap the fact that I don't know a great deal of the Groups, Rings and Fields course, which is very much a prerequisite for this course.

I would very much like to hear any comments (especially corrections), directed to `matt.daws@cantab.net`.

0.2 Disclaimer

These notes are totally unconnected with Dr. P.M.H. Wilson. That said, I would like to offer my gratitude to Dr. Wilson for offering his comments and suggestions, and not least for allowing me to distribute these notes in the first place. Redistribution of these notes may occur, without modification, in any form, provided that the following conditions are met:

1. Redistribution, in any form, must retain this disclaimer.
2. These notes must not be sold for profit, although a small amount may be charged to cover the costs of physical copying.

These notes are provided by the author "as is" and any express or implied warranties, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose are disclaimed. In no event shall the author be liable for any direct, indirect, incidental, special, exemplary, or consequential damages however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of these notes, even if advised of the possibility of such damage.

By which I mean, I'm not accountable for anything, in particular, if the notes are incorrect in places, it's not my fault!

Contents

Chapter 1

Revision from Groups, Rings and Fields

1.1 Field Extensions

Suppose K and L are fields; recall that any non-zero ring homomorphism $\theta : K \to L$ is necessarily injective[1], and $\theta(a/b) = \theta(a)/\theta(b)$ for $b \neq 0$, i.e. θ is a homomorphism of fields.

Definition 1.1.1. A *field extension* of K consists of a field L and a non-zero field homomorphism $\theta : K \to L$.

Remark 1.1.2. Such a θ is also called an *embedding* of K into L.

Of course, K can be a sub-field of L, with θ the inclusion map. In fact, we often just identify K with its image $\theta(K) \subset L$ (as $\theta : K \xrightarrow{\sim} \theta(K)$ is an isomorphism).

If $\theta : K \to L$ is a field extension, L has the structure of a K-vector space (it's certainly an abelian group, with K acting via $a.\lambda := \theta(a)\lambda$, $a \in K, \lambda \in L$). The dimension of this vector space is called the *degree* $[L : K]$ of the extension. Say L is a *finite extension* of K if the vector space is finite dimensional.

Example 1.1.3. $K = \{p + q\sqrt{2} : p, q \in \mathbb{Q}\} \subset \mathbb{C}$ (note that $(p + q\sqrt{2})^{-1} = (p - q\sqrt{2})/(p^2 - 2q^2)$) is a finite extension of $\mathbb{Q}$ of degree 2.

Lemma 1.1.4. *If $\{K_i\}_{i \in I}$ is any collection of subfields of a field L, then $\bigcap_{i \in I} K_i$ is also a subfield.*

Proof. Simple exercise from axioms. □

Definition 1.1.5. Given a subfield $k \subset L$ and $S \subset L$ any subset, the *subfield generated* by k and S, $k(S) := \bigcap\{\text{subfield } K \subset L : k \subset K, S \subset K\}$, i.e. the "smallest" subfield containing both k and S, from lemma. If $S = \{x_1, \ldots, x_n\}$ write $k(x_1, \ldots, x_n)$ for $k(S)$. We say that a field extension $\theta : K \to L$ is *finitely generated* if for some n, $\exists x_1, \ldots, x_n \in L$ such that $L = \theta(k)(x_1, \ldots, x_n)$. If, moreover, $n = 1$ then the extension is called *simple.*

Notation. From now on, we usually denote a field extension by $k \hookrightarrow K$ or K/k. Given a field extension $\theta : k \hookrightarrow K$ and a subset $S \subset K$ denote the field extension $k \hookrightarrow \theta(k)(S)$ by $k(S)/k$.

Definition 1.1.6. Given a field extension K/k, an element $x \in K$ is *algebraic* over k, if $\exists$ non-zero polynomial $f \in k[X]$ such that $f(x) = 0$ in K (otherwise x is called *transcendental*). If x is algebraic over k, the monic polynomial $f = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$ of smallest degree n such that $f(x) = 0$ is called the *minimal polynomial.* Clearly such an f is *irreducible*[2], and the remainder theorem implies uniqueness.

Definition 1.1.7. K/k is *algebraic* if every $x \in K$ is algebraic over k. It is called *pure transcendental* if no $x \in K$ is algebraic over k apart from those in (the image of) k.

Theorem 1.1.8. *Given a field extension K/k and $x \in K$, x is algebraic over k iff $[k(x) : k] < \infty$. When x is algebraic, $[k(x) : k]$ is the degree of the minimal polynomial.*

[1] If $a \neq b$ then $\theta(a) = \theta(b) \Rightarrow \theta(a - b) = 0 \Rightarrow \theta((a - b)(a - b)^{-1}) = 0 \Rightarrow \theta(1) = 0$ contradiction.

[2] $f \in k[X]$ is irreducible if $f = hg$ over $k[X]$ implies h or g is in k.

Proof. ($\Leftarrow$) If $[k(x):k]=n$, then $1,x,\ldots,x^n$ are linearly dependent over k, which implies $\exists$ polynomial f as claimed with $f(x)=0$ in K.
($\Rightarrow$) If x is algebraic over k with minimal polynomial f, then

$$f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0=0 \tag{1.1}$$

in K. Suppose $g\in k[X]$ such that $g(x)\neq 0$; since f is irreducible, we have $\operatorname{hcf}(f,g)=1$. So Euclid's algorithm implies $\exists\ \alpha,\beta$ polynomials in $k[X]$ such that $\alpha f+\beta g=1$ in $k[X]\Rightarrow\ \beta(x)g(x)=1$ in K and so $g(x)^{-1}\in\langle 1,x,x^2,\ldots\rangle$ *subspace* of K generated by powers of x. Now $k(x)$ consists of all elements of the form $h(x)/g(x)$ for $h,g\in k[X]$, $g(x)\neq 0$ (such elements form a subfield, and its the smallest one generated by k and x) and so $k(x)$ is spanned as a k-vector space by $1,x,x^2,\ldots$ and hence from (1.1) by $1,x,\ldots,x^{n-1}$. Minimality of n implies spanning set is a basis and hence $[k(x):k]=n$. □

Given field k and an *irreducible* polynomial $f\in k[X]$ recall that the quotient ring $k[X]/\langle f\rangle$ is a field (Euclid's algorithm yields inverses as above). Therefore we have a simple algebraic extension $k\hookrightarrow k(x)=k[X]/\langle f\rangle$, where x denotes the image of X.

However, given any simple algebraic extension $k\overset{\theta}{\hookrightarrow}k(x)$, we let f be the minimal polynomial for x over k. We then have the commutation $k\overset{\iota}{\hookrightarrow}k[X]\to k(x)$ (where the second map is evaluation $X\mapsto x$) induces an isomorphism of fields $k[X]/\langle f\rangle\xrightarrow{\sim}k(x)$. Thus up to isomorphism any simple algebraic extension of k is of the form $k\hookrightarrow k[X]/\langle f\rangle$ for $f\in k[X]$ irreducible. So classifying simple algebraic extensions of k (up to isomorphism) is equivalent to classifying irreducible monic polynomials in $k[X]$.

1.2 Tests for Irreducibility

Suppose R is a UFD[3] and k it's field of fractions[4], e.g. $R=\mathbb{Z},k=\mathbb{Q}$.

Lemma 1.2.1. (Gauss's Lemma)
A polynomial $f\in R[X]$ is irreducible iff it is irreducible in $k[X]$.

Proof. This is rather long, so see Appendix A. □

Theorem 1.2.2. (Eisenstein's irreducibility criterion)
Suppose $f=a_nX^n+a_{n-1}X^{n-1}+\ldots+a_0$ with R, k as above, and there is an irreducible element $p\in R$ such that $p\not|\,a_n$, $p|a_i$ for $i=n-1,\ldots,0$ and $p^2\not|\,a_0$ then f is irreducible in $R[X]$ therefore irreducible in $k[X]$ by above.

Proof. Suppose that $f=gh$. Reduce[5] mod p to get $\bar{f}=\bar{g}\bar{h}$. By assumption, $\bar{f}=\overline{a_n}x^n$, as all the other terms are $\equiv 0 \mod p$. This means that $g=\overline{a_m}x^m$ and $h=\overline{a_{n-m}}x^{n-m}$ for some $0<m<n$, $a_ma_{n-m}\equiv a_n \mod p$.

Thus $g=b_Nx^N+\ldots+b_0$, $N\geq m$ and $b_i\equiv 0\ \forall i\neq m$; $h=c_Mx^M+\ldots+c_0$, $M\geq n-m$ and $c_i\equiv 0\ \forall i\neq n-m$. This means that $a_0=b_0c_0$ and as $p|b_0$ and $p|c_0$ we have $p^2|a_0$ contrary to assumption. Hence f is irreducible. □

Proposition 1.2.3. (The Tower Law)
If $k\hookrightarrow K\hookrightarrow L$, we have a tower of field extensions, and $[L:k]=[L:K][K:k]$ with the usual convention for ∞.

Proof. Observe first that if $[L:k]<\infty$ then $[K:k]<\infty$ (since K a subspace of L) and $[L:K]<\infty$ (since any basis for L over k is certainly a spanning set for L over K). Hence wlog $[K:k]=m$, $[L:K]=n$. Let $u_1,\ldots,u_n$ be a basis for L over K and $v_1,\ldots,v_m$ be a basis for K over k. Then clearly the elements u_iv_j form a spanning set for L over k. Further, if $\sum_{i,j}\lambda_{i,j}u_iv_j=0$ then $\sum_i u_i\sum_j\lambda_{i,j}v_j=0$ where $\sum_j\lambda_{i,j}v_j\in K$, call them w_i. Thus $\sum_i u_iw_i=0$, but as $\{u_i\}$ as basis for L over K, we have $w_i=0$, so $\sum_j\lambda_{i,j}v_j=0$, but as $\{v_j\}$ a basis for K over k, $\lambda_{i,j}=0$ so $\{u_iv_j\}$ is a basis of L over k. Hence result. □

[3] Unique Factorisation Domain, which is a domain R such that if $a\neq 0$ is not a unit, then a is the product of finitely many irreducible elements; and if $a=x_1\ldots x_n=y_1\ldots y_m$ with all x_i,y_j irreducible, then $m=n$ and $(\forall i)x_i\sim y_{\sigma(i)}$ for suitable permutation $\sigma\in S_n$

[4] k is the field of fractions for a domain R if k is the "smallest" field containing R, i.e. it is the set of equivalence classes $\frac{a}{b},a,b\in R,b\neq 0$ such that $\frac{a}{b}=\frac{c}{d}\Leftrightarrow ad=bc$ (in R), $\frac{a}{b}\pm\frac{c}{d}=\frac{ad\pm bc}{bd}$ and $\frac{a}{b}\cdot\frac{c}{d}=\frac{ac}{bd}$.

[5] I.e. a map$R[X]\to\mathbb{F}_p[X]$; $a_nX^n+\ldots+a_0\mapsto b_nX^n+\ldots+b_0$ where $b_n\equiv a_n \mod p$, which by definition means that $p|(b_n-a_n)$. It is an easy check to see that this is in fact a ring homomorphism.

Corollary 1.2.4. *If K is a finitely generated field extension of k, say $K = k(a_1, \dots, a_m)$, and each a_i is algebraic over k, then K/k is a finite field extension.*

Proof. Each a_i is algebraic over $k(a_1, \dots, a_{i-1})$ so by (1.1.8)
$[k(a_1, \dots, a_i) : k(a_1, \dots, a_{i-1})] < \infty$ for all i. So induction and (1.2.3) implies the result. □

1.3 Splitting Fields

Recall that if K/k is a field extension and $f \in k[X]$, then we say that f *splits* over K if (the image of) $f \in K[X]$ splits into linear factors $f = c(X - \alpha_1) \dots (X - \alpha_n)$, $c \in k$, $\alpha_i \in K$. K is called the *splitting field* (or *splitting extension*) for f if f fails to split completely over any subfield of K. Clearly equivalent to saying $K = k(\alpha_1, \dots, \alpha_n)$.

Splitting fields always exist since if g is any irreducible factor of f in $k[X]$ then $k[X]/\langle g \rangle = k(x)$ is an extension of k for which $g(x) = 0$ (x=image of X). Remainder theorem implies g (and hence f) splits off a linear factor. Induction implies $\exists$ splitting field, K, for f with $[K : k] \leq n!$ ($n = \deg f$) by the tower law.

1.4 Splitting fields are unique up to isomorphism

Proposition 1.4.1. *Suppose $\theta : k \to k'$ is an isomorphism of fields with $f \in k[X]$ corresponding to $g = \theta(f) \in k'[X]$. Then any splitting field K for f over k is isomorphic (over θ) to any splitting field K' for g over k'.*

Proof. If f splits over K, then so does any irreducible factor, f_1, and we have a subfield $L \subset K$ which is a splitting field for f_1 over k. There exists a corresponding irreducible factor g_1 of g and a subfield $L' \subset K'$ which is a splitting field for g_1 over k'. Choose a root $\alpha \in L$ for f_1 and $\beta \in L'$ for g_1. Then the corresponding extensions $k(\alpha)/k$ and $k'(\beta)/k'$ are isomorphic to the field extensions $k[X]/\langle f_1 \rangle$ (respectively $k'[X]/\langle g_1 \rangle$).
If we now set $f = (X - \alpha)h \in k(\alpha)[X]$ and $g = (X - \beta)l \in k'(\beta)[X]$ then

1. $l = \theta_1(h) \in k'(\beta)[X]$ under the induced isomorphism $\theta_1 : k(\alpha)[X] \to k'(\beta)[X]$.
2. K is a splitting field for h over $k(\alpha)$ and K' is a splitting field for l over $k'(\beta)$.

