Math 791 Summation

Will Thomas

May 11, 2023

Contents

Chapter 1

Introduction

This is the introduction to my math textbook.

Chapter 2

Groups

This chapter will focus primarily on Groups and group related theories.

2.1 Basic Definitions

Definition 2.1.1 (Group) *A set G with a binary operation $* : G \times G \to G$ such that*

1. $\exists e \in G$ *s.t.* $\forall g \in G,\ g * e = e * g = g$ *(identity element)*
2. $\forall g_1\ g_2\ g_3 \in G,\ g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$ *(associativity)*
3. $\forall g \in G, \exists g^{-1} \in G$ *s.t.* $g * g^{-1} = e = g^{-1} * g$ *(inverses)*

A good example of a Group (**2.1.1**) is $GL_n(\mathbb{R})$, which is the general linear group of matrices that are all invertible for a given field $\mathbb{R}$.

Definition 2.1.2 (Trivial) *A* trivial *group G is a group with only 1 element. Namely, this element must be the identity element.*

Definition 2.1.3 (Abelian) *A Group (**2.1.1**) G is said to be "Abelian" if*

$$\forall g_1\ g_2 \in G,\ g_1 * g_2 = g_2 * g_1$$

Succinctly, all elements in that group commute.

2.2 Symmetric Groups

Additionally, we can consider the notion of Symmetric Groups:

Definition 2.2.1 (Permutation Group) *Let X be a set with n elements, we can define*

$$S_n := \{\sigma : X \to X \mid \sigma \text{ is 1-1 and onto}\}$$

Which is the "Permutation Group"

The Permutation Group (**2.2.1**) is a group under function composition (so the operation $*$ is composition) and additionally, $|S_n| = n$

Definition 2.2.2 (Dihedral Groups) *We can define D_n as the group of symmetries of a regular $n-$gon (a n sided polygon).*

This consists of rotations about center and reflections about lines of symmetry. All such rotations must land back on itself, aka just the vertices move.

We also know that the following major properties hold for groups:

(i.) Uniqueness of identity element

(ii.) Uniqueness of inverses

(iii.) $\forall g \in G,\ (g^{-1})^{-1} = g$

Definition 2.2.3 (Subgroup) *A subset $H \subseteq G$ is a subgroup if:*

(i.) H is closed under the binary operations of G

(ii.) $\forall h \in H, h^{-1} \in H$

Definition 2.2.4 (The Generated Subgroup) *Let $X \subseteq G$ be a subset. Then the "subgroup of G generated by X" (denoted $\langle X \rangle$), is the set of all finite expressions of the form $x_1^{\epsilon_1} \cdots x_r^{\epsilon_r}$, where all $x_i \in X$ and $\epsilon = -1, 0, 1$.*

Theorem 2.2.5 (Subgroup Intersection Theorem) *$\langle X \rangle =$ the intersectiin of all subgroups of G containing X.*

One thing to note is that if $X := \{a\}$ (it is a single element), then we call $\langle X \rangle = \langle a \rangle =$ *the cyclic subgroup of G generated by a.*

Definition 2.2.6 (Cosets) *If we have a Subgroup (**2.2.3**) $H \subseteq G$, we can define:*

Left Coset $gH := \{gh \mid h \in H\}$ *and the* Right Coset $Hg := \{hg \mid h \in H\}$.

Theorem 2.2.7 (Coset Partition Theorem) *All distinct left (respectively right) cosets of H in G partition G.*

An additional critical properties of groups is the "Cancelation Property", which implies that for any group G, $\forall g\ x\ y \in G, gx = gy \implies x = y$.

This property can be used to see that there is a 1-1 function from a subgroup H to gH for any $g \in G$. Thus $|H| = |gH|$.

Due to Coset Partition Theorem (**2.2.7**) we can now show major result

Theorem 2.2.8 (LaGrange's Theorem) *Let G be a finite group and $H \subseteq G$ a subgroup.*

Then:

$$\begin{aligned}|G| &= |H| \cdot \textit{(number of distinct left cosets of } H\textit{)} \\ &= |H| \cdot \textit{(number of distinct right cosets of } H\textit{)}\end{aligned}$$

An immediately obvious corollary of this is that the number of distinct left cosets equals the number of distinct right cosets. This allows us to define the following notation $[G : H]$ *the index of H in G*, which represents the number of distinct cosets of H in G.

