Abstract Algebra

from the context of the courses
MTH 418H-419H: Honors Algebra

Kaedon Cleland-Host

January 28, 2022

Contents

Chapter 1

Group Theory

1.1 Groups

Definition 1.1.1. A **law of composition** is a map $S^2 \to S$.

Remark. We will use the notation ab for the elements of S obtained as $a, b \to ab$. This element is the product of a and b.

Definition 1.1.2. A **group** is a set G together with a law of composition that has the following three properties:

1. **Identity** There exists an element $1 \in G$ such that $1a = a1 = A$ for all $a \in G$.
2. **Associativity** $(ab)c = a(bc)$ for all $a, b, c \in G$.
3. **Inverse** For any $a \in G$, there exists $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = 1$.

Definition 1.1.3. An **abelian group** is a group with a commutative law of composition. That is for any $a, b \in G$, $ab = ba$.

Definition 1.1.4. The **order** of a group G is the cardinality of the set.

Proposition 1.1.5. Cancellation Law For $a, b, c \in G$ if $ab = ac$ then $b = c$.

Proposition 1.1.6. Let S be a set with an associative law of composition and an identity. The subset of elements of S that are invertible forms a group.

1.2 Subgroups

Definition 1.2.1. A group H is a **Subgroup** of G if H is subset of G, H has the same law of composition as G, and H is also a group. In other words H a group if it is a subset of G with the following properties:

1. **Closure** $a, b \in H$ then $ab \in H$.
2. **Identity** $1 \in H$.
3. **Inverse** For all $a \in H$, $a^{-1} \in H$.

Definition 1.2.2. A subgroup S of G is a **proper subgroup** if $S \neq G$ and $S \neq \{\mathbb{I}\}$.

Proposition 1.2.3. If H and K are subgroup of G, then $H \cap K$ is a subgroup.

Theorem 1.2.4. If S is a subgroup of $\mathbb{Z}^+$, then either

- $S = \{0\}$
- $S = \mathbb{Z}a$, where a is the smallest elements of S.

Definition 1.2.5. For two integers $a, b \in \mathbb{Z}$ we sat that a **divides** b if $\frac{b}{a} \in \mathbb{Z}$ denoted $a|b$.

1.2.6 Greatest Common Divisor

Definition 1.2.7. The **greatest common divisor** of two integers $a, b \in \mathbb{Z}$ is the integer $d \in \mathbb{Z}$ such that

$$\mathbb{Z}d = \mathbb{Z}a + \mathbb{Z}b = \{n \in \mathbb{Z} | n = ra + sb \forall r, s \in \mathbb{Z}\}$$

Proposition 1.2.8. Properties of the greatest common divisor Let $a, b \in \mathbb{Z}$, not both zero, and let d be the greatest common divisor. Then

1. There are integers $r, s \in \mathbb{Z}$ such that $d = ra + sb$.
2. $d|a$ and $d|b$.
3. If $e \in \mathbb{Z}$ such that $e|a$ and $e|b$ then $e|d$.

Definition 1.2.9. Two integers $a, b \in \mathbb{Z}$ are **relatively prime** if $\gcd(a, b) = 1$.

Corollary 1.2.10. A pair $a, b \in \mathbb{Z}$ is relatively prime if an only if there are integers $r, s \in \mathbb{Z}$ such that $ra + sb = 1$.

Corollary 1.2.11. Let p be a prime integer. If p divides a product ab if integers, then at least one of $p|a$ or $p|b$ holds.

1.2.12 Least Common Multiple

Definition 1.2.13. The **least common multiple** of two integers $a, b \in \mathbb{Z}$ is the integer $m \in \mathbb{Z}$ such that

$$\mathbb{Z}m = \mathbb{Z}a \cap \mathbb{Z}b$$

Proposition 1.2.14. Properties of least common multiple Let a, b be non-zero integers and let m be there least common multiple. Then

1. $a|m$ and $b|m$.
2. If $n \in \mathbb{Z}$ such that $b|n$ and $a|n$, then $m|n$.

