Summary Portfolio

Alex Thies
athies@uoregon.edu

March 15, 2018

Contents

7 Polynomials over a Ring **1**
- 7.1 Polynomials over a Ring . . . 1
- 7.2 Properties of Polynomial Rings . . . 2
- 7.3 Polynomial Functions and Roots . . . 3

8 Factoring Polynomials **3**
- 8.1 Factors and Irreducible Polynomials . . . 3
- 8.2 Roots and Factors . . . 4
- 8.3 Factorization over $\mathbb{Q}$ . . . 4

9 Field Extensions **5**
- 9.1 Extension Field . . . 5
- 9.2 Minimum Polynomial . . . 6
- 9.3 Algebraic Extensions . . . 6
- 9.4 Root Field of a Polynomial . . . 7

10 Galois Theory **8**
- 10.1 Isomorphisms and Extension Fields . . . 8
- 10.2 Automorphisms of Root Fields . . . 8
- 10.3 The Galois Group of a Polynomial . . . 9
- 10.4 The Galois Correspondence . . . 9

11 Solvability **9**
- 11.1 Three Construction Problems . . . 9
- 11.2 Solvable Groups . . . 10
- 11.3 Solvable by Radicals . . . 10

12 Constructible Numbers **11**

7 Polynomials over a Ring

7.1 Polynomials over a Ring

Definition 1. *Let A be a commutative ring with unity. For each nonnegative integer n and elements $a_0, a_1, \ldots, a_n \in A$ we can define a polynomial over A, $a(x)$, by:*

$$a(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \qquad \text{or} \qquad \sum_{i=0}^{n} a_i x^i.$$

The set of all polynomials over a ring A is denoted $A[x]$.

Definition 4. *Suppose A is a commutative ring with unity and $a(x) \in A[x]$ with $a(x) = a_0 + a_1 x + \cdots + a_n x^n$ for some nonnegative integer n.*

(i) The elements $a_0, a_1, \ldots, a_n \in A$ are the coefficients of $a(x)$.

(ii) For each $0 \leq i \leq n$, $a_i x^i$ is called a term of $a(x)$.

(iii) The largest nonnegative integer n with $a_n \neq 0_A$ (if one exists) is the degree of $a(x)$, denoted $\deg(a(x)) = n$. So for $k > n$ we know $a_k = 0_A$.

(iv) If all coefficients of $a(x)$ are 0_A we say the degree of $a(x)$ is $-\infty$.

(v) For $n \geq 0$ if $\deg(a(x)) = n$ then a_n is called the leading coefficient of $a(x)$.

Definition 5. *Let A be a commutative ring with unity. For polynomials $a(x), b(x) \in A[x]$ we say $a(x) = b(x)$ if and only if they have the same degree and if the degree is equal to $n \geq 0$ then for every $i \leq n$, $a_i = b_i$.*

Definition 6. *Let A be a commutative ring with unity and let $a(x), b(x) \in A[x]$ as shown below.*

$$a(x) = \sum_{i=0}^{n} a_i x^i \qquad\qquad b(x) = \sum_{i=0}^{m} b_i x^i$$

We define the new polynomial $c(x) = a(x) + b(x)$ as follows where $k = \max\{n, m\}$.

$$c(x) = \sum_{i=0}^{k} c_i x^i \quad \textit{and} \quad c_i = a_i + b_i$$

Remember, if $i > n$ or $i > m$ we assume $a = 0_A$ or $b = 0_A$, respectively.