Definition 2.2.9 (Normal Subgroup) *A subgroup N is called* normal *if*

$$\forall g \in G, n \in N, \exists n' \in N, gn = n'g$$

Essentially allowing a form of commutativity, at the expense of changing n to n'.

Definition 2.2.10 (Simple) *A group G is* simple *if the only Normal Subgroup (**2.2.9**) 's of G are G and the* **??** *(**??**)*

Definition 2.2.11 (Quotient Group) *The quotient group (also called factor group) of G by N is the set of left cosets of N under G.*

This will be denoted as G/N or $G \mod N$.

This forms a group under the binary operation "coset multiplication" where $g_1 N g_2 N = g_1 g_2 N$

2.3 Group Homomorphisms

Definition 2.3.1 (Group Homomorphism) *Given groups G_1, G_2, a function $\phi : G_1 \to G_2$ is a* group homomorphism *if*

$$\forall a\ b \in G_1,\ \phi(a *_1 b) = \phi(a) *_2 \phi(b)$$

Where $*_1$ is the binary operation of G_1 and $*_2$ is the binary operation in G_2

Some noteworthy properties of a group homomorphism that can be proven fairly trivially are:

(i.) $\phi(e_1) = e_2$ (where e_i represents the identity element from a respective group)

(ii.) $\forall g \in G,\ \phi(g^{-1}) = \phi(g)^{-1}$ (the inverse elements are preserved by a homomorphism)

If we take the classic definition of *Kernel* where $\ker(\phi) := \{g \in G_1 \mid \phi(g) = e_2\}$, we uncover some nice properties.

Proposition 2.3.2 (Group Hom. Properties) *Let $\phi : G_1 \to G_2$ be a group hom. (homomorphism), with kernel K. Then:*

*(i) K is a Normal Subgroup (**2.2.9**) of G_1*

(ii) If H is a subgroup of G_1, then $\phi(H)$ is a subgroup of G_2. Essentially, the structure preserving properties of a Group Hom. are so strong, they preserve subgroup orderings!

Furthermore, we can find properties of Normal subgroups.

Proposition 2.3.3 (Normal Subgroup Properties) *(i.) If H is a normal subgroup of G_1, then ϕ being surjective $\implies$ $\phi(H)$ is normal as well*

(ii.) Any normal subgroup N of a group G is the kernel of a group homomorphism. This homomorphism can be discovered as $\phi : G \to G/N$ defined by $\phi(g) = gN$.

Theorem 2.3.4 (Surjective Group Hom. Theorem) *Let $\phi : G_1 \to G_2$ be a surjective group homomorphism with kernel K. Then: There is a 1-1 correspondence between the subgroups of G_1 containing K and the subgroups of G_2 given by $H \to \phi(H)$ for $H \subseteq G_1$ containing K and $L \to \phi^{-1}(L)$ for $L \subseteq G_2$. Under this correspondence, $\phi(H)$ is normal in G_2 if H is normal in G_1 and $\phi^{-1}(L)$ is normal in G_1, if L is normal in G_2.*

Restated more simply: In an onto group hom. normal subgroups are preserved by the mapping.

Corollary 2.3.5 (Normal Subgroup Theorem) *Let G be a group and N a normal subgroup. Then: There is a 1-1 correspondence between the subgroups of G containing N and the subgroups of G/N. Under this correspondence, the normal subgroups of G containing N correspond to the normal subgroups of G/N.*

*This is fairly straightforward when we take Surjective Group Hom. Theorem (**2.3.4**) where $\phi : G \to G/N$ as $\phi(g) = gN$*

2.4 Isomorphisms

First we will look into the primary Isomorphism Theorems (as they specifically apply to Groups)

Definition 2.4.1 (Isomorphism) *A Group Homomorphism (**2.3.1**) ϕ that is also 1-1, and onto, is an* Isomorphism