Corollary 1.2.15. For $d = \gcd(a, b)$ and $m = \text{lcm}(a, b)$ then $ab = dm$.

1.2.16 Cyclic Groups

Definition 1.2.17. Let G be a group and $x \in G$. The **cyclic subgroup** generated by x denoted $\langle x \rangle$ is

$$\langle x \rangle = \{\dots, x^{-2}, x^{-1}, 1, x^1, x^2, \dots\}$$

Remark. For any subgroup S that contains x we have $S \subset \langle x \rangle$.

Definition 1.2.18. The **order of an element** $x \in G$ is the order of the group $\langle x \rangle$. This is the smallest positive integer n such that $x^n = 1$.

Proposition 1.2.19. Let $\langle x \rangle \subset G$ and consider the set $S = \{k \in \mathbb{Z} | x^k = 1\}$

1. The set S is a subgroup of $\mathbb{Z}^+$
2. $x^r = x^s$ $(r \geq s)$ if and only if $x^{r-s} = 1$.
3. If $S \neq \{0\}$, then $S = \mathbb{Z}n$ for some positive $n \in \mathbb{Z}$ and $\langle x \rangle = \{1, x^1, x^2, \dots, x^{n-1}\}$

Proposition 1.2.20. Let x be an element of finite order n in a group and let $k \in \mathbb{Z}$. Let $k = nq + r$, where $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then

1. $x^k = x^r$
2. $x^k = 1$ if an only if $r = 0$.
3. The order of x^k is $n/\gcd(k, n)$.

1.3 Homomorphisms

Definition 1.3.1. A **homomorphism** $\varphi : G \to G'$ is a map from a group G to a group G' such that for any $a, b \in G$ we have

$$\varphi(ab) = \varphi(a)\varphi(b)$$

Proposition 1.3.2. Let $\varphi : G \to G'$ be a homomorphism

1. $\varphi(1) = 1$
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ for any $a \in G$

Definition 1.3.3. A homomorphism $\varphi : G \to G'$ is **injective** if $\varphi(x) = \varphi(u) \Rightarrow x = y$

Definition 1.3.4. A homomorphism $\varphi : G \to G'$ is **surjective** if for every $b \in G'$, there exists $a \in G$ such that $\varphi(a) = b$.

Definition 1.3.5. Let $\varphi : G \to G'$ be a homomorphism

1. The **kernal** of φ denoted $\ker(\varphi)$ is the set
$$\ker(\varphi) = \{a \in G | \varphi(a) = 1\}$$
2. The **image** of φ denoted $\text{Im}(\varphi)$ is the set
$$\text{im}(\varphi) = \{b \in G' | \exists a \in G, \varphi(a) = b\}$$

Corollary 1.3.6. A homomorphism $\varphi : G \to G'$ is injective if $\ker(\varphi) = \{1\}$

Corollary 1.3.7. A homomorphism $\varphi : G \to G'$ is surjective if $\text{Im}(\varphi) = G'$

Proposition 1.3.8. Let $\varphi : G \to G'$ be a homomorphism the $\ker(\varphi)$ and $\text{Im}(\varphi)$ are subgroups of G and G'

Definition 1.3.9. An **isomorphism** is a **bijective** homomorphism. A homomorphism is **bijective** if it is both injective and surjective.

Proposition 1.3.10. If $\varphi : G \to G'$ is an isomorphism, then $\varphi^{-1} : G' \to G$ is also an isomorphism.

Definition 1.3.11. Two groups G and G' are **isomorphic** if there is an isomorphism $\varphi : G \to G'$.

Definition 1.3.12. An **automorphism** is an isomorphism $\varphi : G \to G$.

