Outline of a Course in Field Theory (Expanded Version)

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

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 (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 2. *The polynomial ring $F[x]$ is a PID.* □

Definition 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 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 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 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 7. *Let $f \in F[x]$ be irreducible. Then the quotient ring $F[x]/(f)$ is a field.* □

Theorem 8 (Gauss Lemma)**.** *A polynomial $f \in \mathbb{Z}[x]$ is irreducible* over $\mathbb{Q}$ *iff it is irreducible in the ring $\mathbb{Z}[x]$, that is, it cannot be expressed as a product of polynomials in $\mathbb{Z}[x]$ of lower degree.* □

Theorem 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 $\mathbb{Q}$.

Ex. 10. Extend the last theorem as follows. Let R be a ring, and P a prime ideal of R. Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$. 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. 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. 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. 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. 14. $\Phi_{p^2}(x) := \frac{x^{p^2} - 1}{x^p - 1}$ is irreducible. Apply the trick of the last exercise.

Ex. 15. Let R be an integral domain. Then $f(x) = a_0 + \cdots + a_n x^n$ with $a_0 \neq 0$ is irreducible over R iff the *reciprocal polynomial* $\tilde{f}(x)$ defined by $\tilde{f}(x) = x^n f(1/x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n$ 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 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 $s | a_n$.*

Corollary 17. *If $f(x) \in \mathbb{Z}[x]$ is monic, then any rational root must be an integer dividing a_0.* $\square$

Ex. 18. Show that 3 is the only rational root of $x^3 - 2x^2 - 2x - 3$.

Ex. 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. 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. 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. 22. Show that $f(x) = x^2 - 8x - 2$ is irreducible over $\mathbb{Q}$.

Ex. 23. Show that $f(x) = x^3 + 3x^2 - 8$ is irreducible over $\mathbb{Q}$.

Ex. 24. Show that $x^4 - 10x^2 + 1$ is irreducible in $\mathbb{Q}[x]$.

Ex. 25. Show that the polynomial $x^2 + x + 1$ is irreducible in $\mathbb{Z}_3[x]$.

Ex. 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 27. 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 28. 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 29. Let E be any field and F its prime subfield. Then E/F is an extension. (It may happen $E = F$!)

Example 30. Let F be any field and $E := F(x)$, the field of rational functions on F. Then E/F is a simple extension.

Example 31. 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 32 (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 $[K : F] = [K : E][E : F]$.*

Proposition 33. *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 $f(\alpha) = 0$.*

Definition 34. 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 35. *Any finite extension E/F is algebraic.*

Proposition 36 (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.*

Definition 37. The polynomial m_α of the last proposition is said to be the *minimal polynomial* of α over F.

Theorem 38. *A simple extension $F(\alpha)/F$ is finite iff α is algebraic over F. Also, in such a case, we have $[F(\alpha) : F] = \deg m_\alpha$.*

Corollary 39. *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.* □

Ex. 40. 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. 41. 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. 42. Let p and q be distinct primes. Show that $\mathbb{Q}(\sqrt{p}, \sqrt{q})/Q$ is of degree 4. Using induction show that $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.

Ex. 43. 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. 44. Show that a finite extension of prime degree is a simple extension.

Ex. 45. 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. 46. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Ex. 47. 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. 48. 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. 49. Let $a, b \in \mathbb{Q}$. Find the minimal polynomial of $a + b\sqrt{2}$.

Ex. 50. 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. 51. 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. 52. (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. 53. 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. 54. 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. 55. 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. 56. 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. 57. 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. 58. 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. 59. 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. 60. 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. 61. 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. 62. 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. 63. 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. 64. 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. 65. 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. 66. Let $E = F(\alpha)$ be algebraic over F with $[F(\alpha) : F]$ being odd. Show that $F(\alpha) = F(\alpha^2)$.

Ex. 67. Let E/F be a finite extension of degree n. If F is finite with q elements, then E has q^n elements.

Ex. 68. Exhibit an irreducible degree 3 polynomial in $\mathbb{Z}_3[x]$. Hence conclude that there exists an field of 27 elements.

Ex. 69. Show that there exist finite fields of p^2 elements for every prime $p \in \mathbb{N}$.

Ex. 70. Let $\alpha \in E/F$ be transcendental over F. Show that any $\beta \in F(\alpha)\backslash F$ is transcendental over F.

Ex. 71. 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. 72. 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. 73. Let F be a finite field with prime characteristic p. Show that every element of F is algebraic over the prime field..

Ex. 74. Show that every finite field has p^n elements for some prime p.