Theorem 2.4.2 (First Isomorphism Theorem) *Given $\phi : G_1 \to G_2$ a surjective (onto) group hom. with kernel K. Then: $G_1/K \cong G_2$.*

Theorem 2.4.3 (Second Isomorphism Theorem) *Let $K \subseteq N \subseteq G$ be groups such that K and N are normal in G. Then: N/K is a normal subgroup of G/K and $(G/K)/(N/K) \cong G/N$*

Theorem 2.4.4 (Third Isomorphism Theorem) *Given $H, K \subseteq G$ (all groups), and K is Normal Subgroup (**2.2.9**) of G. Then:*

$$HK/K \cong H/(H \cap K)$$

Theorem 2.4.5 (Symmetric Group Cycle Theorem) *Let $\sigma \in S_n$ (the Permutation Group (**2.2.1**)). Then:*

(i) σ can be written uniquely (up to order) as a product of disjoint cycles

(ii) σ can be written as a product of (not necessarily disjoint) $2-$cycles.

(iii) This rewriting as a product of $2-$cycles is guaranteed to preserve the degree of the order (even or odd) no matter the way it is rewritten.

Definition 2.4.6 (Alternating Group) *The* Alternating Group *is the set of all "even" order permutations on a set with n elements. This is typically represented as A_n*

Theorem 2.4.7 (Alternating Simple Group Theorem) *A_n is a simple group for $n \geq 5$.*

This can be intuitively stated as "there are no proper normal subgroups of A_n for $n \geq 5$.

2.5 Group Actions

Definition 2.5.1 (Group Action) *Given a set X and a group G, we say G* acts on X *if:*

(i.) There is a binary map $G \times X \to X$ with the below properties

(ii.) $e \cdot x = x$

(iii.) $\forall a, b \in G,\ (ab) \cdot x = a \cdot (b \cdot x)$

Proposition 2.5.2 (Group Action Homomorphism) *A group G acts on a set with n elements. $\iff$ There exists a group homomorphism $\phi : G \to S_n$*

Theorem 2.5.3 (Prime Degree Subgroups) *If G is a finite group, $H \subseteq G$ a subgroup, and $[G : H] = p$, where p is the smallest prime dividing the order of G. Then: H is normal in G*

Definition 2.5.4 (Orbit) *The* Orbit of $x \in X$ *is defined as* $orb := \{g \cdot x \mid g \in G\}$ *Given that* G *acts on* X*.*

Definition 2.5.5 (Stabilizer) *The* Stabilizer of x *is defined as* $G_x := \{g \in G \mid g \cdot x = x\}$ *Given* G *acts on* X*.*

It is worth noting that all the distinct orbits under the a given action will partition X. This will follow immediately from the following proposition

Proposition 2.5.6 (Orbit Correspondence Theorem) *Given a group* G *acting on a set* X*. If we fix* $x \in X$*, there is a 1-1, onto set map between* $orb(x)$ *and the set of distinct left cosets of* G_x*.*

Furthermore, this can be given by $g \cdot x \to gG_x$*. Allowing us to see that whenever* $|orb(x)|$ *or* $[G : G_x]$ *is finite, then* $|orb(x)| = [G : G_x]$

Proposition 2.5.7 (Groups acting via Conjugation) *In the case that* G *acts on itself via conjugation* $(g \cdot x := gxg^{-1})$ *then* $orb(x) = \{gxg^{-1} \mid g \in G\}$ *which is then called the* Conjugacy Class of G *which we denote* $c(x)$*. Then* $G_x := \{g \in G \mid gx = xg\}$ *which is called the* Centralizer of X*, and we denote* $C_G(x)$*.*

Thus $|c(x)| = [G : C_G(x)]$ *if either is finite.*

Definition 2.5.8 (Center of a Group) *For a given group* G*, we can take* $Z(G)$ *to be the* center of G *and it is defined as* $Z(G) := \{g \in G \mid gx = xg\}$*.*

