Modern Algebra II: Lecture Notes

by Ken Monks
Department of Mathematics
University of Scranton
Revised: Spring 2003

This is **not** a complete set of lecture notes for Math 449, Modern Algebra II. Additional material will be covered in class and discussed in the textbook.

Fun Facts

Section 8.1 - Direct Products

Definition *Let* $G_1, \ldots, G_k$ *be groups and* $G = G_1 \times \ldots \times G_k$. *Then* G *is said to be the* ***direct product*** *of* $G_1, \ldots, G_n$. *If the groups are abelian then we call* G *the* ***direct sum*** *of the groups. In this case we write* $G = G_1 \oplus \ldots \oplus G_k$.

Lemma *If* $M \triangleleft G$ *and* $N \triangleleft G$ *and* $M \cap N = \{e\}$ *then* $\forall a \in M, \forall b \in N, ab = ba$.

Theorem *Let* $N_1, N_2, \ldots, N_k$ *be normal subgroups of a group* G *such that every* $a \in G$ *can be expressed uniquely in the form* $a_1 a_2 \cdots a_k$ *where* $a_i \in N_i$ *for all* i *(i.e. if*

$$a = a_1 a_2 \cdots a_k = b_1 b_2 \cdots b_k$$

where $\forall i \in \mathbb{I}_k, a_i \in N_i$ *and* $b_i \in N_i$ *then* $\forall i \in \mathbb{I}_k, a_i = b_i$*). Then*

$$G \cong N_1 \times \ldots \times N_k$$

Theorem *If* $M \triangleleft G$ *and* $N \triangleleft G$ *and* $G = MN$ *and* $M \cap N = \langle e \rangle$ *then*

$$G \cong M \times N$$

Section 8.2 - Classification of Finite Abelian Groups

Definition *Let* G *be and abelian group and* p *a positive prime integer. Then*

$$G(p) = \left\{ a \in G : \exists n \in \mathbb{N}, |a| = p^n \right\}$$

Remark $G(p)$ *is a group. Closure:* $a^{p^n} = e$ *and* $b^{p^m} = e$ *implies* $(ab)^{p^{m+n}} = e$. *Inverses:* $|a| = |a^{-1}|$

Theorem *If G is a finite abelian group then*

$$G \cong G(p_1) \oplus G(p_2) \oplus \cdots \oplus G(p_t)$$

where $p_1, p_2, \ldots, p_t$ are the distinct positive primes that divide the order of G.

p-groups

Definition *Let p be a positive prime and G a group.*

$$G \text{ is a } \textbf{\textit{p-group}} \Leftrightarrow \forall x \in G, \exists n \in \mathbb{N}, |x| = p^n$$

i.e. a p-group is a group such that the order of all of its elements is a power of p.

Definition *Let G be a p-group and $a \in G$. Then*

$$a \text{ is an } \textbf{\textit{element of maximal order}} \text{ in } G \Leftrightarrow \forall b \in G, |b| \leq |a|.$$

Lemma *Let G be a finite abelian p-group and $a \in G$ an element of maximal order. Then*

$$\exists K \triangleleft G,\ G \cong \langle a \rangle \oplus K$$

Remark *Note: In the proof K is the largest subgroup of G such that $K \cap \langle a \rangle = \langle e \rangle$.*

The Fundamental Theorem of Finite Abelian Groups

Theorem (Fund Thm of Finite Abelian Groups I) *Every finite abelian group is a direct sum of cyclic groups, each of prime power order.*

Theorem *Let $m, k \in \mathbb{N} - \{0,1\}$ and $\gcd(m,k) = 1$. Then*

$$\mathbb{Z}_{mk} \cong \mathbb{Z}_m \oplus \mathbb{Z}_k$$

Corollary *If $n = p_1^{n_1} p_2^{n_2} \cdots p_t^{n_t}$ with $p_1, p_2, \cdots, p_t$ distinct primes then*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$$

Definition *Let G be a finite abelian group, and*

$$G \cong \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_t^{n_t}}$$

with $p_1 \leq p_2 \leq \cdots \leq p_t$ positive primes and $n_i \leq n_{i+1}$ whenever $p_i = p_{i+1}$. Then the sequence

$$p_1^{n_1}, p_2^{n_2}, \cdots, p_t^{n_t}$$

*is called the **sequence of elementary divisors** of G.*

Theorem (Fund Thm of Abelian Groups II) *Let G,H be finite abelian groups. Then $G \cong H \Leftrightarrow G$ and H have the same sequence of elementary divisors.*