Thus required result follows by induction on the degree of the polynomial. □

Thus we have existence and uniqueness of splitting fields for any finite set of polynomials (just take splitting field of the product). With appropriate use of Zorn's Lemma[6] this extends to any set of polynomials (see chapter 3 where we prove existence and uniqueness of algebraic closures).

[6] Oh dear, here it comes...

Chapter 2

Separability

Definition 2.0.2. An irreducible polynomial $f \in k[X]$ is called *separable* over k if it has distinct roots (zeros) in a splitting field K, i.e. $f = c(X-\alpha_1)\dots(X-\alpha_n)$ in $K[X]$ with $c \in k$, $\alpha_i \in K$, α_i distinct. By uniqueness of splitting fields (up to isomorphism) this is independent of any choices. An arbitrary polynomial $f \in k[X]$ is separable over k if all its irreducible factors are. If not, it is called *inseparable.*

To determine whether an irreducible polynomial f has distinct roots in a splitting field we introduce formal differentiation of polynomials, $D : k[X] \to k[X]$, a linear map as vector spaces over k, defined by $D(X^n) = nX^{n-1}$ $\forall n > 0$, $D(c) = 0$ for $c \in k$.

Proposition 2.0.3. $D(fg) = fD(g) + gD(f)$

Proof. Using linearity, we can reduce this to the case when f and g are *monomials*, in which case it is a trivial check. □

From now on denote $D(f)$ by f'.

Lemma 2.0.4. *A polynomial $0 \neq f \in k[X]$ has a repeated root in a splitting field iff f and f' have a common factor of degree ≥ 1.*

Proof. ($\Rightarrow$) Suppose f has a repeated zero α in a splitting field K, i.e. $f = (X-\alpha)^2 g$ in $K[X]$. Thus $f' = (X-\alpha)^2 g' + 2(X-\alpha)g$ so f and f' have a common factor $(X-\alpha)$ in $K[X]$, so f and f' have a common factor in $k[X]$ (namely, the minimal polynomial of α).
($\Leftarrow$) Suppose f has no repeated roots in a splitting field K. We show that f and f' have no common factor in $K[X]$. Sufficient to prove $(X-\alpha)|f$ in $K[X] \Rightarrow (X-\alpha) \not| f'$. Writing $f = (X-\alpha)g$ with $(X-\alpha) \not| g$ we observe $f' = (X-\alpha)g' + g$ so $(X-\alpha) \not| f'$. □

If now f is irreducible, (2.0.4) says that f has repeated roots in a splitting field iff $f' = 0$ (as $\deg f' < \deg f$ and f irreducible). But if $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ then $f' = na_n X^{n-1} + \ldots + a_1$ implies $f' = 0$ iff $ia_i = 0$ in k for all i. So if $\deg f = n > 0$, $f' = 0$ iff $\operatorname{char} k = p > 0$ and $p|i$ whenever $a_i \neq 0$ iff $\operatorname{char} k = p > 0$ and f of form $f = b_r X^{pr} + b_{r-1}X^{p(r-1)} + \ldots + b_1 X^p + b_0 \in k[X^p]$.

So if char $= 0$, all polynomials are separable. If $\operatorname{char} k = p > 0$, an irreducible polynomial f is separable $\iff f \in k[X^p]$.

Definition 2.0.5. Given a field extension K/k and an element $\alpha \in K$, we say that α is *separable over* k if its minimal polynomial $f_\alpha \in k[X]$ is separable. The extension is called *separable* if α is separable for all $\alpha \in K$. Otherwise it's called *inseparable.*

Example 2.0.6. Let $K = \mathbb{F}_p(t)$, field of rational functions over the finite field $\mathbb{F}_p$ with p elements. Let $k = \mathbb{F}_p(t^p)$. The field extension K/k is inseparable, since the minimal polynomial of t over k is $X^p - t^p \in k[X]$. In $K[X]$ this splits as $X^p - t^p = (X-t)^p$ and so is inseparable.

Lemma 2.0.7. *If we have a tower of finite extensions $k \hookrightarrow K \hookrightarrow L$ with L/k separable then both L/K and K/k are separable.*

Proof. Given an element $\alpha \in L$, the minimal polynomial of α over K divides the minimal polynomial of α over k and so again has distinct zeros in a splitting field. K/k is separable is obvious from the definition. □

The converse is true, but more difficult and needs a little preparation.

Proposition 2.0.8. *Let $k(\alpha)/k$ be a finite extension, with $f \in k[X]$ the minimal polynomial for α. Given a field extension $\theta : k \hookrightarrow K$, the number of embeddings $\tilde{\theta} : k(\alpha) \hookrightarrow K$ extending[1] θ is precisely the number of distinct roots of $\theta(f)$ in K. In particular, $\exists$ at most $n = [k(\alpha) : k]$ such embeddings with equality $\Leftrightarrow$ $\theta(f)$ splits completely in K and f is separable.*

Proof. This much is essentially clear[2]. An embedding $k(\alpha) \hookrightarrow K$ extending θ must send α to a root of $\theta(f)$ [3], and is determined by this information, i.e. if β a zero of $\theta(f)$ in K then the ring homomorphism $k[X] \to K$; $g \mapsto \theta(g)(\beta)$ factors to give an embedding $k[X]/\langle f \rangle \hookrightarrow K$ where $k(\alpha) \cong k[X]/\langle f \rangle$ extending θ and sending α to β. Therefore $\exists$ at most $n = \deg f$ by (1.1.8), $n = [k(\alpha) : k]$ such embeddings $\tilde{\theta}$, and we have equality $\Leftrightarrow$ $\theta(f)$ has n distinct roots in K $\Leftrightarrow$ splits completely in K and f separable. □

Theorem 2.0.9. *Suppose $K = k(a_1, \ldots, a_r)$ is a finite extension of k and L/k is any field extension for which all the minimal polynomials of the a_i split.*

1. *The number of embeddings $K \hookrightarrow L$ extending $k \hookrightarrow L$ is at most the degree of the extension, $[K : k]$. If each a_i is separable over $k(a_1, \ldots, a_{i-1})$ then we have equality.*
2. *If the number of embeddings $K \hookrightarrow L$ extending $k \hookrightarrow L$ is $[K : k]$ then K/k is separable (i.e. converse of 1).*
3. *Hence if each a_i is separable over $k(a_1, \ldots, a_{i-1})$ then K/k is separable. (By (2.0.7) this happens, for instance, when each a_i is separable over k).*

Proof.

1. Follows by induction on r, and (2.0.8). (2.0.8) $\Rightarrow$ true for $r = 1$. Suppose true for $r-1$, then $\exists$ at most $[k(a_1, \ldots, a_{r-1}) : k]$ embeddings $k(a_1, \ldots, a_{r-1}) \hookrightarrow L$ extending $k \hookrightarrow L$, with equality if each a_i $(i < r)$ is separable over $k(a_1, \ldots, a_{i-1})$. For each such embedding, (2.0.8) implies $\exists$ at most $[K : k(a_1, \ldots, a_{r-1})]$ embeddings $K \hookrightarrow L$ extending given embedding $k(a_1, \ldots, a_{r-1}) \hookrightarrow L$, with equality if a_r separable over $k(a_1, \ldots, a_{r-1})$. Tower law gives required result.
2. Suppose $\alpha \in K$. (1) implies $\exists$ *at most* $[k(\alpha) : k]$ embeddings $k(\alpha) \hookrightarrow L$ extending $k \hookrightarrow L$ and for each such embedding $k(\alpha) \hookrightarrow L$, $\exists$ *at most* $[K : k(\alpha)]$ embeddings $K \hookrightarrow L$ extending it. By tower law, our assumption implies both these must be equalities. In particular, (2.0.8) gives that α is separable.

□

Corollary 2.0.10. *If we have a tower $k \hookrightarrow K \hookrightarrow L$ of finite extensions with L/K and K/k separable then so too is L/k.*

Proof. If $\alpha \in L$ with (separable) minimal polynomial $f \in K[X]$, write $f = X^n + a_{n-1}X^{n-a} + \ldots + a_0$ with each a_i separable over k. The minimal polynomial of α over $k(a_0, \ldots, a_{n-1})$ is still f, and so α separable over $k(a_0, \ldots, a_{n-1})$. (2.0.9)(3) implies $k(a_0, \ldots, a_{n-1}, \alpha)/k$ separable so α is separable over k. Hence L/k separable. □

Lemma 2.0.11. *Let $G \subset K^*$ be a finite subgroup of multiplicative group $K^* = \{K \setminus \{0\}, \times\}$ (K a field). Then G is cyclic.*

Proof. Pick $a \in G$, then as G finite, $\exists n, m$ such that $a^n = a^m$, and as $a \neq 0$, this implies $a^{n-m} = 1$. Denote $(n-m)$ the order of a, $o(a)$.

As $|G| = n$ finite, we can let M be the least common multiple of the orders of all the elements in G, so $g^M = 1 \; \forall \; g \in G$. Thus $o(a) \mid M \; \forall \; a \in G$. If $m = o(a)$ is the maximum of $\{o(g) : g \in G\}$ and $m < M$ then $\exists o(b) \mid M$ such that $o(b) \not| \, m$. Then $o(ab) = \mathrm{lcm}(m, o(b)) > m$, contradiction. Hence $m = M$, so $\exists x \in G$ such that $o(x) = M$.

Hence $X^M - 1$ has at least n roots in K (i.e. all the members of G), hence $M \geq n$. But Lagrange applied to $\langle x \rangle$ implies that $M \mid n$, so $M = n$. Hence $\langle x \rangle = G$. □

Theorem 2.0.12.

1. *If $K = k(\alpha, \beta)$ a finite extension of k with β separable then $\exists \theta \in K$ such that $K = k(\theta)$.*

[1] i.e. $\tilde{\theta}(x) = \theta(x) \; \forall \; x \in k$

[2] If you're the lecturer, or from Trinity. The rest of us need to do some work here I think.

[3] If $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in k[X]$ then $\theta(f) = X^n + \theta(a_{n-1})X^{n-1} + \ldots + \theta(a_0) \in K[X]$. Thus if $f(\alpha) = 0$ in $k(\alpha)$ then $\theta(f)(\alpha) = \alpha^n + \ldots + \theta(a_0) = \theta(\alpha^n + \ldots + a_0) = \theta(0) = 0$. Thus if $\tilde{\theta}$ extends θ then $\tilde{\theta}(f) = \theta(f)$ in the sense that the coefficients are the same, and hence $\tilde{\theta}(f)(\alpha) = 0$ as required.

2. Any finite separable extension K/k is simple.

Proof. If k is finite then so too is K and so (2.0.11) implies K^* cyclic, say $K^* = \langle\theta\rangle$. Then $K = k(\theta)$ as required. So wlog assume k infinite. Let f, g be minimal polynomials for α, β. Take a splitting field extension L for fg over K. Identify K with its image in L, and so α, β my be considered as elements of L. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_r$ b denote the *distinct* zeros of f ($r \leq \deg f$). Since β separable, g splits into distinct linear factors over L and denote zeros by $\beta = \beta_1, \beta_2, \ldots, \beta_s$ ($s = \deg g$). Then choose $c \in k$ such that the elements $\alpha_i + c\beta_j$ are all distinct[4], and set $\theta = \alpha + c\beta$.

Let $F \in k(\theta)[X]$ be given by $F(X) = f(\theta - cX)$. We have $g(\beta) = 0$ and $F(\beta) = f(\alpha) = 0$. Deduce β is a common zero of F and g. Any other common zero would be a β_j ($j > 1$), but then $F(\beta_j) = f(\alpha + c\beta - c\beta_j)$, since by assumption $\alpha + c(\beta - \beta_j)$ is never an α_i, so contradiction. The linear factors of g are distinct, we deduce $(X - \beta)$ is the h.c.f. of f, g in $L[X]$. However, the minimal polynomial h of β over $k(\theta)$ divides both F and g in $k(\theta)[X]$ and hence in $L[X]$, $\Rightarrow h = X - \beta \Rightarrow \beta \in k(\theta) \Rightarrow \alpha = \theta - c\beta \in k(\theta) \Rightarrow k(\alpha, \beta) = k(\theta)$.

$K = k(a_1, \ldots, a_r)$ with each a_i separable over k, and so (2) follows from (1) by induction on r. □

2.1 Trace and Norm

Let K/k be a finite field extension, $\alpha \in K$. Multiplication by α defines a linear map $\theta_\alpha : K \to K$ of vector spaces over k. The trace and norm of α, $\mathrm{Tr}_{K/k}(\alpha)$, $\mathrm{N}_{K/k}(\alpha)$ are *defined* to be the trace and determinant of θ_α, i.e. of any matrix representing θ_α with respect to some basis of K over k.