1.4 Cosets

Definition 1.4.1. Let H be a subgroup of G. The **left coset** of H induced by an element $a \in G$ is the set

$$aH = \{ah|h \in H\}$$

The **right coset** of H induced by an element $a \in G$ is the set

$$Ha = \{ha|h \in H\}$$

Proposition 1.4.2. Let H be a subgroup of G. The left cosets partition G. The right cosets partition G.

Definition 1.4.3. For a subgroup H of G. The **index of** H **in** G denoted $[G : H]$ is the number of left cosets of H in G.

Lemma 1.4.4. All left cosets aH and all right cosets Ha of a subgroup H of a group G have the same order.

Lemma 1.4.5. Counting Formula. For a subgroup H of G we have

$$|G| = |H|[G : H]$$

Theorem 1.4.6. Lagrange's Theorem. Let H be a subgroup of a finite group G. The order of H divides the order of G.

Corollary 1.4.7. The order of an element of a finite group divides the order of the group.

Corollary 1.4.8. If G is a group of prime order then for $a \in G$ where $a \neq \mathbb{I}$, we have $G = \langle a \rangle$.

Corollary 1.4.9. If $\varphi : G \to G'$ is a homomorphism of finite groups then

$$|G| = |\ker(\varphi)||\mathrm{Im}(\varphi)|$$

1.5 Normal Subgroups

Definition 1.5.1. A subgroup N of a group G is **normal** if for every $a \in N$ and $g \in G$, $gag^{-1} \in N$.

Proposition 1.5.2. For any homomorphism $\varphi : G \to G'$ the $\ker(\varphi)$ is a normal subgroup of G.

Proposition 1.5.3. Let $H \subset G$ be a subgroup. Then the following are equivalent

1. H is a normal subgroup.
2. For all $g \in G$, $gHg^{-1} = H$
3. For all $G \in G$, $gH = Hg$
4. Every left coset of H in G is a right coset of H in G.

Corollary 1.5.4. If a group G has just one subgroup of order n, then that subgroup is normal.

1.6 Quotient Groups

Definition 1.6.1. If $H \subset G$ is a subgroup. The **Quotient** is defined $G/H = \{\text{left cosets of } H\}$.

Proposition 1.6.2. If $H \subset G$ is a normal subgroup, then G/H is a group with law of composition $[aH][bH] = [abH]$.

Theorem 1.6.3. Correspondence Theorem Let $\varphi : G \to G'$ be a surjective homomorphism with kernal K. There is a bijective correspondence between subgroups of G' and subgroups of G that contain K.

$$\{\text{subgroups of } G \text{ that contain } K\} \leftrightarrow G/K$$

1.7 Product Groups

Definition 1.7.1. If G and G' are groups, $G \times G'$ is the **product group** defined

$$G \times G' = \{(g, g')|g \in G, g' \in G'\}$$

with the law of composition

$$(a, a')(b, b') = (ab, a'b')$$

Proposition 1.7.2. Let G be a cyclic group of order mn where $\gcd(m, n) = 1$ then $G \equiv C_m \times C_n$.

Proposition 1.7.3. Let H, K be subgroups of a group G. Consider the multiplication map

$$f : H \times K \to G$$

given by $f(h, k) = hk$. Then

1. f is a homomorphism if an only if $kh = hk$ for all $h \in H$ and $k \in K$
2. f is injective if and only if $H \cap K = \{1\}$
3. if H is normal the image HK of f is a subgroup of G.

In particular, $G \cong H \times K$ under f if and only if $H \cap K = \{1\}$, $HK = G$ and K and H are both normal.

Proposition 1.7.4. The map $\pi : G \to G/N$ defined by $\pi(x) = [aN]$ such that $x \in aN$ is a surjective homomorphism with kernal N.

Theorem 1.7.5. First Isomorphism Theorem Let $\varphi : G \to G'$ be a surjective homomorphism and let N be its kernal.

$$G' \cong G/N$$

1.8 Group Actions

Definition 1.8.1. An **action** of a group G on a set S is a map

$$G \times S \to S$$

$$(g, s) \mapsto g * s$$

such that

1. $1 * s = s$ for all $s \in S$.
2. **Associativity**: $(gg') * s = g * (g * s)$ for all $g, g' \in G$ and $s \in S$.