Invariant Factors

Theorem *Every finite abelian group is the direct sum of cyclic groups of orders $m_1, m_2, \ldots, m_t$ such that $m_1 | m_2, m_2 | m_3, \ldots, m_{t-1} | m_t$.*

Definition *The numbers $m_1, m_2, \ldots, m_t$ in the previous theorem are called the **invariant factors** of G.*

Section 8.3 - Classification of Finite Non-Abelian Groups

The Sylow Theorems

Remark *From now on, when ever we say p is a prime, we will mean p is a positive prime integer unless stated otherwise.*

Remark *Recall that Lagrange's theorem says that the order of a subgroup must divide the order of the group. What about the converse?*

Sylow I

Theorem (Sylow I) *Let G be a finite group, p a prime, and $k \in \mathbb{N}$. If $p^k \mid |G|$ then G has a subgroup of order p^k.*

Corollary (Cauchy's Thm) *If p is a prime and $p \mid |G|$ then G has an element of order p.*

Definition *Let G be a finite group and p a prime. If p^n is the largest power of p that divides $|G|$ then a subgroup of order p^n is called a **Sylow p-subgroup**.*

Notation *We write $H \sqsubseteq_p G$ if and only if H is a Sylow p-subgroup of G. We write $\#_p(G)$ to denote the number of Sylow p-subgroups of G.*

Sylow II

Definition *Let G be a group and $x \in G$. Let $f_x : G \to G$ by $\forall a \in G,\ f_x(a) = x^{-1}ax$. Then f_x is called the **inner automorphism of G induced by x**.*

Theorem *Let G be a group and $x \in G$. Then f_x is an isomorphism.*

Corollary *Let G be a group, $x \in G$, and $K \sqsubseteq G$. Then $f_x(K) \cong K$. i.e.*

$$\forall x \in G,\ x^{-1}Kx \cong K$$

Theorem (Sylow II) *Let G be a finite group, p a prime.*

$$P \underset{p}{\sqsubseteq} G \text{ and } K \underset{p}{\sqsubseteq} G \Rightarrow \exists x \in G,\ P = x^{-1}Kx$$

i.e. any two Sylow p-subgroups of G are conjugate.

Corollary *Any two Sylow p-subgroups of G are isomorphic.*

Corollary *Let G be a finite group, p a prime, and $K \underset{p}{\sqsubseteq} G$.*

$$K \triangleleft G \Leftrightarrow \#_p(G) = 1$$

i.e. a Sylow p-subgroup is normal if and only if it is the only Sylow p-subgroup.

Sylow III

Theorem (Sylow III) *Let G be a finite group and p a prime. Then*

$$\#_p(G) \mid |G|$$

and

$$\#_p(G) \underset{p}{\equiv} 1$$

CLASSIFY!

Theorem *Let G be a finite group, p,q primes, and $|G| = pq$. If $q < p$ and $q \nmid p-1$ then*

$$G \cong \mathbb{Z}_{pq}$$

Section 8.4 - Proof of the Sylow Theorems

Preliminary Definitions

Definition *Let G be a group and $a,b \in G$. We say b is **conjugate** to a if and only if $b = x^{-1}ax$ for some $x \in G$. In this case we write $b \underset{G}{\sim} a$.*

Theorem $\underset{G}{\sim}$ *is an equivalence relation on* G.

Definition *Let* G *be a group and* $a \in G$. *The* ***centralizer*** *of* a *is*

$$C(a) = \{x \in G : xa = ax\}$$

i.e. $C(a)$ *is the set of all elements of* G *that commute with* a.

Theorem *Let* G *be a group and* $a \in G$. *Then* $C(a)$ *is a subgroup of* G.

Definition *Let* G *be a group and* $H,K \sqsubseteq G$. *We say* H *is* ***conjugate*** *to* K *if and only if* $H = x^{-1}Kx$ *for some* $x \in G$. *In this case we write* $H \underset{G}{\sim} K$.

Theorem $\underset{G}{\sim}$ *is an equivalence relation on the set of subgroups of* G.

Definition *Let* G *be a group and* $H \sqsubseteq G$. *The* ***normalizer*** *of* H *is*

$$N(H) = \{g \in G : Hg = gH\}$$

i.e. $N(H)$ *is the set of all elements of* G *that commute with* H.

