Outline of a Course in Field Theory

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* 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 $g_j \in F[x]$, $1`j \leq n$, 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.*

Definition 8. A polynomial $f \in \mathbb{Z}[x]$ is said to be *primitive* if the GCD of the coefficients is 1. In particular, any monic polynomial is primitive.

Lemma 9 (Gauss Lemma). *Let $f, g \in \mathbb{Z}[x]$ be primitive. Then the product fg is primitive.*

Theorem 10. *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 11 (Eisenstein's Irreducibilty 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 $\mathbb{Q}$.

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 12. 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 $[E : F]$ 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 $S = \{\alpha_1, \dots, \alpha_k\}$, we denote $F(S)$ by $F(\alpha_1, \dots, \alpha_k)$.

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

Example 13. 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 14. Let E be any field and F its prime subfield. Then E/F is an extension. (It may happen $E = F$!)

Example 15. Let F be any field and $E := F(x)$, the field of rational functions on F. Then E/F is a simple extension.

Example 16. 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 17 (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 $[K : F] = [K : E][E : F]$.*

Ex. 18. Show that a finite extension of prime degree is a simple extension.

Ex. 19. Find the degrees of the following extensions: (i) $E := \mathbb{Q}(\sqrt[3]{2}, i)$ and $F = \mathbb{Q}$, (ii) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/Q$.

Ex. 20. Let E, K, F are fields such that $F \subset K \subset E$. Show that if $[E : F]$ is finite then $[E : K]$ and $[K : F]$ are finite and that $[E : F] = [E : K][K : F]$.

Ex. 21. Let p and q be distinct primes. Show that $\mathbb{Q}(\sqrt{p}, \sqrt{q})/Q$ is of degree 4. Using induction show that $[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.

Ex. 22. Show that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Ex. 23. This is an extension of the last exercise. 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. 24 (A proposition)**.** 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 $f(\alpha) = 0$. *Hint:* Consider the kernel of the ring homomorphism $f \mapsto f(\alpha)$ from $F[x]$ to $E; F(\alpha)$.

Definition 25. 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 26. *Any finite extension E/F is algebraic.*

Proposition 27 (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 $m_\alpha = m_{\alpha,F} \in F[x]$ with the following property: $f \in F[x]$ is such that $f(\alpha) = 0$, iff m_α divides f.*

Definition 28. The polynomial m_α of the last proposition is said to be the *minimal polynomial* of α over F.

Ex. 29. 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. 30. Find the minimal polynomial

Ex. 31. Let E/F be an extension and let $\alpha \in E$ be algebraic over F. Show that the subfield $F(\alpha) = \{p(\alpha) : p \in F[x]\}$.

Theorem 32. *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 33. *A field extension E/F is finite iff there exist $\alpha_1, \dots, \alpha_k \in E$ such that $E = F(\alpha_1, \dots, \alpha_k)$ and each α_j is algebraic over F.*

Ex. 34. 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. 35. Let E/F and L/E be algebraic extensions. Show that L/F is an algebraic extension.

Ex. 36. Let E/F be an extension, $\alpha_j \in E$, $1 \leq j \leq n$ be algebraic over F. Show that $F(\alpha_1, \dots, \alpha_n)/F$ is a finite extension.

Ex. 37. 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. *Hint:* Last exercise.

Ex. 38. 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.)

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

Ex. 39. 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. 40. Let $E = F(\alpha)$ be algebraic over F with $[F(\alpha) : F]$ being odd. Show that $F(\alpha) = F(\alpha^2)$.

Definition 41. 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. 42. 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 43. 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 44. *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 45 (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 46. *Let $f \in F[x]$. Then there exists a splitting field of f over F.*

Corollary 47. *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 48. *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 49. *Any tow splitting fields of $f \in F[x]$ are F-isomorphic.*

Corollary 50. *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. 51. 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 52. 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 53. *An extension E/F is a splitting field of some polynomial $f \in F[x]$ if the extension E/F is finite and normal.*

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 54. 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 55. 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 56. *A polynomial $f \in F[x]$ has a repeated root in a splitting field over F iff there exists a non-constant polynomial $g \in F[x]$ that divides both f and its derivative Df in $F[x]$.*

Proposition 57. *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 $f(x) = g(x^p)$.

Definition 58. 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 59. *An irreducible polynomial is separable iff $Df = 0$.*

Definition 60. An algebraic extension E/F is said to be separable iff the minimal polynomial of each element of E is separable over F.

Corollary 61. *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.*

5 Finite Fields

Lemma 62. *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 63. *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 64. *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.

Lemma 65. *For any $n \in \mathbb{N}$, we have $\sum_{d|n} \varphi(d) = n$.*

Theorem 66. *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.

Theorem 67 (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.*

6 Galois Theory

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

Definition 68. 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 69. *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 70. 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 71. *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 72. An extension E/F is said to be a Galois extension if it is separable and normal.

Theorem 73. *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 74. *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 75. *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 76 (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 $\mathrm{Gal}\,(K/F) \simeq \mathrm{Gal}\,(E/F)/\mathrm{Gal}\,(E/K)$.