Definition 1.8.2. Given an action of a group G on the set S, the **orbit** O_s of an element $s \in S$ is

$$O_s = \{gs \in S|g \in G\}$$

Definition 1.8.3. An action of G on S is **transitive** if $S = O_s$ for some $s \in S$.

Definition 1.8.4. The **stabilizer** G_s of an element $s \in S$ is

$$G_s = \{g \in G|gs = s\}$$

Proposition 1.8.5. Let G be a subgroup of a group G.

1. The action of G on G/H is transitive.
2. The stabilizer $G_{[H]}$ of $[H]$ is the subgroup H.

Theorem 1.8.6. textbfOrbit Stabilizer Theorem Let G be a group action on a set S. For any $s \in S$, there is a bijection

$$\epsilon : G/G_s \leftrightarrow O_s$$

$$[aG_s] \mapsto as$$

such that $\epsilon(g[C]) = g\epsilon([C])$ for all $g \in G$ and $[C] \in G/G_s$

Corollary 1.8.7. Let G be a group acting on a finite set S. Then for any $s \in S$

$$|G| = |O_s||G_s|$$

1.9 Conjugation

Definition 1.9.1. The **conjugate** of $a \in G$ by $g \in G$ is gag^{-1}.

Definition 1.9.2. The **conjugation action** is the action of a group G defined by $G \times G \to G$ with $(g, x) \mapsto gxg^{-1}$.

Lemma 1.9.3. G is abelian $\Leftrightarrow$ conjugation map is the identity

Definition 1.9.4. The **centralizer** of x is the stabilizer of x under conjugation.

$$Z(x) = \{g \in G | gxg^{-1} = x\} = \{g \in G | gx = xg\}$$

Definition 1.9.5. The conjugacy class of x is the orbit of x under conjugation.

$$C(x) = \{gxg^{-1} \in G | g \in G\}$$

Definition 1.9.6. The **center** of a group G is the subgroup

$$Z = \{z \in G | zg = gz \text{ for all } g \in G\}$$

Corollary 1.9.7. The center of a group is a normal subgroup.

Corollary 1.9.8. Every centralizer contains the center.

Proposition 1.9.9. The Class Equation The orbits of of conjugation partition the group.

$$|G| = \sum_{\text{conjugacy classes } C} |C|$$

1.10 p-Groups

Definition 1.10.1. A $p-group$ is a group of order p^n for some prime p.

Proposition 1.10.2. The center of a p-group is non-trivial.

Theorem 1.10.3. Fixed Point Theorem Let G be a p-group action on a finite set S If $|S|$ is not divisible by p, then there is a fixed point for the action of G on S.

Proposition 1.10.4. Every group of order p^2 is abelian.

Corollary 1.10.5. A group of order p^2 is either cyclic or a product of two cyclic groups

Definition 1.10.6. A subgroup $H \subset G$ of order p^e is called a **Sylow p-subgroup**.

Theorem 1.10.7. First Sylow Theorem A finite group whose order is divisible by a prime contains a Sylow p-subgroup.

Corollary 1.10.8. A group whose order is divisible by a prime p contains an element of order p.

Theorem 1.10.9. Second Sylow Theorem Let G be a finite group whose order is divisible by a prime p.

1. The Sylow p-subgroups of G are conjugate subgroups.
2. Every subgroup of G that is a p-group is contained in a Sylow p-subgroup.

Corollary 1.10.10. A group G has just one Sylow p-subgroup H if and only if H is normal.

Theorem 1.10.11. Third Sylow Theorem Let G be a finite group whose order $n = p^e m$, with p prime and p not dividing m. Let s be the number of Sylow p-subgroups of G. Then s divides m and $s \equiv 1 \mod p$.