Definition 75. 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. 76. Let E/F be an extension such that $E = F(\alpha_1, \dots, \alpha_k)$. If an F-automorphism θ of E leaves each of α_j, $1 \le j \le k$ 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 77. 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 $\alpha_1, \dots, \alpha_n \in E$ 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.

Lemma 78. *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

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

Theorem 79 (Kronecker)**.** *Let $f \in F[x]$ be a nonconstant polynomial. Then there exists an extension E/F and an $\alpha \in E$ such that $f(\alpha) = 0$.*

Corollary 80. *Let $f \in F[x]$. Then there exists a splitting field of f over F.*

Corollary 81. *Let E/F and K/F be extensions. Let $f \in F[x]$. Assume that there exist $\alpha \in E$ and $\beta \in K$ such that $f(\alpha) = 0 = f(\beta)$. Then $F(\alpha)$ and $F(\beta)$ are F-isomorphic.*

Theorem 82. *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.* □

Corollary 83. *Any tow splitting fields of $f \in F[x]$ are F-isomorphic.* □

Corollary 84. *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.* □

Ex. 85. 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 86. 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 87. *An extension E/F is a splitting field of some polynomial $f \in F[x]$ if the extension E/F is finite and normal.* □

Example 88. $f(x) = x^p - a$, p a prime and $a \neq 0$ over $\mathbb{Q}[x]$.

Example 89. $f(x) = x^6 - 1$ 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 90. $f(x) = x^6 + 1$ 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 $|\mathbb{Q}(i, \xi) : \mathbb{Q}| = 4$.

Example 91. $f(x) = x^2 + ax + b \in F[x]$.

Ex. 92. 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. 93. 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. 94. 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. 95. 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. 96. Let $|E : F| = 2$. Show that E is the splitting field over F.

Ex. 97. Let E be a splitting field of $f(x) \in F[x]$. Show that any F-automorphism of E permutes the roots of f.

Ex. 98. Let $p \in \mathbb{N}$ be a prime. Show the the splitting field of $x^p - 1$ over $\mathbb{Q}$ is of degree $p - 1$.

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 99. Let $f = a_0 + a_1 x + \cdots + a_n x^n \in F[x]$. Then the formal derivative $Df \in F[x]$ is defined by $Df = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$. Note that $D\colon F[x] \to F[x]$ is F-linear.

Definition 100. Let $f \in F[x]$. An element $\alpha \in E$ where E/F is an extension field, is said to be *repeated root* if $(x - \alpha)^2$ is a divisor of f in $E[x]$. A root of f, which is not a repeated root is called a simple root.

Proposition 101. *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 ad 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 $f(x)$. ∎

Proposition 102. *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, $f(x) = a_0 + a_1 x^p + a_2 x^{2p} + \cdots + a_n x^{np}$.*

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

Definition 104. 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 105. *An irreducible polynomial is separable iff $Df = 0$.* □

Definition 106. An algebraic extension E/F is said to be separable iff the minimal polynomial of each element of E is separable over F.

Corollary 107. *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 108. 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 e 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.

5 Finite Fields

Lemma 109. *Let F be a field of characteristic $p > 0$. Then $(x + y)^p = x^p + y^p$ and $(xy)^p = x^p y^p$ for all $x, y \in F$. In particular, $x \mapsto x^p$ is an injective field homomorphism of F to itself.* □

Theorem 110. *A field E has p^n elements iff it is a splitting field of the polynomial $x^{p^n} - x$ over its prime subfield $\mathbb{Z}_p$.* □

Corollary 111. *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.* □

The field $GF(p^n)$ is called the Galois field of order p^n. Recall the Euler's function $\varphi(n)$ defined on $\mathbb{N}$: $\varphi(n)$ is the number of integers m such that $0 < m < n$ such that m and n are coprime.

Theorem 112. *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 $G = \langle a \rangle$. □

Theorem 113 (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 $E = K(\alpha, \beta)$. Then α and β are algebraic over F. Let f and g be the minimal polynomials of α and β. Let $K := \mathrm{Split}(fg, F)$ 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 g 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 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 114. 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 115. $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\sqrt{2} + i)$.

Example 116. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Example 117. $\mathbb{Q}(\sqrt{2}, \sqrt{3}, i) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + i)$.

Example 118. 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 119. 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 $\alpha = t^2$ 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

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

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

6 Galois Theory

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

Definition 120. 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.

Lemma 121. *Let E/F be a finite separable extension. Then $|\mathrm{Gal}\,(E/F)| \leq [E : F]$, that is, the order of the Galois group of E/F is at most the degree of E/F.*

Definition 122. 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.