Definition 8. *Let A be a commutative ring with unity and polynomials $a(x), b(x) \in A[x]$ as shown below.*

$$a(x) = \sum_{i=0}^{n} a_i x^i \qquad\qquad b(x) = \sum_{i=0}^{m} b_i x^i$$

Define the new polynomial $d(x) = a(x)b(x)$ *as follows.*

$$d(x) = \sum_{i=0}^{n+m} d_i x^i \quad \textit{where} \quad d_i = \sum_{j+t=i} a_j \cdot_A b_t$$

Note: $0 \leq j \leq n$ *and* $0 \leq t \leq m$*.*

Theorem 11. *Let* A *be a commutative ring with unity. The operations of polynomial addition and polynomial multiplication from Definitions 7.6 and 7.8 are associative in* $A[x]$*.*

Theorem 13. *Let* A *be a commutative ring with unity. In* $A[x]$*, polynomial addition and polynomial multiplication are both commutative.*

Theorem 14. *Let* A *be a commutative ring with unity. Then the distributive laws hold in* $A[x]$*.*

Theorem 15. *Let* A *be a commutative ring with unity. Then the set* $A[x]$ *of polynomials over* A *is a commutative ring with unity.*

7.2 Properties of Polynomial Rings

Theorem 17. *If* A *is an integral domain then* $A[x]$ *is also an integral domain.*

Theorem 20. *Let* A *be an integral domain, and nonzero* $a(x), b(x) \in A[x]$*. If* $\deg(a(x)) = n$ *and* $\deg(b(x)) = m$*, then* $\deg(a(x)b(x)) = n + m$*.*

Theorem 22. *If* A *is a commutative ring with unity then* $char(A) = char(A[x])$*.*

Theorem 24 (The Division Algorithm)**.** *Let* K *be a field and* $a(x), b(x) \in K[x]$*. If* $b(x) \neq 0(x)$ *then there exist unique polynomials* $q(x), r(x) \in K[x]$*, for which* $a(x) = b(x)q(x) + r(x)$ *and either* $\deg(r(x)) < \deg(b(x))$ *or* $r(x) = 0(x)$*.*

Theorem 26. *Let* K *be a field. Then every ideal of* $K[x]$ *is a principal ideal.*

Theorem 27. *Let* A *be a commutative ring with unity. Then the function* $f : A \to A[x]$ *defined by* $f(a) = a + 0_A x$ *is an injective ring homomorphism.*

Theorem 28. *Let* A *and* K *be commutative rings with unity, and suppose that* $f : A \to K$ *is a ring homomorphism. Then the function* $\bar{f} : A[x] \to K[x]$ *defined below is also a ring homomorphism.*

$$\bar{f}(a_0 + a_1 x + \cdots + a_n x^n) = f(a_0) + f(a_1)x + \cdots + f(a_n)x^n$$

Theorem 30. *Let* A, K *be commutative rings with unity, and suppose that* $f : A \to K$ *is an isomorphism. Then the extension* $\bar{f} : A[x] \to K[x]$ *is also an isomorphism.*

7.3 Polynomial Functions and Roots

Definition 33. *Let A be a commutative ring with unity and $a(x) \in A[x]$ with $a(x) \neq 0(x)$. If $c \in A$ and $\deg(a(x)) = n$, we define the element $a(c) \in A$ as follows:*

$$a(c) = a_0 +_A (a_1 \cdot_A c) +_A (a_2 \cdot_A c^2) +_A \cdots +_A (a_n \cdot_A c^n).$$

If $a(x) = 0(x)$ we say $a(c) = 0_A$ for all $c \in A$.

Theorem 35. *Let A be an integral domain. The substitution function $h_c : A[x] \to A$ defined by $h_c(a(x)) = a(c))$ is a ring homomorphism.*

Definition 37. *Let A be a commutative ring with unity, $c \in A$, and $a(x) \in A[x]$ $a(x) \neq 0(x)$. We say that c is a root of the polynomial $a(x)$ exactly when $a(c) = 0_A$. We do not say any element of A is a root of $0(x)$ even though $0(c) = 0_A$ for each $c \in A$.*

8 Factoring Polynomials

8.1 Factors and Irreducible Polynomials

Definition 1. *Let A be a commutative ring with unity and $a(x), d(x) \in A[x]$. We say that $a(x)$ is a factor of $d(x)$ if there exists a polynomial $b(x) \in A[x]$ with $d(x) = a(x)b(x)$.*

Definition 4. *Let A be an integral domain. Polynomials $a(x), b(x) \in A[x]$ are called associates if there is a nonzero element $c \in A$ so that the constant polynomial $c(x) = c$ has $a(x) = c(x)b(x)$.*

We will frequently write $a(x) = cb(x)$ instead of first defining the constant polynomial $c(x) = c$.