Theorem *Let* G *be a group and* $H \sqsubseteq G$. *Then* $N(H)$ *is a subgroup of* G *and* $H \lhd N(H)$.

Definition *Let* G *be a group and* $a \in G$. *The* ***center*** *of* a *is*

$$Z(G) = \{x \in G : \forall a \in G, xa = ax\}$$

i.e. $Z(G)$ *is the set of all elements of* G *that commute with every element of* G.

Theorem $Z(G) \lhd G$

The Class Equation

Theorem (Conjugacy Class Size) *Let* G *be a finite group and* $a \in G$. *The number of elements in the conjugacy class* $[a]$ *is* $[G : C(a)]$.

Remark *Here* $[a]$ *is the equivalence class of* a *with respect to* $\underset{G}{\sim}$.

Definition *The* ***class equation*** *of a finite group* G *is*

$$|G| = [G : C(a_1)] + [G : C(a_2)] + \cdots + [G : C(a_t)]$$

where $a_1, a_2, \ldots, a_t$ *are representatives of the distinct conjugacy classes of* G *with respect to* $\underset{G}{\sim}$.

Remark *The class equation follows immediately from the conjugacy class size theorem and the fact that*

$$|G| = |C_1| + |C_2| + \cdots + |C_t|$$

where $C_1, C_2, \ldots, C_t$ *are the distinct conjugacy classes of* G *with respect to* $\underset{G}{\sim}$.

Theorem *Let* G *be a group and* $a \in G$. *The conjugacy class of* a *is* $\{a\}$ *if and only if* $a \in Z(G)$.

Remark *The class equation can also be written as*

$$|G| = |Z(G)| + |C_1| + |C_2| + \cdots + |C_t|$$

where $C_1, C_2, \ldots, C_t$ *are the distinct conjugacy classes of* G *with respect to* $\underset{G}{\sim}$ *having more than one element.*

Example *Here is the multiplication table for* S_3

$\cdot$	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(132)	(123)	(23)	(13)
(13)	(13)	(123)	e	(132)	(12)	(23)
(23)	(23)	(132)	(123)	e	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	e
(132)	(132)	(23)	(12)	(13)	e	(123)

What are the centralizers and conjugacy classes?

Section 8.5 - Classification

Remark *We have seen that Abelian and simple finite groups have been classified. Let's turn our attention to groups of order less than 100.*

Fact: There is only one group of order one, $\{e\}$.
Conclusion: Classifies order 1.
Scoreboard: 1/100

Theorem (7.28) *If* $|G| = p$ *and* p *is prime then*

$$G \cong \mathbb{Z}_p$$

Conclusion: Classifies orders 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.
Scoreboard: 26/100

Corollary (8.18) *If* $|G| = pq$ *and* p, q *are prime,* $p > q$*, and* $q \nmid p-1$ *then*

$$G \cong \mathbb{Z}_{pq}.$$

Conclusion: Classifies orders 15,33,35,51,65,69,77,85,87,91,95.
Scoreboard: 37/100

Theorem *If* $|G| = p^n$, p *prime, and* $n > 1$ *then* $|Z(G)| > 1$, *i.e.* $|Z(G)| = p^k$ *for some* $1 \leq k \leq n$.

Corollary *If* p *is prime and* $n > 1$ *then there is no simple group of order* p^n.

Corollary *If* $|G| = p^2$ *and* p *is prime then* G *is abelian (and therefore isomorphic to* $\mathbb{Z}_{p^2}$ *or* $\mathbb{Z}_p \oplus \mathbb{Z}_p$*)*

Conclusion: Classifies orders 4,9,25,49.
Scoreboard: 41/100

Theorem *If* $|G| = p^2q$*, where* p*,* q *are distinct primes such that* $p^2 \underset{q}{\not\equiv} 1$ *and* $q \underset{p}{\not\equiv} 1$ *then* G *is abelian (and therefore* $G \cong \mathbb{Z}_{p^2q}$ *or* $G \cong \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_q$*)*

Conclusion: Classifies orders 45, 99.
Scoreboard: 43/100

Corollary *If* p, q *are distinct primes there is no simple group of order* p^2q.