Proposition 2.1.1. *Suppose $r = [K : k(\alpha)]$ and $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ the minimal polynomial of α over k. If $b_i = (-1)^{n-i}a_i$ then $\mathrm{Tr}_{K/k}(\alpha) = rb_{n-1}$, $\mathrm{N}_{K/k}(\alpha) = b_0^r$.*

Proof. We first need to prove that the characteristic polynomial of θ_α if f^r. Prove this first for $r = 1$: take a basis $1, \alpha, \ldots, \alpha^{n-1}$ for K/k. With respect to this basis, θ_α has matrix

$$M = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & \vdots \\ 0 & & & 1 & -a_{n-1} \end{pmatrix}$$

and hence the characteristic polynomial is f via column ops.

In general case, choose a basis $1 = \beta_1, \ldots, \beta_r$ for $K/k(\alpha)$ and take basis $1, \alpha, \ldots, \alpha^{n-1}, \beta_2, \alpha\beta_2, \ldots$ for K/k (c.f. proof of the Tower Law). With respect to this basis θ_α has matrix of the form

$$\begin{pmatrix} M & & & \\ & M & & \\ & & \ddots & \\ & & & M \end{pmatrix}$$

i.e. r copies of M on the diagonal, from which the claim follows immediately. □

[4] We can do this as k infinite, and the ratios $(\alpha_i - \alpha_{i'})/(\beta_{j'} - \beta_j)$ take only finitely many values.

Chapter 3

Algebraic Closures

Definition 3.0.2. A field K is *algebraically closed* if any $f \in K[X]$ splits into linear factors over K. This is equivalent to there being no non-trivial algebraic extensions of K, i.e. any algebraic extension $K \hookrightarrow L$ is an isomorphism. An extension K/k is called an *algebraic closure* of k if K/k is algebraic and K algebraically closed.

Lemma 3.0.3. *Suppose K/k is a field extension. Then the set of elements of K which are algebraic over k form a subfield of K, call it L. If K is* algebraically closed*, the extension of L/k is an algebraic closure of k.*

Proof. L is a subfield of K, since if $\alpha, \beta \in L$, the Tower Law and (1.1.8) imply that $k(\alpha, \beta)/k$ is a finite extension. If γ is now any combination of α, β (say $\alpha + \beta$, $\alpha\beta$, α/β etc.) then $k(\gamma) \subseteq k(\alpha, \beta)$ and Tower Law gives $[k(\gamma) : k]$ finite implies γ algebraic over k, i.e. $\gamma \in L$. So L is a subfield of K.

Now consider case of K algebraically closed. Required to prove L is algebraically closed. Any polynomial $f \in L[X]$ splits completely over K by assumption– we must show that all the roots of f are in fact in L. Suppose α is such a root; write f as $f = c(X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0)$ with $c, a_i \in L$ and $L_0 = k(a_0, \ldots, a_{n-1}) \subset L$. Then the Tower Law and (1.1.8) implies L_0/k is finite. But (1.1.8) implies $L_0(\alpha)$ finite over L_0. Thus $L_0(\alpha)/k$ finite gives $k(\alpha)/k$ finite, so $\alpha \in L$. □

Example 3.0.4. Algebraic numbers in $\mathbb{C}$ form a subfield, the algebraic closure of $\mathbb{Q} \subset \mathbb{C}$.

3.1 Existence of algebraic closure

A simple-minded approach leads to set-theoretic problems. The approach we adopt is perhaps not the most natural, but avoids these problems in a clean[1] way.

Theorem 3.1.1. *An algebraic closure exists for any field k.*

Proof. Let A be the set of all pairs $\alpha = (f, j)$ where f is a non-constant monic polynomial in $k[X]$ and $1 \leq j \leq \deg f$. Then for each α, introduce an indeterminate $X_\alpha = X_{f,j}$ and then consider the polynomial ring $k[X_\alpha : \alpha \in A]$ in all these indeterminates.

Let $b_{f,l}$ $(l = 0, \ldots, \deg f - 1)$ denote the coefficients of

$$f - \prod_{j=1}^{\deg f} (X - X_{f,j}) \in k[X_\alpha : \alpha \in A]$$

and let I be the ideal generated by all these elements $b_{f,j}$ $(\forall j, \forall f)$. Let $R = k[X_\alpha : \alpha \in A]/I$ (the idea here is that we're forcing the monic polynomials to split completely).

Claim 1: $I \neq k[X_\alpha : \alpha \in A]$ i.e. $R \neq 0$. If we did have equality, then $\exists$ a finite sum $g_1 b_{f_1,l_1} + \ldots + g_N b_{f_N,l_N} = 1$ (call this †) in $k[X_\alpha : \alpha \in A]$. Let L be the splitting field extension for $f_1, \ldots, f_N$. For each i, f_i splits over L, as $f_i = \prod_{j=1}^{\deg f}(X - \alpha_{ij})$ $\alpha_{ij} \in L$. Let $\theta : k[X_\alpha : \alpha \in A] \to L$ be the evaluation map (a ring homomorphism) sending $X_{f_i,j} \mapsto \alpha_{ij}$ for $1 \leq i \leq N$, $1 \leq j \leq \deg f_i$ and all the other indeterminates $X_\alpha \mapsto 0$. Since $f_i = \prod_j (X - \alpha_{ij})$ in L, we have $\theta(b_{f_i,l}) = 0$ for all $1 \leq i \leq N$, $0 \leq l \leq \deg f_i - 1$. Thus taking image of † under θ we get $0 = 1$ in L, contradiction.

[1] If you consider the use of AC to be 'clean' is open to debate, but not here.

Thus R is non-zero and we may use Zorn's Lemma (see appendix B) to choose a maximal ideal $\mathcal{M}$ of R. Let $K = R/\mathcal{M}$. This gives a field extension of $k \hookrightarrow K$, composite of $k \hookrightarrow k[X_\alpha : \alpha \in A] \to R \to R/\mathcal{M} = K$.

Claim 2: Any $f \in k[X]$ splits complete over K. For, given any monic, non-constant polynomial $f \in k[X]$, let x_j $(1 \leq j \leq \deg f)$ denote the image in K of $X_{f,j} \in k[X_\alpha : \alpha \in A]$. By construction $b_{f,l} \mapsto 0$ in K and so $f - \prod_j (X - X_j) = 0$ in $K[X]$, so f splits completely, as required. □

This field extension K/k has properties

1. K/k algebraic, since it's generated over k by images $x_{f,j}$ of the $X_{f,j}$ (which satisfy $f(x_{f,j}) = 0$ by construction).

2. Any $f \in k[X]$ will split completely over K.

(1) and (2) imply K is algebraically closed and hence is an algebraic closure of k. (Since given a finite extension $K(\alpha)/K$, then α is algebraic over k by (1) and argument of (3.0.3) and hence $K \hookrightarrow K(\alpha)$ is an isomorphism by (2)).

3.2 Uniqueness of Algebraic Closures

Proposition 3.2.1. *Suppose that $i : k \hookrightarrow K$ with K algebraically closed. For any algebraic extension $\phi : k \hookrightarrow L$, $\exists$ embedding $j : L \to K$ extending i in the sense that $i = j \circ \phi$.*

Proof. Let S denote the set of all pairs (M, θ) where M is a subfield of L containing $\phi(k)$ and θ an embedding of M into K such that $\theta\phi = i$ (Clearly S is non-empty). Partially order S by setting $(M_1, \theta_1) \leq (M_2, \theta_2)$ iff $M_1 \subseteq M_2$ and $\theta_2|_{M_1} = \theta_1$. If $\mathcal{C}$ is a chain in S, let $N = \cup\{M : (M, \theta) \subset \mathcal{C}\}$, a subfield of L. Moreover, if $\alpha \in N$, then $\alpha \in M$ for some $(M, \theta) \in \mathcal{C}$ and we can define $\psi(\alpha) = \theta(\alpha)$. This is clearly well-defined and define an embedding $\psi : N \hookrightarrow K$ such that $\psi\phi = i$. Thus (N, ψ) is an upper bound for $\mathcal{C}$. Zorn's Lemma implies S has a maximal element (M, θ).

Required to Prove: $M = L$. Given $\alpha \in L$, α is algebraic over M. If f denotes it's minimal polynomial over M, $\theta(f)$ splits over K since K algebraically closed, say $\theta(f) = (X - \beta_1) \dots (X - \beta_r)$. Since $\theta(f)(\beta_1) = 0$ there exists an embedding $M(\alpha) \cong M[X]/\langle f \rangle \hookrightarrow K$. This extends θ and sends α to β_1. Maximality of (M, θ) implies $\alpha \in M$, so $M = L$ as required. □

Corollary 3.2.2. *If $i_1 : k \hookrightarrow K_1$, $i_2 : k \hookrightarrow K_2$ are two algebraic closures of k then $\exists$ an isomorphism $\theta : K_1 \to K_2$ such that $i_2 = \theta i_1$.*

Proof. By (3.2.1), $\exists$ embedding $\theta : K_1 \hookrightarrow K_2$ such that $i_2 = \theta i_1$. Since K_2/k algebraic, so too is K_2/K_1. Since K_1 algebraically closed, deduce θ an isomorphism as claimed. □

For a general field k, the construction and proof of uniqueness of algebraic closure of $\bar{k}$ has involved Zorn's Lemma, and so preferable to avoid use of $\bar{k}$. Note however, that we can construct $\mathbb{C}$ by bare hands, without use of the Axiom of Choice, so this objection is less valid for, say, $k = \mathbb{R}, \mathbb{Q}$, algebraic number field etc. Here, it is often useful to choose a particular zero of a polynomial in $\mathbb{C}$, e.g. a real root[2].

[2] Here I think the lecturer means that instead of considering $\mathbb{Q}(\sqrt{2})$ to be the abstract extension of $\mathbb{Q}$ by some element α with minimum polynomial $X^2 - 2$, we consider α to be the concrete number $\sqrt{2} \in \mathbb{R}$. This is a subtle point, but consider how we might differentiate $\sqrt{2}$ from $-\sqrt{2}$ using purely algebraic methods. The answer is that we can't, to do so required analysis/geometry. So it is in some ways better not to consider α as $\sqrt{2}$ as it hides the (important in the following sections) fact that $-\sqrt{2}$ would do just as well. But then again, if we take the concrete view point, we don't get lost in the world of abstract set theory. Some middle ground is called for, or, better yet, ignore the whole point...

Chapter 4

Normal Extensions and Galois Extensions

Definition 4.0.3. An extension K/k is *normal* if every irreducible polynomial $f \in k[X]$ having a root in K splits completely over K.

Example 4.0.4. $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is not normal since $X^3 - 2$ doesn't split over any real field.

Theorem 4.0.5. *An extension K/k is normal and finite iff K is a splitting field for some polynomial over k.*

Proof. ($\Rightarrow$) Suppose K/k is normal and finite. Then $K = k(\alpha_1, \ldots, \alpha_r)$ with α_i algebraic, and having minimum polynomial $f_i \in k[X]$ say. Let $f = f_1 \ldots f_r$; claim K is a splitting field for f. Each f_i is irreducible with a zero in $K \Rightarrow$ each f_i splits completely over $K \Rightarrow f$ splits completely. Since K generated by k and the zeros of f, it is a splitting field for f over k.

($\Leftarrow$) Suppose K is the splitting field of a polynomial $g \in k[X]$. The extension is clearly finite. To prove normality, required to prove given an irreducible polynomial $f \in k[X]$ with a zero in K, f splits completely over K.

Suppose L/K is a splitting field extension for polynomial gf (considered as a polynomial over K), and that α_1, α_2 are zeros of f in L.

Claim: $[K(\alpha_1) : K] = [K(\alpha_2) : K]$. This yields required result, since can choose $\alpha_1 \in K$ by assumption, and so for any root α_2 of f in L, $[K(\alpha_2) : K] = 1$ so $K(\alpha_2) = K$, i.e. f splits completely.

Proof of claim: Observe the following:

1. Since f irreducible (1.1.8) implies $k(\alpha_1) \cong k(\alpha_2)$ over k. In particular, $[k(\alpha_1) : k] = [k(\alpha_2) : k]$.

2. For $i = 1, 2$, $K(\alpha_i)$ is a splitting field for g over $k(\alpha_i)$, and so by (1.4.1) $K(\alpha_1) \xrightarrow{\sim} K(\alpha_2)$ due to $k(\alpha_1) \cong k(\alpha_2)$. In particular, $[K(\alpha_1) : k(\alpha_1)] = [K(\alpha_2) : k(\alpha_2)]$.

3. Tower Law implies $[K(\alpha_1) : k] = [K(\alpha_2) : k]$. But for $i = 1, 2$, $[K(\alpha_i) : k] = [K(\alpha_i) : K][K : k]$ and so $[K(\alpha_1) : K] = [K(\alpha_2) : K]$ as claimed.

□

4.1 Normal Closures

Given a finite field extension K/k we write $K = k(\alpha_1, \ldots, \alpha_r)$ with f_i minimal polynomial of α_i over k and let L/K be a splitting field for $F = f_1 \ldots f_r$, considered as a polynomial in $K[X]$. Then (4.0.5) implies L/K normal implies L/k normal – it is called the *normal closure* for K/k.

Any extension M/K for which M/K normal, must split F and so for some subfield $L' \subset M$, L'/K is also a splitting field for F, and isomorphic over K to L/K by (1.4.1). Thus the normal closure of K/k may be characterised as the *minimal* extension for which L/k is normal, and it is unique up to isomorphism (and Zorn's Lemma is not required).