Theorem 5. *Let A be an integral domain and suppose $a(x), b(x) \in A[x]$ are associates. Then $c \in A$ is a root of $a(x)$ if and only if c is a root of $b(x)$.*

Definition 7. *Let A be an integral domain with $a(x) \in A[x]$ and $\deg(a(x)) > 0$. We say that $a(x)$ is irreducible over A if every factor of $a(x)$ in $A[x]$ is either a constant polynomial or an associate of $a(x)$. If instead a nonconstant factor of $a(x)$ which is not an associate of $a(x)$ exists in $A[x]$, we say that $a(x)$ is reducible over A.*

Theorem 8. *Let K be a field and suppose $a(x), b(x) \in K[x]$ are associates. The polynomial $a(x)$ is irreducible over K if and only if $b(x)$ is irreducible over K.*

Theorem 9. *Let K be a field. Every polynomial in $K[x]$ of degree 1 is irreducible over K.*

Theorem 10. *Suppose K is a field, and $p(x) \in K[x]$. If $p(x)$ is irreducible over K then $\langle p(x) \rangle$ is a maximal ideal of $K[x]$.*

Theorem 11. *Let K be a field, and assume that $p(x) \in K[x]$ is irreducible over K. If $a(x), b(x) \in K[x]$ and $p(x)$ is a factor of the product $a(x)b(x)$, then $p(x)$ is a factor of at least one of $a(x)$ or $b(x)$.*

Theorem 12. *Let K and E be fields, and suppose that $\bar{f} : K \to E$ is an isomorphism. The polynomial $p(x) \in K[x]$ is irreducible over K if and only if $\langle p(x) \rangle$ is irreducible over E.*

8.2 Roots and Factors

Theorem 13. *Let K be a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. The element $c \in K$ is a root of $a(x)$ if and only if $b(x) = -c + x$ is a factor of $a(x)$.*

Theorem 17. *Suppose K is a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. If the distinct elements $c_1, c_2, \ldots, c_n \in K$ are all roots of $a(x)$, then the product $b(x) = (-c_1 + x)(-c_2 + x) \cdots (-c_n + x)$ is a factor of $a(x)$.*

Theorem 19. *Let K be a field. If $c_1, c_2, \ldots, c_n \in K$ are distinct roots of the nonzero polynomial $a(x) \in K[x]$, then $\deg(a(x)) \geq n$.*

Theorem 20. *Suppose K is a field and $a(x) \in K[x]$. If $\deg(a(x)) > 0$ then there exist a positive integer m and polynomials $b_1(x), b_2(x), \ldots, b_m(x) \in K[x]$ which are irreducible over K and $a(x) = b_1(x)b_2(x) \cdots b_m(x)$.*

Theorem 22. *Let K be a field and $a(x) \in K[x]$ with $\deg(a(x)) = 2$ or $\deg(a(x)) = 3$. The polynomial $a(x)$ is reducible over K if and only if $a(x)$ has a root in K.*

Definition 24. *Let K be a field and $a(x) \in K[x]$. Suppose $a(x) \neq 0(x)$, with $\deg(a(x)) = n$. The polynomial $a(x)$ is* ***monic*** *if $a_n = 1_K$.*

Definition 26. *Let K be a field and $a(x) \in K$ with $a(x) \neq 0(x)$. Suppose $c \in K$ is a root of $a(x)$. If there is an integer $m > 0$ for which the polynomial $b(x) = (-c + x)^m$ is a factor of $a(x)$ but $d(x) = (-c + x)^{m+1}$ is not a factor of $a(x)$, then we say that c is a root of $a(x)$ with multiplicity m.*