Theorem 123. *Let E be a field and G be a group of automorphisms of E. Let $F := E^G$ be the fixed field of G. Then*
(i) *E/F is algebraic,*
(ii) *for each $\alpha \in E$, the minimal polynomial $m_\alpha(x) = (x-\alpha_1)\cdots(x-\alpha_k)$ where $\{ga_1, \ldots, \alpha_k\}$ is the G-orbit of α, that is, the set $\{\sigma(\alpha) : \sigma \in G\}$.*

Definition 124. An extension E/F is said to be a Galois extension if it is separable and normal.

Theorem 125. *Let E be a field and G a group of automorphisms of E. Let F be the fixed field of G. Then*
(i) *E/F is a Galois extension,*
(ii) *The Galois group of E/G is G,*
(iii) *We have $[E : F] = |\mathrm{Gal}\,(E/)|$.*

Theorem 126. *Let E/F be a finite extension and let $\mathrm{Gal}\,(E/F)$ be the Galois group of E/F. Then*
(i) *$|\mathrm{Gal}\,(E/F)|$ divides $[E : F]$,*
(ii) *$|\mathrm{Gal}\,(E/F)| = [E : F]$ iff E/F is a Galois extension, in which case F is the fixed field of $\mathrm{Gal}\,(E/F)$.*

Proposition 127. *Let E, F, K be fields such that $F \subset K \subset E$. Assume that E/F is Galois. Then E/K is Galois. If K/F is normal, then K/F is also Galois.*

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 $\mathrm{Gal}\,(E/F)$. Let $\mathcal{K}$ denote the set of intermediate fields of E/F and $\mathcal{H}$, the set of subgroups of G. Consider the maps

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

The next theorem, the main result of Galois theory related these two maps.

Theorem 128 (Galois Correspondence)**.** *Let E/F be a Galois extension and let* $\mathrm{Gal}\,(E/F)$ *be its Galois group. The maps from $\mathcal{K}$ to $\mathcal{H}$ and vice-versa*

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

are inverses of each other.

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

7 Appendices

7.1 Roth's Paper

The following theorem is by Roth. (AMM Vol 78 Pages 392-393)

Theorem 129. *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 $\sqrt{q_1 \cdots q_r} \notin F$.*

Proof. We prove this by induction on n. Let $n = 0$. Then $F = \mathbb{Q}$. If $q_1, \ldots, q_r$ are distinct primes, then the polynomial $x^2 - q_1 q_2 \cdots q_r$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein criterion. Hence $\sqrt{q_1 \cdots q_r} \notin F$. One may also adapt the classic proof of the irrationality of $\sqrt{2}$ to show that $\sqrt{q_1 \cdots q_r} \notin F$.

Now assume the result for $n-1$, $n > 1$. Let $F = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$. If we let $F_0 := \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$, then $F = F_0(\sqrt{p_n})$. Since result is true for $n-1$ and since $p_n \neq p_j$, $1 \leq j \leq n-1$, it follows that F is a degree 2 extension of F_0. Let $q_1, \ldots, q_r$ be distinct primes none of which lie in $\{p_1, \ldots, p_n\}$.

Let, if possible, $\sqrt{q_1 \cdots q_r} \in F$. Then we can write $\sqrt{q_1 \cdots q_r} = a + b\sqrt{p_n}$, with $a, b \in F_0$. We have

$$q_1 \cdots q_r a^2 + b^2 p_n + 2ab\sqrt{p_n}. \tag{1}$$

We consider 3 cases.

(i) $ab \neq 0$. Then (1) shows that

$$\sqrt{p_n} = \frac{q_1 \cdots r_q - a^2 - p_n b^2}{2ab} \in F_0,$$

a contradiction.

(ii) $b = 0$. Then $\sqrt{q_1 \cdots q_r} = a \in F_0$, contradiction to the induction hypothesis.

(iii) $a = 0$. Then $\sqrt{q_1 \cdots q_r} = b\sqrt{p_n}$. Therefore, $\sqrt{q_1 \cdots q_r p_n} = bp_n \in F_0$. This contradicts the induction hypothesis.

Hence we conclude that the result is true. □

Corollary 130. *If a prime $q \notin \{p_1, \ldots, p_n\}$, a set of primes, then $\sqrt{q} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$.* $\square$

Corollary 131. *If $p_1, \ldots, p_n$ are distinct primes, then $|\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}| = 2^n$.* $\square$

Example 132. We list some of the typical uses of the result.