Definition 4.1.1. Given field extensions K/k and L/k, a $k-$*embedding* of K in L is a map from K to L such that $k \hookrightarrow K \hookrightarrow L$ is the same as $k \hookrightarrow L$.

In the case when $K/k = L/k$ and extension is finite, then $K \hookrightarrow L = K$ (where L in some sense is K) is also surjective (an injective linear map of a finite dimensional vector space to itself is an isomorphism) and hence a field isomorphism over k. These are called k-automorphisms. Much of Galois theory is concerned with the group $\operatorname{Aut}(K/k)$ of all k-automorphisms of extension K/k.

Theorem 4.1.2. *If K/k is a finite extension, let $\theta : K \hookrightarrow L$ be an extension of K containing a normal closure of K/k, and set $K' = \theta(K) \subset L$.*

1. *$|\{k\text{-embeddings } K \hookrightarrow L\}| \leq [K : k]$, with equality iff K/k separable.*
2. *K/k normal iff any k-embedding $\phi : K \hookrightarrow L$ has image K' iff any k-embedding $\phi : K \hookrightarrow L$ is of the form $\phi = \theta \circ \alpha$ for some k-automorphism α of K.*

Proof. 1. Follows directly from (2.0.9)(1) and (2).

2. Observe first

   (a) K/k normal iff K'/k normal

   (b) Any k-embedding $\phi : K \hookrightarrow L$ gives rise to a k-embedding $\psi : K' \hookrightarrow L$ such that $\psi = \phi\theta^{-1}$ and conversely.

   (c) Any k-embedding $\phi : K \hookrightarrow L$ with image K' gives rise to an automorphism α of K/k such that $\phi = \theta \circ \alpha$. Conversely, any ϕ of this form is a k-embedding with image K'.

   Hence we are required to prove K'/k normal iff any k-embedding $\psi : K' \hookrightarrow L$ has image K'.

   Proof: ($\Rightarrow$) Suppose $\alpha \in K'$ with minimal polynomial $f \in k[X]$, K'/k normal implies f splits completely over K'. Moreover, $\psi(\alpha)$ is another root of f and so $\psi(\alpha) \in K'$. Hence $\psi : K' \hookrightarrow K'$ implies $\psi(K') = K'$. (K' finite dimensional vector space over k).

   ($\Leftarrow$) Conversely, suppose f an irreducible polynomial in $k[X]$ has a zero α in K'. By assumption, L contains a normal closure L' of K/k, and so f splits completely over L'. Also, since K'/k is finite, $K' \subset L'$. Let $\beta \in L'$ by any other root of f. Then $\exists$ an isomorphism over k, $k(\alpha) \cong k[X]/\langle f \rangle \cong k(\beta)$. Since L' is a splitting field for some polynomial F over k, it is also a splitting field for F over $k(\alpha)$ or $k(\beta)$. So (1.4.1) implies that the isomorphism $k(\alpha) \cong k(\beta)$ extends to an isomorphism $k(\alpha) \subset L' \xrightarrow{\sim} L' \supset f(\beta)$ with $k(\alpha) \xrightarrow{\sim} k(\beta)$, which in turn restricts to a k-embedding $K' \hookrightarrow L$ sending α to β. Therefore, our assumption implies that $\beta \in K'$. Since this is true for all roots β of f, f splits completely over K', i.e. K'/k normal.

□

Corollary 4.1.3. *If K/k is a finite extension, then $|\operatorname{Aut}(K/k)| \leq [K : k]$ with equality iff K/k is normal and separable.*

Proof. From (4.1.2), $|\operatorname{Aut}(K/k)| = |\{k\text{-embeddings } K \hookrightarrow L \text{ of form } \theta \circ \alpha, \alpha \in \operatorname{Aut}(K/k)\}| \leq$ $|\{k\text{-embeddings } K \hookrightarrow L\}| \leq [K : k]$ with equality iff K/k normal and separable. □

From now on, we'll deal with field extensions $k \subset K$ (subfield)– we don't lose generality by doing this now, as for any extension $k \hookrightarrow K$ we can always identify k with its image.

Definition 4.1.4. If K a field and G is a (finite) group of automorphisms of K, we denote the *fixed subfield* $K^G \subset K$ where

$$K^G := \{x \in K : g(x) = x \ \forall g \in G\}$$

Easy to check this is a subfield.

We say that a finite extension $k \subset K$ is *Galois* if $k = K^G$ for some finite group G of automorphisms. Clearly $G \subset \operatorname{Aut}(K/k)$, and below we show that in fact $G = \operatorname{Aut}(K/k)$.

Before we've take a "bottom up" approach, taking extensions of base fields: here the approach is "top down". We'll see that these two ways of developing Galois theory are equivalent.

Proposition 4.1.5. *Let G be a finite group of automorphisms acting on a field K, with $k = K^G \subset K$.*

1. *Every $\alpha \in K$ has $[k(\alpha) : k] \leq |G|$.*
2. *K/k is separable.*

3. *K/k finite with $[K:k] \leq |G|$.*

Proof. (1) and (2). Suppose $\alpha \in K$, **claim** its minimum polynomial f is separable of degree $\leq |G|$. (Thus α separable and $[k(\alpha):k] \leq |G|$). Consider the set $\{s(\alpha) : s \in G\}$, and suppose its *distinct* elements are $\alpha = \alpha_1, \ldots, \alpha_r$. Set $g = \prod_i (X - \alpha_i)$. Then g is invariant under G, since its linear factors are just permuted by elements of G and so $g \in k[X]$. Since $g(\alpha) = 0$, have $f|g$, and hence f clearly separable and $\deg f \leq \deg g \leq |G|$.

(3). By (1) we can find $\alpha \in K$ such that $[k(\alpha):k]$ is maximal. If $K = k(\alpha)$ then done, as by (1), $[k(\alpha):k] \leq |G|$. Suppose then $\beta \in K$, required to prove $\beta \in k(\alpha)$. By (1), β satisfies a polynomial over k of degree $\leq |G| \Rightarrow [k(\alpha,\beta):k(\alpha)] < \infty \Rightarrow [k(\alpha,\beta):k] < \infty$. However, (2) implies $k(\alpha,\beta)/k$ is separable. The Primitive Element Theorem (2.0.12) implies $\exists \gamma$ such that $k(\alpha,\beta) = k(\gamma)$. Since $[k(\gamma):k] = [k(\gamma):k(\alpha)][k(\alpha):k]$, but as $[k(\alpha):k]$ maximal, $[k(\gamma):k(\alpha)] = 1$ implies $\beta \in k(\alpha)$ as required. □

Theorem 4.1.6. *Let $k \subset K$ be a finite extension of fields. Then the following are equivalent*

1. *K/k Galois*

2. *k is the fixed field of* $\mathrm{Aut}(K/k)$

3. $|\mathrm{Aut}(K/k)| = [K:k]$

4. *K/k is normal and separable*

Moreover, if $k = K^G$ for some finite group G of automorphisms, we have that $G = \mathrm{Aut}(K/k)$.

Proof. (3) $\Leftrightarrow$ (4) follows from (4.1.3).

(2) $\Rightarrow$ (1) is clear, since (4.1.3) implies $|\mathrm{Aut}(K/k)|$ finite.

Suppose now (1) holds, $k = K^G$. Then (4.1.5)(3) implies $[K:k] \leq |G|$, but $G \subset \mathrm{Aut}(K/k)$ and so $|G| \leq |\mathrm{Aut}(K/k)| \leq [K:k]$ by (4.1.3). Thus $G = \mathrm{Aut}(K/k)$ as claimed in the last paragraph, k is the fixed field of $\mathrm{Aut}(K/k)$ and $|\mathrm{Aut}(K/k)| = [K:k]$. In particular, (1) $\Rightarrow$ (2) and (3). Hence required to prove (3) $\Rightarrow$ (1) and (2) then done.

Set $G = \mathrm{Aut}(K/k)$ finite group, $|G| = [K:k]$. Set $F = K^G$, the fixed field, $k \subseteq F$. Then K/F Galois, so previous argument implies $|G| = [K:F] = [K:k]$. Hence $F = k$, i.e. (2)($\Rightarrow$ (1)) are true. □

If $k \subset K$ is Galois, we often write $\mathrm{Gal}(K/k)$ for the automorphism group, $\mathrm{Aut}(K/k)$, the Galois group of the extension.

4.2 Fundamental Theorem of Galois Theory

Let K/k be a finite extension of fields. The group $G = \mathrm{Aut}(K/k)$ has $|G| \leq [K:k]$ by (4.1.3). Let $F = K^G \supset k$, then (4.1.6) implies $|G| = [K:F]$.

1. If H is a subgroup of G, then the fixed field $L = K^H$ is an intermediate field $F \subset L \subset K$ and (4.1.6) implies $\mathrm{Aut}(K/L) = H$.

2. For any intermediate field $F \subset L \subset K$, let H be the subgroup $\mathrm{Aut}(K/L)$ of $G = \mathrm{Aut}(K/k)$.

Claim 4.2.1. *K/L is a Galois extension and $L = K^H$.*

Proof. Since K/F Galois, it is normal and separable by (4.1.6). Since K/F normal, so too is K/L (K is the splitting field for some polynomial $f \in F[X]$ by (4.0.5) implies K is a splitting field over L for f implies via (4.0.5) that K/L normal). Since K/F separable, so too is K/L, hence K/L is Galois by (4.1.6) and $L = K^H$ by (4.1.6)(2). □

So we conclude that

$$\begin{aligned} & H \leq G \longmapsto F \subset K^H \subset K \\ \text{and} \quad & F \subset L \subset K \longmapsto \mathrm{Aut}(K/L) \leq G \end{aligned}$$

are mutually inverse.

Theorem 4.2.2. *Fundamental Theorem of Galois Theory*
With notation as above:

1. *$\exists$ order reversing bijection between subgroups $H \leq G$ and intermediate fields $F \subset L \subset K$, where a subgroup H corresponds to its fixed field $L = K^H$; and an intermediate field $F \subset L \subset K$ corresponds to* $\mathrm{Gal}(K/L) \subset G$.
2. *A subgroup H of G is normal*[1] *iff K^H/F is Galois (iff K^H/F is normal).*
3. *If $H \lhd G$, the map $\sigma \in G \mapsto \sigma|_{K^H}$ determines a group homomorphism of G onto* $\mathrm{Gal}(K^H/F)$ *with kernel H, and hence* $\mathrm{Gal}(K^H/F) \cong G/H$.

Proof. 1. Already done.

2. If $L = K^H$, observe that the fixed field of a conjugate subgroup $\sigma H \sigma^{-1}$ $(\sigma \in G)$ is just σL. From the bijection proved in (1), deduce that $H \lhd G$ (i.e. $\sigma H \sigma^{-1} = H \ \forall \sigma \in G$) iff $\sigma L = L \ \forall \sigma \in G$. Now observe K is normal over F (in particular a splitting field for some polynomial $f \in F[X]$) and so K contains a normal closure N of L/F. Any $\sigma \in G = \mathrm{Gal}(K/F)$ determines an F-embedding $L \hookrightarrow N$, and conversely any F-embedding of $L \hookrightarrow N$ extends by (1.4.1) to an F-automorphism σ of the splitting field K of f. Thus (4.1.2)(2) says L/F is normal iff $\sigma L = L \ \forall \sigma \in G$. Since L/F is always separable (K/F is Galois and so use (2.0.7)) and so L/F normal iff L/F Galois.
3. In the case $H \lhd G$, we have $\sigma(L) = L \ \forall \sigma \in G$ and so $\sigma|_L$ is an automorphism of $L = K^H$ implies $\exists$ homomorphism of groups, $\theta : G \to \mathrm{Gal}(L/F)$ with $\ker \theta = \mathrm{Gal}(K/L) = H$ by (4.1.6) implies $\theta(G) \cong G/H$. Thus $|\theta(G)| = |G : H| = |G|/|H| = [K : F]/[K : L] = [L : F]$. But $|\mathrm{Gal}(L/F)| = [L : F]$ by (4.1.6) since L/F Galois, implies θ is surjective and induces an isomorphism of $G/H \xrightarrow{\sim} \mathrm{Gal}(L/F)$. □

4.3 Galois Groups of Polynomials

Suppose now $f \in k[X]$ a separable polynomial and K/k a splitting field. The Galois group of f is $\mathrm{Gal}(f) := \mathrm{Gal}(K/k)$. Suppose now f has distinct roots in K, say $\alpha_1, \ldots, \alpha_d \Rightarrow K = k(\alpha_1, \ldots, \alpha_d)$. Since a k-automorphism of K is determined by it's action on the roots α_i, we have an injective homomorphism $\theta : G \hookrightarrow S_d$. Properties of f will be reflected in the properties of G.

Lemma 4.3.1. *With assumptions as above, $f \in k[X]$ irreducible iff G acts transitively*[2] *on the roots of f, i.e. $\theta(G)$ is a transitive subgroup of S_d.*

Proof. ($\Leftarrow$) If $f \in k[X]$ reducible, say $f = gh$ with $g, h \in k[X]$, $\deg g > 0$, $\deg h > 0$, let α_1 be a root of g say, then for $\sigma \in G$, $\sigma(\alpha_1)$ is also a root of g and so G only permutes roots within the irreducible factors and so its action is not transitive.

