Outline of a Course in Field Theory

S. Kumaresan
School of Math. & Stat.
University of Hyderabad
Hyderabad 500046
kumaresa@gmail.com

August 2, 2015

F stands for a field in the sequel.

1 Polynomial Ring $F[x]$

Topics: Reducible and irreducible; Various facts such as Euclidean domain, Irreducibility criterion such as Eisenstein's.

Theorem 1.1 (Division Algorithm)**.** *Let F be a field, and let $f \in [F[x]$ be a nonzero polynomial with coefficients in F. Then given any polynomial $g \in F[x]$, there exist unique polynomials $q, r \in F[x]$ such that $g = fq + r$ with either $r = 0$ or $\deg r < \deg f$.* □

Corollary 1.2. *The polynomial ring $F[x]$ is a PID.* □

Definition 1.3. Let $f_1, \ldots, f_k \in F[x]$. They are said to be *coprime* or *relatively prime* if a polynomial q divides each f_j, then q is a constant.

Proposition 1.4. *Let $f_j \in F[x]$, $1 \leq j \leq k$, be coprime. Then there exist $g_j \in F[x]$, $1 \leq j \leq n$, such that*

$$f_1(x)g_1(x) + \cdots + f_k(x)g_k(x) = 1.$$

□

Definition 1.5. A *non-constant* polynomial $f \in F[x]$ is said to be *irreducible* over F if $q \in F[x]$ divides, then q is a constant.

Proposition 1.6. *Let $f \in F[x]$ be irreducible. Let f divide gh where $g, h \in F[x]$. The either f divides g or f divides h.* □

Theorem 1.7. *Let $f \in F[x]$ be irreducible. Then the quotient ring $F[x]/(f)$ is a field.* □

Theorem 1.8 (Gauss Lemma)**.** *A polynomial $f \in \mathbb{Z}[x]$ is irreducible* over $\mathbb{Q}$ *iff it is irreducible in the ring $\mathbb{Z}[x]$.*

Proof. Assume $f(x) = g(x)h(x) \in \mathbb{Q}[x]$ with $\deg g < \deg f$ and $\deg h < \deg f$. Choose $m \in \mathbb{Z}$ such that $mg \in Z[x]$. Hence $f(x) = (m \cdot g(x))\left(\frac{1}{m} \cdot h(x)\right)$. Let c be the GCD of all the coefficients in $m \cdot g(x)$. We have

$$f(x) = \left(\frac{m}{c} \cdot g(x)\right)\left(\frac{c}{m} \cdot h(x)\right) = G(x) \cdot H(x), \text{ say.}$$

We show that H has integer coefficients. Let n be the smallest natural number such that $n \cdot H(x) \in \mathbb{Z}[x]$. We claim $n = 1$. If not, let p be any prime dividing n. Let $\pi\colon \mathbb{Z}[x] \to \mathbb{Z}_p[x]$ be the standard homomorphism. Then $\pi(n \cdot f(x)) = \pi(G(x) \cdot n \cdot H(x)) = 0$. Since the GCD of coefficients of $G(x)$ is 1, at least one of its coefficients is not divisible by p and hence $\pi(G(x)) \neq 0$. Since $\mathbb{Z}_p[z]$ is an integral domain, it follows that $\pi(n \cdot H(x)) = 0$. In other words, all the coefficients of $n \cdot H(x)$ are divisible by p. This means that $\frac{n}{p}H(x) \in \mathbb{Z}[x]$. This contradicts the minimality of n. □

Theorem 1.9 (Eisenstein's Irreducibility Criterion)**.** *Let $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$. Let $p \in \mathbb{N}$ be a prime. Assume that (i) p does not divide a_n, (ii) p divides a_j, $0 \leq j \leq n-1$, and (iii) p^2 does not divide a_0. Then f is irreducible* over $\mathbb{Q}$.

Proof. Let, if possible, $f(x) = (b_0 + b_1x \cdots + b_rx^s)(c_0 + c_1x + \cdots + c_sx^s$. Look at $a_0 = b_0c_0$. Since p divides a_0 but not p^2 says that p divides exactly one of b_0 and c_0. Assume that p divides b_0 and not c_0. Again look at $a_1 = b_0c_1 + b_1c_0$. Since p divides a_1, and b_0, it follows that p divides b_1c_0. Since p does not divide c_0, it follows that p divides b_1. Proceed by induction. □

Ex. 1.10. Extend the last theorem as follows. Let R be a ring, and P a prime ideal of R. Let $f(x) = a_0 + a_1x + \cdots + a_nx^n \in R[x]$. Assume that (i) $a_i \in P$ for $0 \leq i < n$, (ii) $a_n \notin P$ and (iii) $a_0 \notin P^2$, the product ideal. Then f is irreducible in $R[x]$.

Ex. 1.11. Show that the polynomials (i) $x^2 + 8x - 2$ and (ii) $x^2 + 6x + 12$ are irreducible over $\mathbb{Q}$. Are they irreducible over $\mathbb{R}$? Over $\mathbb{C}$?

Ex. 1.12. This observation is needed when we want to transform a given polynomial into one to which Eisenstein criterion may be applied.

Let $a \in R^*$ and $b \in R$, an integral domain. Then $f(x)$ s irreducible in $R[x]$ iff $g(x) := f(ax + b)$ is irreducible in $R[x]$.

Apply the transformation $x \mapsto x + 1$ to establish th irreducibility of $f(x) = x^4 + 4x^3 + 10x^2 + 12x + 7 \in \mathbb{Z}[x]$.

Ex. 1.13. $\Phi_p(x)$ is irreducible. The key observation is that $\Phi_p(x) = \frac{x^p-1}{x-1}$. Now look at $g(x) = \Phi_p(x + 1) = \sum_{r=0}^{p-1} \binom{p}{r} x^r$. Eisenstein criterion applied to g yields the irreducibility of g.

Ex. 1.14. $\Phi_{p^2}(x) := \frac{x^{p^2}-1}{x^p-1}$ is irreducible. Apply the trick of the last exercise.

Ex. 1.15. Let R be an integral domain. Then $f(x) = a_0 + \cdots + a_nx^n$ with $a_0 \neq 0$ is irreducible over R iff the *reciprocal polynomial* $\tilde{f}(x)$ defined by $\tilde{f}(x) = x^n f(1/x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ is irreducible over R.

Use this observation to prove the irreducibility of the following polynomials: (i) $2x^4 + 4x^2 + 4x + 1$ and (ii) $5x^7 + 4$.

Theorem 1.16 (Rational Roots Theorem)**.** *Let $f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$. Assume that $a_n a_0 \neq 0$. If $r/s \in \mathbb{Q}$ (in lowest terms) is a root of $f(x)$, then $r|a_0$ and $s|a_n$.*

Proof. Look at $s^n f(r/s)$. We have

$$0 = s^n f(r/s) = a_n r^n + a_{n-1}(r/s)^{n-1} s + \cdots + a_1 r s^{n-1} + a_0 s^n.$$

RHS is divisible by r and hence $r|a_0$ as all the other terms on LHS are divisible by r. RHS is divisible by s and hence $s|a_n$, as all other terms on LHS are divisible by s. □

Corollary 1.17. *If $f(x) \in \mathbb{Z}[x]$ is monic, then any rational root must be an integer dividing a_0.* □

Ex. 1.18. Show that 3 is the only rational root of $x^3 - 2x^2 - 2x - 3$.

Ex. 1.19. Show that $f(x) = x^5 + 9x^3 + 2$ has rational roots. Show that it has only one ral root in $(-1, 0)$.

Ex. 1.20. Show that $f(x) = x^3 + ax^2 + bx + 1 \in \mathbb{Z}[x]$ is reducible iff either $a = b$ or $a + b + 2 = 0$.

Ex. 1.21. Show that $x^4 + 2x^2 + 1 \in \mathbb{Q}[x]$ is irreducible. *Hint:* Use the rational roots theorem to show that it has no linear factors. Use Gauss lemma to show that if it were reducible, then the irreducible factors are quadratic, say, $f(x) = (x^2 + ax + 1)(x^2 + bx + 1)$. Compare the coefficients to arrive at equations which have no integer solutions.

Ex. 1.22. Show that $f(x) = x^2 - 8x - 2$ is irreducible over $\mathbb{Q}$.

Ex. 1.23. Show that $f(x) = x^3 + 3x^2 - 8$ is irreducible over $\mathbb{Q}$.

Ex. 1.24. Show that $x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Q}[x]$.

Ex. 1.25. Show that the polynomial $x^2 + x + 1$ is irreducible in $\mathbb{Z}_3[x]$.

Ex. 1.26. Show that $f(x) = 4x^3 - 3x + \frac{1}{2} \in \mathbb{Q}[x]$ is irreducible in two ways: one using the rational root theorem and the other applying Eisenstein criterion to $f(\frac{1+x}{2})$.

2 Extension of Fields

Topics: Algebraic element, minimal polynomial of an algebraic element, algebraic extension, degree of extension, finite extensions, tower theorem: $[L : F] = [L : K][K : F]$, Kronecker's theorem, Adjunction of roots. $K(\alpha) = K[\alpha]$ if α is algebraic over K.

Definition 2.1. Let F be a field. An *extension* E/F is an imbedding of F into some field E, in other words, F is a 'subfield' of E, then we say that E is an extenion of F and write it as E/F (read as extension field E over F).

Let E/F be an extension of F. Then E is a vector space over F in an obvious way. The *degree* of the extension, denoted by $[E : F]$ or by $|E : F|$ is by definition $\dim_F E$, the dimension of the vector space E over the underlying field F.

The extension E/F is *finite* if $[E : F]$ is finite.

Let E/F be an extension. Let $S \subset E$. Then $F(S)$ denotes the smallest subfield of E containing F and S. We then say that $F(S)$ is the field obtained from F by *adjoining* S.

If $S = \{\alpha_1, \ldots, \alpha_k\}$, we denote $F(S)$ by $F(\alpha_1, \ldots, \alpha_k)$.

A field extension E/F is said to be *simple* if $E = F(\alpha)$ for some $\alpha \in E$.

Example 2.2. Let $F = \mathbb{Q}$ and $E = \mathbb{R}$ or $E = \mathbb{C}$. Then E/F is an extension, which are not finite extensions.

$\mathbb{C}/\mathbb{R}$ is a simple extension.

Example 2.3. Let E be any field and F its prime subfield. Then E/F is an extension. (It may happen $E = F$!)

Example 2.4. Let F be any field and $E := F(x)$, the field of rational functions on F. Then E/F is a simple extension.

Example 2.5. Let $F := \mathbb{Q}$ and $E := \mathbb{Q} + \sqrt{2}\mathbb{Q} := \{a + b\sqrt{2} : a, b \in \mathbb{Q}\} \subset \mathbb{R}$. It is easy to check that E is a subfield of $\mathbb{R}$ and that E/F is an extension. (What is the inverse of $a + b\sqrt{2}$?)

Theorem 2.6 (Tower Law)**.** *Let E/F and K/E be extension fields. Then the extension K/F is finite iff the extensions E/F and K/E are finite and we have $[K : F] = [K : E][E : F]$.*

Proof. If $\{u_i : 1 \leq i \leq m\}$ is an F-basis of E and $\{v_j : 1 \leq j \leq n\}$ is an E-basis of K, then $\{x_i y_j : 1 \leq i \leq m; 1 \leq j \leq n\}$ is an F-basis of K over F. Work out the details. □

Proposition 2.7. *Let E/F be a simple extension, say, $E = F(\alpha)$. Then precisely, one of the following holds:*

(i) *There does not exist any nonzero-polynomial $f \in F[x]$ with $f(\alpha) = 0$.*

(ii) *There exists a unique monic polynomial $f \in F[x]$ of least degree with $f(\alpha) = 0$.*

Proof. Consider the kernel of the ring homomorphism $f \mapsto f(\alpha)$ from $F[x]$ to E. □

Definition 2.8. Let E/F be an extension and $\alpha \in E$. Then α is said to be *algebraic* over F if there exists $0 \neq f \in F[x]$ such that $f(\alpha) = 0$. The extension E/F is *algebraic* if each element $\alpha \in E$ is algebraic over F.

An element $\alpha \in E$ is *transcendental* over F if it is not algebraic over F.

Proposition 2.9. *Any finite extension E/F is algebraic.*

Proof. Let $|E : F| = n$ and $\alpha \in E$. The set $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ is F-linearly independent. □

Proposition 2.10 (Minimal polynomial of an algebraic element)**.** *Let E/F be an extension and $\alpha \in E$ be algebraic over F. Then there exists a unique irreducible monic polynomial $m_\alpha = m_{\alpha,F} = \min(\alpha, F) \in F[x]$ with the following property: $f \in F[x]$ is such that $f(\alpha) = 0$, iff m_α divides f.*

Proof. Let $I := \{f(x) \in F[x] : f(\alpha) = 0\}$. Then I is a principal ideal in $F[x]$. Choose the polynomial of minimal degree with leading coefficient 1. □

Definition 2.11. The polynomial m_α of the last proposition is said to be the *minimal polynomial* of α over F.

Theorem 2.12. *A simple extension $F(\alpha)/F$ is finite iff α is algebraic over F. Also, in such a case, we have $[F(\alpha) : F] = \deg m_\alpha$.*

Proof. The evaluation map $F[x] \to E = F(\alpha)$ given by $f(x) \mapsto f(\alpha)$ is a ring homomorphism. Its kernel is the principal ideal $(\min(\alpha, F))$. By the first homomorphism theorem, $F[x]/(\min(\alpha, F)) \simeq F[\alpha]$. But the set of polynomials $\{x^r : 0 \leq r < \deg \min(\alpha, F)\}$ is linearly independent *modulo* $(\min(\alpha, F))$. □

Corollary 2.13. *A field extension E/F is finite iff there exist $\alpha_1, \ldots, \alpha_k \in E$ such that $E = F(\alpha_1, \ldots, \alpha_k)$ and each α_j is algebraic over F.*

Proof. If E/F is finite, then $E = F(\alpha_1, \ldots, \alpha_n)$. Since E/F is finite. any $\alpha \in E$ is algebraic over F. In particular, each α_i is algebraic.

Conversely, let $E = F(\alpha_1, \ldots, \alpha_n)$ with each α_i being algebraic over F. We need to show that $|E : F|$ is finite. Let $F_i := F(\alpha_1, \ldots, \alpha_i)$ $1 \leq i \leq n$, with $F_0 = F$. We have $F_i = F_{i-1}(\alpha_i)$. If $\alpha \in E$ is algebraic over F, then it is also algebraic over any K with $F \leq K \leq E$. Hence, each α_i is algebraic over F_{i-1} and hence the extension $F_i : F_{i-1}$ is finite. Observe that we have a tower of extensions

$$F_0 \leq F_1 \leq F_2 \leq \cdots F_n = E.$$

Since each of the two consecutive extensions is finite, the result follows from tower law. □

Corollary 2.14. *If $E : F$ is algebraic and K/E is algebraic, then K/F is algebraic.*

Proof. Let $\alpha \in K$. Since α is algebraic over E, there exist $a_i \in E$ such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Note that each $a_i \in F(a_0, a_1, \ldots, a_n)$. Consequently, α is algebraic over $F(a_0, \ldots, a_n)$. Since each $a_i \in E$ is algebraic over F, it follows from the last result that $F(a_0, \ldots, a_n) : F)$ is finite. Hence $F(a_0, \ldots, a_n, \alpha) : F$ is finite. That is, α is algebraic over F. □

Ex. 2.15. Find the degree and a basis for the given field extension: (a) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$, (b) $\mathbb{Q}(\sqrt{2}, \sqrt{3}.\sqrt{18}) : \mathbb{Q}$, (c) $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}$, (d) $\mathbb{Q}(\sqrt{2}\sqrt{3}) : \mathbb{Q}$, (e) $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2} + \sqrt{3})$, (f) $\mathbb{Q}(\sqrt{2}, \sqrt{6} + \sqrt{10}) : \mathbb{Q}(\sqrt{3} + \sqrt{5})$.

Ex. 2.16. Let $p_1, \ldots, p_n$ be n-distinct positive prime numbers. Let $F := \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. Let $q_1, \ldots, q_r$ be distinct primes none of which appear in the list $\{p_1, \ldots, p_n\}$. Then $\sqrt{q_1 \cdots q_r} \notin F$.

Ex. 2.17. Let p and q be distinct primes. Show that $\mathbb{Q}(\sqrt{p},\sqrt{q})/Q$ is of degree 4. Using induction show that $[\mathbb{Q}(\sqrt{p_1},\ldots,\sqrt{p_n}):\mathbb{Q}]=2^n$.

Example 2.18. We wish to compute $|\mathbb{Q}(\sqrt{2},\sqrt{3},i,\sqrt[5]{7},\sqrt[7]{11}:\mathbb{Q}|$.