Theorem 27. *Let K be a field and $a(x) \in K[x]$ with $a(x) \neq 0(x)$. If $\deg(a(x)) = n$ then there can be at most n distinct roots of $a(x)$ in K.*

Theorem 28. *Let K be an infinite field. If $a(x), b(x) \in K[x]$, and $a(x) \neq b(x)$, then there must exist some $c \neq K$ for which $a(c) \neq b(c)$.*

8.3 Factorization over $\mathbb{Q}$

Theorem 29. *If $a(x) \in \mathbb{Q}[x]$ with $a(x) \neq 0(x)$ then there is a polynomial $b(x) \in \mathbb{Z}[x]$ with $\deg(a(x)) = \deg(b(x))$ which has exactly the same rational roots as $a(x)$.*

Theorem 31 (The Rational Roots Theorem)**.** *Let $a(x) \in \mathbb{Z}[x]$ with $a(x) \neq 0(x)$ and $\deg(a(x)) = n$. If the rational number $\frac{s}{t}$ ($s, t \in \mathbb{Z}$ with no common prime factors and $t \neq 0$) is a root of $a(x)$ then s must evenly divide a_0 and t must evenly divide a_n.*

Theorem 33. *If $a(x) \in Z[x]$ and $a(x) = b(x)c(x)$ with $b(x), c(x) \in \mathbb{Q}[x]$, $\deg(b(x)) > 0$, and $\deg(c(x)) > 0$, then there exist polynomials $u(x), w(x) \in \mathbb{Z}[x]$ with $a(x) = u(x)w(x)$, $\deg(u(x)) > 0$, and $\deg(w(x)) > 0$.*

Theorem 35 (Eisenstein's Criterion)**.** *Suppose $a(x) \in \mathbb{Z}[x]$ and $\deg(a(x)) = n$ with $n > 0$. If there exists a prime number p which divides coefficients $a_0, a_1, \ldots, a_{n-1}$ but not a_n, and p^2 does not divide a_0, then $a(x)$ is irreducible over $\mathbb{Q}$.*

Theorem 37. *Suppose $a(x) \in \mathbb{Z}[x]$ is a monic polynomial and $\deg(a(x)) = k$ with $k > 0$. If there exists $n > 1$ so that $\bar{f}_n(a(x))$ is irreducible in $\mathbb{Z}_n[x]$ then $a(x)$ is also irreducible in $\mathbb{Z}[x]$.*

9 Field Extensions

9.1 Extension Field

Definition 1. *Suppose that K and E are fields with $K \subseteq E$. If for all $a, b \in K$ we have $a +_K b = a +_E b$ and $a \cdot_K b = a \cdot_E b$, then K is a subfield of E or E is an extension field of K.*

Definition 2. *Suppose E is an extension field of K, and $c \in E$*

*(i) If there exists $a(x) \in K[x]$ with $a(x) \neq 0(x)$ and $a(c) = 0_E$, then c is **algebraic over** K.*

*(ii) If for <u>every nonzero</u> $a(x) \in K[x]$ we have $a(c) \neq 0_E$, then c is **transcendental over** K.*

Theorem 4. *Suppose E is an extension field of K, $a(x) \in K[x]$, and there is $c \in E$ with $a(c) = 0_E$.*

(i) If $\deg(a(x)) = 1$, then $c \in K$.

(ii) If $a(x)$ is irreducible over K and $\deg(a(x)) > 1$, then $c \notin K$

Theorem 5. *Suppose K is a field. E is an extension field of K and $c \in E$. If c is algebraic over K, then there exists a field $K(c)$ ("**K adjoin c**") with:*

(i) $K \subseteq K(c) \subseteq E$.

(ii) $c \in K(c)$.

(iii) For any subfield S of E with $K \subseteq S$ and $c \in S$ we have $K(c) \subseteq S$.