Theorem *If* $|G| = 2p$ *where* p *is an odd prime, then*

$$G \cong \mathbb{Z}_{2p} \text{ or } G \cong D_p$$

Conclusion: Classifies orders 6, 10, 14, 22, 26, 34, 38, 46, 58, 62, 74, 82, 86, 94.
Scoreboard: 57/100

Definition *Let* $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $I = \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}$, $J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$ *and* $Q = \{e, -e, I, -I, J, -J, K, -K\} \subseteq M_2(\mathbb{C})$.

Theorem *Q with matrix multiplication is a group.*

Definition *Q is called the **quaternion group**.*

Theorem *If $|G| = 8$ then G is isomorphic to one of the following groups:*

$$\mathbb{Z}_8$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_2$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$
$$D_4$$
$$Q$$

Conclusion: Classifies order 8.
Scoreboard: 58/100

Not bad!

Section 9.1 - Euclidean Domains

Memory Lane...

Definition *A ring $(R,+,\cdot)$ is an **integral domain** $\Leftrightarrow$ $(R,+,\cdot)$ is a commutative ring with identity $1_R \neq 0_R$ and $\forall a,b \in R, ab = 0_R \Rightarrow a = 0_R$ or $b = 0_R$.*

Definition *Let $(R,+,\cdot)$ be a ring and $a \in R$. Then a is called a **zero divisor** of R if and only if*

$$a \neq 0 \text{ and } \exists b \in R, b \neq 0_R \text{ and } \left(ab = 0_R \text{ or } ba = 0_R\right).$$

Definition *Let $(R,+,\cdot)$ be a ring with identity and $a \in R$. If a has a multiplicative inverse then we say a is a **unit** in R.*

Definition *Let R be a commutative ring with identity and $a,b \in R$. We say a is an **associate** of b in $R \Leftrightarrow a = bu$ for some $u \in \mathcal{U}(R)$. If a is an associate of b we write $a \diamond b$.*

Definition *Let R be a commutative ring with identity, and $a,b \in R$. We say a **divides** b and write $a \mid b \Leftrightarrow a \neq 0$ and $ax = b$ for some $x \in R$.*

Definition *Let R be a commutative ring with identity and $p \in R$. Then p is* ***irreducible*** *if and only if p is not a unit and the only divisors of p are units and associates of p.*

Lemma *$\diamond$ is an equivalence relation.*

Theorem *Let R be an integral domain and $p \in R - \{0\}$. Then p is irreducible $\Leftrightarrow$ $\forall r,s \in R,\ p = rs \Rightarrow r$ is a unit or s is a unit.*

Euclidean Domains

Definition *An integral domain R is a* ***Euclidean domain*** *if and only if there exists a function $\delta : R - \{0\} \to \mathbb{N}$ such that*

1. $\forall a,b \in R - \{0\}, \delta(a) \le \delta(ab)$
2. $\forall a,b \in R,\ b \ne 0 \Rightarrow$
$\exists q,r \in R, a = bq + r$ and ($r = 0_R$ or $\delta(r) < \delta(b)$).

Theorem (Killer Death Nice Important) *Let R be a Euclidean domain and $u \in R - \{0\}$. T.F.A.E.*
1. u is a unit
2. $\delta(u) = \delta(1_R)$
3. $\delta(c) = \delta(uc)$ for some $c \in R - \{0\}$.

Section 9.2 - Principal Ideal Domains

Memory Lane...

Definition *Let R be a ring and $I \subseteq R$.*

I is an **ideal** $\Leftrightarrow$ (1) I is a subring of R
(2) $\forall r \in R, \forall a \in I, ra \in I$ and $ar \in I$

Definition *An ideal I of a commutative ring with identity R is a* ***principal ideal*** *if and only if*

$$\exists a \in R,\ I = (a)$$

where $(a) = \{ra : r \in R\}$.

PID's

Definition *A* ***principal ideal domain (PID)*** *is an integral domain in which every* *ideal is principal.*

Theorem *Every Euclidean domain is a PID.*

Divisibility vs Principal Ideals

Theorem *Let R be an integral domain and $a,b \in R$.*

1. $(a) \subseteq (b) \Leftrightarrow b \mid a$
2. $(a) = (b) \Leftrightarrow a \mid b$ and $b \mid a$
3. $(a) \subsetneq (b) \Leftrightarrow b \mid a$ and $\sim(b \diamond a)$

Ascending Chain Condition

Definition *An integral domain R satisfies the* ***ascending chain condition (ACC)*** *if and only if for any collection of principal ideals satisfying*

$$(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq \cdots$$

there exists $n \in \mathbb{N}$ such that $(a_i) = (a_n)$ for all $i \geq n$.