By earlier exercise, we have $|\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}|=4$. Since $\mathbb{Q}(\sqrt{2},\sqrt{3})\subset\mathbb{R}$, we have $i\notin\mathbb{Q}(\sqrt{2},\sqrt{3})$. We have $|\mathbb{Q}(\sqrt{2},\sqrt{3})(i):\mathbb{Q}(\sqrt{2},\sqrt{3})|=2$. Hence $|\mathbb{Q}(\sqrt{2},\sqrt{3},i):\mathbb{Q}|=8$.

$\sqrt[5]{7}$ (resp. $\sqrt[7]{11}$) is a root of the polynomial x^5-7 (resp. x^11-7). These polynomials are irreducible by Eisenstein. Therefore, $|\mathbb{Q}(\sqrt[5]{7}):\mathbb{Q}|=5$ and $|\mathbb{Q}(\sqrt[7]{11}):\mathbb{Q}|=7$. So, $|\mathbb{Q}(\sqrt{2},\sqrt{3},i,\sqrt[5]{7},\sqrt[7]{11}:\mathbb{Q}|$ is divisible by 8, 5 and 7 and so by 280.

We estimate the degree by the tower law in a different way. We have

$$\mathbb{Q}\leq\mathbb{Q}(\sqrt{2},\sqrt{3},i)\leq\mathbb{Q}(\sqrt{2},\sqrt{3},i,\sqrt[5]{7})\leq\mathbb{Q}(\sqrt{2},\sqrt{3},i,\sqrt[5]{7},\sqrt[7]{11}).$$

The first inclusion gives 5 as a bound and the second inclusion gives 7 as a bound and the last one is 8. Hence the degree is at most 280.

Ex. 2.19. Let E/F be a finite extension. Assume that R be a subring $F\subset R\subset E$. Show that R is a field.

Ex. 2.20. Show that a finite extension of prime degree is a simple extension.

Ex. 2.21. Let $a,b\in\mathbb{Q}$. Assume that $\sqrt{a}+\sqrt{b}\neq 0$. Show that $\mathbb{Q}(\sqrt{a}+\sqrt{b})=\mathbb{Q}(\sqrt{a},\sqrt{b})$.

Ex. 2.22. Show that $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Ex. 2.23. Find the degrees of the following extensions: (i) $\mathbb{Q}(\sqrt[3]{2},i)/\mathbb{Q}$, (ii) $\mathbb{Q}(\sqrt{2},\sqrt{3})/Q$.

Ex. 2.24. Let $\alpha\in\mathbb{C}$ be a root of the polynomial $x^2+x+1\in\mathbb{Q}[x]$. Show that $\alpha^2-1\neq 0$ and that $\frac{\alpha^2+1}{\alpha^2-1}\in\mathbb{Q}(\alpha)$ is $\frac{1+2\alpha}{3}$.

Ex. 2.25. Let $a,b\in\mathbb{Q}$. Find the minimal polynomial of $a+b\sqrt{2}$.

Ex. 2.26. Let E/F be an extension of degree 2. Show that $E=F(\alpha)$ where $\alpha\in E\setminus F$ is arbitrary element with $\deg\min(\alpha,F)$ is 2.

Ex. 2.27. Show that $f(x)=x^3+x+1\in\mathbb{Q}[x]$ is irreducible. Let $\alpha\in\mathbb{C}$ be a root of f. Express $1/\alpha$ as a polynomial in α.

Ex. 2.28. (i) Show that $\mathbb{Q}(\sqrt{2},\sqrt{3})=\mathbb{Q}(\sqrt{2}+\sqrt{3})$.
(ii) Show that $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2},\sqrt{3})$.
(iii) Show that $\min(\sqrt{2}+\sqrt{3},\mathbb{Q})=x^4-10x^2+1$.

Ex. 2.29. Keep the notation of the last exercise. (a) Show that $\sqrt{3}\notin\mathbb{Q}(\sqrt{2})$. (b) Find $\min(\sqrt{3}+\sqrt{2},\mathbb{Q}(\sqrt{3}))$.

Ex. 2.30. Consider the extension $\mathbb{C}/\mathbb{Q}$. Find the minimal polynomial of the following elements: (i) $\sqrt{2}$, (ii) $\sqrt{-1}$, (iii) $\sqrt{2}+\sqrt{3}$, (iv) ζ, a primitive root of unity where p is a prime and (v) ζ_6, a primitive sixth root of unity.

Ex. 2.31. Given $\alpha\in\mathbb{C}$, find an $f(x)\in\mathbb{Q}[x]$ such that $f(\alpha)=0$. (a) $1+\sqrt{3}$, (b) $\sqrt{2}+\sqrt{3}$, (c) $\sqrt{1+\sqrt[3]{2}}$ (d) $1+i$, and $(e)\sqrt{\sqrt[3]{2}-i}$.

Ex. 2.32. Find $\min(\sqrt{3-\sqrt{6}}, \mathbb{Q})$ and hence find $|\mathbb{Q}(\sqrt{3-\sqrt{6}}) : \mathbb{Q}|$.

Ex. 2.33. Let $\operatorname{Char} F \neq 2$. Assume that $E = F(\alpha, \beta)$ such that $\alpha^2 = a \in F$ and $\beta^2 = b \in F$ with $a \neq b$. Show that $E = F(\alpha + \beta)$.

Ex. 2.34. Let E/F be finite with $|E : F| = n$. Let $p(x) \in F(x)$ be irreducible of degree m. Show that if m does not divide n, then p has no root in E.

Ex. 2.35. Let E/F be an extension and let $\alpha \in E$ be algebraic over F. Show that the subfield $F(\alpha) = \{p(\alpha) : p \in F[x]\}$.

Ex. 2.36. Let E/F be an extension with $\alpha \in E$. Show that the following are equivalent:
(i) α is algebraic over F.
(ii) The evaluation map $p \mapsto p(\alpha)$ from $F[x]$ to E has nonzero kernel.
(iii) $F(\alpha)/F$ is a finite extension.

Ex. 2.37. Let $F \leq E \leq K$ be fields. The extensions need not be finite. Show that K/F is algebraic iff K/E is algebraic and E/F is algebraic.

Ex. 2.38. Let $F \leq E \leq K$ be a tower of fields. Let $\alpha \in K$ be such that $F(\alpha) : F$ is a finite extension. Show that $|E(\alpha) : E| \leq |F(\alpha) : F|$.

Ex. 2.39. Let E/F be an extension, $\alpha_j \in E$, $1 \leq j \leq n$ be algebraic over F. Show that $F(\alpha_1, \ldots, \alpha_n)/F$ is a finite extension.

Ex. 2.40. Let E/F be an extension. Assume that $\alpha, \beta \in E$ are algebraic over F. Show that $\alpha \pm \beta$, $\alpha\beta$ and α/β (if $\beta \neq 0$) are algebraic over F.

Ex. 2.41. Let E/F be an extension. Let $\overline{F}$ be the set of all elements of E which are algebraic over F. Show that $\overline{F}$is a subfield of F. ($\overline{F}$ is called the *algebraic closure* of F *in* E.)

Let $\overline{\mathbb{Q}}$ stand for the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$. Show that $\overline{\mathbb{Q}}$ is not a finite extension of $\mathbb{Q}$.

Ex. 2.42. Let E/F be a finite extension. Assume that for any two subfields K_1, K_2 of E either $K_1 \subset K_2$ or $K_2 \subset K_1$. Show that E/F is a simple extension.

Ex. 2.43. Let $E = F(\alpha)$ be algebraic over F with $[F(\alpha) : F]$ being odd. Show that $F(\alpha) = F(\alpha^2)$.

Ex. 2.44. Let E/F be a finite extension of degree n. If F is finite with q elements, then E has q^n elements.

Ex. 2.45. Exhibit an irreducible degree 3 polynomial in $\mathbb{Z}_3[x]$. Hence conclude that there exists an field of 27 elements.

Ex. 2.46. Show that there exist finite fields of p^2 elements for every prime $p \in \mathbb{N}$.

Ex. 2.47. Let $\alpha \in E/F$ be transcendental over F. Show that any $\beta \in F(\alpha) \setminus F$ is transcendental over F.

Ex. 2.48. Let E/F be an extension. Let $\alpha, \beta \in E$. Assume that α is transcendental over F but algebraic over $F(\beta)$. Show that β is algebraic over $F(\alpha)$.

Ex. 2.49. Let α, β be transcendental numbers. Which of the following are true?
(a) $\alpha\beta$ is transcendental.
(b) $\mathbb{Q}(\alpha)$ is isomorphic to $\mathbb{Q}(\beta)$.
(c) α^β is transcendental.
(d) α^2 is transcendental.

Ex. 2.50. Let F be a finite field with prime characteristic p. Show that every element of F is algebraic over the prime field..

Ex. 2.51. Let $f, g \in F[x]$ be polynomials, not both zero, and let h be their greatest common divisor as computed in $F[x]$. Let E be an extension field of F. Prove that h is the greatest common divisor of f and g when considered as polynomials in $E[x]$.

Ex. 2.52. Show that every finite field has p^n elements for some prime p.

Definition 2.53. Let E/F and K/F be two extensions of F. Then an F-homomorphism θ is a field homomorphism $\theta\colon E \to K$ such that $\theta(a) = a$ for all $a \in F$.

An F-automorphism of E/F is an F-isomorphism of E onto itself.

The extensions E/F and K/F are said to be K-isomorphic if there exists an isomorphism $\theta\colon E \to K$ which is also an F-homomorphism.

Ex. 2.54. Let E/F be an extension such that $E = F(\alpha_1, \ldots, \alpha_k)$. If an F-automorphism θ of E leaves each of α_j, $1 \leq j \leq k$ fixed, then show that θ is the identity. Hence deduce that any two F-automorphism that agree on α_j's must be the same.

3 Splitting Fields and Normal Extensions

Topics: Definition of a splitting field of a polynomial, uniqueness, normal extensions, elements conjugate over a field F.

Definition 3.1. Let $f \in F[x]$ and E/F be an extension. We say that f *splits* over E if either f is a constant polynomial or if there exist $\alpha_1, \ldots, \alpha_n \in E$ such that $f = c(x-\alpha_1)\cdots(x-\alpha_n)$ where $c \in F$ is the leading coefficient of f.

The field E is said to be a *splitting field* of f over F if (i) f splits in E and (ii) f does not split in any proper subfield of E.

Ex. 3.2. The extension E/F be a splitting field of $f(x) \in F[x]$ iff (i) $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$ in E and (ii) $E = F(\alpha_1, \ldots, \alpha_n)$.

Lemma 3.3. *Let E/F be an extension. Assume that $f \in F[x]$ splits in E. Then there exists a unique subfield K of E such that K is a splitting field of f over F.*

Given $\sigma\colon K \to L$ be a homomorphism of fields, then we have a natural homomorphism $\sigma_*\colon K[x] \to L[x]$ defined by

$$\sigma_*(a_0 + a_1x + \ldots + a_nx^n) = \sigma(a_0) + \sigma(a_1)x + \cdots + \sigma(a_n)x^n.$$

Theorem 3.4 (Kronecker)**.** *Let $f \in F[x]$ be a nonconstant polynomial. Then there exists an extension E/F and an $\alpha \in E$ such that $f(\alpha) = 0$.*

Proof. WLOG, assume f is irreducible. Then $I := (f)$ is maximal in $F[x]$ and $F[x]/I$ is a field. The map $a \mapsto a + I$ is a field homomorphism of F into $F[x]/I$. So we may consider $F[x]/I$ is an extension of F. Let $\alpha := x + I$. It is easy to check that α is a root of $f(x)$. For,

$$f(\alpha) = f(x + I) = f(x) + I = I.$$

□

Corollary 3.5. *Let $f \in F[x]$. Then there exists a splitting field E of f over F such that $|E : F| \leq n!$.*

Proof. By induction. Kronecker assure at least one linear factor in an extension. □

Definition 3.6. Let E/F be an extension. An automorphism σ of E is said to be an F-automorphism if $\sigma(x) = x$ for $x \in F$.

Proposition 3.7. *Let $\sigma\colon F \to K$ be an onto isomorphism. Let $f(x) := \sum_i a_ix^i \in F[x]$ be irreducible. Let $g(x) := (\sigma_*f)x = \sum \sigma(a_i)x^i$. Let α and β be roots of f and g respectively in some extensions E/F and L/K. Then σ can be extended as an isomorphism $\sigma\colon F(\alpha) \to K(\beta)$.*

Proof. σ extends to an isomorphism of $F[x]$ onto $K[x]$. This induces an F-isomorphism on the quotient rings $F[x]/(f)$ and $K[x]/(g)$. But then, $F(\alpha) \simeq F[x]/(f)$ via an F-isomorphism. Complete the proof. □

Corollary 3.8. *Let E/F be an extensions. Let $p(x) \in F[x]$ be irreducible. Assume that $\alpha, \beta \in E$ are roots of p. Then $F(\alpha)$ and $F(\beta)$ are F-isomorphic.*

Proof. While this is an immediate consequence of the last result, it is worth writing this map explicitly.

Given any element $a \in F(\alpha)$, there is a unique polynomial $f_a(x) \in F[x]$ such that $f_a(\alpha) = a$ and $\deg f_a < \deg p$ or $f_a = 0$. (Why?) Similar observation about elements of $F(\beta)$. The map $\pi\colon F(\alpha) \to F(\beta)$ is given by

$$\pi(c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}) = c_0 + c_1\beta + \cdots c_{n-1}\beta^{n-1}.$$

A better way of understanding this map is as follows. Let $f(x), g(x) \in F[x]$. Then $f(\alpha) = g(\alpha)$ iff $f - g$ is divisible by p. It follows that $f(\alpha) = g(\alpha)$ iff $f(\beta) = g(\beta)$. Therefore, we get a well-defined homomorphism $\pi\colon F(\alpha) \to F(\beta)$ which sends $f(\alpha)$ to $f(\beta)$. Clearly, $\pi(\alpha) = \beta$. □

Theorem 3.9. *Let F_1 and F_2 be fields and let $\sigma\colon F_1 \to F_2$ be an isomorphism. Let $f \in F_1[x]$. Assume that E_1 and E_2 are splitting fields of f and $\sigma_*(f)$ over F_1 and F_2 respectively. Then there exist an isomorphism $\tau\colon E_1 \to E_2$ which extends σ.*

Proof. By induction on the degree $n = \deg f$, the case $n = 0$ being trivial.

Question: What is the exact induction hypothesis?

Let α be a root of an irreducible factor f_1 of f. Let β be a root of $g_1 := \sigma(f_1)$. We then have an F-isomorphism σ_1 which extends σ of $F_1(\alpha)$ onto $F_2(\beta)$. Let $f(x) = (x-\alpha)\varphi(x) \in F(\alpha)[x]$. Let $\sigma_*(f)(x) = (x - \beta)\sigma_*(\varphi)(x)$. Then E_1 is the splitting field of $\varphi(x)$ over $F(\alpha)$. Similar statement holds for $\sigma_*(\varphi)$ and E_2. By induction, σ_1 extends to an isomorphism τ of E_1 onto E_2. It is clear that $\tau(x) = \sigma(x)$ if $x \in F$. □

Corollary 3.10. *Any two splitting fields of $f \in F[x]$ are F-isomorphic.* □

Corollary 3.11. *Let E/F be a splitting field of some polynomial. Let $\alpha, \beta \in E$. Then there exists an F-isomorphism of E mapping α to β iff $m_{\alpha,F} = m_{\beta,F}$, that is, iff α and β have the same minimal polynomial over F.*

Proof. Let $E = \mathrm{Split}(f(x); F)$. Let $m_{\alpha,F} = m_{\beta,F}$. We know from Corollary 3.8 that there exists an F-isomorphism $\sigma\colon F(\alpha) \simeq F(\beta)$. Observe that $E = \mathrm{Split}(f(x); F(\alpha))$ as well as $E = \mathrm{Split}(f(x); F(\beta))$. By Theorem 3.9, there exists an extension $\tau\colon E \to E$ of σ. Clearly, $\tau(\alpha) = \beta$.

If $\tau\colon E \to E$ is an F-automorphism, then τ maps $m_{\alpha,F}$ to itself so that $\tau(\alpha) = \beta$ is a root of $m_{\alpha,F}$. □

Definition 3.12. Let E/F be an extension. We say that $\alpha, \beta \in E$ are conjugate over F if there exists an F-automorphism of E taking α to β.

Ex. 3.13. Find the splitting fields (in $\mathbb{C}$) of (i) $(x^4 - 4) \in \mathbb{Q}[x]$ and (ii) $x^3 - 2 \in \mathbb{Q}[x]$.

Definition 3.14. An extension E/F is said to be *normal* iff every irreducible polynomial in $F[x]$ that has a root in E splits over E, that is, any polynomial $f \in F[x]$ that has a root in E has all its roots in E.