($\Rightarrow$) If f irreducible, then for any i, j, $\exists k$-isomorphism, $k(\alpha_i) \xrightarrow{\sim} k(\alpha_j)$. This isomorphism extends by (1.4.1) to give a k-automorphism of K (which is the splitting field of f), say σ, with property $\sigma(\alpha_i) = \alpha_j$, implies G is transitive on roots. □

So for low degree, the Galois groups of polynomials are very restrictive.
Degree 2: Either f reducible ($G = 0$) or irreducible ($G = C_2$).
Degree 3: Either f reducible ($G = 0, C_2$) or irreducible ($G = S_3, C_3$).

Definition 4.3.2. The *discriminant* D of a polynomial $f \in k[X]$ with distinct roots in a splitting field (e.g. f irreducible and separable) is defined as follows. Let $\alpha_1, \ldots, \alpha_d$ be roots of f in a splitting field K and set $\Delta = \prod_{i<j}(\alpha_i - \alpha_j)$. The *discriminant*

$$D = \Delta^2 = (-1)^{d(d-1)/2} \prod_{i \neq j} (\alpha_i - \alpha_j)$$

is fixed by all the elements of $G = \mathrm{Gal}(K/k)$ and hence is an element of k.

Question 4.3.3. *For $f \in k[X]$ irreducible and separable of degree d, when is the image of the Galois group in A_d?*

Answer: Assuming f irreducible and separable, we have $\Delta \neq 0$ and for $\mathrm{char}(k) \neq 2$, $\theta(G) \subset A_d$ iff Δ fixed under G (since for any odd permutation σ, $\sigma(\Delta) = -\Delta$) iff $\Delta \in k$ iff D is a square in k.

[1] Recall that a subgroup H of G is said to be *normal*, denoted $H \lhd G$, iff $xHx^{-1} = H$ for all $x \in G$.
[2] If a group G acts on a set X, then it acts *transitively* iff for all $x, y \in X$, $\exists g \in G$ such that $g(x) = y$.

Examples 4.3.4.

1. $d = 2$, $f = X^2 + bX + c$ ($\mathrm{char}(k) \neq 2$) $\Rightarrow \alpha_1 + \alpha_2 = -b, \alpha_1\alpha_2 = c \Rightarrow D = (\alpha_1 - \alpha_2)^2 = b^2 - 4c$ so the quadratic splits iff $b^2 - 4c$ is a square (which we knew before).

2. $d = 3$, $f = X^3 + bX^2 + cX + d$, ($\mathrm{char}(k) \neq 2, 3$) ($f$ irreducible and separable). The Galois group $G = A_3 (= C_3)$ iff $D(f)$ a square, or S_3 otherwise.

   To calculate $D(f)$, set $g = f(X - \frac{b}{3})$, of form $X^3 + pX + q$. Since α a root of f iff $\alpha + \frac{b}{3}$ a root of g, deduce $\Delta(f) = \Delta(g)$ and so $D(f) = D(g)$.

Lemma 4.3.5. *If f irreducible, separable polynomial in $k[X]$, L/k a splitting field, $\alpha \in L$ a root of f and $K = k(\alpha) \subset L$, then $D(f) = (-1)^{d(d-1)/2}\,\mathrm{N}_{K/k}(f'(\alpha))$.*

Proof. Observe, (c.f. Example sheet 1, Q14),

$$\begin{aligned}\prod_{i\neq j}(\alpha_i - \alpha_j) &= \prod_i \prod_{j\neq i}(\alpha_i - \alpha_j) = \prod_i f'(\alpha_i) \\ &= \prod_i \sigma_i(f'(\alpha)) \qquad (\sigma_1 \dots \sigma_d : k(\alpha) \hookrightarrow L \text{ distinct}) \\ &= \mathrm{N}_{K/k}(f'(\alpha))\end{aligned}$$

□

Example 4.3.6. Thus for cubic, $g = X^3 + pX + q$, $g = g'(\alpha)$, α root, $g'(\alpha) = y = 3\alpha^2 + p = -2p - 3q\alpha^{-1}$. Minimal polynomial of y is

$$(q(y + 2p)^3 - 3pq(y + 2p)^2 - 27q^3)/q$$

whose constant term is $-4p^3 - 27q^2 = -\mathrm{N}(y) = D(g)$.

When $k = \mathbb{Q}$ we can consider the splitting field of polynomial $f \in \mathbb{Q}[X]$ as a subfield of $\mathbb{C}$– this may be useful.

For example, if $f \in \mathbb{Q}[X]$ irreducible, of degree d, with precisely 2 imaginary roots, then the Galois group contains a transposition (complex conjugation is an element of the Galois group and switches two imaginary roots). Elementary group theory shows that if $G \subset S_p$ (p prime) is transitive and contains a transposition then it contains all transpositions and hence $G = S_p$. Many cubics $f \in \mathbb{Q}[X]$ have Galois group S_3 because they have two complex roots.

It is a help to know what the transitive subgroups of S_n are, if we're trying to calculate the Galois group of an irreducible polynomial. The following classification for $n = 4, 5$ is left an extended exercise in group theory[3].

Proposition 4.3.7. *The transitive subgroups of S_4 are S_4, A_4, D_8, C_4 and $V = C_2 \times C_2$, the group $\{1, (12)(34), (13)(24), (14)(23)\}$.*

The transitive subgroups of S_5 are $S_5, A_5, G_{20}, D_{10}, C_5$ where G_{20} is generated by any 5 cycle and a 4 cycle.

Remark 4.3.8. All these possibilities occur.

[3] Ho ho.

Chapter 5

Galois Groups Of Finite Fields

Proposition 5.0.9. *If F is a finite field and* $\operatorname{char} F = p$ *then* $|F| = p^r$ *for some* r.

Proof. The map $\theta : \mathbb{Z} \to F; n \mapsto n.1$ is a ring homomorphism with kernel $\{0, \pm p, \pm 2p, \ldots\} = \langle p \rangle$, as $\operatorname{char} K = p$. Thus F contains $\mathbb{F}_p$ as a subfield, and so F is a $\mathbb{F}_p$ vector space, so is isomorphic to $\mathbb{F}_p^r$. I.e. $|F| = p^r$. □

Definition 5.0.10. Given such a finite field F, $\exists$ $\mathbb{F}_p$-automorphism, $\phi : F \to F$ given by $\phi(x) = x^p$, called the *Fröbenius* automorphism. (Since $(x+y)^p = x^p + y^p$ and $x^p = 0 \Rightarrow x = 0$, ϕ is injective field homomorphism $F \hookrightarrow F$, finite fields, so bijective, and hence an automorphism. Now observe $x^p = x$ for all $x \in \mathbb{F}_p$, the prime subfield).

Moreover, since $a^{q-1} = 1$ ($q = |F|$) for all $a \in F^*$, we have $a^q = a$ for all $a \in F$. Hence every element of F is a root of the polynomial $X^q - X$. But $X^q - X$ has at most q roots, so these are all the roots. So F is the splitting field of $X^q - X$ over $\mathbb{F}_p$, and as such is unique up to isomorphism.

If $q = p^r$, then let F be the splitting field of $X^q - X$ over $\mathbb{F}_p$. We have Fröbenius automorphism $\phi : F \to F$ and we can take the fixed field F' of ϕ^r. Observe that $\phi^r(x) = x$ iff x is a root of $X^q - X$, and so $F' = F$ is the splitting field of $X^q - X$; and it consists entirely of roots of $X^q - X$. These roots are distinct (since derivative of polynomial is -1 which has no roots) and so $|F| = q$.

We denote the unique field of order $p^r = q$ by $\mathbb{F}_q$.

If k a finite field containing $\mathbb{F}_{p^s}$, then $|k| = p^{st}$ for $t = [k : \mathbb{F}_{p^s}]$, so there is a bijection $\{\text{subfield of } \mathbb{F}_{p^r}\} \leftrightarrow \{\mathbb{F}_{p^s} : s|r\}$. These subfields are just the fixed fields of ϕ^s $(s|r)$. Observe that $\phi^r = 1$ on $\mathbb{F}_{p^r}$; $\phi^{r-1} \neq 1$ (since $X^{r-1} - X$ doesn't have enough roots), therefore ϕ generates a *cyclic* group of automorphisms of $\mathbb{F}_{p^r}$ of order r, and the fixed field of $\langle \phi \rangle$ is just $\mathbb{F}_p$ (roots of $X^p - X$) and so $\mathbb{F}_{p^r}/\mathbb{F}_p$ a Galois extension with Galois group $G = \langle \phi \rangle$, cyclic of order r. Note we've now checked the bijection between intermediate fields and subgroups of G.

Since $\mathbb{F}_{p^r}/\mathbb{F}_p$ Galois, we know that $\mathbb{F}_{p^r}/\mathbb{F}_{p^s}$ is also Galois $(s|r)$ with Galois group, cyclic, generated by ϕ^s. Since the subgroups of $G = \langle \phi \rangle$ are just those of the form $\langle \phi^s \rangle$ with $s|r$ and G cyclic, we have all these subgroups are normal and Fundamental Theorem of Galois Theory follows immediately for such extensions of finite fields.

Recap.

1. Any finite extension K/k of finite fields is *Galois.*

2. The Galois group is cyclic of order $[K : k]$, generated by appropriate power of Fröbenius.

3. If $f \in k[X]$ irreducible of degree d with $|k| < \infty$, and an extension K/k contains a root of f, it contains *all* the roots of f (since K/k normal). Therefore splitting field of f is of form $k(\alpha)$, where α has minimal polynomial f over k. Moreover, $\operatorname{Gal}(f) = \operatorname{Gal}(k(\alpha)/k)$ *cyclic of order* d, and a generator of $\operatorname{Gal}(f)$ acts cyclically on the roots of f.

   If $k = \mathbb{F}_{p^s}$, then the splitting field, $\mathbb{F}_{p^{sd}}$, is unique, and in particular doesn't depend on which irreducible polynomial of degree d we choose, i.e. if we've split one irreducible polynomial of degree d, we've split them all.

Consider the general situation of K a field, $f = X^n + \ldots + c_0 \in K[X]$ with distinct roots in a splitting field L/K, $\alpha_1, \ldots, \alpha_n \in L$ and $G = \operatorname{Gal}(f) = \operatorname{Gal}(L/K) \hookrightarrow S_n$. Let $Y_1, \ldots, Y_n$ be independent indeterminates. For $\sigma \in S_n$, $H_\sigma = (X - (\alpha_{\sigma(1)}Y_1 + \ldots + \alpha_{\sigma(n)}Y_n)) \in L[Y_1, \ldots, Y_n][X]$

We can define an action of σ on $H = X - (\alpha_1 Y_1 + \ldots + \alpha_n Y_n)$ by $\sigma H = H_{\sigma^{-1}}$, i.e. σ acting on $Y_1, \ldots, Y_n$. Set

$$\begin{aligned} F = \prod_{\sigma \in S_n} H_\sigma = \prod_{\sigma \in S_n} \big(X - (\alpha_1 Y_{\sigma(1)} + \ldots + \alpha_n Y_{\sigma(n)})\big) = \prod_{\sigma \in S_n} \sigma H \\ = \sum_{j=0}^{n!} \left(\sum_{i_1 + \ldots + i_n = n! - j} a_{i_1, \ldots, i_n} Y_1^{i_1} \ldots Y_n^{i_n} \right) X^j \end{aligned}$$

Since S_n preserves F, it preserves the coefficients $a_{i_1,\ldots,i_n}$, then coefficients are in fact certain symmetric polynomials in the α_i's (which could be given explicitly independent of f), and hence are polynomials in the coefficients $c_0, \ldots, c_{n-1}$ (again can be given explicitly independent of specific polynomial of degree n). (c.f. Symmetric Function Theorem). Hence $F \in K[Y_1, \ldots, Y_n][X]$.

Now factor $F = F_1 \ldots F_N$ into irreducibles in $K[Y_1, \ldots, Y_n][X]$ with F_i irreducible in
$K(Y_1, \ldots, Y_n)[X]$ by Gauss.

Remark 5.0.11. In the case $K = \mathbb{Q}$, $c_i \in \mathbb{Z}$, all the polynomials in the $c_0, \ldots, c_{n-1}$ have coefficients in $\mathbb{Z}$ and then $F \in \mathbb{Z}[Y_1, \ldots, Y_n][X]$ and we can take factorisation $F = F_1 \ldots F_N$ with $F_i \in \mathbb{Z}[Y_1, \ldots, Y_n][X]$ (by Gauss).

Now choose one of the factors $H = H_\sigma$ of F_1. By reordering F_i's (or roots $\alpha_1, \ldots, \alpha_n$) we may assume without loss of generality $H = (X - (\alpha_1 Y_1 + \ldots + \alpha_n Y_n))$ divides F_1 in $L[Y_1, \ldots, Y_n][X]$. Recall that the images σH are all distinct. Now consider $\prod_{g \in G} gH$ with g^{-1} acting on coefficients of H. This has degree $|G|$, and is in $K[Y_1, \ldots, Y_n][X]$, since invariant under action of G. Since H divides F_1 in $L[Y_1, \ldots, Y_n][X]$, gH divides F_1 in polynomial F_1 in $K[Y_1, \ldots, Y_n][X]$ and hence is $F_1 \implies \deg F_1 = |G|$, and there are $N = n!/|G|$ irreducible factors F_i, permuted transitively by the action of S_n. Therefore orbit-stabiliser theorem implies $\frac{n!}{|\operatorname{Stab}(F_1)|} = \frac{n!}{|G|}$ so $|G| = |\operatorname{Stab}(F_1)|$. Since G fixes F_1, $G \subset \operatorname{Stab}(F_1)$ and hence $G = \operatorname{Stab}(F_1)$.