Theorem 7. *Let K be a field and assume $a(x) \in K[x]$ is irreducible over K. Then there exists a field E so that E is an extension field of K and $a(x)$ has a root in E.*

9.2 Minimum Polynomial

Theorem 9. *If K is a field, E is an extension field of K, and $c \in E$ is algebraic over K, then there is a* ***unique monic*** *polynomial $p(x) \in K[x]$ that is irreducible over K and has c as a root.*

Definition 10. *Let K be a field, E and extension field of K, and $c \in E$ algebraic over K. The unique monic polynomial $p(x) \in K[x]$ that is irreducible over K and has c as a root is called* ***the minimum polynomial*** *for c over K.*

Theorem 12. *Suppose K be a field, E and extension field of K, and $c \in E$ algebraic over K with minimum polynomial $p(x) \in K[x]$.*

(i) Using the homomorphism $f_c : K[x] \to E$ as defined in Theorem 9.5, $\ker(f_c) = \langle p(x) \rangle$.

(ii) If $b(x) \in K[x]$ is a nonzero polynomial with $b(c) = 0_E$, then $b(x) = p(x)q(x)$ for some $q(x) \in K[x]$.

Theorem 13. *Suppose K be a field, E and extension field of K, and $c \in E$ algebraic over K. If $p(x)$ is the minimum polynomial for c over K, and $\deg(p(x)) = n$, then:*

$$K(c) = \{a(c) : a(x) \in K[x] \text{ and either } a(x) = 0(x) \text{ or } \deg(a(x)) < n\}.$$

9.3 Algebraic Extensions

Definition 16. *Let K be a field and E an extension field of K. If every element of E is algebraic over K we say that E is an* ***algebraic extension*** *of K.*

Definition 17. *Let K be a field and E an extension field of K. A nonempty subset of E, $B = \{u_1, u_2, \ldots, u_m\}$ is called a* ***basis for E over K*** *when the following hold:*

(i) For every element $s \in E$ there exist $a_1, a_2, \ldots, a_m \in K$ so that $s = a_1u_1 + a_2u_2 + \ldots a_mu_m$ (B spans E over K).

(ii) If $a_1, a_2, \ldots, a_m \in K$ with $a_1u_1 + a_2u_2 + \ldots a_mu_m = 0_E$ then $a_i = 0_K$ for all $i = 1, \ldots, m$ (B is independent over K).

If there exist m elements of E that form a basis for E over K we say E is a ***finite extension*** *of K of degree m, and write $[E : K] = m$.*

Theorem 19. *Let K be a field and E an extension field of K.*

(i) Every basis for E over K has the same cardinality.

(ii) Every subset of E that spans E contains a basis for E over K.

Theorem 20. *Suppose K is a field, c is algebraic over K with minimum polynomial $p(x)$, and $\deg(p(x)) = n$. Then the set $B = \{1_K, c, c^2, \ldots, c^{n-1}\}$ is a bsis for $K(c)$ over K and $[K(c) : K] = \deg(p(x))$.*

Theorem 21. *Let K be a field and E an extension field of K with $[E : K] = n$ for some $n > 0$. Then E is an algebraic extension of K.*

Theorem 22. *Suppose that K is a field and L is a finite extension of K. If E is a finite extension of L, then E is also a finite extension of K and $[E : K] = [E : L][L : K]$.*

9.4 Root Field of a Polynomial

Definition 23. *Let K be a field and $a(x) \in K[x]$ have $\deg(a(x)) > 0$. The **root field for** $a(x)$ **over** K is a field extension E of K with the following properties:*

(i) In $E[x], a(x)$ can be factored into a product of polynomials of degree 1.

(ii) For any extension of K, L, which satisfies (i), we have $K \subseteq E \subseteq L$.