Theorem 3.15. *An extension E/F is a splitting field of some polynomial $f \in F[x]$ if the extension E/F is finite and normal.*

Proof. Let E/F be a finite and normal extension. We then can write $E = F(\alpha_1, \ldots, \alpha_n)$. Each α_i is algebraic over F, say, with minimal polynomial p_i, $1 \leq i \leq n$. Since p_i has a root, namely, α_i in E and since E/F is normal, it follows that each p_i splits in E over F. Hence $p(x) = p_1(x) \cdots p_n(x)$ also splits in E over F. Clearly $E = \text{Split}(p(x); F)$.

Conversely, let $E = \text{Split}(f(x); F)$. Assume that $E = F(\alpha_1, \ldots, \alpha_n)$ where α_i are the roots of $f(x)$. By Corollary 3.5, $|E : F| \leq n!$. Let $p(x) \in F[x]$ be an irreducible polynomial with a root $\alpha \in E$. Consider $p(x)$ as an element in $E[x]$. Let $K := \text{Split}(p(x); E)$. Note that $F \leq E \leq K$. Let $\beta \in K$ be any root of $p(x)$. We need to show that $\beta \in E$. By Corollary 3.8, there exists an F-isomorphism $F(\alpha) \simeq F(\beta)$. Consider the field $E(\beta)$. We have

$$E(\beta) = F(\alpha_1, \ldots, \alpha_n)(\beta) = F(\alpha_1, \ldots, \alpha_n, \beta) = F(\beta)(\alpha_1, \ldots, \alpha_n).$$

This shows that $E(\beta) = \text{Split}(f(x); F(\beta))$. Also, since $\alpha \in E$ and $E = \text{Split}(f(x); F)$, we infer that $E = \text{Split}(f(x); F(\alpha))$. Hence the isomorphism $F(\alpha) \simeq F(\beta)$ extends to an isomorphism of E to $E(\beta)$ in such a way that $\alpha \mapsto \beta$ and $u \mapsto u$ for $u \in F$. In particular, $|E : F| = |E(\beta) : F|$. We have, by the tower law,

$$|E : F| = |E(\beta) : F| = |E(\beta) : E||E : F|.$$

Since $|E : F|$ is finite, we conclude that $|E(\beta) : E| = 1$, that is, $E(\beta) = E$ or $\beta \in E$. □

Example 3.16. Let E be splitting field of $x^p - 1$ over $\mathbb{Q}$, where p is a prime. Then $E = \mathbb{Q}(\xi)$ where $\xi := e^{\frac{2\pi i}{p}}$. Then all the roots of $x^p - 1$ are of the form ξ^j where $0 \leq j \leq p-1$. obviously, $\xi^j \in \mathbb{Q}(\xi)$. Hence $E = \mathbb{Q}(\xi)$. Since $x^p - 1 = (x-1)(1 + x + \cdots + x^{p-1})$, all the roots of $1 + x + \cdots + x^{p-1}$ are of the form ξ^j for $1 \leq j \leq p-1$. We also know from Ex. 1.13 that this polynomial is irreducible. It follows that $|\mathbb{Q}(\xi) : \mathbb{Q}| = p - 1$.

Example 3.17. Let $p \geq 3$ be a prime and $a \neq 0$. Assume that $x^p - a$ is *irreducible*. We now look at the splitting field of $f(x) = x^p - a$ over $\mathbb{Q}$.

Let $\alpha \in \mathbb{R}$ be such that $\alpha^p = a$. Let $\xi := e^{\frac{2\pi i}{p}}$ be a primitive p-th root of unity. Then $\{\alpha\xi^j : 1 \leq j \leq p\}$ are roots of $x^p - a$. Since these elements are distinct, these are all the roots of $x^p - a$. Hence $\text{Split}(x^p - a; \mathbb{Q}) = \mathbb{Q}(\alpha, \xi)$.

What is the degree $|\mathbb{Q}(\alpha, \xi) : \mathbb{Q}|$? Since α is a root of $x^p - a$, we see that $\min(\alpha, \mathbb{Q}(\xi))$ has degree at most p. Thus, $|\mathbb{Q}(\alpha, \xi) : \mathbb{Q}(\xi)| \leq p$. By the last example, $|\mathbb{Q}(\xi) : \mathbb{Q}| = p - 1$. It follows that

$$|\mathbb{Q}(\alpha, \xi)| = |\mathbb{Q}(\alpha, \xi) : \mathbb{Q}(\xi)| \cdot |\mathbb{Q}(\xi) : \mathbb{Q}| \leq (p-1) \cdot p.$$

Since $x^p - a$ is irreducible by hypothesis, we also have

$$|\mathbb{Q}(\alpha, \xi)| = |\mathbb{Q}(\alpha, \xi) : \mathbb{Q}(\alpha)| \cdot |\mathbb{Q}(\alpha) : \mathbb{Q}| = |\mathbb{Q}(\alpha, \xi) : \mathbb{Q}(\alpha)| \cdot p.$$

Thus the required degree is divisible both by p and $p-1$ and is at most $p(p-1)$. Hence it is $p(p-1)$.

Example 3.18. The last example begs the question: When is $x^p - a$ irreducible? Our answer uses the existence of splitting fields!

Let $f(x) = x^p - a \in F[x]$, where p is a prime. Then f is reducible iff it has a root in F.

If f has a root in F, then f is reducible. Before proving the converse, let us pay heed to our intuition. It says the roots are likely to be of the from $\alpha\xi$ where $\alpha^p = a$ and ξ is a p-th

root of unity. To exploit this idea, let us assume that f is reducible and produce a p-th root of a in F. We start with $E = \mathrm{Split}(x^p - a; F)$ and write

$$x^p - a = (x - \alpha_1) \cdots (x - \alpha_p).$$

If $\alpha_1 = 0$, then f has a root in F. So assume that $\alpha := \alpha_1 \neq 0$. If we let $\xi_i := \alpha_i/\alpha$, then the equation $\xi^p = a/a = 1$ shows that ξ is a p-th root of unity. Thus, for each i, we have $\alpha_i = \xi_i \alpha$. Since $x^p - a = (x - \xi_1\alpha)(x - \xi_2\alpha) \cdots (x - \xi_p\alpha)$, and the constant term lies in F, we conclude that $\xi_1 \cdots \xi_p \cdot \alpha^p = \xi_1 \cdots \xi_p \cdot a \in F$. It follows that $\xi_1 \cdots \xi_p \in F$.

Now, let $f(x) = g(x)h(x)$ be a proper factorization. Assume that $\deg g = r < n$. In $E(x)$, thanks to unique factorization, we see that g must be a product of r terms of the form $(x - \alpha_i)$. WLOG, we let $g(x) = (x - \alpha_1) \ldots (x - \alpha_r)$. Observe that $\alpha_1 \cdots \alpha_r = \xi_1 \cdots \xi_r \alpha^r = \xi\alpha^r \in F$ where $\xi = \xi_1 \cdots \xi_r$. Note that $\xi^p = 1$. Since r and p are relatively prime, there exist integers m and n such that $mr + np = 1$. We have

$$\xi^m \alpha = \xi^m \alpha^{mr+np} = (\xi\alpha^r)^m (\alpha^p)^n \in F.$$

What is $(\xi^m\alpha)^p = (\xi^p)^m \alpha^p = a$. Thus, the element $\xi^m\alpha \in F$ is a p-th root of a. That is, $f(x) = x^p - a$ has a root in F.

Example 3.19. $f(x) = x^6 - 1$ over $\mathbb{Q}$. We factorize f as

$$f(x) = (x^3 - 1)(x^3 + 1) = (x - 1)(x^2 + x + 1)(x + 1)(x^2 - x + 1).$$

If ξ is a primitive 3rd root of unity, then

$$f(x) = (x - 1)(x - \xi)(x - \xi^2)(x + 1)(x + \xi)(x + \xi^2).$$

Thus, $\mathbb{Q}[\xi]$ is the splitting field of f over $\mathbb{Q}$. We have $|\mathbb{Q}(\xi) : \mathbb{Q}| = 2$.

Example 3.20. $f(x) = x^6 + 1$ over $\mathbb{Q}$.

Keeping the notation of the last example. Then the roots are $\pm i$, $\pm i\xi$, $\pm i\xi^2$. Hence $\mathbb{Q}(\xi, i)$ is the splitting field of f over $\mathbb{Q}$. Since $\xi = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, we find that $\xi \notin \mathbb{Q}(i)$. Hence we conclude that $|\mathbb{Q}(i, \xi) : \mathbb{Q}| = 4$.

Lemma 3.21. *Let E/F be an extension. Let $F \leq K \leq E$ be such that K/F is the splitting field of a polynomial $f(x) \in F[x]$. Let σ be an automorphism of E which fixes F pointwise. Then $\sigma(K) \subset K$.*

Proof. Let $u \in K$. Since K/F is normal, u is algebraic over F, say, with $p(x) = \min(u; F)$. Since K is the splitting field of $f(x)$, it is a normal extension by Theorem 3.15. Hence $\sigma(u)$ must be a root of f. Hence $\sigma(u) \in K$. □

Example 3.22. $f(x) = x^2 + ax + b \in F[x]$.

Ex. 3.23. Show that $x^2 - 3$ and $x^2 - 2x - 2$ both have the same splitting field over $\mathbb{Q}$.

Ex. 3.24. Show that $\mathrm{Split}(x^4 - 4x^2 - 5; \mathbb{Q})$ is of degree 4 over $\mathbb{Q}$.

Ex. 3.25. Let $F \leq K \leq E$. Assume that $E = \mathrm{Split}(f(x); F)$. Show that $E = \mathrm{Split}(f(x); K)$.

Ex. 3.26. If $\alpha \in E$ is algebraic over F and $E = F(\alpha)$ is normal, show that $E = \mathrm{Split}(\min(\alpha, F); F)$.

Ex. 3.27. Find the splitting fields of the following polynomials over $\mathbb{Q}$. Also, find the degrees of the splitting fields over $\mathbb{Q}$. (i) $x^4 - 1$, (ii) $(x^2 - 2)(x^2 - 3)$, (iii) $x^3 - 3$, (iv) $x^3 - 1$, (v) $(x^2 - 2)(x^3 - 2)$.

Ex. 3.28. Find the splitting fields over $\mathbb{Q}$ of the following polynomials and find their degree over $\mathbb{Q}$: (i) $x^6 - 1$, (ii) $x^6 + 1$ and (iii) $x^6 - 27$.

Ex. 3.29. Show that the splitting field of $x^4 + 3$ over $\mathbb{Q}$ is $\mathbb{Q}(i, \alpha\sqrt{2})$, where $\alpha = \sqrt[4]{3}$. What is its degree over Q?

Ex. 3.30. Let $E : F$ be a finite extension which is the splitting field of a set of polynomials in $F[x]$. Show that E is the splitting field of a single polynomial in $f[x]$.

Ex. 3.31. Let $|E : F| = 2$. Show that E is the splitting field over F.

Ex. 3.32. Let E be a splitting field of $f(x) \in F[x]$. Show that any F-automorphism of E permutes the roots of f.

4 Separable Extensions

Topics: Formal derivative, An irreducible polynomial over a field of characteristic 0 has only simple roots, An irreducible polynomial f over a field of characteristic p has only multiple roots iff its is of the form $f(x) = g(x^p)$. All roots of an irreducible polynomial have the same multiplicity.

Separable polynomial, separable extension, perfect fields, fields of characteristic 0 and finite fields are perfect.

Definition 4.1. Let $f = a_0 + a_1x + \cdots + a_nx^n \in F[x]$. Then the formal derivative $Df \in F[x]$ is defined by $Df = a_1 + 2a_2x + \cdots + na_nx^{n-1}$. Note that $D\colon F[x] \to F[x]$ is F-linear.

Definition 4.2. Let $f \in F[x]$. An element $\alpha \in E$ where E/F is an extension field, is said to be *repeated root* of f (or a root of f with multiplicity m) if $(x-\alpha)^m$ with $m \geq 2$ is a divisor of f in $E[x]$. A root of f, which is not a repeated root is called a simple root.

Proposition 4.3. *Let $(x) \in F[x]$ be nonzero. Let E be the splitting filed of $f(x)$. Then the following are equivalent:*

(i) *f has a repeated root in E.*

(ii) *There exists $\alpha \in E$ such that $f(\alpha) = 0 = (Df)(\alpha)$.*

(iii) *There exists a non-constant polynomial $g \in F[x]$ that divides both f and its derivative Df in $F[x]$.*

Proof. Let (i) hold. Then there exists $\alpha \in E$ and $k \geq 2$ such that $f(x) = (x-\alpha)^k g(x) \in E[x]$. Clearly, $f(\alpha) = 0 = (Df)(\alpha)$. Hence (ii) is true.

Let (ii) hold. Let $g := \min(\alpha, F)$. Since $f(\alpha) = 0 = (Df)(\alpha)$, it follows that f and Df lie in the kernel of the evaluation homomorphism $h(x) \mapsto h(\alpha)$. Since the kernel is the principal ideal $(g) \subset F[x]$, the polynomial g is a common divisor of both f and Df. That is, (iii) is proved.

Suppose that (iii) holds. Write $f(x) = g(x)h(x) \in F[x]$. Since f splits in E, we see that g also splits in E. Let $\alpha \in E$ be a root of g. We then have $f(\alpha) = 0$ and $f(x) = (x-\alpha)h(x)$ for some $h(x) \in E[x]$. Now, $Df(x) = h(x) + (x-\alpha)(Dh)(x)$. Since g divides both f and Df and since $(x-\alpha)$ divides $g(x)$, it follows that $(x-\alpha)$ is a divisor of $h(x) = Df(x) - (x-\alpha)(Dh)(x)$, say, $h(x) = (x-\alpha)h_1(x)$. But then $f(x) = (x-\alpha)(x-\alpha)h_1(x)$. Thus, α is a repeated root of f in E, the splitting field of $f(x)$. □

Ex. 4.4. An irreducible polynomial $f(x) \in F[x]$ is not separable iff $Df = 0$.

Proposition 4.5. *Let $f(x) \in F[x]$ be irreducible. Then f is not separable iff (i) the characteristic of F is a prime p and (ii) $f(x) = g(x^p)$, that is, $f(x) = a_0 + a_1x^p + a_2x^{2p} + \cdots + a_nx^{np}$.*

Proof. Assume that f is not separable. Hence there exists a non-constant $g(x) \in F[x]$ such that g divides f and Df. Since f is irreducible and $g|f$, we deduce that f and g are associates. Since g and hence f divides Df, a polynomial of degree less than that of f, it follows that $Df(x) = 0$. But this means that each of the coefficients of $Df(x)$ is zero, say, $ka_k = 0$. If $a_k \neq 0$, this can happen iff the characteristic of F is $p > 0$ and k is a multiple of p. □

Corollary 4.6. *An irreducible polynomial over a field F of characteristic 0 has only simple roots. Hence every $f(x) \in F[x]$ is separable.*

Proof. Let $f(x) \in F[x]$ be irreducible. If f has a repeated root, then f and Df have a non-constant divisor. This violated the irreducibility of f. □

Definition 4.7. An irreducible polynomial $f \in F[x]$ is said to be *separable* over F iff f does not have multiple roots in a splitting field of f.

A polynomial is said to be separable iff each of its irreducible factors is separable over F.

Corollary 4.8. *An irreducible polynomial is separable iff* $Df = 0$. □

Definition 4.9. An algebraic extension E/F is said to be separable iff the minimal polynomial of each element of E is separable over F.

Corollary 4.10. *Let F be a field of characteristic 0. Then every polynomial in $F[x]$ is separable over F and hence every algebraic extension E/F is separable.* □

Example 4.11. Let $\operatorname{Char} F = p > 0$. Let $a \in F$ be such that $f(x) = x^p - a$ has no root in F. We claim that f is an inseparable polynomial. For, if α, β are roost of $f(x)$ in a splitting field, we have $\alpha^p = a = \beta^p$. Hence $(\alpha - \beta)^p = \alpha^p - \beta^p = 0$. Hence we have $\alpha = \beta$. Thus f has only one root, say, α, with multiplicity p. We now show that f is irreducible. If g is an irreducible factor of f, then $\gamma(ga) = 0$. Hence $g = \min(\alpha, F)$ and so g divides f. Since $\deg f = p$ and $\deg g \geq 1$, it follows that $\deg = p$ and hence $f = g$.

In particular, if $E = F(y)$, where y is transcendental, then $f(x) = x^p - y \in E[x]$ is irreducible. Any extension K/E in which f has a root will be inseparable.

Example 4.12. Let $F := \mathbb{Z}_p(t)$ where t is an indeterminate. Consider $f(x) := x^p - t \in F[x]$. We claim that f is irreducible but not separable.

It is irreducible by Eisenstein criterion with t as the prime for testing.