Theorem *Every PID satisfies the ACC.*

Unique Factorization Domains

Definition *An integral domain is a* ***unique factorization domain (UFD)*** *if and only if every nonzero nonunit element of R is the product of irreducibles and this factorization is unique up to the ordering of the terms and replacement of factors with one of their associates, i.e. it is a UFD iff*

$$\forall a \in R - (\{0\} \cup \mathcal{U}(R)), a = p_1 p_2 \cdots p_r$$

for some irreducibles $p_1, \ldots, p_r \in R$, and if

$$a = q_1 q_2 \cdots q_s$$

for some irreducibles $q_1, \ldots, q_s \in R$ then $s = r$ and

$$\exists \sigma \in S_r, \forall i \in \mathbb{I}_r, p_{\sigma(i)} \diamond q_i.$$

Theorem *Every PID is a UFD.*

Theorem *Every UFD satisfies the ACC.*

Theorem *Let R be a UFD, $p \in R$ irreducible, $b,c \in R$.*

$$p \mid bc \Rightarrow p \mid b \text{ or } p \mid c$$

Theorem *An integral domain R is a UFD if and only if*

1. *it satisfies the ACC*
2. $\forall p, b, c \in R$, p *irreducible and* $p \mid bc \Rightarrow p \mid b$ or $p \mid c$

Section 9.3 - Quadratic Integers

Definition *An integer $d \in \mathbb{Z}$ is* ***square free*** *if and only if*

$$d \neq 1 \text{ and } \forall c \in \mathbb{Z},\ c^2 \mid d \Rightarrow c = \pm 1$$

Remark *From now on we shall always assume that d is a square free integer when discussing $\mathbb{Z}\left[\sqrt{d}\,\right]$.*

Definition *Let $N : \mathbb{Z}\left[\sqrt{d}\,\right] \to \mathbb{Z}$ by*

$$N\left(s + t\sqrt{d}\right) = s^2 - dt^2$$

N is called the ***norm***.

Theorem *Let $a, b \in \mathbb{Z}\left[\sqrt{d}\,\right]$. Then*

1. $N(a) = 0 \Leftrightarrow a = 0$
2. $N(ab) = N(a)N(b)$

Theorem (Killer Death Nice Important II) *Let $u \in \mathbb{Z}\left[\sqrt{d}\,\right]$. Then*

$$u \text{ is a unit } \Leftrightarrow N(u) = \pm 1$$

Theorem *Let d be square free.*

1. *If $d > 1$ then $\mathbb{Z}\left[\sqrt{d}\,\right]$ has infinitely many units.*
2. *If $d = -1$ then $\mathbb{Z}\left[\sqrt{d}\,\right]$ has only $\pm 1, \pm i$ as units.*
3. *If $d < -1$ then $\mathbb{Z}\left[\sqrt{d}\,\right]$ has only ± 1 as units.*

Theorem *Let $p \in \mathbb{Z}\left[\sqrt{d}\,\right]$. If $N(p)$ is prime then p is irreducible.*

Theorem *Every nonzero nonunit element of $\mathbb{Z}\left[\sqrt{d}\,\right]$ is a product of irreducibles.*

Section 9.4 - The Field of Quotients

Definition *Let R be an integral domain and define a relation $\sim$ on $R \times (R - \{0\})$ by*

$$(a,b) \sim (c,d) \Leftrightarrow ad = bc \text{ in } R$$

Theorem *$\sim$ is an equivalence relation.*

Notation *$[a,b]$ is an abbreviation for $[(a,b)]$.*

Definition *Let R be an integral domain. The **field of quotients** of R (or **field of fractions**) is the set*

$$F_R = R \times (R - \{0\})/\sim$$

with addition and multiplication defined by

$$[a,b] \oplus [c,d] = [ad + bc, bd]$$

$$[a,b] \odot [c,d] = [ac, bd]$$

Notation *We will usually use $+$, for $\oplus$ and $\cdot$ or concatenation for $\odot$ just like in any other ring.*

Theorem *The field of quotients of an integral domain is a field.*

Properties of the Field of Quotients

Theorem *Let F_R be the field of quotients of an integral domain R and let $a,b,c,k \in R$ and $b \neq 0_R$. Then*