Definition 25. *Let K be a field and c_1, c_2 algebraic over K. Let $L = K(c_1)$, then the field $K(c_1, c_2) = L(c_2)$ is called the **iterated extension** of K.*

Theorem 26. *Let K be a field and $a(x) \in K[x]$ with $\deg(a(x)) > 0$. If E is the root field of $a(x)$ over K, and the elements $c_1, c_2, \ldots, c_n \in E$ are all of the distinct roots of $a(x)$, then $E = K(c_1, c_2, \ldots, c_n)$.*

Definition 28. *Suppose that E is an extension field of K with $c \in E$. A field extension $K(c)$ is called a **simple extension** of K.*

Definition 29. *Let K be a field and $p(x) \in K[x]$. We say $p(x)$ is **separable** if no irreducible factor of $p(x)$ has multiple roots in any extension field of K. Otherwise, we say $p(x)$ is **inseparable**.*

Theorem 31. *Let K be a field with char$(K) = 0$. Then every irreducible polynomial in $K[x]$ is separable.*

Theorem 32. *Let K be a finite field with char$(K) = q$ for some prime q.*

(i) For any polynomial $b(x) = b_0 + b_1x + \cdots + b_tx^t \in K[x]$ we have $(b(x))^q = b_0^q + b_1^qx^q + \cdots + b_t^qx^{qt}$.

(ii) For any element $s \in K$ there is $r \in K$ with $s = r^q$.

Theorem 33. *Let K be a finite field. Then every irreducible polynomial in $K[x]$ is separable.*

Theorem 34. *Let K be a field of characteristic 0, and E a finite extension of K. Then E is a simple extension of K, meaning there is some $c \in E$ with $E = K(c)$.*

10 Galois Theory

10.1 Isomorphisms and Extension Fields

Definition 2. *Let K be a field and $f : K \to K$ be a function. If f is an isomorphism we say that f is an* ***automorphism of K****.*

Definition 3. *Let K be a field and E_1, E_2 be exention fields of K. Suppose $f : E_1 \to E_2$ is an isomorphism. If for every $a \in K$ we have $f(a) = a$, then we say that* ***f fixes K****.*

Theorem 4. *Suppose K_1, K_2 are fields, $f : K_1 \to K_2$ is an isomorphism, and $p(x) \in K_1[x]$ is irreducible over K_1. Then there exist extension fields $K_1(c_1)$ and $K_2(c_2)$ with the following properties:*

(i) c_1 is a root of $p(x)$ and c_2 is a root of $\bar{f}(p(x))$ (as defined in Theorem 7.28).

(ii) There exists an isomorphism $g : K_1(c_1) \to K_2(c_2)$ with $g(c_1) = c_2$ for any $a \in K_1$, $g(a) = f(a)$.

Theorem 7. *Let K be a field and $p(x) \in K[x]$ an irreducible polynomial. If c_1 and c_2 are roots of $p(x)$ in some extension of K, then $K(c_1) \cong K(c_2)$ where the isomorphism $g : K(c_1) \to K(c_2)$ maps $g(c_1) = c_2$ and fixes K.*

Theorem 9. *Let K be any field and E_1, E_2 extension fields of K, with $f : E_1 \to E_2$ an isomorphism fixing K. If $p(x) \in K[x]$ and $c \in E_1$ is a root of $p(x)$, then $f(c) \in E_2$ is also a root of $p(x)$.*

10.2 Automorphisms of Root Fields

Theorem 10. *Let K be a field and $a(x) \in K[x]$. If $\deg(a(x)) = n > 0$, then $a(x)$ is <u>exactly</u> n roots in its root field.*

Theorem 12. *Suppose that K is a field and E_1, E_2 are both finite exentions of K. If there exists an isomorphism $f : E_1 \to E_2$ which fixes K, and E_1 is a root field of the polynomial $p(x) \in K[x]$, then $E_1 = E_2$.*

Theorem 13. *Suppose K is a field and E is the root field for some nonconstant $p(x) \in K[x]$. Suppose L_1 and L_2 are finite extension fields of K with $K \subseteq L_1 \subseteq E$. If there exists $f : L_1 \to L_2$ an isomorphism fixing K, then $L_2 \subseteq E$ and there exist an automorphism g of E, with $g(a) = f(a)$ for all $a \in L$.*