Theorem 2.5.9 (Class Equation) *Let* G *be a finite group. Then:*

$$\begin{aligned} |G| &= |Z(G)| + \sum_{i=1}^{r} |c(x_i)| \\ &= |Z(G)| + \sum_{i=1}^{r} [G : C_G(x_i)] \end{aligned}$$

Theorem 2.5.10 (Groups of Prime Power Orders) *Let* G *be a finite group where* $|G| = p^n$ *(*p *is prime) and* $n \geq 1$*. Then:*

(i) $Z(G) \neq \{e\}$

(ii) For each $1 \leq i < n$*,* G *has a subgroup of order* p^i

2.6 Sylow Theorems

Theorem 2.6.1 (First Sylow Theorem) *Let* G *be a finite group such that* $|G| = p^n m$*, where* p *is prime and* p *does not divide* m*. Then:* G *has a Sylow* $p-$*subgroup. Which means there exista a subgroup* $P \subseteq G$ *such that* $|P| = p^n$*.*

Corollary 2.6.2 (Sylow Corollary) *A couple neat properties fall out of this theorem.*

(i) If $|G| = p^n m$, then for each $1 \leq i \leq n$, there exist subgroups $H_1 \subseteq \cdots \subseteq H_n$ such that $|H_i| = p^i$. Essentially allowing us to know that there is a descending chain of prime power order subgroups.

(ii) If $|G| = pq^n$, $(p, q$ both prime) and $p < q$, then G has a normal Sylow $q-$subgroup (which is the unique Sylow q-subgroup).

Theorem 2.6.3 (Second Sylow Theorem) *Let G be a finite gorup such that $|G| = p^n m$, where p is prime and p does not divide m. Supposed $H \subseteq G$ is a subgroup of order p^i, with $1 \leq i \leq n$ and P is a Sylow $p-$subgroup. Then: $\exists a \in G,\ H \subseteq aPa^{-1}$*

Essentially allowing us to conclude that any two Sylow p-subgroups are conjugate.

Theorem 2.6.4 (Third Sylow Theorem) *Let G be a finite group such that $|G| = p^n m$, where p is prime and p does not divide m and write n_p for the number of Sylow p-subgroups. Then: n_p divides $|G|$ and is congruent to $1 \mod p$.*

Overall, the Sylow Theorems can be very helpful for showing that groups of an order like $p^n m$ will have a non-trivial normal subgroup.

Lemma 2.6.5 (Orbits for Prime Power Fields) *Let G be a group of order p^t (p prime) and assume G acts on the finite set X. If r denotes the number of orbits with just one element, then $|X| = r \mod p$*

Theorem 2.6.6 (Simple Group of Order 60) *Let G be a simple group of order 60. Then: $G \cong A_5$*

Chapter 3

Rings

3.1 Basic Definitions

Definition 3.1.1 (Ring) *A ring R is a set X with two binary operations $+$ and $\cdot$ such that the following properties hold:*

(i) $(R, +)$ *is an Abelian (**2.1.3**) group*

(ii) Multiplication $(\cdot)$ *is associative*

(iii) $\forall a, b, c \in R,\ a \cdot (b + c) = a \cdot b + a \cdot c$ *and* $(b + c) \cdot a = b \cdot a + c \cdot a$

(iv) R has a multiplicative identity, denoted as 1 satisfying $\forall a \in R,\ 1 \cdot a = a = a \cdot 1$

Definition 3.1.2 (Ideals) *Given a ring R, a left ideal $I \subseteq R$ is a set satisfying:*

$$\forall i \in I, \forall r \in R, ir \in I$$

Similarly, a right ideal $I \subseteq R$ is a set satisfying:

$$\forall i \in I, \forall r \in R, ri \in I$$

A natural further definition is a two-sided ideal (sometimes just referred to as an ideal), which is an $I \subseteq R$ that is both a left and a right ideal.

Definition 3.1.3 (Generated Ideals) *Given a ring R and a set $X \subseteq R$, the* left ideal of R generated by X *that we denote $\langle X \rangle_L$ is the interesection of all left ideals of R containing X. This could also be characterized as all finite expressions $\forall r_i \in R, \forall x_i \in X,\ r_1x_1 + \cdot + r_nx_n$*

It is fairly straightforward to see what a corresponding right ideal of R *or* two sided ideal of R generated by X.