If α is a root of f in a splitting field, then

$$(x - \alpha)^p = x^p - \alpha^p = x^p - t.$$

Thus it has multiple roots.

Ex. 4.13. Assume that $\gcd(f(x), DF(x)) = 1$. Prove that f is separable.

Ex. 4.14. Let $f(x) \in F[x]$ be irreducible. Show that f is separable iff $Df(x) \neq 0$.

Ex. 4.15. Assume that $\operatorname{Char} F = 0$ and K is the splitting field of $f(x) \in F[x]$. Let $d(x) = \gcd(f(x), Df(x))$. Let $g(x)$ be defined by $f(x) = d(x)g(x)$. Show that the roots of f and g are the same and that g is separable.

Ex. 4.16. Let F be infinite. Let $\alpha, \beta \in E$ are algebraic over F. Assume that α is the root of a separable polynomial in $F[x]$. Show that $F(\alpha, \beta)$ is a simple extension.

5 Finite Fields

Topics: Existence, uniqueness, cyclicity of a finite subgroups of F^*, subfields of finite fields, Primitive element theorem.

Let R be a ring. Recall that for $n \in \mathbb{N}$, the element $n \cdot 1 = 1 + \cdots + 1$ (n-times). If for each $n \in \mathbb{N}$, we have $n \cdot 1 \neq 0$, we then say that the *characteristic* of R is 0 (zero). If there exists an $n \in \mathbb{N}$ with $n \cdot 1 = 0$ and if p is the least such with this property, then R is said to have positive characteristic p.

Lemma 5.1. *Let R be an integral domain. Then the characteristic of R is either 0 or a prime $p \in \mathbb{N}$.*

Proof. Let the characteristic of R be positive $m \in \mathbb{N}$. If m is composite, say $m = pq$ with p and q nonunits, then $p \cdot 1 \neq 0 \neq q \cdot 1$ but their product is zero. □

Lemma 5.2. *(i) The set $P := Z \cdot 1 = \{n \cdot 1 : n \in \mathbb{Z}\}$ is a subring of R, called the prime ring.*
(ii) $P \simeq \mathbb{Z}$ if the characteristic of R is 0.
(iii) $P \simeq \mathbb{Z}_m$ if the characteristic of R is m. □

Corollary 5.3. *The characteristic of any finite field F is a prime $p \in \mathbb{N}$ and we have $\mathbb{Z}_p \leq F$. Furthermore, $|F| = p^n$ for some $n \in \mathbb{N}$.*

Proof. $F : \mathbb{Z}_p$ is a finite extension. □

Lemma 5.4. *Let F be a field of characteristic $p > 0$. Then $(x + y)^{p^n} = x^{p^n} + y^{p^n}$ and $(xy)^{p^n} = x^{p^n} y^{p^n}$ for all $x, y \in F$. In particular, $x \mapsto x^p$ is an injective field homomorphism of F to itself.*

Proof. Observe that the standard binomial theorem is valid in any commutative ring and except for the extreme terms, all the binomial coefficients $\binom{p^n}{r}$, $r \neq 0, p^n$ are divisible by p. □

Theorem 5.5. *A field E has p^n elements iff it is a splitting field of the polynomial $x^{p^n} - x$ over its prime subfield $\mathbb{Z}_p$.*

Proof. Let $K := \text{Split}(p(x) := x^{p^n} - x; \mathbb{Z}_p)$. Let E be the set of roots of the polynomial $x^{p^n} - x$. Since $Dp(x) = -1$, we see that p is separable and hence all the roots of $p(x)$ are distinct. Using Lemma 5.4, one easily shows that E is a field. Since K is the splitting field of $p(x)$, we conclude that $E = K$. In particular, $|K| = p^n$.

To prove the converse, observe that the multiplicative group E^* is of order $p^n - 1$. Hence for any $a \in E^*$, we have $a^{p^n - 1} = 1$ and hence $a^{p^n} = a$. Also, $0 \in E$ has the same property. Thus, all elements of E are roots of the polynomial $x^{p^n} - x$. Since $|E| = p^n$, it follows that E is the splitting field of $p(x) = x^{p^n} - x$ over $\mathbb{Z}_p$. □

Corollary 5.6. *There exists a finite field $GF(p^n)$ of order p^n for each prime p and $n \in \mathbb{N}$. Two finite fields are isomorphic iff they have the same number of elements.*

Proof. The splitting field of $x^{p^n} - x$ over $\mathbb{Z}_p$ exists by Corollary 3.5. Its order is p^n by the last theorem.

If two fields E and K have the same order p^n, then they the splitting fields of $x^{p^n} - x$ over $\mathbb{Z}_p$ by Theorem 5.5. Then K and E are isomorphic by Corollary 3.10. □

The field $GF(p^n)$ is called the Galois field of order p^n.

Theorem 5.7. *Let G be a finite subgroup of F^*, the multiplicative group of a field F. Then G is cyclic.*

In particular, if F is a finite field, then F^* is cyclic.

Proof. Let $a \in G$ be of maximal order, say, m. Then $o(g)|o(a)$ for any $g \in G$. Hence $g^m = 1$ for every $g \in G$. That is, every $g \in G$ is a root of the polynomial $x^m - 1$. This polynomial has at most m roots in F. Hence $|G| \leq m$. But $\{a^k : 1 \leq k \leq m\}$ are m distinct elements. Hence we conclude that $G = \langle a \rangle$. □

Ex. 5.8. Let R be a ring with prime characteristic p. The map $\varphi\colon x \mapsto x^p$ is called the Frobenius map and it is a ring homomorphism. It is one-one if R is an integral domain.

Ex. 5.9. Let K be a field of characteristic p. Fix $r \in \mathbb{N}$. Then the subset $F := \{x \in K : \varphi^r(x) = x\}$ is a subfield of K.

Ex. 5.10. Let K be a finite field with p^n elements. Then any subfield K has p^r elements for $1 \leq r \leq n$ with r dividing n. Furthermore, for any such r, there exists a unique subfield $F \leq K$ with p^r elements. *Hint:* $F := \{x \in K : \varphi^r(x) = x\}$ (existence). For uniqueness, observe that if E is any such field, each of its elements is a root of $x^{p^r} - x$.

Ex. 5.11. Let E be a finite field and $F \leq E$. Then E/F is a simple extension.

Ex. 5.12. Let $p \in \mathbb{N}$ be a prime. For any $n \in \mathbb{N}$, there exists an irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ of degree n.

Ex. 5.13. Show that the Frobenius map $\varphi\colon GF(p^n) \to GF(p^n)$ is an automorphism of order n.

Ex. 5.14. Let $F := GF(p^n)$. Show that $x^{p^n} - x = \prod_{t \in F}(x - t)$.

Ex. 5.15. Let $f(x) \in \mathbb{Z}_p[x]$ be of degree greater than 1. Show the number of roots of f in $GF(p^n)$ is the degree of $\gcd(f(x), x^{p^n} - x)$. *Hint:* You may compute the gcd in $F := GF(p^n)$ where $x^{p^n} - x = \prod_{t \in F}(x - t)$. You need Ex. 2.51.

Ex. 5.16. Show that each $a \in GF(p^n)$ can be written in the form b^p for a unique $b \in GF(p^n)$.

Ex. 5.17. Show that no finite field is algebraically closed. When do we say a field is algebraically closed? Need to define.

Ex. 5.18. Show that every irreducible polynomial $f(x) \in \mathbb{Z}_p[x]$ divides $x^{p^n} - x$ for some n.

Ex. 5.19. Show that $x^{p^n} - x$ is the product of all monic irreducible polynomials in $\mathbb{Z}_p[x]$ of degree d where d runs through all divisors of n.

Theorem 5.20 (Primitive Element Theorem)**.** *Let E/F be a finite separable extension. Then $E = F(\alpha)$ for some $\alpha \in E$. Thus, any finite separable extension is simple.*

Proof. Let us start with the case when F is infinite. Let $E = F(\alpha, \beta)$. Then α and β are algebraic over F. Let f and g be the minimal polynomials of α and β. Let $K := \text{Split}(fg; F)$ be the splitting field of fg over F. Then f and g split in K. (Why?) Let $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_m$

be the roots of f. Let $\beta_1 = \beta, \beta_2, \ldots, \beta_n$ be the roots of g. Note that the roots of f and g are distinct, since the extension $E : F$ is separable.

Since F is infinite we can find a non-zero $c \notin \left\{ \frac{\beta - \beta_j}{\alpha - \alpha_i} : 1 \leq i \leq m, 1 < j \leq n \right\}$. Let $\theta = \beta - c\alpha$. We claim that $E = F(\theta)$.

Consider $h(x) = g(c(x - \alpha) + \beta) = g(cx + (\beta - c\alpha)) \in F(\theta)[x]$. Note that $f(x) \in F(\theta)[x]$. We also have $f(\alpha) = 0$ and $h(\alpha) = g(\beta) = 0$. Thus α is a common root of both f and h in $F(\theta)$. Also, for any $i \neq 1$, α_i is not a root of h. For, $c(\alpha_i - \alpha) + \beta \neq \beta_j$ for $i > 1$ and any j, by our choice of c. Hence α is the only root of h in $F(\theta)$. It follows (Why?) that $(x - \alpha)$ is the GCD of $f(x)$ and $h(x)$ in the ring $F(\theta)[x]$. This means that $\alpha \in F(\theta)$. But then $\beta = \theta + c\alpha \in F(\theta)$. Hence $E = F(\theta)$.

The general case, namely when $E = F(\alpha_1, \ldots, \alpha_n)$ follows by induction.

If F is finite, then E is finite and we know $E^* = \langle a \rangle$. Hence $E = F(a)$. □

Remark 5.21. The proof, in fact, gives us a method to find θ. In the case of characteristic 0, we can choose a non-zero integer m such that m is not of the form $\frac{\beta - \beta_j}{\alpha - \alpha_i}$. See the examples below.

Example 5.22. $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$.

Example 5.23. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Example 5.24. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + i)$.

Example 5.25. Lest that you believe that $\mathbb{Q}(\alpha, \beta)$ is always $\mathbb{Q}(\alpha + \beta)$, we look at another example. $\mathbb{Q}(\sqrt{2} + i, \sqrt{3} - i) = \mathbb{Q}((\sqrt{3} - i) - (\sqrt{2} + i))$.

Example 5.26. Let $F := \mathbb{Z}_2(t)$ be the field of rational functions over $\mathbb{Z}_2$. Consider $f(x) := x^2 - t$ and $g(x) = x^2 - (t + t^3)$. Let α and β be roots of f and g in a splitting field. We have $\alpha^2 = t$ and $\beta^2 = t + t^3$. It is easy to see that f is irreducible over $F(\beta)$ and g is irreducible over $F(\alpha)$. We therefore have $|F(\alpha, \beta) : F| = 4$. Let $\theta \in F(\alpha, \beta)$. We write it as $\theta = p(t) + q(t)\alpha + r(t)\beta$. On squaring, we get

$$\theta^2 = p(t)^2 + q(t)^2\alpha^2 + r(t)^2\beta^2 = p(t)^2 + tq(t)^2 + (t + t^3)r(t)^2 \in F(t).$$

In particular, $|F(\theta) : F| \leq 2$ for any $\theta \in F(\alpha, \beta)$. This shows that we cannot find a primitive element for the extension $F(\alpha, \beta) : F$.

6 Galois Group

Topics: Galois group: Definition and examples.

Definition 6.1. Let E/F be an extension. The set of all automorphisms σ of F that leave F pointwise fixed is a group under composition and it is called the Galois group of E/F. We let $\mathrm{Gal}\,(E/F)$ denote this group.

The following simple observation is the moving principle of Galois theory!

Lemma 6.2. *Let E/F be an extension. Let $f(x) \in F[x]$ and let $\alpha \in E$ be a root of f and $\sigma \in \mathrm{Gal}\,(E/F)$. Then $\sigma(\alpha)$ is a root of f.* □

Proposition 6.3. *Let E/F be the splitting field of $f(x) \in F[x]$. Let $\alpha, \beta \in E$. Then there exists $\sigma \in \mathrm{Gal}\,(E/F)$ iff $\min(\alpha, F) = \min(\beta, F)$.*

Proof. If $\alpha, \beta \in E$ have the same polynomial, then there is an F-isomorphism $\sigma\colon F(\alpha) \simeq F(\beta)$ such that $\sigma(\alpha) = \beta$. Since E is also the splitting field of $f(x)$ over $F(\alpha)$ as well over $F(\beta)$, there exists an extension $\tau\colon E \to E$ which extends σ. In particular, $\tau \in \mathrm{Gal}\,(E/F)$ and $\tau(\alpha) = \beta$.

The converse follows from the last lemma. □

Lemma 6.4. *Let $E = F(\alpha_1, \ldots, \alpha_n)$ be an algebraic extension over F. If $\sigma, \tau \in \mathrm{Gal}\,(E/F)$ are such that $\sigma(\alpha_i) = \tau(\alpha_i)$ for $1 \leq i \leq n$, then $\sigma = \tau$.*

Proof. Prove this by induction on n. Note that any $u \in E$ is a polynomial p in $\alpha = \alpha_1$ and hence $\sigma(p(\alpha)) = \tau(p(\alpha))$. □

Corollary 6.5. *If $E = \mathrm{Split}(f(x); F)$ and if f is separable of degree n, then $\mathrm{Gal}\,(E/F)$ is isomorphic to a subgroup of S_n and hence $|\mathrm{Gal}\,(E/F)|$ is a divisor of $n!$*

Proof. Let $\alpha_, \ldots, \alpha_n$ be the distinct roots of f and $\sigma \in \mathrm{Gal}\,(E/F)$. Then σ induces a permutation of the set $\{\alpha_i : 1 \leq i \leq n\}$. Distinct elements of $\mathrm{Gal}\,(E/F)$ induce distinct permutations. □

Theorem 6.6. *Let $f(x) \in F[x]$ be separable. Let $E := \mathrm{Split}(f(x); F)$. Then $|\mathrm{Gal}\,(E/F)| = |E : F|$.*

Proof. First observe that E/F is separable. By the primitive element theorem, there exists $\alpha \in E$ such that $E = F(\alpha)$. Let $p(x) = \min(\alpha, F)$. Let $n = \deg p(x)$. Note that $p(x)$ and α are separable. We have $|E : F| = |F(\alpha) : F| = \deg p(x) = n$. Since E is the splitting field and since $\alpha \in E$, all the roots, say, $\alpha = \alpha_1, \ldots, \alpha_n$ of $p(x)$ lie in E. They are all distinct, since E is separable. By Proposition 6.3, there exist distinct elements (why?) $\sigma_i \in \mathrm{Gal}\,(E/F)$ such that $\sigma_i(\alpha) = \alpha_i$. Thus $\mathrm{Gal}\,(E/F)$ has at least n elements. If $\sigma \in \mathrm{Gal}\,(E/F)$, then $\sigma(\alpha)$ must be one of α_i's and hence σ must be σ_i. We therefore conclude that $\mathrm{Gal}\,(E/F) = n$. □

Example 6.7. We compute the Galois group $\mathrm{Gal}\,(\mathbb{C}/\mathbb{R})$.

Let $\sigma \in \mathrm{Gal}\,(\mathbb{C}/\mathbb{R})$. Then $\sigma(i)$ must be a root of the minimal polynomial $z^2 + 1$ of i. Hence $\sigma(i) = \pm i$. The maps $\mathbf{1}(a + ib) = a + ib$ and $\sigma(a + ib) = a - ib$ are $\mathbb{R}$-automorphisms of $\mathbb{C}$. Hence $\mathrm{Gal}\,(\mathbb{C}/\mathbb{R}) = \langle\sigma\rangle$.

Example 6.8. Let us look at the Galois group $\mathrm{Gal}\,(\mathbb{Q}(2^{1/3})/\mathbb{Q})$. If σ is an element of this group, then $\sigma(2^{1/3})$ must be a root of the polynomial x^3-2. Its roots are $\alpha := 2^{1/3}, \alpha\xi$ and $\alpha\xi^2$ where ξ is a primitive cube root of unity. Except α, no other root lies in $\mathbb{Q}(2^{1/3}) \subset \mathbb{R}$. This is a facile argument. For, this argument uses an extraneous data such as our knowledge of complex numbers and that all roots of x^3-2 can be found in $\mathbb{C}$ etc.

A correct way of showing this is to show that the function $x \mapsto x^3-2$ in strictly increasing and hence it has a unique zero in $\mathbb{R}$. As $\mathbb{Q}(2^{1/3}) \subset \mathbb{R}$, the only root of x^3-2 in $\mathbb{Q}(2^{1/3})$ is $2^{1/3}$. Hence $\sigma(2^{1/3}) = 2^{1/3}$.

Hence $\sigma(2^{1/3}) = 2^{1/3}$ and hence we conclude that the Galois group is trivial.