1. $0_{F_R} = [0_R, b]$
2. $[a,b] = [ak, bk]$
3. $1_{F_R} = [b,b] = [1_R, 1_R]$
4. $[a,b]^{-1} = [b,a]$ *if* $a \neq 0_R$
5. $-[a,b] = [-a,b]$

Definition *Let F_R be the field of quotients of an integral domain R. Define*

$$R^* = \{[a, 1_R] : a \in R\}$$

Theorem *Let F_R be the field of quotients of an integral domain R. Then R^* is a* *subring of F_R which is isomorphic to R.*

Theorem *F_R is the smallest field containing R, i.e. if K is any field with $R \sqsubseteq K$ (or containing a subring that is isomorphic to R), then there is a subfield $E \sqsubseteq K$ such that $R \sqsubseteq E$ (or E contains a subring isomorphic to R) and $E \cong F_R$.*

Fractions!!!

Definition *Let R be an integral domain, F_R its field of quotients, and $a,b \in R, b \neq 0$. Then we define*

$$\boxed{\frac{a}{b} = [a,b]}$$

Yeeeehaaa!!!

Section 9.5 - R a UFD $\Rightarrow$ $R[x]$ is a UFD

Theorem (IXDOTVE) *If R is a UFD then so is $R[x]$*

Corollary *$\mathbb{Z}[x]$ is a UFD but not a PID*

Corollary *$\mathbb{Z}[x]$ is not a Euclidean domain*

The proof... in stages

Definition *Let R be a UFD. Then $f \in R[x]$ is **primitive** if and only if*
$\forall c \in R, c \mid f \Rightarrow c \in \mathcal{U}(R)$

Lemma *Let R be a UFD, $f \in R[x]$, and $\deg(f) \geq 1$.*

$$f \text{ is irreducible } \Rightarrow f \text{ is primitive}$$

Lemma *Let R be a UFD, $f \in R[x] - \{0\}$.*

$$\exists c \in R, \exists g \in R[x], f = cg \text{ and } g \text{ is primitive}$$

Lemma *Let R be a UFD, $f \in R[x] - \{0\}$, and f not a unit. Then f is a product of irreducibles.*

Lemma *Let R be a UFD and $g,h \in R[x]$. If $p \in R$ is irreducible and $p \mid gh$ then $p \mid g$ or $p \mid h$.*

Corollary (Gauss's Lemma) *Let R be a UFD. The product of primitives in $R[x]$ is primitive.*

Lemma *Let R be a UFD, $r,s \in R - \{0\}$, $f,g \in R[x]$ primitive, and $rf = sg$. Then $r \diamond s$ and $f \diamond g$.*

Corollary *Let R be a UFD, F_R its field of quotients, $f,g \in R[x]$ primitives.*

$$f \diamond g \text{ in } F_R[x] \Rightarrow f \diamond g \text{ in } R[x]$$

Corollary *Let R be a UFD, F_R its field of quotients, and $f \in R[x]$. If $\deg(f) > 0$ and f is irreducible in $R[x]$ then f is irreducible in $F_R[x]$.*

Section 10.1 - Vector Spaces

Definition *A* ***vector space*** *is a tuple $(V,+,F,*,\oplus,\bullet)$ where*

1. $(V,+)$ *is an abelian group*
2. $(F,*,\oplus)$ *is a field*
3. $\bullet : F \times V \to V$ *and* $\forall a,a_1,a_2 \in F, \forall v,v_1,v_2 \in V$

   (i) $a \bullet (v_1 + v_2) = (a \bullet v_1) + (a \bullet v_2)$

   (ii) $(a_1 \oplus a_2) \bullet v = (a_1 \bullet v) + (a_2 \bullet v)$

   (iii) $a_1 \bullet (a_2 \bullet v) = (a_1 * a_2) \bullet v$

   (iv) $1_F \bullet v = v$

Remark *In this situation we say "V is an F-vector space" or "V is a vector space over F". As usual, we als write $+$ for both $\oplus$ and $+$ and we use juxtaposition for both $*$ and $\bullet$. Let's be somewhat careful about 0_F vs 0_V however.*

Memory Lane...

Definition *Let V be an F-vector space and $v_1,\ldots,v_n,w \in V$. We say w is an F-**linear combination** of $v_1,\ldots,v_n$ if and only if*

$$w = a_1v_1 + a_2v_2 + \ldots + a_nv_n$$

for some $a_1,\ldots,a_n \in F$.