Chapter 2

Field Theory

2.1 Rings and Fields

Definition 2.1.1. A **ring** R is a set with two laws of composition denoted $+$ and $\times$ that satisfy the following axioms:

- **Identity** $\exists$ elements denoted $0, 1 \in R$ such that $1 \times a = a$ and $0 + a = a$, $\forall\ a \in R$.
- **Additive Inverse** For all $a \in R$, there exists an element $-a \in R$ such that $-a + a = 0$.
- **Associativity** For all $a, b, c \in R$, $a \times (b \times c) = (a \times b) \times c$ and $a + (b + c) = (a + b) + c$.
- **Commutativity** For all $a, b \in R$, $a \times b = b \times a$ and $a + b = b + a$.
- **Distributivity** For all $a, b, c \in R$, $a \times (b + c) = (a \times b) + (a \times c)$.

Definition 2.1.2. A **field** F is a ring where every nonzero element has a multiplicative inverse.

- **Multiplicative Inverse** For all nonzero $a \in F$, there exists an element $a^{-1} \in R$ such that $a \times a^{-1} = 1$.

Definition 2.1.3. A **subring** H is a subset of a ring R with the following properties

- **Closure** For all $a, b \in H$, $a \times b, a + b \in H$.
- **Identity** $0, 1 \in H$.
- **Additive Inverse** For all $a \in H$, $-a \in H$.

Definition 2.1.4. A **subfield** H is a subring of a field F that contains multiplicative inverses of nonzero elements.

- **Multiplicative Inverse** For all $a \in H$, $a^{-1} \in H$.

Proposition 2.1.5. Let R be a ring. $0 = 1$ in R if and only if R is the zero ring.

2.2 Ring Homomorphisms

Definition 2.2.1. A **ring homomorphism** $\varphi : R \to R'$ is a map such that for all $a, b \in R$

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$
2. $\varphi(ab) = \varphi(a)\varphi(b)$
3. $\varphi(1) = 1$

Definition 2.2.2. A **ring isomorphism** is a bijective ring homomorphism.

Proposition 2.2.3. Let F be a field. If $f : F \to R$ is a ring homomorphism and R is nonzero, then f is injective.

Corollary 2.2.4. Any homomorphism between fields is injective.

2.3 Product Rings

Definition 2.3.1. If R and R' are rings, $R \times R'$ is the **product ring** defined

$$R \times R' = \{(r, r')|r \in R, r' \in R'\}$$

with the laws of composition

$$(a, a') + (b, b') = (a + b, a' + b')$$
$$(a, a')(b, b') = (a \times b, a'b')$$

2.4 Quotient Rings

Definition 2.4.1. The **quotient ring** R/I where I is and ideal of the ring R is the ring of cosets of I with ring structure

$$(a+I)+(b+I)=(a+b+I)$$

$$(a+I)(b+I)=(ab+I)$$

Proposition 2.4.2. Let $f : R \to S$ be a ring homomorphism and R/I be a quotient ring, f defines a ring homomorphism $R/I \to S$ if an only if $I \subset \ker(f)$.

2.5 Characteristic

Definition 2.5.1. A field F has **characteristic** n if $\sum^n 1 = 0$. If no such sum is possible a field has characteristic 0.

Proposition 2.5.2. The characteristic of a field must be prime.

Definition 2.5.3. For prime $p \in \mathbb{N}$, let $\mathbb{F}_p$ denote the field $\mathbb{Z}/(p)$.

Proposition 2.5.4. If a field F has characteristic $p > 0$ then there exists a unique homomorphism $\mathbb{F}_p \to F$ and if $p = 0$ then there exists a unique homomorphism $\mathbb{Q} \to F$.

2.6 Polynomial Rings

Definition 2.6.1. A **polynomial** with coefficients $a_i \in R$ in a ring R is a finite linear combination of powers of x^i

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

Definition 2.6.2. The **degree** of a polynomial f is the largest n such that $a_n \neq 0$.