Note that we used Lemmas 6.2 and 6.4 to arrive at the conclusion.

Example 6.9. Galois group G of $\mathrm{Split}((x^2-2)(x^2-3);\mathbb{Q})$.

By Lemma 6.2, any $\sigma \in G$ must take $\sqrt{2}$ to either $\sqrt{2}$ or to $-\sqrt{2}$. Similarly, $\sigma(\sqrt{3}) \in \{\pm\sqrt{3}\}$. Thus G has at most 4 elements:

$$\begin{array}{cccc} 1 & \tau & \alpha & \beta \\ \sqrt{2}\mapsto\sqrt{2} & \sqrt{2}\mapsto-\sqrt{2} & \sqrt{2}\mapsto\sqrt{2} & \sqrt{2}\mapsto-\sqrt{2} \\ \sqrt{3}\mapsto\sqrt{3} & \sqrt{3}\mapsto\sqrt{3} & \sqrt{3}\mapsto-\sqrt{3} & \sqrt{3}\mapsto-\sqrt{3} \end{array}$$

We now show that there do exist such elements in the Galois group. Let us construct τ. Since x^2-2 is the minimal polynomial of both $\pm\sqrt{2}$, there exists a $\mathbb{Q}$-isomorphism of $\mathbb{Q}(\sqrt{2})$ to $\mathbb{Q}(-\sqrt{2})$. Since $\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q} = 4$, it follows that the minimal polynomial x^2-3 of $\sqrt{3}$ is also the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$. Hence σ extends to a $\mathbb{Q}$-automorphism τ such that $\tau(\sqrt{3}) = \sqrt{3}$. Thus, $\tau \in G$ exists with the required properties.

Arguing similarly, we construct the other elements α and β of G. It is easy to check that each of τ, α and β is of order 2. We conclude that $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Question: What is $\beta \circ \alpha$?

Example 6.10. Let us find the Galois group G of the splitting field E of x^3-2 over $\mathbb{Q}$. Let $\alpha := 2^{1/3}$ be the unique cube root of 2. Let ξ be a primitive cube root of unity. Then the roots of x^3-2 are $\alpha, \alpha\xi, \alpha\xi^2$. By Proposition 6.3, there exists $\sigma \in G$ which takes α to $\alpha\xi$.

If $\alpha(\xi) = \xi$, then $\sigma(\alpha\xi^2) = \alpha$ so that σ may be considered as the cycle $(123) \in S_3$.

If $\alpha(\xi) = \xi^2$, then $\sigma(\alpha\xi^2) = \alpha\xi^2$ so that σ may be considered as the transposition $(12) \in S_3$.

By Corolalry 6.5, we have $\mathrm{Gal}\,(E/\mathbb{Q})$ is a subgroup of S_3. From Theorem 6.6, we know $|\mathrm{Gal}\,(E/\mathbb{Q})| = |E : \mathbb{Q}| = 6$. Hence $\mathrm{Gal}\,(E/\mathbb{Q})$ is a subgroup of order 6 in S_3. Hence we conclude that $\mathrm{Gal}\,(E/\mathbb{Q}) = S_3$.

Example 6.11. We now compute the Galois group of $\mathrm{Split}((x^p-1);\mathbb{Q})$ where p is a prime.

Let $\xi := e^{\frac{2\pi i}{p}}$. Then ξ is a primitive p-th root of unity and ξ^k, $0 \le k < p$ are all the roots of the polynomial x^p-1. Hence $\mathrm{Split}(x^p-1;\mathbb{Q})$ is $\mathbb{Q}(\xi)$. We know from Theorem 2.12 that $|\mathbb{Q}(\xi) : \mathbb{Q}| = p-1$.

Now if σ is an element of the Galois group, then $\sigma(\xi) = \xi^k$ for some $1 \le k \le p-1$ by Lemma 6.2. Note that if $\sigma(\xi) = \xi^r$ and $\tau(\xi) = \xi^s$ with $r \ne s$, (where $1 \le r, s \le p-1$), then $\sigma \ne \tau$. It follows that $|\mathrm{Gal}\,(\mathbb{Q}(\xi)/\mathbb{Q})| \le p-1$.

Note that $\mathbb{Q}(\xi^k) = \mathbb{Q}(\xi)$ for $1 \le k \le p-1$. Using Proposition 6.3, we see that there do exist $\mathbb{Q}$-isomorphisms σ_k of $\mathbb{Q}(\xi)$ onto $\mathbb{Q}(\xi^k)$ such that $\sigma_k(\xi) = \xi^k$, for $1 \le k \le p-1$. These are, of course, $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\xi)$ and hence elements of the Galois group.

We claim that the Galois group is Abelian, in fact, cyclic. For, if we let $\sigma(\xi) = \xi^2$, then σ^j, $1 \le j \le p-1$ are all distinct. See also the next example.

Example 6.12. Let $\xi \in \mathbb{C}$ be a primitive n-th root of unity. Let $E := F(\xi)$. Then $\mathrm{Gal}\,(E/\mathbb{Q})$ is isomorphic to a subgroup of $U(\mathbb{Z}_n)$, the group of units modulo n.
(i) In particular, $\mathrm{Gal}\,(E/\mathbb{Q})$ is abelian.
(ii) If $n = p$, a prime, then $\mathrm{Gal}\,(E/\mathbb{Q})$ is cyclic.

If $\sigma \in \mathrm{Gal}\,(E/F)$, then $\sigma(\xi) = \xi^j$ where j is unique modulo n. Also, since σ is an automorphism, $\sigma(\xi)$ must be a primitive root of unity. Thus, j is relatively prime to n. Denote it by σ_j. We thus have a map

$$\varphi\colon \mathrm{Gal}\,(E/\mathbb{Q}) \to U(\mathbb{Z}_n) \text{ given by } \sigma_j \mapsto [j] \in U(\mathbb{Z}_n).$$

It is easy to see that this map is a group homomorphism.

$$\sigma_i\sigma_j(\alpha) = \alpha_i(\alpha^j) = \alpha^{ij}.$$

Hence $\varphi(ij) = [ij] = \varphi(i)\varphi(j)$.

Let us look at a special case. Let $n = 8$. If ξ is the a primitive 8th root of unity, then $|\mathbb{Q}(\xi) : \mathbb{Q}| = 4$. The minimal polynomial of ξ over $\mathbb{Q}$ is $x^4 + 1$. The possible automorphisms correspond to the maps

$$\xi \mapsto \xi, \xi \mapsto \xi^3, \xi \mapsto \xi^5, \xi \mapsto \xi^7.$$

If we list the roots of the minimal polynomial in the order $\xi, \xi^3, \xi^5\xi^7$, then the automorphism σ which sends ξ to ξ^3 has the following action:

$$\xi \mapsto \xi^3, \xi^3 \mapsto \xi, \xi^5 \mapsto \xi^7, \xi^7 \mapsto \xi^5.$$

Thus it corresponds to $(12)(34) \in S_4$. Similarly, σ which send ξ to ξ^5 corresponds to $(13)(24)$ and the last one to $(14)(23)$. Thus we arrive at

$$\mathrm{Gal}\,(E/Q) = \{e, (12)(34), (13)(24), (14)(23)\} \leq S_4.$$

Example 6.13. Let $f(x) := x^n - c \in \mathbb{Q}[x]$. Let $F := \mathbb{Q}(\xi)$ where ξ is a primitive n-th root of unity. Let $E := \mathrm{Split}(f(x); F)$. To compute $\mathrm{Gal}\,(E/F)$ we proceed as in the last example. Let α be a root of f. The roots of f are $\alpha\xi^j$, $0 \leq j \leq n-1$. If $\sigma \in \mathrm{Gal}\,(E/F)$ is given, then $\sigma(\alpha) = \alpha^j$ for some j, which is unique modulo n. We denote such a σ by σ_j. The map $\varphi\colon \mathrm{Gal}\,(E/F) \to \mathbb{Z}_n$ is given by $\varphi(\sigma_j) = [j]$. This map is easily checked to be a one-one homomorphism.

When is this map onto? The next exercise answers this question.

Ex. 6.14. Let $f(x) \in F[x]$ be separable. Let $E = \mathrm{Split}(f(x); F)$. Then the Galois group $\mathrm{Gal}\,(E/F)$ acts transitively on the roots of f iff f is irreducible.

Let $f$be separable and irreducible with distinct roots $\alpha_1, \ldots, \alpha_n$. The transitivity of $\mathrm{Gal}\,(E/F)$ follows from Proposition 6.3.

Let the Galois group act transitively on the roots of f. Let if possible g and h be (non-trivial) irreducible factors of f. Let α and β be their roots. There exists $\sigma \in \mathrm{Gal}\,(E/F)$ such that $\sigma(\alpha) = \beta$. Hence we have

$$0 = \sigma(g(\alpha)) = g(\sigma(\alpha)) = g(\beta).$$

Hence h is a factor of g. Since both g and h are irreducible, it follows that $g = h$ and that g^2 is a factor of f. This contradicts the separability of f. Hence f is irreducible.

Another way of seeing this is as follows: Let α_i, $1 \leq i \leq n = \deg f$ be the roots of f in E. Since f is separable all the roots are distinct. Let g be an irreducible factor of f. We may assume WLOG that α_1 is a root of g. Given $i > 1$, there exists $\sigma = \sigma_i \in \mathrm{Gal}\,(E/F)$ such that $\sigma(\alpha_1) = \alpha_i$. We claim that α_i is a root of g. For,

$$0 = g(\alpha_i) = \sigma(g(\alpha_1)) = g(\sigma(\alpha_1)) = g(\alpha_1).$$

It follows that all the distinct α_i's are roots of g and hence $\deg g \geq n = \deg f$. We conclude that f and g are associates and hence f is irreducible.

Example 6.15. Consider $f(x) = (x^2+1)(x^2+2)$ and $g(x) = x^4 - 2x^2 + 9$ in $\mathbb{Q}[x]$. The roots of f are $\pm i$ and $\pm i\sqrt{2}$. The roots of g are $\pm(\sqrt{2} \pm i)$. The splitting fields of f and g is $E := \mathbb{Q}(i, \sqrt{2})$. The Galois group has four elements that correspond to $i \mapsto \pm i$ and $\sqrt{2} \mapsto \pm\sqrt{2}$. Let us order the roots of f and g as follows:

$$f : (i, -i, i\sqrt{2}, -i\sqrt{2}; \quad g : (\sqrt{2}+i, \sqrt{2}-i, -\sqrt{2}+i, -\sqrt{2}-i.$$

The Galois group $\mathrm{Gal}\,(E/\mathbb{Q})$ acts on the roots of f and g. The action yields the following subgroups of S_4.

$$\mathrm{Gal}\,(f/\mathbb{Q}) = \{Id, (12, (34), (12)(34)\}$$
$$\mathrm{Gal}\,(g/\mathbb{Q}) = \{Id, (12)(34), (13)(24), (14)(23)\}.$$

Observe that $\mathrm{Gal}\,(f/\mathbb{Q})$ does not act transitively on the roots of f whereas $\mathrm{Gal}\,(g/\mathbb{Q})$ acts transitively on the roots of g.

Note that $\mathrm{Gal}\,(f/\mathbb{Q}) \simeq \mathrm{Gal}\,(E/\mathbb{Q})$ and $\mathrm{Gal}\,(g/\mathbb{Q}) \simeq \mathrm{Gal}\,(E/F)$. But they are not conjugate in S_4, since the cycle decomposition of the elements are different.

Exercise 6.14 is therefore about how the Galois group is realized as group of permutations of the roots and not about its structure as an abstract group.

Example 6.16. Galois group of $\mathrm{Split}((x^p - c); \mathbb{Q})$ where p is an odd prime. Assume that $f(x) := x^p - c$ is irreducible. (This is same as requiring that c is not a p-th power in $\mathbb{Q}$. See) Give Ref!

Let $ga := c^{1/p}$ be the unique real root of f. Let $\xi = e^{\frac{2\pi i}{p}}$ be a primitive root of unity. Then $E := \mathrm{Split}(f(x); \mathbb{Q}) = \mathbb{Q}(\xi, \alpha)$.

We have already seen that $|E : \mathbb{Q}| = p(p-1)$. In view of Theorem 6.6, we have $|\mathrm{Gal}\,(E/\mathbb{Q})| = p(p-1)$. If $\sigma \in \mathrm{Gal}\,(E/F)$, then Give Ref!

$$\sigma(\alpha) = \alpha\xi^i \quad \text{and} \quad \sigma(\xi) = \xi^j,$$

where $0 \leq i \leq p-1$ and $1 \leq j \leq p-1$. Denote suchσ by σ_{ij}. There are the elements of $\mathrm{Gal}\,(E/F)$. We now show that this group is not abelian.

$$\sigma_{11}\sigma_{12}(\alpha) = \alpha\xi^2,$$
$$\sigma_{12}\sigma_{11}(\alpha) = \alpha\xi^3.$$

We have a pretty description of this group. This is gleaned if we carry out the computation above in a more general setting.

$$\sigma_{ij} \circ \sigma_{rs}(\xi) = \xi^i r$$
$$\sigma_{ij} \circ \sigma_{rs}(\alpha) = \xi^{is+j}\alpha.$$

Thus reading modulo p in the variable i, we have

$$\sigma_{ij} \circ \sigma_{rs} = \sigma_{ir,is+j}.$$

Those who has seen affine group of $\mathbb{R}$ will immediately recognize a similar structure here. Consider $G = \mathbb{Z}_p^* \times \mathbb{Z}_p$ as sets. We define a binary operation

$$(a, b) \star (c, d) := (ac, ad + b).$$

Check that this makes G into a group called the one-dimensional affine linear group over the field $\mathbb{Z}_p$. What we have found is that $\mathrm{Gal}\,(E/F)$ is isomorphic to this affine group.

Example 6.17. Let us find $\mathrm{Gal}\,(GF(p^n)/\mathbb{Z}_p)$. We know that there exists $\alpha \in E := GF(p^n)$ such that $E = F(\alpha)$ where $F := GF(p)$. If $f(x) = \min(\alpha, F)$, then we know $\deg f = n$ and that $E = \mathrm{Split}(f(x); F)$. Hence $\deg f = n$. Now any $\sigma \in \mathrm{Gal}\,(E/F)$ is determined by $\sigma(\alpha)$ as any nonzero element of E is of the form α^i. By Lemma 6.2, $\sigma(\alpha)$ is a root of f and hence $\mathrm{Gal}\,(E/F)$ will have at most n elements. If we let $\sigma(u) = u^p$, then $\sigma \in \mathrm{Gal}\,(E/F)$ by Lemma 5.4. We observe that if $0 < j < n$, then σ^j is not the identity. Assume the contrary. Then for any $u \in E$, we have $\sigma^j(u) = u^{p^j} = 1$ and hence all p^n elements of E are the roots of the polynomial $x^{p^j} - 1$. Since $j < n$, this is a a contradiction. We therefore conclude that $|\mathrm{Gal}\,(E/F)| \geq n$ and hence n.

Observe that $\mathrm{Gal}\,(E/F)$ is a cyclic group with σ as a generator. The automorphism σ is called the Frobenius automorphism.

Example 6.18. Let $F = \mathbb{Z}_p(t)$. Let $E := \mathrm{Split}(x^p - t; F)$. Then $\mathrm{Gal}\,(E/F)$ is trivial. It follows from Example 4.12 that $E = F(\alpha)$ and that $f(x) = (x - \alpha)^p$. Hence α is the only root of f in E. We therefore conclude that the Galois group is trivial.

Example 6.19. Galois group of $x^4 - 2$. Let $E = \mathrm{Split}(x^4 - 2; \mathbb{Q})$. Then $E = \mathbb{Q}(\xi, \gamma)$ where ξ is a primitive fourth root of unity and $\alpha \in \mathbb{R}$ is such that $\alpha^4 = 2$. By now standard arguments we have $|E : \mathbb{Q}| = 8$. Hence, by Theorem 6.6, we have $|\mathrm{Gal}\,(E/\mathbb{Q})| = 8$. It is easy to see that the Galois group is generated by σ and τ:

$$\sigma \colon \alpha \mapsto i\alpha \text{ and } i \mapsto i$$

and

$$\tau \colon \alpha \mapsto \alpha \text{ and } i \mapsto -i.$$

We note that $\sigma^4 = 1 = \tau^2$. Also, we have $\tau\sigma = \sigma^3\tau$. Hence we conclude that $\mathrm{Gal}\,(E/\mathbb{Q})$ is isomorphic to D_8, the dihedral group of order 8.