One could see the connections between Normal Subgroup (**2.2.9**) 's and two-sided Ideals (**3.1.2**) . For any two sided ideal, the abelian group $(R/I, +)$ has a ring structure when we look at coset multiplication. Very similarly to the way it operates on normal subgroups.

3.2 Ring Homomorphisms

Definition 3.2.1 (Ring Homomorphism) *A mapping $f : R \to S$ (where R, S are rings) is a* ring homomorphism *if the mapping preserves the structure within the ring.*

Similar results as the First Isomorphism Theorem (**2.4.2**) through the Third Isomorphism Theorem (**2.4.4**) can be generalized to the ring world.

Theorem 3.2.2 (Fundamental Theorem of Arithmetic) *Every positive integer n can be written uniquely as a product $n = p_1^{e_1} \cdots p_r^{e_r}$ where each p_i is prime and $e_i \geq 1$.*

The uniqueness of this statement means that if $n = q_1^{f_1} \cdots q_s^{f_s}$ and $n = p_1^{e_1} \cdots p_r^{e_r}$ then after re-indexing, $q_i = p_i$ and $e_i = f_i$ and $r = s$.

A corollary of this generalized to any field can be created

Corollary 3.2.3 (General Field FTA) *For a given field F, every monic polynomial $f(x) \in F[x]$ can be factored uniquely as a product $f(x) = p_1(x)^{e_1} \cdots p_r(x)^{e_r}$ where each $p_i(x)$ is a monic irreducible polynomial in F.*

This all hinges on the key fact that $F[x]$ will always have a division algorithm.

3.3 Integral Domains

Definition 3.3.1 (Integral Domain) *A commutative ring R is an* integral domain *(ID) if the product of non-zero elements is always non-zero.*

Definition 3.3.2 (Unit) *A* unit *is an element within a ring that has a multiplicative inverse. That is, any $u \in R$ is a unit if $\exists u' \in R,\ uu' = 1 = u'u$*

Definition 3.3.3 (Prime) *When in an integral domain R, an element $p \in R$ is* prime *if $p \mid ab \implies p \mid a \vee p \mid b$*

Definition 3.3.4 (Irreducible) *When in an integral domain R, an element $q \in R$ is* irreducible *if $q = ab \implies a \vee b$ is a Unit (**3.3.2**)*

Proposition 3.3.5 (Integral Domain Properties) *This lends to some useful properties in integral domains:*

*(i) Cancelation: $\forall a, b, c \in R$ (where R is an Integral Domain (**3.3.1**)), $a \neq 0 \wedge ab = ac \implies b = c$*

Additionally, the following are equivalent:

*(a) Every non-zero, non-unit element of R can be written as a product of Prime (**3.3.3**) elements.*

(b) *Every non-zero, non-unit elements in R can be written uniquely (up to order and unit multiples) as a product of irreducible elements.*

Definition 3.3.6 (Unique Factorization Domain) *A* Unique Factorization Domain *or (UFD) as a ring that satisfies the unique factorization properties laid out in Integral Domain Properties (**3.3.5**)*

Definition 3.3.7 (Principal Ideal Domain) *A* Principal Ideal Domain *or (PID) is any ring with a division algorithm.*

Proposition 3.3.8 (Principal Ideal Properties) *For any Integral Domain (**3.3.1**) R*

(i) $a \mid b \iff \langle b\rangle \subseteq \langle a\rangle$

(ii) $\langle a\rangle = \langle b\rangle \iff b = au$ *for some unit* $u \in R$

(iii) $q \in R$ *is irreducible* $\iff \langle q\rangle$ *is maximal among principal ideals.*

(iv) $p \in R$ *is prime* $\iff ab \in \langle p\rangle \implies a \in \langle p\rangle \vee b \in \langle p\rangle$