I.e. $\operatorname{Gal}(f) \cong$ subgroup of S_n (acting on $Y_1, \ldots, Y_n$) which fixes F_1.

Theorem 5.0.12. *Suppose $f \in \mathbb{Z}[X]$ monic polynomial of degree n with distinct roots in a splitting field. Suppose p a prime such that the reduction $\bar{f}$ of f mod p also has distinct roots in a splitting field. If $\bar{f} = g_1 \ldots g_r$ is the factorisation of $\bar{f}$ in $\mathbb{F}_p[X]$, say $\deg g_i = n_i$, then* $\operatorname{Gal}(f) \subset S_n$ *has an element of cyclic type $(n_1, \ldots, n_r)$.*

Proof. This will follow if we can show $\operatorname{Gal}(\bar{f}) \subset \operatorname{Gal}(f) \subset S_n$ since the action of Fröbenius ϕ on roots of $\bar{f}$ clearly has the cyclic type claimed.

We now run the above programme twice: First run over $K = \mathbb{Q}$, identifying $\operatorname{Gal}(f)$ as the subgroup of S_n fixing $F_1 \in \mathbb{Z}[Y_1, \ldots, Y_n][X]$.

Secondly, with $K = \mathbb{F}_p$ and $\bar{f}$, and the resulting polynomial $\tilde{f}$ we obtain, $\tilde{f} \in \mathbb{F}_p[Y_1, \ldots, Y_n][X]$, has coefficients given by our (potentially explicit) polynomial in the coefficients of $\bar{c}_i$ of $\bar{f}$. Thus $\bar{F}$ is just the reduction mod p of F, i.e. $\bar{F} = \tilde{F}$. But $\bar{F} = \bar{F}_1 \ldots \bar{F}_N$ in $\mathbb{F}_p[Y_1, \ldots, Y_n][X]$, and we can then factor $\bar{F}_1 = h_1 \ldots h_m$, h_i irreducible. With appropriate choice of the order of the roots $\beta_1, \ldots, \beta_n$ of $\bar{f}$ in a splitting field, we may identify $\operatorname{Gal}(\bar{f})$ as the subgroup of S_n (acting on $Y_1, \ldots, Y_n$) fixing h_1 say. Since, however, the linear factors of $\bar{F}$ are *distinct*, the subgroup of S_n fixing $\bar{F}_1$ is the same as the subgroup fixing F_1, and $\operatorname{Stab}(h_1)$ is a subgroup of $\operatorname{Stab}(\bar{F}_1) = \operatorname{Stab}(F_1)$. Thus $\operatorname{Gal}(\bar{f}) \subset \operatorname{Gal}(f) \subset S_n$ as claimed. □

Chapter 6

Cyclotomic Extensions

Definition 6.0.13. Suppose $\operatorname{char} k = 0$ or $\operatorname{char} k = p$, $p|m$. The mth *cyclotomic extension* of k is just the splitting field K over k of $X^m - 1$. Since mX^{m-1} and $X^m - 1$ have no common factor, the roots of $X^m - 1$ are distinct, the mth *roots of unity* (K/k Galois). They form a finite subgroup μ_m of K^*, and hence by (2.0.11), a cyclic subgroup $\langle \xi \rangle$. Thus $K = k(\xi)$ is *simple.*

Definition 6.0.14. An element $\xi' \in \mu_m$ is called *primitive* if $\mu_m = \langle \xi' \rangle$, i.e. $\xi' = \xi^r$ from some r coprime to m.

Choosing a primitive mth root ξ of unity determines an isomorphism of cyclic groups $\mu_m \xrightarrow{\sim} \mathbb{Z}/m\mathbb{Z}$, $\xi^i \mapsto i$. So the primitive roots correspond to the elements of $U(m) := (\mathbb{Z}/m\mathbb{Z})^*$, the units in $\mathbb{Z}/m\mathbb{Z}$. Since $X^m - 1$ is separable, K/k is Galois with Galois group G say.

An element $\sigma \in G$ sends a primitive mth root of unity to another primitive mth root of unity, i.e. sends a primitive root ξ to ξ^i for some $i \in U(m)$ (and knowing i determines σ). Therefore, having chosen a primitive mth root ξ, we can define an injective map $\theta : G \hookrightarrow U(m)$; $\sigma \mapsto i$ where $\sigma(\xi) = \xi^i$. If, however, $\theta(\sigma) = i$ and $\theta(\tau) = j$ then $\sigma\tau(\xi) = \sigma(\xi^j) = \xi^{ij}$, i.e. $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$ in $U(m)$. So, via the map θ, the Galois group G may be considered as a (multiplicative) subgroup of $U(m)$.

θ is an isomorphism (i.e. surjective) iff G is *transitive* on the primitive mth roots of unity, i.e. given $i \in U(m), \exists \sigma \in G$ such that $\sigma(\xi) = \xi^i$.

Definition 6.0.15. The mth *cyclotomic polynomial* Φ_m is given by

$$\Phi_m = \prod_{i \in U(m)} (X - \xi^i)$$

Observe that $X^m - 1 = \prod_{i \in \mathbb{Z}/m\mathbb{Z}} (X - \xi^i) = \prod_{d|m} \Phi_d$ by induction. For example where $k = \mathbb{Q}$, $\Phi_1 = X-1, \Phi_2 = X+1, \Phi_4 = X^2+1, X^8-1 = (X^4-1)(X^4+1) = (X^2-1)(X^2+1)(X^4+1) = \Phi_1\Phi_2\Phi_4\Phi_8$.

Recall. If $\operatorname{char} k = 0$, k has prime subfield $\mathbb{Q}$. If $\operatorname{char} k = p > 0$, k has prime subfield $\mathbb{F}_p$.

Lemma 6.0.16. *Φ_m defined over the prime subfield of k. When $\operatorname{char} k = 0$, Φ_m defined over $\mathbb{Z} \subset \mathbb{Q}$, i.e. $\Phi_m \in \mathbb{Z}[X]$.*

Proof. Induction on m. $X^{m-1} = \Phi_m \prod_{d|m, d<m} \Phi_d = \Phi_m g$ where g monic and by induction hypothesis is defined over prime subfield or $\mathbb{Z}$ if $\operatorname{char} k = 0$. Therefore Gauss Lemma (or direct argument via monic remainder theorem) implies Φ_m also defined over prime subfield (and over $\mathbb{Z}$ if $\operatorname{char} k = 0$). □

Proposition 6.0.17. *$\theta : G \to U(m)$ is an isomorphism iff $\Phi_m \in k[X]$ is irreducible.*

Proof. This is clear since Φ_m irreducible iff (via (4.3.1)) G acts transitively on roots. □

Remark 6.0.18. Thus if $U(m)$ not cyclic, the homomorphism θ is *never* an isomorphism when k is *finite* and hence Φ_m is always reducible in $k = \mathbb{F}_q$. In general, when $k = \mathbb{F}_q$ we have

Proposition 6.0.19. *If K is the mth cyclotomic extension of $k = \mathbb{F}_q$, $q = p^r, p \not| \, m$, the Galois group G is isomorphic to the cyclic subgroup of $U(m)$ generated by q.*

Proof. G is cyclic generated by automorphism $x \mapsto x^q$, so $G \cong \theta(G) = \langle q \rangle \leq U(m)$. □

Now consider the case $k = \mathbb{Q}$ (i.e. $\Phi_m \in \mathbb{Z}[X]$ by (6.0.16)). If we can show Φ_m irreducible over $\mathbb{Z}$ then Gauss implies Φ_m irreducible over $\mathbb{Q}$ and hence (6.0.17) implies $G \cong U(m)$.

Proposition 6.0.20. *$\Phi_m \in \mathbb{Z}$ is irreducible for all $m > 0$.*

Proof. Suppose not; we can then write $\Phi_m = fg$ with $f, g \in \mathbb{Z}[X]$, f an irreducible polynomial, $1 \leq \deg f < \phi(m) := \deg \Phi_m$. Let $K/\mathbb{Q}$ be the mth cyclotomic extension of $\mathbb{Q}$, and let ϵ be a root of f in K.
Claim: If p a prime, $p \not| \, m$, the ϵ^p also a root of f.
Proof: Suppose not: ϵ^p is a primitive mth root of 1 and hence $g(\epsilon^p) = 0$. Define $h \in \mathbb{Z}[X]$ by $h(X) = g(X^p)$; then $h(\epsilon) = 0$. Since f is the minimal polynomial of ϵ over $\mathbb{Q}$, $f|h$ in $\mathbb{Q}[X]$, and Gauss Lemma implies we can write $h = fl$ with $l \in \mathbb{Z}[X]$, (note: f monic). Now reduce mod p to get $\bar{h} = \overline{fl}$ in $\mathbb{F}_p[X]$. But $\bar{h}(X) = \bar{g}(X^p) = \bar{g}(X)^p$. If $\bar{q}$ is an irreducible factor of $\bar{f}$ in $\mathbb{F}_p[X]$, then $\bar{q}|\bar{g}^p \Rightarrow \bar{q}|\bar{g} \Rightarrow \bar{q}^2|\bar{f}\bar{g} = \Phi_m$, i.e. $\exists$ repeated roots of $X^m - 1$ in splitting field over $\mathbb{F}_p$. Contradiction since $(p, m) = 1$.

In general, now consider a root ξ for f and a root θ for g. Then $\theta = \xi^r$ for some r coprime to m. Write $r = p_1 \ldots p_k$ as product of primes p_i, $p_i \not| \, m$ for all i. Repeated use of claim implies θ is a root of f implies Φ_m has a repeated root, contradiction. Hence Φ_m is irreducible. □

Remark 6.0.21. When $m = p$ prime, $\exists$ simple proof of (6.0.20). Φ_p irreducible iff $g(X) = \Phi_p(X+1)$ irreducible. But $g(X) = \frac{(X+1)^p - 1}{(X+1)-1} = X^{p-1} + pX^{p-2} + \ldots + \binom{p}{p-2} X + p$ and since $p \mid \binom{p}{r}$ for all r, the result follows by Eisenstein.

Chapter 7

Kummer Theory and Solving by Radicals

When is a Galois extension L/K a splitting field for a polynomial of the form $X^n - \theta$.

Theorem 7.0.22. *Suppose $X^n - \theta \in K[X]$ and $\operatorname{char} K \not| \ n$. Then the splitting field L contains a primitive nth root of unity, ω, and the Galois group of $L/K(\omega)$ is cyclic of order dividing n. Moreover $X^n - \theta$ is irreducible over $K(\omega)$ iff $[L : K(\omega)] = n$.*

Proof. Since $X^n - \theta$ and nX^{n-1} coprime, $X^n - \theta$ has distinct roots $\alpha_1, \ldots, \alpha_n$ in its splitting field L. Moreover, L/K Galois.

Since $(\alpha_i \alpha_i^{-1})^n = \theta\theta^{-1} = 1$, the elements $1 = \alpha_1\alpha_1^{-1}, \alpha_2\alpha_1^{-1}, \ldots, \alpha_n\alpha_1^{-1}$ are n distinct nth roots of unity in L, i.e. roots of $X^n - 1$.

So $X^n - \theta = (X - \beta)(X - \omega\beta) \ldots (X - \omega^{n-1}\beta)$ in $L[X]$. Therefore $L = K(\omega, \beta)$ and if $\sigma \in \operatorname{Gal}(L/K(\omega))$, it is determined by its action on β. $\sigma(\beta)$ is another root of $X^n - \theta$, say $\sigma(\beta) = \omega^{j(\sigma)}\beta$ for some $0 \leq j(\sigma) < n$.

If $\sigma, \tau \in \operatorname{Gal}(L/K(\omega))$, $\tau\sigma(\beta) = \tau(\omega^{j(\sigma)}\beta) = \omega^{j(\sigma)}\tau(\beta) = \omega^{j(\sigma)+j(\tau)}\beta$. Therefore the map $\sigma \mapsto j(\sigma)$ induces a homomorphism $G(L/K(\omega)) \to \mathbb{Z}/n\mathbb{Z}$. As $j(\sigma) = 0$ iff $\sigma(\beta) = \beta$ iff σ =identity, the homomorphism is injective and so $\operatorname{Gal}(L/K(\omega))$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$, hence cyclic of order dividing n.

Observe $[L : K(\omega)] \leq n$ with equality iff $X^n - \theta$ irreducible over $K(\omega)$, since $L = K(\omega)(\beta)$. □

Example 7.0.23. $X^6 + 3 \in \mathbb{Q}[X]$ is irreducible (Eisenstein) but not over $\mathbb{Q}(\omega)$ ($\omega = \frac{1}{2}(1 + \sqrt{-3})$ since splitting field $L = \mathbb{Q}((-3)^{1/6}, \omega) = \mathbb{Q}((-3)^{1/6})$ has degree 3 over $\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$ i.e. $X^6 + 3 = (X^3 + \sqrt{-3})(X^3 - \sqrt{-3})$.