Theorem 14. *Suppose K is a field, E is the root field of a polynomial in $K[x]$, and $p(x) \in K[x]$ is irreducible over K with $\deg(p(x)) > 1$. For any two distinct roots $c_1, c_2 \in E$ of $p(x)$, there exists an automorphism of E fixing K, mapping c_1 to c_2.*

Theorem 16. *Suppose K is a field and E is the root field of a polynomial in $K[x]$. If the irreducible polynomial $a(x) \in K[x]$ has one root in E then every root of $a(x)$ is in E.*

10.3 The Galois Group of a Polynomial

Theorem 18. *Let K be a field and $p(x) \in K[x]$. If E is the root field of $p(x)$ over K then the set pf all automorphisms of E fixing K is a group under composition.*

Definition 19. *Let Kbe a field and $p(x) \in K[x]$ with root field E. The group of automorphisms of E fixing K is called the* ***Galois group of E over K****, denoted $Gal(E/K)$. It can also be called the* ***Galois group of p(x) over K****.*

Theorem 20. *Let K be a field and E the root field for some $p(x) \in K[x]$. The number of automorphisms of E fixing K is equal to $[E : K]$.*

Theorem 23. *Let K be a field and $p(x) \in K[x]$ with root field E. Let $G = Gal(E/K)$. If H is a subgroup of G then the set $E_H = \{y \in E : \alpha(y) = y \text{ for every } \alpha \in H\}$ is a subfield of E and $K \subseteq E_H \subseteq E$. The field E_H is called* ***the fixed field for H****.*

Theorem 24. *Let K be a field, $p(x) \in K[x]$ with root field E, and $G = Gal(E/K)$. Ifn L is a subfield of E with $K \subseteq L$, then $G_L = \{\alpha \in G : \text{ for every } y \in L, \alpha(y) = y\}$ is a subgroup of G. The subgroup G_L is called* ***the fixer of L****.*

10.4 The Galois Correspondence

Theorem 25. *Let K be a field, $p(x) \in K[x]$ with root field E, and $G = Gal(E/K)$. If L is a subfield of E with $K \subseteq L \subseteq E$, then L is the fixed field of G_L, i.e., $E_{G_L} = L$.*

Theorem 27. *Let K be a field, $p(x) \in K[x]$ with root field E, and $G = Gal(E/K)$. If H is a subgroup of G then the fixer of the field E_H is H, i.e., $G_{E_H} = H$.*

Theorem 29. *Let K be a field and E the root field for a polynomial over K. If L is a subfield of E with $K \subseteq L$ and L is a root field over K, then $Gal(E/L) \triangleleft Gal(E/K)$ and $Gal(L/K) \cong Gal(E/K)/Gal(E/L)$.*

Theorem 30. *Let K be a field, E the root field for a polynomial over K, and L an intermediate field $K \subseteq L \subseteq E$. If $Gal(E/L) \triangleleft Gal(E/K)$ then L is a root field over K.*

11 Solvability

11.1 Three Construction Problems

There are no definitions or theorems in this subsection.

11.2 Solvable Groups

Definition 1. *A group G is called a* ***solvable group*** *if there are subgroups $\{e_G\} = H_0, H_1, \ldots, H_n = G$, so that for each $0 \leq i \leq n-1$, $H_i \lhd H_{i+1}$ and H_{i+1}/H_i is an abelian group.*

Theorem 3. *The permutation group S_5 is not solvable.*

Theorem 4. *The permutation group S_4 is not solvable.*

Theorem 5. *Let G be a group and J a subgroup of G.*

(i) If G is a solvable group then J is a solvable group.

(ii) If $J \lhd G$ and both J and G/J are solvable groups, then G is a solvable group.