A set of useful propositions over a PID are as following

Proposition 3.3.9 (PID Propositions) *For an ID R*

1. *R satisfies the ascending chain condition on principal ideals*
2. *Every non-empty collection of principal ideals has a maximal element*
3. *Every non-zero, non-unit in R is a product of finitely many irreducible elements.*

$$((i) \iff (ii)) \implies (iii)$$

For the next two R is a PID

(a) *R satisfies the ascending chain condition on principal ideals*

(b) *Every irreducible element is a prime element.*

These can all be combined into the ultimate theorem

Theorem 3.3.10 (PID UFD Theorem) *Every PID is a UFD.*

3.4 Advanced Ring Theorems

Definition 3.4.1 (Quotient Field) *A* Quotient Field K *can be constructed from any arbitrary integral domain* R*. If we take* $R* = R \setminus 0$ *(removing the element* 0*), then we can define an equivalence relation on* $R \times R*$ *by letting* $(n, d) \sim (m, b) \iff nb = md$

Using this, we can form the Quotient Field $K = (R \times R*, +, \cdot)$ *where any two elements are equivalent via the above definition.*

This may also be called the field of fractions.

Proposition 3.4.2 (UFD Prime Element Proposition) *For a UFD* R*, if* $p \in R$ *is prime, then* p *is also prime in* $R[x]$

Definition 3.4.3 (Primitive) *A polynomial* $f(x)$ *is primitive if the Greatest Common Divisor of all coefficients of the polynomial is* 1.

This is more simply stated as "no prime number divides this element"

Lemma 3.4.4 (Gauss's Primitive Polynomial Lemma) *Let* R *be a UFD. Then: The product of primitive polynomials is Primitive (**3.4.3**)*

We can build some further propositions in the ultimate goals of proving that the UFD property for a ring can extend to a polynomial ring over that ring.

Proposition 3.4.5 (Quotient Field Irreducible Element Proposition) *Suppose* R *is a UFD with a Quotient Field (**3.4.1**)* K *and* $f(x) \in R[x]$ *is primitive. Then:* $f(x)$ *is irreducible in* $R[x] \iff$ *it is irreducible in* $K[x]$

Proposition 3.4.6 (UFD Prime Element Proposition) *Suppose* R *is a UFD and* $f(x) \in R[x]$ *is primitive and irreducible. Then:* $f(x)$ *is a Prime (**3.3.3**) element*

Theorem 3.4.7 (UFD Polynomial Ring Theorem) *If* R *is a UFD. Then:* $R[x]$ *is a UFD.*

Definition 3.4.8 (Eisenstein's Criterion) *Given a polynomial* $f(x) = a_n x^n + \cdots + a_1 x + a_0$ *with integer coefficients*

If $\exists p$ *(prime) such that:*

(i) $\forall 0 \leq i < n,\ p \mid a_i$

(ii) $p \nmid a_n$

(iii) $p^2 \nmid a_0$

Then $f(x)$ *is Irreducible (**3.3.4**) over the rational numbers.*

Proposition 3.4.9 (Commutative Ring Properties) *We have some nice properties if we are a commutative ring* *(i) An ideal* $P \subseteq R$ *is a prime ideal* $\iff$ R/P *is an Integral Domain (**3.3.1**)*

(ii) An ideal $M \subseteq R$ *is a maximal ideal* $\iff$ R/M *is a field*

Definition 3.4.10 (Noetherian) *A commutative ring that satisfies any one of the following equivalent conditions is considered* Noetherian

(i) R *satisfies the ascending chain condition.*

(ii) R *satisfies the maximal condition (where any collection of ideals has a maximal element)*

(iii) Every ideal of R *is finitely generated.*

Theorem 3.4.11 (Hilbert's Basis Theorem) *Let* R *be a Noetherian commutative ring.*

Then: $R[x]$ *is Noetherian (**3.4.10**)*

Chapter 4

Fields

4.1 Basic Definitions

Definition 4.1.1 (Field) *A* Field F *is a commutative ring where every non-zero element have a multiplicative inverse.*

*Note: If F is a field, F is also an Integral Domain (**3.3.1**)*

Definition 4.1.2 (Degree) *If $F \subseteq K$ are fields, K can be regarded as a vector space over F.*

We refer to the dimension of this vector space K over F as the degree of K over F.