We now consider the converse problem to (7.0.22), we need a result proved on example sheet 1, q13.

Proposition 7.0.24. *Suppose K, L are fields and $\sigma_1, \ldots, \sigma_n$ distinct embeddings of K into L. Then there does not exist $\lambda_1, \ldots, \lambda_n \in L$ (not all zero) such that $\lambda_1\sigma_1(x) + \ldots + \lambda_n\sigma_n(x) = 0$ for all $x \in K$.*

Proof. If such a relation did exist, choose one with the least number $r > 0$ of non-zero λ_i. Hence wlog $\lambda_1, \ldots, \lambda_r$ all non-zero and $\lambda_1\sigma_1(x) + \ldots + \lambda_r\sigma_r(x) = 0$ for all $x \in K$. Clearly we have $r > 1$, since $\lambda_1\sigma_1(x) = 0$ for all x implies $\lambda_1 = 0$. We now produce a relation with less than r terms, and hence a contradiction.

Choose $y \in K$, such that $\sigma_1(y) \neq \sigma_r(y)$. The above relation implies that $\lambda_1\sigma_1(yx) + \ldots + \lambda_r\sigma_r(yx) = 0$ for all $x \in K$. Thus $\lambda_1\sigma_1(y)\sigma_1(x) + \ldots + \lambda_r\sigma_r(y)\sigma_r(x) = 0$, so multiply original relation by $\sigma_r(y)$ and subtract to get $\lambda_1\sigma_1(x)(\sigma_1(y) - \sigma_r(y)) + \ldots + \lambda_{r-1}\sigma_{r-1}(x)(\sigma_{r-1}(y) - \sigma_r(y)) = 0$ for all $x \in K$, which gives the required contradiction. □

Definition 7.0.25. An extension L/K is called *cyclic* if it is Galois, and $\operatorname{Gal}(L/K)$ cyclic.

Theorem 7.0.26. *Suppose L/K a cyclic extension of degree n where $\operatorname{char} k \not| \ n$, and that K contains a primitive nth root of unity ω. Then $\exists\theta \in K$ such that $X^n - \theta$ irreducible over K and L/K is a splitting field for $X^n - \theta$. If β' is a root of $X^n - \theta$ in a splitting field then $L = K(\beta')$ (such an extension is called a* radical extension*).*

Proof. Let σ be a generator of the cyclic group $\mathrm{Gal}(L/K)$. Since $1, \sigma, \sigma^2, \dots, \sigma^{n-1}$ are distinct automorphisms of L, (7.0.24) implies $\exists \alpha \in L$ such that $\beta = \alpha + \omega\sigma(\alpha) + \dots + \omega^{n-1}\sigma^{n-1}(\alpha) \neq 0$. Observe $\sigma(\beta) = \omega^{-1}\beta$; thus $\beta \notin K$ and $\sigma(\beta^n) = \sigma(\beta)^n = \beta^n$. Therefore $\theta := \beta^n \in K$.

As $X^n - \theta = (X-\beta)(X-\omega\beta)\dots(X-\omega^{n-1}\beta)$ in L, we have $K(\beta)$ is a splitting field for $X^n - \theta$ over K. Since $1, \sigma, \dots, \sigma^{n-1}$ are distinct automorphisms of $K(\beta)$ over K, (4.1.3) implies $[K(\beta) : K] \geq n$, and hence $L = K(\beta)$. Thus $L = K(\beta')$ for any root β' of $X^n - \theta$, since $\beta' = \omega^i\beta$ for some $0 \leq i \leq n-1$.

The irreducibility of $X^n - \theta$ over K follows (since it is the minimal polynomial for β, $[L : K] = n$). □

Definition 7.0.27. A field extension L/K is an *extension by radicals* if $\exists$ tower $K = L_0 \subset L_1 \subset \dots \subset L_n = L$ such that each extension L_{i+1}/L_i is a radical extension. A polynomial $f \in k[X]$ is said to be *soluble by radicals* if its splitting field lies in an extension of k by radicals.

7.1 Cubics

Suppose $\mathrm{char}\, k \neq 2, 3$ and $f \in k[X]$ an irreducible cubic. Let K be the splitting field for f, ω a primitive cube root of unity. D =discriminant $= \Delta^2$ (recall that if $f = X^3 + pX + q$, $D = -4p^3 - 27q^2$). In chapter 4, we saw that $[K : k(\Delta)] = 3$ and $\mathrm{Gal}(K/k(\Delta)) \cong C_3$. Suppose $L = K(\omega)$; L is Galois over $k(w)$ since it's the splitting field of f. The tower law implies $[L : k(\Delta, w)] = 3$. Hence $\mathrm{Gal}(L/k(\Delta, w)) = C_3$, observing that $L/k(\Delta, w)$ is Galois since $L/k(w)$ is. (7.0.26) implies $L = k(\Delta, w)(\beta)$, where β is a root of an irreducible polynomial $X^3 - \theta$ over $k(\Delta, w)$, and in fact a proof of (7.0.26) implies $\beta = \alpha_1 + w\alpha_2 + w^2\alpha_3$ where α_i are the roots of f. Since all extensions $k \subset k(\Delta) \subset k(\Delta, w) \subset L$ are radical, any cubic is soluble by radicals.

Explicitly, we reduce to the case of cubic $g(X) = X^3 + pX + q \Rightarrow D = -4p^3 - 27q^2$. Set $\beta = \alpha_1 + w\alpha_2 + w^2\alpha_3$, $\gamma = \alpha_1 + w^2\alpha_2 + w\alpha_3$. Then $\beta\gamma = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + (w + w^2)(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -3p$. So $\beta^3\gamma^3 = -27p^3$. $\beta^3 + \gamma^3 = (\alpha_1 + w\alpha_2 + w^2\alpha_3)^3 + (\alpha_1 + w^2\alpha_2 + w\alpha_3)^3 + (\alpha_1 + \alpha_2 + \alpha_3)^3 = 3(\alpha_1^3 + \alpha_2^3\alpha_3^3) + 18\alpha_1\alpha_2\alpha_3$. But $\alpha_i^3 = -p\alpha_i - q$ and so $\sum \alpha_i^3 = -3q$ therefore $\beta^3 + \gamma^3 = -27q$. So β^3 and γ^3 are roots of $X^2 + 27qX - 27p^3$, i.e. are $-\frac{27}{2}q \pm \frac{3\sqrt{-3}}{2}(-27q^2 - 4p^3)^{1/2} = -\frac{27}{2}q \pm \frac{3\sqrt{-3}}{2}\sqrt{D}$. Therefore we can solve for β^3, γ^3 in $k(\sqrt{-3D}) \subset k(\Delta, w)$ and obtain β by adjoining a cube root of β^3, and then $\gamma = -3p/\beta$. Finally, we solve in L for $\alpha_1, \alpha_2, \alpha_3$. Namely, $\alpha_1 = \frac{1}{3}(\beta + \gamma)$, $\alpha_2 = \frac{1}{3}(w^2\beta + w\gamma)$, $\alpha_3 = \frac{1}{3}(w\beta + w^2\gamma)$.

7.2 Quartics

Recall $\exists$ action of S_4 on the set $\{\{1,2\},\{3,4\}\}$, $\{\{1,3\},\{2,4\}\}$, $\{\{1,4\},\{2,3\}\}$ of unordered pairs of unordered pairs. Therefore we have a surjective homomorphism $S_4 \to S_3$ with kernel the 4-group $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ and hence an isomorphism $S_4/V \cong S_3$.

Suppose now f is an irreducible separable quartic over k; the Galois group G is a transitive subgroup of S_4, with normal subgroup $G \cap V$, with $G/G \cap V \hookrightarrow S_4/V \cong S_3$. Let L be the splitting field of f and $K = L^{G \cap V}$.

Since $V \subset A_4$, $K \supset L^{G \cap A_4} = k(\Delta)$. Moreover, $\mathrm{Gal}(K/k(\Delta))$ is isomorphic to a subgroup of $A_4/V \cong C_3$ (namely $G \cap A_4/G \cap V$). So we have a tower, $k \hookrightarrow k(\Delta) \hookrightarrow K \hookrightarrow L$.

Claim 7.2.1. *f is soluble by radicals*

Proof. If we adjoin a primitive cube root of unity, then either f splits over $K(w)$ (in which case we're done), or f is irreducible over $k(w)$. So wlog we may assume k contains a cube root of unity.

The $k(\Delta)/k$ is a radical extension. (7.0.26) implies $K/k(\Delta)$ is a radical extension. L/K is the composite of at most 2 (quadratic) radical extensions. Hence claim. □

We now see explicitly how this works. Assume char $\neq 2, 3$, wlog, we reduce polynomial to $f = X^4 + pX^2 + qX + r$. If L is the splitting field of f, let $\alpha_1, \dots, \alpha_4$ denote the roots of f in L. By assumption note $\sum \alpha_i = 0$. Set $\beta = \alpha_1 + \alpha_2$, $\gamma = \alpha_3 + \alpha_4$, $\delta = \alpha_1 + \alpha_4$. Then we have

$$\begin{aligned}
\beta^2 &= (\alpha_1 + \alpha_2)^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\
\gamma^2 &= (\alpha_1 + \alpha_3)^2 = -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \\
\delta^2 &= (\alpha_1 + \alpha_4)^2 = -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)
\end{aligned}$$

Note that these are distinct, e.g. if $\beta^2 = \gamma^2$, i.e. $\beta = \pm\gamma$, then either $\alpha_2 = \alpha_4$ or $\alpha_1 = \alpha_4$, contradiction. β^2, γ^2, δ^2 are permuted by the action of G, and are invariant under only the elements of $G \cap V$. So $\mathrm{Gal}(L/k(\beta^2, \gamma^2, \delta^2)) = G \cap V$ therefore $K = L^{G \cap V} = k(\beta^2, \gamma^2, \delta^2)$.

Consider now the cubic $g = (X - \beta^2)(X - \gamma^2)(X - \delta^2)$. Since elements of G can only permute the three factors of g, g must have co-efficients fixed by G, i.e. $g \in k[X]$, the resolvant cubic. Explicit checks yield $\beta^2 + \gamma^2 + \delta^2 = -2p$, $\beta^2\gamma^2 + \gamma^2\delta^2 + \delta^2\beta^2 = p^2 - 4r$, $\beta\gamma\delta = -q$. Thus the resolvant cubic is $X^3 + 2pX^2 + (p^2 - 4r)X - q^2$.

There are other forms, e.g. we could take the cubic whose roots are $\alpha_1\alpha_2 + \alpha_3\alpha_4$, $\alpha_1\alpha_3 + \alpha_2\alpha_4$, $\alpha_1\alpha_4 + \alpha_2\alpha_3$, and the cubic takes the form $X^3 - pX^2 - 4rX + (4pr - q^2)$.

K is the splitting field for g over k. So if we solve g for β^2, γ^2, δ^2 by radicals, we can then solve for β, γ, δ by taking square roots (taking care to choose signs so that $\beta\gamma\delta = -q$). Then solve for the roots $\alpha_1 = \frac{1}{2}(\beta + \gamma + \delta)$, $\alpha_2 = \frac{1}{2}(\beta - \gamma - \delta)$, $\alpha_3 = \frac{1}{2}(-\beta + \gamma - \delta)$ and $\alpha_4 = \frac{1}{2}(-\beta - \gamma + \delta)$.

Chapter 8

Insolubility of General Quintic by Radicals

Definition 8.0.2. A group G is *soluble* if $\exists$ finite series of subgroups $\{e\} = G_n \subseteq G_{n-1} \subseteq \ldots \subseteq G_0 = G$ such that $G_i \lhd G_{i-1}$ with G_{i-1}/G_i cyclic for $1 \le i \le n$.

Examples 8.0.3.

1. S_4 is soluble. $G_1 = A_4$, $G_2 = V$, $G_3 = \langle(12)\rangle = C_2$ then $G_0/G_1 \cong C_2$, $G_1/G_2 \cong C_3$, $G_2/G_3 \cong G_3/G_4 \cong C_2$.
2. Using the structure theorem for abelian groups, easily seen that any finite (or finitely generated) abelian group is soluble.

Theorem 8.0.4.

1. *If G is a soluble group and A a subgroup of G, then A is soluble.*
2. *Suppose G a group, $H \lhd G$, then G soluble iff both H and G/H soluble.*

Proof.

1. Have a series of subgroups $\{e\} = G_n \lhd G_{n-1} \lhd \ldots \lhd G$ such that G_{i-1}/G_i cyclic for $1 \le i \le n$. Let $A_i = A \cap G_i$ and $\theta : A_{i-1} \to G_{i-1}/G_i$ be the composite homomorphism $A_{i-1} \hookrightarrow G_{i-1} \hookrightarrow G_{i-1}/G_i$. $\ker\theta = \{a \in A_{i-1} : aG_i = G_i\} = A_{i-1} \cap G_i = A \cap G_{i-1} \cap G_i = A \cap G_i = A_i$. Hence $A_i \lhd A_{i-1}$ and A_{i-1}/A_i is isomorphic to a subgroup of G_{i-1}/G_i and hence cyclic for all i. Therefore A is soluble.
2. A similar but longer argument, see a book.