Theorem 6. *Suppose G and B are groups. If there is an onto homomorphism $f : G \to B$ and G is a solvable group, then B is a solvable group.*

Theorem 7. *For each $n \geq 5$, S_n is not a solvable group.*

11.3 Solvable by Radicals

Definition 9. *Let K be a field. A* ***radical extension*** *of K is a finite extension of the form $K(c_1, \ldots, c_n)$ where for each $1 \leq i \leq n$, there is a positive integer $m_i \geq 2$ so that $(c_1)^{m_1} \in K$ and for $1 < i \leq n$, $(c_i)^{m_i} \in K(c_1, \ldots, c_{i-1})$*

Definition 11. *Let K be a field and $p(x) \in K[x]$. We say that $p(x)$ is* ***solvable by radicals*** *if the root field of $p(x)$ is contained in a radical extension of K.*

Theorem 13. *Let L be a radical extension of $\mathbb{Q}$. Then there exists a radical extension E of $\mathbb{Q}$, with $\mathbb{Q} \subseteq L \subseteq E$, where E is also a root field over $\mathbb{Q}$.*

Definition 14. *For $n > 1$, the root $\omega_n = \cos\left(\frac{2\pi}{n}\right) + i \sin\left(\frac{2\pi}{n}\right)$ for the polynomial $-1 + x^n \in \mathbb{Q}[x]$ is called a* ***primitive n^{th} root of unity****.*

Theorem 15. *For each positive integer n, the polynomial $p(x) = -1 + x^n$ in $\mathbb{Q}[x]$ is solvable by radicals.*

Theorem 16. *If n is a positive integer with $n \geq 2$ then $Gal(\mathbb{Q}(\omega_n)/\mathbb{Q})$ is abelian.*

Theorem 17. *Let $m_1, m_2, \ldots, m_r$ be distinct positive integers, and $m_j \geq 2$ for each j. Then the field $L = \mathbb{Q}(\omega_{m_1}, \omega_{m_2}, \ldots, \omega_{m_r})$ is a root field over $\mathbb{Q}$, and $Gal(L/\mathbb{Q})$ is a solvable group.*

Theorem 18. *If the polynomial $p(x) \in \mathbb{Q}[x]$ is solvable by radicals, then the Galois group G for $p(x)$ is a solvable group.*

Theorem 20. *If G is a finite solvable group, then there is a sequence of subgroups $\{e_G\} = H_0, H_1, \ldots, H_n = G$ where for each $0 \leq j < n$, $H_j \lhd H_{j+1}$, and H_{j+1}/H_j is cyclic of prime order.*

Theorem 21. *If $p(x) \in \mathbb{Q}[x]$ has root field E and $Gal(E/\mathbb{Q})$ is solvable, then $p(x)$ is solvable by radicals.*

12 Constructible Numbers

Definition 22. *We say that a real number α is constructible if – using an unmarked straight-edge and compass – we can build a line segment of length $|\alpha|$ using the following geometric operations:*

(i) Given a constructed point P and constructed line ℓ, we can construct a unique line ℓ' through P that is perpendicular to ℓ.

(ii) Given a constructed point P and constructed line ℓ, we can construct a unique line ℓ'' through P that is parallel to ℓ.

(iii) Give a constructed point P and constructed length $|\alpha|$, we can construct a point Q on ℓ such that $PQ = |\alpha|$.

Theorem 23. *The set of constructable numbers is a field extension of $\mathbb{Q}$ and is closed under taking square roots.*

Theorem 24. *Let α be a constructible number. Then there exists a sequence ('tower') of finite field extensions $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n$ such that:*

(i) $F_n \subset \mathbb{R}$.

(ii) $\alpha \in F_n$.

(iii) For each i, we have $F_i = F_i(\sqrt{r_i})$ where $r_i \in F_i$.

Conversely, given a sequence of field extensions satisfying conditions (i) and (iii), then all $x \in F_n$ are constructible.

Corollary 25. *If α is a constructible number, then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^n$ for some $n \in \mathbb{N}$.*

Theorem 26. *Using an unmarked straight-edge and compass, it is impossible to construct a cube of volume two units.*

Theorem 27. *It is impossible to trisect an angle of 60 degrees using an unmarked straight-edge and compass.*

Corollary 28. *Using an unmarked straight-edge and compass, it is impossible to construct an angle of 20 degrees.*