Example 6.20. Let $\sigma \in \mathrm{Gal}\,(\mathbb{R}/\mathbb{Q})$. We claim that σ is order-preserving: if $x < y$ then $\sigma(x) < \sigma(y)$. Write $y - x = t^2 > 0$. Then $\sigma(y) - \sigma(x) = \sigma(t^2) = \sigma(t)^2 > 0$. If σ is not the identity, then there exists $x \in \mathbb{R}$ such that $\sigma(x) \neq x$. So, either $x < \sigma(x)$ or $x > g(x)$. If $x < \sigma(x)$, by the density of rationals, there exists $r \in \mathbb{Q}$ such that $x < r < g(x)$. By the order preserving property, we have $\sigma(x) < \sigma(r) = r$, a contradiction to the choice of r. Similarly we see that $x > \sigma(x)$ cannot happen. Thus σ is the identity. That is, $\mathrm{Gal}\,(\mathbb{R}/\mathbb{Q})$ is the trivial group.

Ex. 6.21. Let E/F be a finite separable extension. Prove that $|\mathrm{Gal}\,(E/F)| \leq |E : F|$.

The primitive element theorem says that there exists $\alpha \in E$ such that $E = F(\alpha)$. Let $u \in E$. Then $u = p(\alpha)$ for some polynomial $p(x) \in F[x]$. If $\sigma \in \mathrm{Gal}\,(E/K)$, then $\sigma(u) = \sigma(p(\alpha)) = p(\sigma(\alpha))$. It follows that $\sigma \in \mathrm{Gal}\,(E/K)$ is completely determined by $\sigma(\alpha)$.

Let $p(x) = \min(\alpha, F)$. Then $\sigma(\alpha)$ is a root of p. We conclude that the order $|\mathrm{Gal}\,(E/K)|$ is bounded by the number of roots of p *in* E. Hence we have $|\mathrm{Gal}\,(E/F)| \leq \deg p = |E : F|$.

Ex. 6.22. Let E/F be finite. Show that $\mathrm{Gal}\,(E/K)$ is finite.

7 Galois Correspondence

Topics: Galois Extensions, Galois correspondence, Fundamental Theorem of Galois Theory.

Definition 7.1. Let E be a field and let G be a group of automorphisms of E. Then the set

$$E^G := \{a \in E : \sigma(a) = a \text{ for all } \sigma \in G\}$$

is a subfield of E and is called the fixed field of G.

Example 7.2. Let $\mathbb{C}$ and $G = \mathrm{Gal}\,(\mathbb{C}/\mathbb{R})$. Then $\mathbb{C}^G = \mathbb{R}$.

Example 7.3. Let $E := \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathrm{Split}((x^2-2)(x^2-3); \mathbb{Q})$. Let $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$. We have $\sigma, \tau \in \mathrm{Gal}\,(E/\mathbb{Q})$ such that $\sigma(\alpha) = -\alpha$, $\sigma(\beta) = \beta$ and $\tau(\alpha) = \alpha$ while $\tau(\beta) = -\beta$. Let $H := \langle \sigma\tau \rangle$. If we write

$$E \ni u = u_1 + u_2\alpha + u_3\beta + u_4\alpha\beta,$$

then $\sigma\tau(u) = u$ leads us to conclude that $u_2 = 0 = u_3$. Hence $E^H = \mathbb{Q}(\sqrt{6})$.

Example 7.4. This is an extract from Example 7.26.

Let ξ be a primitive 7th root of unity. Let $E := \mathbb{Q}(\xi)$. Then $|E : \mathbb{Q}| = 6$ and $G := \mathrm{Gal}\,(E/\mathbb{Q}) \simeq \mathbb{Z}_6$ is cyclic. Let $\alpha \in G$ be the element such that $\alpha(\xi) = \xi^3$. Then α is a generator of G. If we let $\sigma = \alpha^3$, then σ is order 2 and $H := \langle \sigma \rangle$ is a normal subgroup of index 3 in G. We let $K := E^H$.

Let $u \in K$ be arbitrary. Then $u = a + b\xi + c\xi^2 + d\xi^3 + e\xi^4 + h\xi^5$. As $\sigma \in H$ and $K = E^H$, we have $\sigma u = u$. Recall that $\sigma = \alpha^3$ so that

$$\sigma\colon \xi \mapsto \xi^6;\ \xi^2 \mapsto \xi^5;\ \xi^3 \mapsto \xi^4;\ \xi^4 \mapsto \xi^3;\ \xi^5 \mapsto \xi^2;\ \xi^6 \mapsto \xi. \tag{1}$$

Equating the coefficients of the same power we arrive at

$$u = a + c(\xi^2 + \xi^5) + d(\xi^3 + \xi^4).$$

(Why is $b = 0$?) Clearly, $\xi^2 + \xi^5 \notin \mathbb{Q}$. It follows that $K = \mathbb{Q}(\xi^2 + \xi^5)$.

Example 7.5. Let $E := \mathrm{Split}(f(x) := x^4 - 7; \mathbb{Q})$. We have $E = \mathbb{Q}(\alpha, i)$ where $\alpha \in \mathbb{R}$ is such that $\alpha^4 = 7$. By standard arguments, we know $|\mathrm{Gal}\,(E/\mathbb{Q})| = |E : \mathbb{Q}| = 8$ and that the Galois group is the dihedral group of order 8. Let $\sigma \in \mathrm{Gal}\,(E/\mathbb{Q})$ be the element of the Galois group such that $\sigma(\alpha) = i\alpha$ and $\sigma(i) = i$. Let $\tau \in \mathrm{Gal}\,(E/\mathbb{Q})$ be such that $\tau(i) = -i$ and $\tau(\alpha) = \alpha$. Then $\sigma^4 = e = \tau^2$ and $\tau\sigma = \sigma^3\tau$.

Let $H := \langle \tau\sigma \rangle$. We wish to find the fixed field of H. Let

$$E \ni u = u_1 + u_2\alpha + u_3\alpha^2 + u_4\alpha^3 + u_5 i + u_6\alpha i + u_7\alpha^2 i + u_8\alpha^3 i.$$

We have

$$\tau\sigma(u) = u_1 - u_2\alpha - u_3\alpha^2 + u_4 i\alpha^3 - u_5 i + u_6\alpha + u_7\alpha^2 i + u_8\alpha^3.$$

Therefore, $\tau\sigma(u) = u$ iff **Verify!**

$$u_3 = 0 = u_5, \quad u_4 = u_8, \quad \text{and} \quad u_2 = -u_6.$$

Hence $u \in E^H$ is of the form

$$u = u_1 + u_2(\alpha - \alpha i) + u_4(\alpha^3 + \alpha^3 i) + u_7\alpha^2 i.$$

We observe that

$$(\alpha - \alpha i)^2 = -2\alpha^2 i \text{ and } (\alpha - \alpha i)^3 = -2(\alpha^3 + \alpha^3 i).$$

It follows that $u \in \mathbb{Q}(\alpha - i\alpha)$ and that $E^H = \mathbb{Q}(\alpha - i\alpha)$.

Example 7.6. Consider $E := \text{Split}(x^6 - 2; \mathbb{Q}(\xi))$ where ξ is a cube root of unity. Note that $\mathbb{Q}(\xi) = \mathbb{Q}(-\xi)$. Let $\alpha := 2^{1/6}$. If $\sigma \in \text{Gal}\,(E/\mathbb{Q}(\xi))$, then $\sigma(\alpha) = \alpha(-\xi)^j$, $0 \leq j \leq 5$ is the generator of the Galois group. Let $H := \langle \sigma^2 \rangle$. Then $E^H := \mathbb{Q}(\sqrt{2}, \xi)$.

Let E/F be an extension and let K be an intermediate field between F and E, that is, $F \subset K \subset E$. Let H stand for a subgroup of $\text{Gal}\,(E/F)$. Let $\mathcal{K}$ denote the set of intermediate fields of E/F and $\mathcal{H}$, the set of subgroups of G. Consider the maps

$$\Phi \colon \mathcal{K} \to \mathcal{H} \text{ defined by } K \mapsto \text{Gal}\,(E/K)$$

and

$$\Psi \colon \mathcal{H} \to \mathcal{K} \text{ defined by } H \mapsto E^H$$

The so-called fundamental theorem of Galois theory relates these two maps when the extension E/F is a finite, separable and normal extension. The mapΦ is called the Galois correspondence.

Theorem 7.7. *Let E be a field and G a finite group of automorphisms of E. Let K be the fixed field of G. The following are true:*

(i) *Each element of E is algebraic over K.*

(ii) *Let the G-orbit of $\alpha \in E$ be $\{\alpha_1, \ldots, \alpha_k\}$. Then* $\min(\alpha, K) = (x - \alpha_1) \cdots (x - \alpha_n)$.

(iii) *E/K is a normal separable extension.*

(iv) *The extension E/K is finite and hence simple.*

(v) *To sum it up, the extension E/K is a simple, normal and separable extension such that $|E : K|$ is a divisor of $|G|$.*

(vi) *We have* $\text{Gal}\,(E/K) = G$ *and* $|G| = |E : K|$.

Proof. Let $f(x) = (x - \alpha_1) \cdots (x - \alpha_k)$. Since each element of G permutes α_i's, and hence $(x - \alpha_i)$'s, the polynomial is invariant under G. Therefore its coefficients lie in K. This shows that α is algebraic over K. We have proved (i).

Let $g(x) \in K[x]$ be any polynomial such that $g(\alpha) = 0$. We claim that $g(\alpha_i) = 0$ for all $1 \leq i \leq k$. For, let $\sigma \in G$ be such that $\sigma(\alpha) = \alpha_i$. Then $0 = \sigma(g(\alpha)) = g(\sigma(\alpha)) = g(\alpha_i)$. It follows that f divides g. (ii) is proved.

(ii) shows that the minimal polynomial of each element of K splits in E and has no multiple roots. Hence the extension E/K is normal and separable. Hence (iii) is proved.

(iv) requires a bit of work. Let M be any field satisfying (a) $K \leq M \leq E$ and (b) M/K is finite. Then M/K is separable since E/F is. Therefore, $M = K(\alpha)$ by the primitive element theorem. Let $m = \deg \min(\alpha, K)$. We know that $m = |M : K|$. By (ii), we have $|M : K|$ the size of the G-orbit of α. In particular, $|M : K|$ is a divisor of $|G|$. This is true for any intermediate field $K \leq M \leq E$ with $|M : K|$ finite.

We now choose the intermediate field M so that $|M : K|$ is the maximum. (This is possible since such $|M : K|$ are divisors of $|G|$.) We claim $M = E$. Let $\lambda \in E$. Then, by (i), λ is algebraic over K. Hence $|M(\lambda) : M|$ is finite. We have by the tower law,

$$|M(\lambda) : K| = |M(\lambda) : M| \cdot |M : K|.$$

Maximality of $|M : K|$ forces us to conclude that $M(\lambda) = M$. That is, if $\lambda \in E$, then $\lambda \in M$. Thus E is a finite extension. Since it is a finite separable extension, it is simple by the primitive element theorem. Thus (iv) is proved.

(v) is merely a summary of (i)–(iv).

We now prove (vi). We know from (iv) that $E = K(\alpha)$. Let $p(x) = \min(\alpha, K)$ be of degree n. Then $|E : K| = \deg p = n$. We know that $\sigma \in \mathrm{Gal}\,(E/K)$ is determined by $\sigma(\alpha)$. Now, $\sigma(\alpha)$ will be a root of $p(x)$. Thus the number of distinct $\sigma \in \mathrm{Gal}\,(E/K)$ is at most the number of roots of f, that is, $\deg p$. But $\deg p = |E : K|$. Hence we arrive at

$$|G| \leq |\mathrm{Gal}\,(E/K)| \leq n = |E : K|.$$

Now, let f be as above in the proof of (i). Then n the degree of $\min(\alpha, K)$ divides k, the degree of f. Also, k (being the number of elements in the G-orbit of α) is a divisor of $|H|$. We therefore obtain

$$|H| \geq k \geq n = |E : K|.$$

The two displayed inequalities lead us to the result. □

Remark 7.8. If we assumed that E/F is a finite extension and $H \leq \mathrm{Gal}\,(E/F)$ in the last theorem, then E is a simple normal and separable extension of the fixed field $K := E^H$.

This is perhaps the standard version of the last theorem.

Theorem 7.9. *Let E/F be a finite extension. Let $H \leq \mathrm{Gal}\,(E/F)$ and $K := E^H$ be the fixed field of H. Then $\mathrm{Gal}\,(E/K) = H$ and $|\mathrm{Gal}\,(E/K)| = |H| = |E : K|$.*

Proof. Observe that $\mathrm{Gal}\,(E/F)$ is finite. The result follows from the last theorem. □

Remark 7.10. This theorem shows the Galois correspondence $\Phi\colon K \mapsto \mathrm{Gal}\,(E/K)$ from the set of intermediate fields $F \leq K \leq E$ to the set of subgroups of $\mathrm{Gal}\,(E/F)$ is onto.

Definition 7.11. An extension E/F is said to be a *Galois extension* if it is normal and separable. We shall deal only with finite Galois extensions.

Ex. 7.12. Let E/F be a finite Galois extension. Show that $E = F(\alpha)$ iff the G-orbit of α has $|G|$ number of elements.

Example 7.13. Let $E := \mathbb{C}(t)$ be the field of rational functions. Let $\sigma(t) = 1/t$. Then σ extends to an automorphism of E with $\sigma^2 = 1$. Let $H = \langle\sigma\rangle$. What is E^H?

Clearly, $t + t^{-1}$ is fixed by H. Hence we obtain

$$\mathbb{C}(t + t^{-1}) \subset E^H \subset E. \tag{2}$$

On the other hand, $\mathbb{C}(t) \subset \mathbb{C}(t + t^{-1})(t) \subset \mathbb{C}(t)$ so that we conclude that $\mathbb{C}(t)$ is obtained from $\mathbb{C}(t + t^{-1})$ by adjoining t.

What is $\min(t, \mathbb{C}(t + t^{-1})$? Observe that t is a root of

$$(x - t)(x - t^{-1}) = x^2 - (t + t^{-1})x + 1 \in \mathbb{C}(t + t^{-1})[x].$$

Hence we arrive at $|C(t) : \mathbb{C}(t + t^{-1})| \leq 2$. But by Theorem 7.9, we know that this degree is 2. It follows from the tower law and (2) that $E^H = \mathbb{C}(t + t^{-1})$.

Theorem 7.14. *Let E/F be a finite Galois extension and K be an intermediate field $F \leq K \leq E$. Then K is the fixed field of* $\mathrm{Gal}\,(E/K)$. *In an ugly notation, we have*

$$K = E^{\mathrm{Gal}\,(E/K)}.$$

Proof. Let L be the fixed field of $\mathrm{Gal}\,(E/K)$. Then $K \leq L$. We need to show that $L \leq K$. Let $\alpha \notin K$. If $p(x) = \min(\alpha, K) \in K[x]$ is the minimal polynomial, then its degree is at least 2. (Why?) Since E/L is normal, all the roots of $p(x)$ lie in E. Since E/K is separable, the roots of $p(x)$ are distinct. If $\beta \neq \alpha$ is another root of $p(x)$, then there exists $\sigma \in \mathrm{Gal}\,(E/K)$ with $\sigma(\alpha) = \beta$. This means that any element outside K is moved by $\mathrm{Gal}\,(E/K)$. Hence $L \subset K$. □

Remark 7.15. The last result shows that the Galois correspondence Φ is one-one. For, if K and L are intermediate fields having the same Galois groups, that is, $\mathrm{Gal}\,(E/K) = \mathrm{Gal}\,(E/L) = H \leq \mathrm{Gal}\,(E/F)$, then $K = L$.

Corollary 7.16. *Let E/F be a finite extension. Then E/F is a Galois extension iff F is the fixed field of* $\mathrm{Gal}\,(E/F)$.

Proof. If E/F is Galois, then the fixed field of $\mathrm{Gal}\,(E/F)$ is F by the last theorem.

If F is the fixed field of $\mathrm{Gal}\,(E/F)$, then by Theorem 7.7, the extension E/F is normal and separable and hence Galois. □

Remark 7.17. In literature, sometimes, a Galois extension is defined as in the Corollary above.

Corollary 7.18. *Let E/F be a (finite) Galois extension. Then* $|\mathrm{Gal}\,(E/F)| = |E : F|$.

Proof. Notice that this is nothing but Theorem 6.6.

Follows from the last result and Theorem 7.9 (in which we take $H = \mathrm{Gal}\,(E/F)$. □

This corollary has interesting applications and helps us to 'find' Galois groups.

Example 7.19. We shall show that the Galois group of the splitting field of $x^3 - 2$ over $\mathbb{Q}$ is S_3.

Let ξ be a primitive cube root of unity. Then $\mathrm{Split}(x^3 - 2; \mathbb{Q}) = \mathbb{Q}(2^{1/3}, 2^{1/3}\xi, 2^{1/3}\xi^2) = \mathbb{Q}(2^{1/3}, \xi)$. By Example 3.17), we have $|\mathbb{Q}(2^{1/3}, \xi) : \mathbb{Q}| = 6$. Hence $|\mathrm{Gal}\,(\mathbb{Q}(2^{1/3}, \xi)/\mathbb{Q})| = 6$. By Corollary 6.5, it is a subgroup of S_3. Hence the claim.