Definition 2.6.3. A polynomial f is **monic** if $a_n = 1$ where $n = \deg f$.

Definition 2.6.4. For a ring R the **polynomial ring** denoted $R[x_1, \ldots, x_r]$ is the ring of polynomials constructed from linear combinations of powers of the variables $x_1, \ldots, x_r$.

Proposition 2.6.5. Let $x = (x_1, \ldots, x_m)$ and $y = (y_1, \ldots, y_n)$ be sets of variables. There is a unique isomorphism

$$R[x, y] \to R[x][y]$$

which is the identity on R and sends $x \mapsto x$, $y \mapsto y$.

2.7 Ideals

Definition 2.7.1. An **ideal** I of a ring R is an additive subgroup such that for all $s \in I$ and $r \in R$, $rs \in I$.

Definition 2.7.2. A **principle ideal** generated by an element $a \in R$ in a ring R is the ideal

$$(a) = aR = Ra = \{ra | r \in R\}$$

Proposition 2.7.3. The kernel of a ring homomorphism is an ideal.

Definition 2.7.4. An **ideal generated by** a set of elements $a_1, \ldots, a_n \in R$ in a ring R is the ideal

$$(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n | r_1, \ldots, r_n \in R\}$$

Definition 2.7.5. An ideal is **proper** if it is neither $\{0\}$ nor R.

Proposition 2.7.6. A ring R is a field if and only if the only proper ideal is the zero ideal.

Definition 2.7.7. A **maximal ideal** M of a ring R is an ideal such that $M \neq R$ and there are not ideals I such that $M \subsetneq I \subsetneq R$.

Proposition 2.7.8. An ideal is maximal if and only if R/I is a field.

2.8 Integral Domains

Definition 2.8.1. A **domain** is a ring R such that $\forall a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$

Proposition 2.8.2. Any field is a domain.

Proposition 2.8.3. Any finite domain is a field.

Definition 2.8.4. An ideal I of a ring R is called **prime** if R/P is a domain

Proposition 2.8.5. Any maximal ideal is prime.

Definition 2.8.6. A **principal ideal domain** is a domain R in which every ideal is principal.

Definition 2.8.7. A **euclidean domain** is a domain R a function $N : R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ such that

1. $\forall x, y \in Rx \neq 0, \exists q, r \in R \text{s.t.} y = xq + r$
2. $\forall x, y \in Rx \neq 0, N(x) \leq N(xy)$

Theorem 2.8.8. Any euclidean domain is a principal ideal domain

Proposition 2.8.9. Let $p(x) \in F[x]$ and $\alpha \in F$ if $p(\alpha) = 0$ then $p(x) = (x - \alpha)q(x)$ for some $q(x) \in F[x]$

2.9 Irreducibility

Definition 2.9.1. A **unit** is a ring R is an element which has a multiplicative inverse.

Proposition 2.9.2. If $x \in R$, x is a unit if and only if $(x) = R$.

Definition 2.9.3. An **irreducible** element $r \in R$ is a nonzero nonunit element where$x = ab$ implies a or b is a unit.

Theorem 2.9.4. If R is a principle ideal domain then a nonzero $I = (x)$ is maximal if and only if x is irreducible.

Lemma 2.9.5. Gauss's Lemma - If $p(x) \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Z}[x]$ then $p(x)$ is still irreducible in $\mathbb{Q}[x]$.

Lemma 2.9.6. Eisenstein's Criterion Let $p(x) \in \mathbb{Z}[x]$, let $\beta \in \mathbb{Z}$ be a prime. $p(x) = \sum_{i=0}^{n} a_i x^i$ If

$$\beta \not| a_n, \quad \beta | a_0, a_1, \ldots, a_{n-1}, \quad \beta \not| a_0$$

then $p(x)$ is irreducible.

2.10 Field Extensions

Definition 2.10.1. A **field extension** is an (injective) homomorphism between fields.