We denote this $[K : F]$

Definition 4.1.3 (Algebraic) *Let $F \subseteq K$ be a field, and $\alpha \in K$. Then: α is* algebraic over F *if α is a root of a polynomial with coefficients in F.*

It then follows that α also has a minimal polynomial over F

Definition 4.1.4 (Algebraic Intersection) *Suppose $F \subseteq K$ are fields, and $\alpha \in K$ is not Algebraic (**4.1.3**) over F.*

We set $F(\alpha) :=$ the interesction of all intermediate field $F \subseteq E \subseteq K$ such that $\alpha \in E$.

Definition 4.1.5 (Splitting Field) *Given a polynomial $p(x) = (x-\alpha_1)\cdots(x-\alpha_d)$ the field $F(\alpha_1, \ldots, \alpha_d)$* splitting field for $p(x)$ over F.

Proposition 4.1.6 (Degree Multiplication Theorem) *Let $F \subseteq K \subseteq L$ be fields. Then: $[L : F]$ is finite $\iff$ $[L : K]$ and $[K : F]$ are finite, and*

$$[L : F] = [L : K] \cdot [K : F]$$

Theorem 4.1.7 (Primitive Element Theorem) *Suppose $F \subseteq K$ is an extension of fields satisfying $[K : F] < \infty$.*

If $\mathbb{Q} \subseteq F$.

Then: There exists a primitive element $\alpha \in K$ such that $K = F(\alpha)$

Proposition 4.1.8 (Splitting Distinct Roots Proposition) *If F is a field containing $\mathbb{Q}$ and $p(x) \in F[x]$ is irreducible,*

Then: $p(x)$ has distinct roots in K, the splitting of $p(x)$ over F.

Definition 4.1.9 (Algebraic Extension) *Let $F \subseteq K$ be an extension of fields.*

(i) $\alpha \in K$ is algebraic *over F if there is a non-constant polynomial $p(x) \in F[x]$ such that $p(\alpha) = 0$.*

(ii) K is an algebraic extension *of F if every element of K is algebraic over F.*

Proposition 4.1.10 (Finite Degree Field Proposition) *For $F \subseteq K$ fields and $\alpha \in K$, α is Algebraic (**4.1.3**) over $K \iff [F(\alpha) : F] < \infty$*

Theorem 4.1.11 (Extended Primitive Element Theorem) *Suppose $F \subseteq K$ is an extension of fields satisfying $[K : F] < \infty$. If $\mathbb{Q} \subseteq F$ or F is finite, Then: There exists a primitive element $\alpha \in K$ such that $K = F(\alpha)$*

Proposition 4.1.12 (Finite Extension Proposition) *Let $F \subseteq K$ be a finit extension, with F an infinite field.*

Then: there is a primitive element for the extension $\iff$ there are finitely many intermediate fields $F \subseteq E \subseteq K$.

Corollary 4.1.13 (Finite Intermediate Field Corollary) *Let $F \subseteq K$ be a finite extension of fields, with $\mathbb{Q} \subseteq F$.*

Then: There are only finitely many intermediate fields $F \subseteq E \subseteq K$.

Proposition 4.1.14 (Algebraic Field Extension) *Let F be a field.*

Then: There exists a field extension $F \subseteq \overline{F}$ with the following property: For all $0 \neq f(x) \in F[x]$, there exists $\alpha \in \overline{F}$ such that $f(\alpha) = 0$.

Theorem 4.1.15 (Algebraic Closure Theorem) *Let F be a field.*

There is an algebraic extension $F \subseteq \overline{F}$ such that if $p(x) \in F[x]$ and the degree of $p(x)$ is $d > 0$.

Then: There exists $\alpha_1, \ldots, \alpha_d \in F$ (not necessarily distinct) such that $p(x) = (x - \alpha_1) \cdots (x - \alpha_d)$

Definition 4.1.16 (Galois Group) *The* Galois group *of a field extension $F \subseteq K$:*

It is the set of automorphisms of K fixing F.