□

Example 8.0.5. For $n \ge 5$, a standard result says that A_n is simple, (i.e. there does not exist a proper normal subgroup) and hence non-soluble. Hence (8.0.4) implies S_n is also non-soluble.

We now relate solubility of the Galois group to solubility of polynomial equations $f = 0$ by radicals. Assume for simplicity char $= 0$. An argument similar to that used for the quartic in chapter 7 shows that:

If f has a soluble Galois group, then f is soluble by radicals (basic idea is if L/k is a splitting field for f, $d = [L : K]$, we first adjoin a primitive dth root of unity and then repeatedly use (7.0.26)).

We're interested mainly in the converse. Suppose then $K = K_0 \subset K_1 \subset \ldots \subset K_r = M$ is an extension by radicals. Even if K contains all the requisite roots of unity and K_i/K_{i-1} is Galois and cyclic, it doesn't follow that M/K is Galois.

Proposition 8.0.6. *Suppose L/K is a Galois extension and $M = L(\beta)$ with β a root of $X^n - \theta$ for some $\theta \in L$. Then $\exists$ extension by radicals N/M such that N/K is Galois.*

Proof. If necessary we adjoin a primitive nth root of unity ϵ to M; so $X^n - \theta = (X - \beta)(X - \epsilon\beta)\ldots(X - \epsilon^{n-1}\beta)$, i.e. $M(\epsilon)$ is a splitting field for $X^n - \theta$ over L, i.e. $M(\epsilon)/L$ is Galois.

If $G = \mathrm{Gal}(L/K)$, let $f = \prod_{\sigma \in G}(X^n - \sigma(\theta))$. The coefficients of f are invariant under the action of G and so $f \in k[X]$.

Since L/K Galois it's the splitting field for some polynomial $g \in K[X]$; let N be the splitting field for fg, therefore N/K normal. Moreover, N is obtained from M by first adjoining ϵ and then adjoining a root of each polynomial $X^n - \sigma(\theta)$ for $\sigma \in G$. So N/M is an extension by radicals. □

Corollary 8.0.7. *Suppose M/K is an extension by radicals, then $\exists$ extension by radicals N/M such that N/K is Galois.*

Proof. Have $K = K_0 \subset K_1 \subset \ldots \subset K_r = M$ with $K_i = K_{i-1}(\beta_i)$ for some $\beta_i \in K_i$ satisfying $X^{n_i} - \theta_i = 0$ ($\theta_i \in K_{i-1}$).

Now argue by induction on r. Suppose true for $r-1$, so that $\exists$ extension by radicals N'/K_{r-1} such that N'/K is Galois.

Let f_r be the minimal polynomial for β_r over K_{r-1} and g_r an irreducible factor of f_r considered now as a polynomial in $N'[X]$. Let $N'(\gamma)/N'$ be the extension of N' obtained by adjoining a root γ of g_r. We consider $K_{r-1} \subset N' \subset N'(\gamma)$, so that γ has minimal polynomial f_r over K_{r-1} (since $f_r(\gamma) = 0$ and by assumption f_r irreducible). We may identify $K_r = K_{r-1}(\beta_r) \cong K_{r-1}(\gamma)$. Therefore $N'(\gamma)$ is an extension by radicals of $K_r = K_{r-1}(\gamma)$.

By assumption N'/K is Galois and a root of $X^{n_r} - \theta_r$ where $\theta_r \in K_{r-1} \subset N'$. So (8.0.6) implies $\exists$ extension by radicals $N/N'(\gamma)$ (and hence N is an extension by radicals over $K_r = M$) such that N/K Galois. □

Theorem 8.0.8. *If $f \in K[X]$ and $\exists$ extension by radicals $K = K_0 \subset K_1 \subset \ldots \subset K_r = M$ where $K_i = K_{i-1}(\beta_i)$ and β_i a root of $X^{n_i} - \theta_i$ ($\theta_i \in K_{i-1}$) over which f splits completely, then* Gal(f) *is soluble.*

Proof. By (8.0.7), we may assume M/K Galois. Let $n = \operatorname{lcm}(n_1, \ldots, n_r)$, and ϵ be a primitive nth root of unity.

If $\operatorname{Gal}(M/K)$ is soluble, then the splitting field of f is an intermediate field $K \subset K' \subset M$ and $\operatorname{Gal}(f) = \operatorname{Gal}(K'/K)$ is a quotient of $\operatorname{Gal}(M/K)$ and hence soluble by (8.0.4).

So it remains to show $\operatorname{Gal}(M/K)$ soluble. Assume first that $\epsilon \in K$, and let $G_i = \operatorname{Gal}(M/K_i)$ therefore $\{e\} = G_r \subset G_{r-1} \subset \ldots \subset G_1 \subset G_0 = \operatorname{Gal}(M/K)$. Moreover, each extension $K_i = K_{i-1}(\beta)/K_{i-1}$ is a Galois extension (since $\epsilon \in K$) with cyclic Galois group (7.0.22). So apply fundamental theorem of Galois theory to Galois extension M/K_{i-1} we have $G_i \lhd G_{i-1}$ with G_{i-1}/G_i cyclic. Therefore $G_0 = \operatorname{Gal}(M/K)$ soluble.

If, however, $\epsilon \notin K$, set $L = K(\epsilon)$. Clearly $M(\epsilon)/K$ is Galois (it is a splitting field extension). Set $G' = \operatorname{Gal}(M(\epsilon)/L)$, and this is soluble by the previous argument ($\epsilon \in L$). If $G = \operatorname{Gal}(M(\epsilon)/K)$, then $G/G' = \operatorname{Gal}(K(\epsilon)/K)$ is the Galois group cyclotomic extension hence abelian hence soluble.

So (8.0.4)(2) implies G soluble and hence $\operatorname{Gal}(M/K)$ (a quotient of $\operatorname{Gal}(M(\epsilon)/K)$) is also soluble. □

Remark 8.0.9. $\exists$ many irreducible quintics $f \in \mathbb{Q}[X]$ with Galois group S_5 (or A_5). Therefore (8.0.8) implies we cannot in general solve quintics by radicals.

Appendix A

Proof of Gauss's Lemma

This is from Groups, Rings and Fields, but it won't hurt. I am indebted to Dr. Nekovár for this section.

Definition A.0.10. Let R be a UFD and $f = a_0X^n + \ldots + a_n \in R[X]$ a non-zero polynomial. The *content* of f is $\text{cont}(f) = \gcd(a_0, \ldots, a_n)$ (this is a non-zero element of R, defined up to a unit). More generally, if $f \in F[X] \setminus \{0\}$ (where F is the field of fractions of R), define $\text{cont}(af)/a \in F^*/R^*$, for any $a \in R \setminus \{0\}$ such that $af \in R[X]$. Note that $\text{cont}(f)$ depends on R, not just on F. Note that in both cases, we have $\text{cont}(bf) = b\,\text{cont}(f)$ for any $b \in F$.

Proposition A.0.11. *For $f \in F[X] \setminus \{0\}$ we have*

1. *$f = \text{cont}(f)g$, where $g \in R[X]$ and $\text{cont}(g) = 1$.*
2. *$f \in R[X]$ iff $\text{cont}(f) \in R$.*
3. *If f monic (more generally, if one of the coefficients of f lies in R^*), then $1/\text{cont}(f) \in R$.*

Proof.

1. Pick $a \in R \setminus \{0\}$ such that $af \in R[X]$. Then as $\text{cont}(af)$ will divide all the coefficients of af, there is a $b \in F^*$ such that $g = bf \in R[X]$ and $\text{cont}(g) = 1$. Then $\text{cont}(f) = \text{cont}(g)/b = 1/b$, and so $\text{cont}(f)g = f$.
2. $\Rightarrow$ is clear. If $\text{cont}(f) \in R$, then from (1), $f = \text{cont}(f)g \in R[X]$.
3. If one of the coefficients of f lies in R^* then from (1), $f = \text{cont}(f)g$ where $g \in R[X]$ and $\text{cont}(g) = 1$. If $f(x) = a_nX^n + \ldots + a_0$, $g(x) = b_nX^n + \ldots + b_0$ and $a_m \in R^*$ with inverse a_m^{-1} then $a_m = \text{cont}(f)b_m \in R^*$ and so $1/\text{cont}(f) = b_m a_m^{-1} \in R$.

□

Lemma A.0.12. $\text{cont}(fg) = \text{cont}(f)\,\text{cont}(g)$ *for* $f, g \in F[X] \setminus \{0\}$.

Proof. Dividing each polynomial by it's content, we may assume $f, g \in R[X]$ and $\text{cont}(f) = \text{cont}(g) = 1$. If $\text{cont}(fg) \in R$ is not a unit, then $\pi | \text{cont}(fg)$ for some irreducible $\pi \in R$. We have

$$f(X) = \sum_{i=0}^{m} a_i X^i, \quad g(X) = \sum_{j=0}^{n} b_j X^j, \quad fg(X) = \sum_{k=0}^{m+n} c_k X^k, \quad c_k = \sum_{i+j=k} a_i b_j$$

Let $i \geq 0$ be the smallest index such that $\pi \not| \, a_i$ (same for j and b_j). These must exist as $\text{cont}(f) = \text{cont}(g) = 1$. In the formula for c_{i+j} each term apart from $a_i b_j$ is divisible by π, but $\pi \not| \, a_i b_j$. Thus $\pi \not| \, \text{cont}(fg)$. Hence $\text{cont}(fg)$ is a unit. □

Lemma A.0.13. Gauss's Lemma
Let R be a UFD and F it's field of fractions. Then $f \in R[X] \setminus \{0\}$ is irreducible in $F[X]$ iff it is irreducible in $R[X]$.

Proof. If $f = gh$ with $g, h \in F[X]$ $(\deg(g), \deg(h) \geq 1)$ then by replacing g, h with $g/\text{cont}(g), h\,\text{cont}(g)$ we may assume that $g \in R[X]$ and $\text{cont}(g) = 1$. It follows from above lemma that $\text{cont}(h) = \text{cont}(g)\,\text{cont}(h) = \text{cont}(f) \in R$, and so $h \in R[X]$. The converse is trivial, as if f factors in $R[X]$, it will factor in $F[X]$. □

Appendix B

Lecturer's Handout on Zorn's Lemma

In order to prove the existence and uniqueness of splitting fields for arbitrary sets of polynomials in $k[X]$ over an arbitrary field k, or equivalently the existence and uniqueness of the algebraic closure of k, we shall need to assume a form of the Axiom of Choice. Note however that this is not necessary for instance when k is a subfield of the complex numbers, since we can construct the complex numbers explicitly. The form of the Axiom of Choice which is most convenient is Zorn's Lemma, which we explain below. We'll not prove that it is equivalent to the axiom of choice (which it is). You may instead assume Zorn's Lemma if it is necessary for a particular problem, but should try to avoid its use when it is unnecessary.

B.1 Partially ordered sets

A relation $\leq$ on a set S is called a *partial ordering* if

1. $x \leq x$ for all $x \in S$,
2. if $x \leq y$ and $y \leq z$ in S, then $x \leq z$,
3. if $x \leq y$ and $y \leq x$ in S, then $x = y$.

For example, if S is a collection of subsets of a set X, then we can partially order S by taking $\leq$ to be inclusion.

A partial ordering $\leq$ on a set S is a *total ordering* if for any elements $x, y \in S$, either $x \leq y$ or $y \leq x$. If S is a partially ordered set, a chain $\mathcal{C}$ of elements of S is just a non-empty subset of S which is totally ordered in the ordering inherited from S.

If T is a subset of a partially ordered set S, an element $x \in S$ is called an *upper bound* for T if $t \leq x$ for all $t \in T$. An upper bound of T may or may not exist; if it exists, it may or may not be in T itself, and it may or may not be unique.

An element x is a partially ordered set S is called *maximal* if, whenever $x \leq y$ for some $y \in S$, we have $x = y$. A maximal element of S is not necessarily an upper bound for S, and a partially ordered set S may have many maximal elements, or none at all.

B.2 Zorn's Lemma

If a non-empty partially ordered set S has the property that every chain $\mathcal{C}$ in S has an upper bound, then S contains at least one maximal element.

As an example of the use of Zorn's Lemma, let us prove the (apparently innocuous) statement that any non-zero commutative ring A has a maximal ideal – this is in fact the statement we'll need in out proof of the existence of algebraic closures.

Let S denote the set of proper ideals of A, with partial order $\leq$ given by inclusion. Recall that an ideal I of A is proper iff $1 \notin I$. For any chain $\mathcal{C}$ of proper ideals, an elementary check confirms that $\cup\{I \in \mathcal{C}\}$ is also a proper ideal of A, and hence is an upper bound for $\mathcal{C}$. Thus S has a maximal element, which is by definition a maximal ideal of A.

Bibliography

[Ar] E. Artin, *Galois Theory*, Dover, ISBN 0486623424, £5.95

[St] I. Stewart, *Galois Theory*, Chapman and Hall, ISBN 0412345501, £21.95

[Wa] B.L. van der Waerden, *Algebra vol. 1*, Springer Verlag, ISBN 3540974245, £28.50

[La] S. Lang, *Algebra*, Addison-Wesley, ISBN 0201555409, £26.99

[Ka] I. Kaplansky, *Fields and Rings*, University of Chicago Press, ISBN 0226424510, $20.00