Proposition 2.10.2. If $F \to K$ is a field extension then K is a vector space over F.

Definition 2.10.3. An extension $F \to K$ is **simple algebraic** if

$$K \cong F(x) \quad \dim_F K = \infty$$

Definition 2.10.4. An extension $F \to K$ is **simple transcendental** if

$$K \cong F[x]/(p(x)) \quad \dim_F K = \deg p(x)$$

Definition 2.10.5. A element of a field $\alpha \in K$ is **algebraic** if for some extension $F \to K$, $F \to F(\alpha)$ is simple algebraic

Definition 2.10.6. A element of a field $\alpha \in K$ is **transcendental** if for some extension $F \to K$, $F \to F(\alpha)$ is simple transcendental.

Definition 2.10.7. An extension $F \to K$ is **algebraic** if every element is $\alpha \in K$ is algebraic over F. In other words, $\exists p_\alpha(x) \in F[x]$ such that $p_{a\alpha}(\alpha) = 0$.

Proposition 2.10.8. If $F \to K$ is algebraic and $K \to L$ is algebraic then the composition $F \to L$ is algebraic.

Definition 2.10.9. The **degree** of a field extension is the dimension of the vector space formed.

Proposition 2.10.10. If $F \to K$ is a degree n field extension and $K \to L$ is a degree m extension, then $F \to K \to L$ is a degree mn extension.

Proposition 2.10.11. Every finite degree extension is a composition of simple algebraic extensions.

Proposition 2.10.12. Every finite degree extension is algebraic.

Definition 2.10.13. A polynomial $p(x) \in F[x]$ **splits** if it factors into

$$c(x-r_1)(x-r_2)\dots(x-r_n) \quad r_i \in F$$

Proposition 2.10.14. Let F be a field, $\exists$ field extension $F \to \Omega$ such that $p(x)$ splits as an element of $\Omega[x]$.

Definition 2.10.15. A field Ω is called algebraically closed if every polynomial $p(x) \in \Omega[x]$ has a root in Ω.

Proposition 2.10.16. The following are equivalent:

1. Ω is algebraically closed.
2. Any polynomial $p(x) \in \Omega[x]$ splits.
3. The only irreducible polynomials in Ω are linear.
4. If $\Omega \to L$ is a finite field extension then $\Omega = L$.

Theorem 2.10.17. Fundamental Theorem of Algebra - $\mathbb{C}$ is algebraically closed.

Theorem 2.10.18. Any field can be embedded into any algebraically closed field.

Definition 2.10.19. An **algebraic closure** of a field F is an algebraic extension of F which is algebraically closed.

Theorem 2.10.20. Any field has an algebraic closure.

2.11 Symmetric Polynomials

Definition 2.11.1. A polynomial $f \in K(x_1, x_2, \dots, x_n)$ is **symmetric** if $\forall \sigma \in S_n$, $f(x_1, x_2, \dots, x_n) = f(x_{O(1)}, x_{O(2)}, \dots, x_{O(n)})$

Definition 2.11.2. The **elementary polynomial** $e_k \in F(x_1, x_2, \dots, x_n)$ for $k \geq 0$ is the symmetric polynomial

$$e_k(x_1, x_2, \dots, x_n) = \sum_{1 \leq j_1 < j_2 < \dots < j_k \leq n} x_{j_1} x_{j_2} \dots x_{j_k}$$

Theorem 2.11.3. Fundemental Theorem of Symmetric Polynomials Any symmetric polynomial $f \in \mathbb{Z}[x_1, x_2, \dots, x_n]$ can be written uniquely as a linear combination of elementary symmetric polynomials with $\mathbb{Z}$ coefficients.

2.12 Field Automorphisms

Definition 2.12.1. An automorphism of a field is an isomorphism from F to itself.

Proposition 2.12.2. If $\mathbb{Q} \to K$ is a finite field extension then

$$|\mathrm{Aut}(k)| \leq [K : Q]$$