1. $|\mathbb{Q}(\sqrt{2}, \sqrt{7}, \sqrt{15}) : \mathbb{Q})| = 8$.
2. $|\mathbb{Q}(\sqrt{14}, \sqrt{15}) : \mathbb{Q})| = 4$. For, $\sqrt{3 \cdot 5} \notin \mathbb{Q}(\sqrt{14}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{7})$.
3. $|\mathbb{Q}(\sqrt{14}, \sqrt{6}) : \mathbb{Q}| = 4$. For, if $\sqrt{14} \in \mathbb{Q}(\sqrt{6}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, then $\sqrt{7} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

7.2 Cyclotomic Polynomials

The proof below is due to Landau and is taken from an article by Weintraub.

Proof. Let $f(x) \in \mathbb{Z}[x]$ be irreducible of degree d. Let ξ be an n-th root of unity such that $f(\xi) = 0$. Let $j \in \mathbb{N}$. By division algorithm, we have unique polynomials $q_j(x)$ and $r_j(x)$ such that $f(x^j) = q_j(x)f(x) + r_j(x)$ where $\deg r_j < d$. Observe that the value of $f(\xi^j)$ depends on the congruence class of j modulo n. Therefore, we have a finite set $\{r_1(x), \ldots, r_{n-1}(x)\}$ of polynomials such that for any $j \in \mathbb{Z}$, we have $f(\xi^j) = r(\xi)$ for some polynomial r in the this finite set. Also, note[1] that if s is any polynomial of degree less than d such that $s(\xi^j) = s(\xi)$, then $s(x) = r(x)$. For, otherwise, ξ will be a root of the nonzero polynomial $s(x) - r(x)$ of degree less than d, a contradiction.

Let us specialize j. Let $j = p$ be a prime. Then we have $f(\xi^p) = f(\xi^p) - f(\xi)^p = r(\xi)$ for some r in the finite list above. It is a trivial verification to see that $f(x^p) \equiv f(x)^p \pmod{p}$. Therefore, we can write this as $f(x^p) - f(x)^p = pg(x)$ for some polynomial g. Again, by division algorithm, there is a unique polynomial h of degree less than d such that $g(\xi) = h(\xi)$. Thus, $r(\xi) = p \times g(\xi)$ with $\deg r(x) < d$ an $\deg ph(x) < d$. In view of the Note 1, we conclude that $r(x) = p \times h(x)$. In particular, each coefficient of r is divisible by p.

Let A be the largest absolute value of the coefficients of all the polynomials $r(x)$ in he finite set. If the prime $p > A$, the observation that p divides the coefficients of r forces us to conclude that $r(\xi) = 0$. That is, $f(\xi^p) = r(\xi) = 0$ for any prime $p > A$. As a consequence of this, if m is an integer not divisible by any prime $p \leq A$, then $f(\xi^m) = 0$.

Let $k \in \mathbb{Z}$ be relatively prime to n. Consider $m := k + n \prod q$ where q runs through all primes $p \leq A$ that do NOT divide k.

Let $p \leq A$ be any prime.
(i) If p divides k, then p does not divide m. For, k and n are relatively prime and p does not divide $\prod q$.
(ii) If p does not divide k, then p appears in $\prod q$ and hence p does not divide m.

We are thus lead to the conclusion that if m is as above, $m \equiv k \pmod{n}$ and so $f(\xi^k) = f(\xi^m) = 0$. That is, if k is relatively prime to n, then ξ^k is also a root of $\Phi_n(x)$. This proves that $\Phi_n(x)$ is irreducible. $\square$

[1]

Also, have a look at We follow Lorenz in this section. See Theorem 3 on page 89 and and Theorem 3' on page 91 of Lorenz' Algebra Volume 1.

Miles: Galois Theory Notes Pages 86-87 for the Irreducibility of the cyclotomic polynomial $\Phi_n(x)$.

This is Landau's proof. A clear detailed exposition is available in Weintraub's article. See Galois Theory folder in Math books.

Schur's proof in the same article is easier and better.

7.3 Dirichlet's Theorem on Primes in Arithmetic Progression

The theorem of the title says that for any two integers n, m with $\gcd(n, m) = 1$, there exist infinitely many primes in the arithmetic progression $m + nk$, $k \in \mathbb{Z}$.

We shall prove a special case of this result when $m = 1$.

7.4 Abelian Groups as Galois Groups over $\mathbb{Q}$

Cyclotomic polynomials and Dirichlet's theorem on primes in AP of the form $1 + nk$. Refer to Fenrick Pages 173–178.

Abelian groups as Galois groups. Refer to Fenrick.