Ex. 7.20. Let $E = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Then $E/\mathbb{Q}$ is a Galois extension. We have identified the Galois group in Example 6.9 whose subgroups are easy to list. List them and find the corresponding fixed fields.

Theorem 7.21. *Let E/F be a Galois extension. Let $F \leq K \leq E$ be an intermediate field. Assume that* $\mathrm{Gal}\,(E/K)$ *is normal in* $\mathrm{Gal}\,(E/F)$. *Then K/F is a normal extension.*

Proof. Let an irreducible polynomial $f(x) \in F[x]$ have a root $\alpha \in K$. Since E/F is normal, $f(x)$ splits in E. Let β be another root of f. Then there exists $\sigma \in \mathrm{Gal}\,(E/F)$ such that $\sigma(\alpha) = \beta$. We show that $\tau(\beta) = \beta$ for any $\tau \in \mathrm{Gal}\,(E/K)$.

Since $\mathrm{Gal}\,(E/K)$ is normal, we have $\sigma\tau\sigma^{-1} = \tau_1 \in \mathrm{Gal}\,(E/K)$. Observe that

$$\tau(\beta) = \tau(\sigma(\alpha)) = \sigma(\tau_1(\alpha)) = \sigma(\alpha) = \beta.$$

Thus, $\tau(\beta) = \beta$ for any $\tau \in \mathrm{Gal}\,(E/K)$. Hence $\beta \in E^{\mathrm{Gal}\,(E/K)} = K$, by Theorem 7.14. □

Before we embark on the main result of this section, we shall dispose of a simple observation.

Lemma 7.22. *Let E/F be a finite normal extension. Let $F \leq K \leq E$ and K/F is a normal extension. Then there is a natural onto homomorphism from* $\mathrm{Gal}\,(E/F)$ *onto* $\mathrm{Gal}\,(K/F)$ *with kernel* $\mathrm{Gal}\,(E/K)$*. Also, we have*

$$\mathrm{Gal}\,(K/F) \simeq \mathrm{Gal}\,(E/F)/\mathrm{Gal}\,(E/K).$$

Proof. The basic observation is that if $\sigma \in \mathrm{Gal}\,(E/F)$, then the restriction $\sigma|_K$ makes sense. (See Lemma 3.21.) Let $\alpha \in K$. Let $p(x) = \min(\alpha, F)$. Since E/F is normal, $p(x)$ splits in E. Since K/F is normal, and since $\alpha \in K$, all the roots of $p(x)$ lie in K, that is, the splitting of $p(x)$ takes place in $K[x]$. Now $\sigma \in \mathrm{Gal}\,(E/F)$ will send α to a root of $p(x0$ and hence to an element of K.

One easily verifies that the map $\sigma \mapsto \sigma|_K$ is a group homomorphism.

We claim that this map is onto. For, let $\tau \in \mathrm{Gal}\,(K/F)$ be given. Since E/F is the splitting field of some $f(x) \in F[x]$, E is also the splitting field of $f(x)$ when considered as an element of $K[x]$. Hence τ extends to an F automorphism σ of E (by Theorem 3.9). □

Note that we used the normality of K/F to show that the map $\sigma \mapsto \sigma|_K$ is onto.

The next theorem, the main result of Galois theory asserts that the maps Φ and Ψ are inverses of each other when the extension E/F is Galois.

Theorem 7.23 (Fundamental Theorem of Galois Theory)**.** *Let E/F be a Galois extension and let* $\mathrm{Gal}\,(E/F)$ *be its Galois group. The maps $\Phi\colon \mathcal{K} \to \mathcal{H}$ and $\Psi\colon \mathcal{H} \to \mathcal{K}$ defined by*

$$\begin{aligned} \Phi\colon K &\mapsto \mathrm{Gal}\,(E/K) \\ \Psi\colon H &\mapsto E^H. \end{aligned}$$

are inverses of each other.

Under the correspondence, we have

$$|E : K| = |\mathrm{Gal}\,(E/K)| \quad \textit{and} \quad |K : F| = |\mathrm{Gal}\,(E/F) : \mathrm{Gal}\,(K/F)|.$$

Furthermore, the extension K/F is normal iff the corresponding subgroup $\mathrm{Gal}\,(E/K)$ *is normal. In such a case, we have* $\mathrm{Gal}\,(K/F) \simeq \mathrm{Gal}\,(E/F)/\mathrm{Gal}\,(E/K)$.

Proof. Follows from the results above. □

Example 7.24. Let us look at $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$, $\mathbb{Q}(\sqrt[3]{2}, i) : \mathbb{Q}$ and at $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q})$.

Example 7.25. Let $E := \mathrm{Split}(x^4 - 2; \mathbb{Q}) = \mathbb{Q}(\alpha, i)$ where $\alpha^4 = 2$. Let $\sigma \in \mathrm{Gal}\,(E/\mathbb{Q})$ be such that $\sigma(\alpha) = i\alpha$ and $\sigma(i) = -i$. Let $H := \langle\sigma\rangle$. If we write

$$E \ni u = u_1 + u_2\alpha + u_3\alpha^2 + u_4\alpha^3 + u_5 i + u_6 i\alpha + u_7 i\alpha^2 + u_8\alpha^3,$$

then $\sigma(u) = u$ iff $u = u_1 + u_2(\alpha + i\alpha) + u_4(\alpha^3 - i\alpha^3) + u_7 i\alpha^2$.We note that $i\alpha^2 \in \mathbb{Q}(\alpha + i\alpha)$ and that $\alpha^3 - i\alpha^3 \in \mathbb{Q}(\alpha + i\alpha)$. Hence $E^H = \mathbb{Q}(\alpha + i\alpha)$. Verify!

We can cut down the work if we observe that $\alpha + i\alpha$ is fixed under σ. Hence $\mathbb{Q}(\alpha + i\alpha) \subset E^H$. If this inclusion is proper, then some other element of the Galois group must be in $\mathrm{Gal}\,(E/\mathbb{Q}(\alpha + i\alpha)$. It is easy to check that no element other than e and σ does it.

Example 7.26. We wish to find an irreducible $f(x) \in \mathbb{Q}[x]$ of degree 3 such that its splitting field K is of degree 3 over $\mathbb{Q}$. The basic idea is to exploit the Galois correspondence to find such a K and then f.

We start with a degree 6 extension over $\mathbb{Q}$ and find a normal subgroup of order 2 in the Galois group. The fixed field will be a degree 3 extension over $\mathbb{Q}$.

Let ξ be a primitive 7th root of unity. Let $E := \mathbb{Q}(\xi)$. Then $|E : \mathbb{Q}| = 6$ and $G := \mathrm{Gal}\,(E/\mathbb{Q}) \simeq \mathbb{Z}_6$ is cyclic. Let $\alpha \in G$ be the element such that $\alpha(\xi) = \xi^3$. Then α is a generator of G. If we let $\sigma = \alpha^3$, then σ is order 2 and $H := \langle\sigma\rangle$ is a normal subgroup of index 3 in G. If we let $K := E^H$, then K is a normal extension of $\mathbb{Q}$ of degree 3 (by Galois correspondence). Therefore, there exists an irreducible polynomial $f(x) \in \mathbb{Q}[x]$ of degree 3 such that $K = \mathrm{Split}(f(x); \mathbb{Q})$.

We need to find $f(x)$ explicitly. Since K is a simple extension, if we find a primitive element, then $f(x)$ is the minimal polynomial of this primitive element.

Let $u \in K$ be arbitrary. Then $u = a + b\xi + c\xi^2 + d\xi^3 + e\xi^4 + h\xi^5$. As $\sigma \in H$ and $K = E^H$, we have $\sigma u = u$. Recall that $\sigma = \alpha^3$ so that

$$\sigma\colon \xi \mapsto \xi^6;\ \xi^2 \mapsto \xi^5;\ \xi^3 \mapsto \xi^4;\ \xi^4 \mapsto \xi^3;\ \xi^5 \mapsto \xi^2;\ \xi^6 \mapsto \xi. \tag{3}$$

Equating the coefficients of the same power we arrive at

$$u = a + c(\xi^2 + \xi^5) + d(\xi^3 + \xi^4).$$

(Why is $b = 0$?) Clearly, $\xi^2 + \xi^5 \notin \mathbb{Q}$. Since $|K : \mathbb{Q}| = 3$, it follows that $K = \mathbb{Q}(\xi^2 + \xi^5)$. What is the minimal polynomial $f(x)$ of $\theta = \xi^2 + \xi^5$? The roots are f are the distinct images of θ under α. The displayed equation (3) makes our life easy! We obtain

$$\begin{aligned}
f(x) &= (x - (\xi^2 + \xi^5))(x - (\xi^4 + \xi^3))(x - (\xi + \xi^6)) \\
&= -\xi^{15} - \xi^{14} + x\xi^{11} - \xi^{12} + x\xi^{10} - \xi^{11} + 2\,x\xi^9 - \xi^{10} + 2\,x\xi^8 - \xi^9 - x^2\xi^6 \\
&\qquad - x^2\xi^5 + 2\,x\xi^6 - \xi^7 - x^2\xi^4 + 2\,x\xi^5 - \xi^6 - x^2\xi^3 + x\xi^4 - x^2\xi^2 + x\xi^3 + x^3 - x^2\xi \\
&= -\xi^{15} - \xi^{14} - \xi^{12} - \xi^{11} - \xi^{10} - \xi^9 - \xi^7 - \xi^6 - \big(\xi^6 + \xi^5 + \xi^4 + \xi^3 + \xi^2 + \xi\big)x^2 + x^3 \\
&\qquad + \big(\xi^{11} + \xi^{10} + 2\,\xi^9 + 2\,\xi^8 + 2\,\xi^6 + 2\,\xi^5 + \xi^4 + \xi^3\big)x \\
&= x^3 + x^2 - 2x - 1.
\end{aligned}$$

We shall indicate another method of finding this polynomial. Using the standard trigonometric identities (use $\theta = \frac{2\pi}{7}$), we obtain the following:

$$\begin{aligned}
\xi + \xi^6 &= 2\cos\frac{2\pi}{7} \\
\xi^2 + \xi^5 &= 2\cos\frac{4\pi}{7} = 4\cos^2\frac{2\pi}{7} - 2 \\
\xi^3 + \xi^4 &= 2\cos\frac{6\pi}{7} = 8\cos^3\frac{2\pi}{7} - 6\cos\frac{2\pi}{7}.
\end{aligned}$$

We now use the cyclotomic equation

$$\begin{aligned}
0 &= 1 + (\xi + \xi^6) + (\xi^2 + \xi^5) + (\xi^3 + \xi^4) \\
&= 1 + 2\cos\frac{2\pi}{7} + 4\cos^2\frac{2\pi}{7} - 2 + 8\cos^3\frac{2\pi}{7} - 6\cos\frac{2\pi}{7}.
\end{aligned}$$

Thus $\cos\theta$ is a root of the polynomial $x^3 + x^2 - 2x - 1$. This polynomial is irreducible by the rational roots theorem.

8 Solvability by Radicals

Topics: Defn of a Radical extension; An improved definition which includes a primitive n-th root of unity for $n \gg 0$; Galois group of a radical extension is solvable; Existence of a radical extension which is also normal (assuming the existence of a radical extension); $F \leq K \leq L$ where $K = \text{Split}(f; F)$ and L is a normal radical extension. Then $\text{Gal}\,(K/F)$ is a quotient of $\text{Gal}\,(L/F)$. (To establish surjectivity of the map $\sigma \mapsto \sigma|_K$, we need L/F normal.);

Example of a quintic polynomial which is not solvable.

Convention: In this chapter, we shall assume all out fields are of zero characteristic.

Definition 8.1. An extension E/F is sadi to be a *radical extension* if there is a tower of fields

$$F = F_0 \subset F_1 \subset \cdots \subset F_k = E,$$

such that there exist an $\alpha_i \in F_i$ and an integer m_i with $\alpha_i^{m_i} \in F_{i-s}$ for $1 \leq i \leq k$.

Example 8.2. $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ is a radical extension:

$$\mathbb{Q} = F_0 \subset F_1 = \mathbb{Q}(\sqrt{2}) \subset F_2 = \mathbb{Q}(\sqrt{2+\sqrt{2}}).$$

Note that $\alpha_1 = \sqrt{2}$ and $\alpha_2 = \sqrt{2+\sqrt{2}}$. We have $m_1 = m_2 = 2$ and $\alpha_2^2 = 2 + \sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Ex. 8.3. Any radical extension is a finite extension.

Remark 8.4. Let us say we want to consider the extension $\mathbb{Q}(\sqrt[5]{7-\sqrt{52}})$. The expression $\sqrt[5]{7-\sqrt{52}}$ stands for a complex 5th root of $7 - \sqrt{52}$. Which one? To avoid the ambiguity and also for other technical reason, it is expedient to include a primitive m-th root of unity in the definition of a radical extension for some $m \gg 0$. For example, in this example, if we include ξ, a primitive fifth root of unity, and consider the radical extension

$$\mathbb{Q} \subset \mathbb{Q}(\xi) \subset \mathbb{Q}(\xi)\left(\sqrt[5]{7-\sqrt{52}}\right)$$

there is no ambiguity which of the five roots is included.

How to do this for a general radical extension? Keep the notation as above. Let m be the least common multiple of $m_1, m_2, \ldots, m_k$. Let $\xi = \xi_m$ be a primitive m-th root of unity. For each i, we let $E_i := F_i(\xi)$. Then for each i

$$E_i = F_i(\xi) = F_{i-1}(\alpha_i)(\xi) = F_{i-1}(\alpha_i, \xi) = F_{i-1}(\xi)(\alpha_i) = E_{i-1}(\alpha_i).$$

Since $\alpha_i^{m_i} \in F_{i-1} \subset E_{i-1}$, we see that

$$F \subset E_0 \subset E_1 \subset \cdots \subset E_k$$

is a radical extension that contains the given radical extension E/F.

In the next theorem, we shall assume that any radical extension is of the form $E = F(\xi, \alpha_1, \ldots, \alpha_k)$ where $\alpha_i^{m_i} \in F_{i-1} := F(\xi, \alpha_1, \ldots, \alpha_{i-1})$ and where m is the LCM of the m_i's.

Theorem 8.5. *Let E/F be a radical extension. Assume that $E = F(\xi, \alpha_1, \ldots, \alpha_k)$ where $\alpha_i^{m_i} \in F_{i-1} := F(\xi, \alpha_1, \ldots, \alpha_{i-1})$, where m is the LCM of the m_i's and ξ is a primitive m-th root of unity. Then* $\text{Gal}\,(E/F)$ *is solvable.*

Proof. We keep the notation above. Corresponding to the chain of fields

$$F \subset E_0 \subset E_1 \subset \cdots \subset E_k,$$

we get a chain of subgroups

$$G = \mathrm{Gal}\,(E/F) \subseteq \mathrm{Gal}\,(E/E_0) \supseteq \cdots \supseteq \mathrm{Gal}\,(E/E_{k-1}) \supseteq \mathrm{Gal}\,(E/E_k) = \{e\}.$$

To prove that $\mathrm{Gal}\,(E/F)$ is solvable, it suffices to show that
(a) $ghg^{-1}h^{-1} \in \mathrm{Gal}\,(E/E_0)$, for all $g, h \in \mathrm{Gal}\,(E/F)$, and
(b) $ghg^{-1}h^{-1} \in \mathrm{Gal}\,(E/E_{i+1})$, for all $g, h \in \mathrm{Gal}\,(E/E_i)$ for $0 \leq i \leq k-1$.

Let us prove (a). Since $E_0 = F(\xi)$, we need to show that $\sigma := ghg^{-1}h^{-1}(\xi) = \xi$. Since $\sigma(\xi)$ must again be a root of $x^m - 1$ and any root of this polynomial is of the form ξ^j, we see that $\sigma(\xi) = xi^j$ for some j modulo m. Let $g^{-1}(\xi) = \xi^i$ and $h^{-1}(\xi) = \xi^j$. We easily see that $\sigma(\xi) = \xi$. Thus, we conclude that $\sigma \in \mathrm{Gal}\,(E/E_0)$.