If $f(x) \in F[x]$, $\alpha \in K$ satisfies $f(\alpha) = 0$, then $f(\sigma(\alpha)) = 0$ for all $\sigma \in Gal(K/F)$.

If $K = F(\alpha)$ for $\alpha \in K$ is a primitive element, then $Gal(K/F)$ is finite. In particular, if $F \subseteq K$ is a finite extension, with $\mathbb{Q} \subseteq F$, then $Gal(K/F)$ is a finite group.

Proposition 4.1.17 (Crucial Proposition) *Let $F_1 \subseteq K_1, F_2 \subseteq K_2$ be fields. $p_1(x) \in F_1[x], p_2(x) \in F_2[x]$ be monic irreducible polynomials of degree d, and $\alpha_1 \in K_1, \alpha_2 \in K_2$ roots of $p_1(x), p_2(x)$ (respectively).*

Suppose $\sigma : F_1 \to F_2$ is an Isomorphism such that $p_2(x) = p_1(x)^\sigma$.

Then: There exists an isomorphism $\overline{\sigma} : F_1(\alpha_1) \to F_2(\alpha_2)$ extending σ such that $\overline{\sigma}(\alpha_1) = \alpha_2$

Simply stated, this means that the roots of polynomials are rotated by the isomorphisms (and will specifically apply to the automorphisms that are in the Galois Group (**4.1.16**)).

We get 2 very nice corollaries of this

Proposition 4.1.18 (Crucial Proposition Corollaries) *(i) If $p(x) \in F[x]$ is irreducible over F and $\alpha_1, \alpha_2 \in \overline{F}$ are two roots of $p(x)$, then there is an isomorphism from $F(\alpha_1) \to F(\alpha_2)$ that fixes F and takes α_1 to α_2*

(ii) If $K = F(\alpha)$ for α algebraic over F, then $|Gal(K/F)|$ equals the number of distinct roots of $p(x)$ in K, where $p(x)$ is the minimal polynomial of α over F.

Theorem 4.1.19 (Galois Theorem) *Suppose that $F \subseteq K$ is a finit extension with a primitive element, so that $K = F(\alpha)$. Let $p(x)$ denote the minimal polynomial of α over F and write $d = deg(p(x))$.*

Then K is Galois over $F \iff p(x)$ has d-distinct roots in K

NOTE: This is important. K is Galois over F if the number of distinct roots is the degree of the minimal polynomial

Theorem 4.1.20 (Primitive Galois Theorem) *Let $K = F(\alpha)$ be a finite extension of F and assume that K is the splitting field of the minimal polynomial of α over F.*

Then if $f(x) \in F[x]$ is a non-constant, irreducible polynomial with a root in K, then $f(x)$ splits over K.

Definition 4.1.21 (Fixed Field) *For $\sigma \in Gal(K/F)$, $K^\sigma := \{a \in K \mid \sigma(\alpha) = \alpha\}$ is the* fixed field *of σ.*

Theorem 4.1.22 (Galois Correspondence Theorem) *Let $F \subseteq K$ be a finite Galois extension and set $G := Gal(K/F)$.*

Then:

(i) There is a 1-1 onto, order reversing correspondence between the subgroups $H \subseteq G$ and the intermediate fields $F \subseteq E \subseteq K$ given by $H \to K^H$ and $E \to Gal(K/E)$. In particular, for all H and E, $H = Gal(K/K^H)$ and $E = K^{Gal(K/E)}$

(ii) If H and E correspond, then $[G : H] = [E : F]$

(iii) For any intermediate field E, K is Galois over E.

(iv) An intermediate field E is Galois over $F \iff Gal(K/E)$ is a normal subgroup of G. In which case, $Gal(E/F) \cong G/Gal(K/E)$

Definition 4.1.23 (Inverse Galois Problem) *This is an unsolved problem: "Is every finite group the Galois group of a Galois extension of $\mathbb{Q}$?"*

Theorem 4.1.24 (Finite Galois Extension Theorem) *Let G be a finite group. Then there exists a finite, Galois extension of field $F \subseteq K$ such that $Gal(K/F) \cong G$.*

Index