We now prove (b). Let $g, h \in \mathrm{Gal}\,(E/E_i)$. Recall that $E_{i+1} = E_i(\alpha_{i+1})$ with $a = \alpha_{i+1}^{m_{i+1}} \in E_i$. It follows that $g, h \in \mathrm{Gal}\,(E/E_i)$ must send α_{i+1} into some root of the polynomial $x^{m_{i+1}} - a$. So, we conclude that $g(\alpha_{i+1}) = \alpha_{i+1}\xi^r$ and $h(\alpha_{i+1}) = \alpha_{i+1}\xi^s$ so that $g^{-1}(\alpha_{i+1}) = \alpha_{i+1}\xi^r$ and $h^{-1}(\alpha_{i+1}) = \alpha_{i+1}\xi^s$. Since g and h are identity on E_i, they map any power of ξ to the same power of ξ. A trivial compuation now shows that

$$ghg^{-1}h^{-1}(\alpha_{i+1}) = (ghg^{-1})(\alpha_{i+1}\xi^s) = (gh)(\alpha_{i+1}\xi^r\xi^s) = g(\xi^r\alpha_{i+1}) = \alpha_{i+1}.$$

This shows that $ghg^{-1}h^{-1}$ is the identity on $E_i(\alpha_{i+1}) = E_{i+1}$ and hence lies in $\mathrm{Gal}\,(E/E_{i+1})$. □

Definition 8.6. Let $f(x) \in F[x]$. We say that f is *solvable by radicals* if the splitting field $K = \mathrm{Split}(f(x); F)$ is contained in a radical extension E/F.

Remark 8.7. The main result of this section is that if a polynomial $f(x) \in F[x]$ is solvable by radicals, then $\mathrm{Gal}\,(K/F)$ is a solvable group. To deduce this from Theorem 8.5, we shall show that there exists a radical extension L/F which is normal and which contains K. (See Theorem 8.9). Then $\mathrm{Gal}\,(K/F)$ is a homomorphic image of the Galois group $\mathrm{Gal}\,(L/F)$ by Lemma 7.22

So what remains to be shown is the existence L as specified (in Remark 8.7) given that f is solvable by radicals. This is achieved by a technical lemma.

Lemma 8.8. *Let F, E and L be fields of characteristic 0 with*

$$F \subset E \subset L = E(\alpha) \quad \textit{and} \quad \alpha^k \in E.$$

If $|L : F|$ is finite and E/F is normal, then there exists an extension M/L which is a radical extension of E and normal extension of F.

Proof. Let $E := \mathrm{Split}(f(x); F)$. Let $g(x) := \min(\alpha, F)$. Let $M := \mathrm{Split}(f(x)g(x); F)$. Then M/F is normal. Note that $F \leq E \leq L \leq M$. (For, $L = E(\alpha)$ and E is obtained by adjoining the roots of f.) Let $\alpha_1, \ldots, \alpha_k$) be the roots of g. For each $1 \leq i \leq k$, thanks to Proposition 6.3, there exists $\sigma_i \in \mathrm{Gal}\,(M/F)$ such that $\sigma_i(\alpha) = \alpha_i$. Let $\alpha^k = a \in E$. Observe that, since E is a splitting field and $a \in E$,

$$\alpha_i^k = \sigma_i(\alpha)^k = \sigma_i(\alpha^k) = \sigma_i(a) \in E,$$

by Lemma 3.21. Since $E \leq E(\alpha_1, \ldots, \alpha_{i-1})$, we have

$$E \subseteq L = E(\alpha_1) \subseteq E(\alpha_1, \alpha_2) \subseteq \ldots \subseteq E(\alpha_1, \ldots, \alpha_k) = M.$$

Thus M/F is normal and a radical extension of F as per the original definition. □

Theorem 8.9. *Let $f(x) \in F[x]$ be solvable by radicals. Then there exists a normal radical extension L/F that contains $K = \mathrm{Split}(f(x); K)$.*

Proof. Let K be contained in a radical extension

$$F = E_0 \subseteq E_1 \subseteq \ldots \subseteq E_k,$$

where $E_i = E_{i-1}(\alpha_i)$ and $\alpha_i^{m_i} \in E_{i-1}$ for $1 \leq i \leq k$.

Let us apply the last lemma with $E = F$, $L = E_1$ and $\alpha = \alpha_1$. We then get a normal extension M_1 of F that contains E_1. By hypothesis, $\alpha_2^{m_2} \in E_1 \subseteq M_1$. We now apply the last lemma where $E = M_1$, $\alpha = \alpha_2$ and $L = M_1(\alpha_2)$. We get a normal extension M_2 of F that is a radical extension of M_1 and hence a radical extension of F. Also, we have $E_1(\alpha_2) \subset M_2$. We continues this process to arrive at a normal radical extension M_k of F that contains E_k and hence K.

If we want the radical extension as in Remark 8.4, we can adjoin the a primitive m-th root of unity to M as in the remark. Note that $M(\xi)$ is the splitting field of $f(x)g(x)(x^m - 1)$ and hence is normal radical extension. □

Theorem 8.10. *Let $f(x) \in F[x]$ be solvable by radicals. Let $K = \mathrm{Split}(f(x); F)$. Then $\mathrm{Gal}\,(K/F)$ is solvable.*

Proof. We may assume that K is contained in a normal radical extension. By adjoining ξ, a primitive m-th root of unity as detailed in Remark 8.4, we obtain a radical extension L of F which is normal over F and contains K. This extension L satisfies the hypothesis of Theorem 8.5 and hence $\mathrm{Gal}\,(L/F)$ is solvable. By Lemma 7.22, $\mathrm{Gal}\,(K/F)$ is a quotient of $\mathrm{Gal}\,(L/F)$ and hence $\mathrm{Gal}\,(K/F)$ is solvable. □

We now use this theorem to exhibit polynomials of degree greater than or equal to 5, which are not solvable by radicals.

Proposition 8.11. *Let p be a prime. If H is a subgroup of S_p which contains a transposition and a cycle of order p, then $H = S_p$.*

Proof. Assume $\tau := (12)$ and $\sigma := (12 \ldots n)$ lie in $H \leq S_n$. We show that $H = S_n$.

Observe that $\sigma\tau\sigma^{-1} = (23)$, $\sigma(23)\sigma^{-1} = (34)$ and so on. Thus all elements of the from $(k, k+1) \in H$.

Observe that $(12)(23)(12) = (13) \in H$, $(13)(34)(13) = (14) \in H$. In general, $(1k) \in K$.

Observe that $(1r)(1s)(1r) = (rs) \in H$. Thus all transpositions lie in H. Hence $H = S_n$.

Now let us assume that $n = p$ and that $H \leq S_p$ is such that H contains a transposition and a p-cycle. We show that $H = S_p$.

Let τ be a transposition. By relabeling, we may assume that $\tau = (12)$. Let σ be a p-cycle. We may assume WLOG that $\sigma = (1 \ldots 2 \ldots)$, that is, it starts with 1. Let j be the number of elements that lie between 1 and 2 in σ. Note that $0 \leq j \leq p-2$. Consider $f := \sigma^{j+1}$.

Since $1 \leq j+1 \leq p-1$ and since the order of σ is p, we find that f is not the identity.[1] We have $f(1) = 2$ and hence $f = (12a_3 \dots a_p)$. Note that $f \in H$. We may therefore assume σ is already of this form.

Let $\pi := \begin{pmatrix} 1 & 2 & a_3 & \dots & a_p \\ 1 & 2 & 3 & \dots & p \end{pmatrix}$. Then $\pi\sigma\pi^{-1} = (12 \dots p)$. Also, $\pi(12)\pi^{-1} = (12)$. Thus the subgroup $\pi H \pi^{-1}$ has (12) and $(12 \dots p)$. Hence $\pi H \pi^1 = S_p$ by the first part. It follows that $H = S_p$.

Another way of showing directly that $\mathrm{Gal}\,(E/\mathbb{Q}) \simeq S_p$ is to observe that the Galois group acts transitively on the set of roots and use the following fact:

Let $H \leq S_p$ be such that H acts transitively on $X := \{1, \dots, p\}$ and contains a transposition. Then $H = S_p$.

To see this, we define an equivalence relation on $i \sim j$ iff the transposition $(ij) \in H$. To see the transitivity of the relation, observe that $(ij)(jk)(ij) = (ik)$. Let $[i]$ denote the equivalence class of $i \in X$. We claim that all equivalence classes have the same number of elements. For, if $j \in X$, then there exists $\sigma \in H$ such that $\sigma i = j$. Nor, if $k \in [i]$, then

$$\sigma(i,k)\sigma^{-1} = (\sigma(i), \sigma(k)) = (j, \sigma(k)) \in H.$$

Thus, $\sigma(k) \in [j]$. Hence, $\sigma([i]) \subset [j]$ and hence $|[i]| \leq |[j]|$. Interchanging i and j proves the claim. We have now partition of X (whose cardinality is p) into pairwise disjoint subsets (namely, the equivalence classes). This forces us to conclude that X is a single equivalence class. In other words, every transposition $(ij) \in H$. It follows that $H = S_p$. □

Example 8.12. Let $f(x) \in \mathbb{Q}[x]$ be irreducible of prime degree p. Assume that f has $p-2$ real roots and 2 complex roots. Let $E := \mathrm{Split}(f(x); \mathbb{Q})$. Then $\mathrm{Gal}\,(E/\mathbb{Q}) \simeq S_p$.

Since $|\mathrm{Gal}\,(E/\mathbb{Q})|$ is divisible by p (Why?), by Cauchy's theorem, there exists an element of order p in $\mathrm{Gal}\,(E/\mathbb{Q})$. If we consider the Galois group as a subgroup of S_p (by Corollary 6.5), we infer that it has a p-cycle.

Since f has only two roots, the complex conjugation restricts to an automorphism of E which swaps the complex roots and leaves all the other roots invariant. This means the subgroup $\mathrm{Gal}\,(E/\mathbb{Q}) \leq S_p$ has a transposition. Thus $\mathrm{Gal}\,(E/\mathbb{Q}) \leq S_p$ has a transposition and a p-cycle. By Proposition 8.11, we deduce that $\mathrm{Gal}\,(E/\mathbb{Q})$ is S_p.

Example 8.13. Consider the quintic polynomial $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$. It is irreducible over $\mathbb{Q}$ by Eisenstein criterion. We have

$$f(-2) = -17,\ f(-1) = 8,\ f(1) = -2 \text{ and } f(2) = 23.$$

Using the intermediate value theorem, we conclude that f has at least 3 real roots. If f has four real roots, then Rolle's theorem says that there will be at least 3 *distinct* real roots of f' and hence at least two *distinct* roots of f''. Since $f'' = 20x^3$, $\alpha = 0$ is the only (though multiple) root of f''. So we conclude that f has exactly three real roots and 2 complex roots. Hence the Galois group of f is S_5, which is not solvable. We conclude that f is not solvable by radicals over $\mathbb{Q}$.

Ex. 8.14. Show that $2x^5 - 10x + 5 \in \mathbb{Q}[x]$ is not solvable by radicals.

[1] This is the only place where we use the fact that p is a prime!

Example 8.15. Let p be an odd prime and that $2 \leq n \in \mathbb{N}$. Then the polynomial $f(x) = x^5 - npx + p$ is not solvable by radicals.

The polynomial $f(x)$ is irreducible over $\mathbb{Q}$ by Eisenstein criterion. The roots of the derivative $5x^4 - np$ are $\pm\sqrt[4]{np/5}$. Since f' has only two roots, Rolle's theorem says that f has at most three real roots.

When $x \ll 0$, then $f(x) < 0$ and $f(0) = p > 0$. So, there is a negative real root.

We have $f(1) < 0$. So, f has a root between 0 and 1.

Since for $x \gg 0$, $f(x) > 0$. So there is a real root between 1 and such an x. We conclude that f has exactly 3 real roots. Proposition 8.11 asserts that $\mathrm{Gal}\,(K/\mathbb{Q})$ is S_5. From Theorem 8.10, it follows that f is not solvable by radicals.

Example 8.16. For each $n \geq 5$ there exist polynomials $f(x) \in \mathbb{Q}[x]$ of degree n which are not solvable by radicals.

Let $p(x)$ be any quintic polynomial whose Galois group is S_5. Let $f(x) = x^{n-5}p(x)$. Let K be the splitting field of f over $\mathbb{Q}$. Then $\mathrm{Gal}\,(K/\mathbb{Q})$ contains a subgroup that is isomorphic to S_5. It follows that $\mathrm{Gal}\,(K/\mathbb{Q})$ is not solvable and therefore the polynomial is not solvable by radicals.

Example 8.17. Any polynomial of degree less than 5 is solvable by radicals.

8.1 Solvable Groups

Topics: Solvable groups: Definition, examples, subgroups and quotients are solvable, A_5 is not solvable.

Definition 8.18. A group G is said to be *solvable* if it has a chain of subgroups

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{n-1} \supset G_n = \{e\},$$

such that each G_i is normal in its immediate predecessor G_{i-1} (for $1 \leq i \leq n$) and the quotient G_{i-1}/G_i is abelian.

Example 8.19. Every abelian group is solvable.

Example 8.20. Let $H := \langle(123)\rangle \leq S_3$. Then $S_3 \supset H \supset \{e\}$ shows that S_3 is solvable.

Example 8.21. Show that the dihedral group D_{2n} is solvable.

Theorem 8.22. *Let $n \geq 5$. Then S_n is not solvable.*

Proof. Assume, on the contrary, that S_n is solvable. Let

$$S_n = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\},$$

as required by the definition. Let $(a_1a_2a_3)$ be any 3-cycle. Choose a_4, a_5 distinct from a_1, a_2, a_3. Since G_1 contains the commutator of G_0, we have

$$\begin{aligned}(a_1a_2a_4)(a_1a_3a_5)(a_1a_2a_4)^{-1}(a_1a_3a_5)^{-1} &= \left((a_1a_2a_4)(a_1a_3a_5)(a_1a_2a_4)^{-1}\right)(a_1a_5a_3)\\ &= (a_2a_3a_5)(a_1a_5a_3)\\ &= (a_1a_2a_3) \in G_0.\end{aligned}$$

Thus any 3-cycle of S_n lies in G_1. Repeating this argument for the pair (G_1, G_2) in place of (G_0, G_1), we see that G_2 contains all 3-cycles. Proceeding this way, we find that $G_n = \{e\}$ contains all 3-cycles! □

Theorem 8.23. *A group is solvable iff there is a chain of groups*

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_{n-1} \supset G_n = \{e\},$$

such that for any $x, y \in G_i$ we have $aba^{-1}b^{-1} \in G_{i+1}$ for $0 \leq i \leq n-1$.

Proof. The proof depends on the following well-known facts: (i) If G/H is abelian, then the commutator subgroup $[G, G]$ (generated by $\{xyx^{-1}y^{-1} : x, y \in G\}$ is a subgroup of H.
(ii) If $K \leq G$ is such that the commutator subgroup $[G, G] \subset K$, then K is normal in G. To see this, let $x \in K$ and $a \in G$. Observe that

$$K \ni axa^{-1}x^{-1} = (axa^{-1})x^{-1} \text{ and } x \in K.$$

Let G be solvable. Keep the notation of Definition 8.18. Since G_i/G_{i+1} is abelian, in view of (i), it follows that $xyx^{-1}y^{-1} \in G_{i+1}$ for $0 \leq i \leq n-1$.

To see the converse, we need only show that the subgroups G_{i+1} is normal in G_i. This is an immediate consequence of (ii). □

Theorem 8.24. *Every homomorphic image of a solvable group is solvable.*

Proof. Easy. If we keep the notation of the definition (or as in Theorem 8.23), then the chain $H_0 \supset H_1 \supset \cdots \supset H_n$ where $H_i := f(G_i)$ is as required by the definition (or as by Theorem 8.23). □

We can prove a result stronger than the last.

Theorem 8.25. *Let $N \trianglelefteq G$. Then G is solvable iff N is solvable and the quotient group G/N is solvable.*

Proof. Let G be solvable. We use the standard notation. Let $N_i := N \cap G_i$. Then it is easy show that the chain $N_0 \supset N_1 \supset \cdots \supset N_n$ satisfies the conditions of Theorem 8.23 and hence N is solvable.

Since G/N is the homomorphic image under the quotient map $\pi\colon G \to G/N$, solvability of G/N follows from Theorem 8.24.

To prove the converse, let $N_0 \supset N_1 \supset \cdots \supset N_r = \{e\}$ be chain assured by the solvability of N via Theorem 8.23.

Similarly, if we let $H := G/N$, we have a chain $H_0 \supset N_1 \supset \cdots \supset H_s = \{e_H\}$. This gives rise to a chain $G_0 \supset G_1 \supset \cdots \supset G_s = N$ where $G_i := \pi^{-1}(H_i)$. To this we adjoin the chain for N to get

$$G_0 \supset G_1 \supset \cdots \supset G_s = N = N_0 \supset N_1 \cdots N_r = \{e\}.$$

This chain satisfies the conditions of Theorem 8.23. □

Note: I plan include the following topics: (i) Symmetric functions, (ii) Cyclotomic polynomials, (iii) Special case of Primes in AP, (iv) Inverse Galois theory: Finite abelian groups as galois groups of extensions over $\mathbb{Q}$. Possibly another 10 pages and quite probably by the end of December 2014!