Definition *Let V be an F-vector space and $S \subseteq V$. If every element of V can be written as a linear combination of finitely many elements of S we say S **spans** V.*

Definition *Let V be an F-vector space and $v_1, \ldots, v_n \in V$. We say that $v_1, \ldots, v_n$ are F-**linearly independent** if and only if $\forall a_1, \ldots, a_n \in F$*

$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = 0_V \Rightarrow a_1 = a_2 = a_3 = \cdots = a_n = 0_F$$

In this situation we also say that the set $\{v_1, \ldots, v_n\} \subseteq V$ is also linearly independent over F.

Definition *Let V be an F-vector space and $B \subseteq V$. We say B is a **basis for V over F** if and only if B spans V and every finite subset of B is linearly independent.*

Theorem *Let V be an F-vector space which has a finite basis. Any two bases of V have the same number of elements.*

Definition *If a vector space V has a finite basis over F then we say that V is a **finite dimensional** vector space over F. The **dimension** of V over F is the number of elements in any basis and is denoted*

$$[V : F]$$

*If V does not have a finite basis over F then we say that V is **infinite dimensional** and write $[V : F] = \infty$.*

Theorem *Let F, K, L be fields with $F \sqsubseteq K \sqsubseteq L$. If $[K : F]$ and $[L : K]$ are finite then*

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

Theorem *Let F, K, L be fields with $F \sqsubseteq K$ and $F \sqsubseteq L$. Let $f : K \to L$ be an isomorphism such that $\forall c \in F, f(c) = c$. Then*

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

Section 10.2 - Simple Extensions

Definition *Let $F \sqsubseteq K$ be fields and $u \in K$.*

$$F(u) = \bigcap_{J \in I} J$$

*where $I = \{J : F \sqsubseteq J \sqsubseteq K \text{ and } J \text{ is a field and } u \in J\}$, i.e. $F(u)$ is the intersection of all subfields of K that contain F and u. $F(u)$ is called a **simple extension** of F.*

Theorem *Let $F \sqsubseteq K$ be fields and $u \in K$. Then $F(u)$ is a field.*

Algebraic vs Transcendental

Definition *Let $F \sqsubseteq K$ be fields and $u \in K$. We say u is* ***algebraic over*** *F if and only if u is a root of an nonzero polynomial in $F[x]$. If F is not algebraic over F we say u is* ***transcendental*** *over F.*

Minimal Polynomials

Theorem *Let $F \sqsubseteq K$ be fields an $u \in K$ algebraic over F. Then there exists a unique monic irreducible polynomial $p \in F[x]$ such that u is a root of p. Furthermore, for all $g \in F[x]$, u is a root of $g \Leftrightarrow p \mid g$.*

Definition *Let $F \sqsubseteq K$ be fields and $u \in K$ algebraic over F. The unique monic irreducible polynomial in $F[x]$ having u as a root is called the* ***minimal polynomial*** *of u over F.*

Theorem *Let $F \sqsubseteq K$ be fields, $u \in K$ algebraic over F, $p \in F[x]$ the minimal polynomial of u, and $n = \deg(p)$.*

1. $F(u) \cong F[x]/(p)$
2. $\{1_F, u, u^2, \ldots, u^{n-1}\}$ *is a basis for $F(u)$ as a vector space over F.*
3. $[F(u) : F] = n$

Extending isomorphisms

Definition *Let F, E be fields and $\sigma : F \to E$ an isomorphism. Define $\Phi : F[x] \to E[x]$ by*

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

The map Φ is called the ***extension*** *of σ to $F[x]$.*

Lemma *Let F, E be fields and $\sigma : F \to E$ an isomorphism and $i_F : F \to F[x]$ and $i_E : E \to E[x]$ the inclusion maps. Then the extension of σ to $F[x]$ is an isomorphism and*

$$\begin{array}{ccc} F & \xrightarrow{\sigma} & E \\ i_F \downarrow & & \downarrow i_E \\ F[x] & \xrightarrow[\Phi]{} & E[x] \end{array}$$

commutes.

Corollary *Let E, F be fields, $\sigma : F \to E$ an isomorphism, u algebraic over F with minimum polynomial $p \in F[x]$, and v algebraic over E with minimal polynomial $\Phi(p)$. There exists an extension isomorphism $\overline{\sigma} : F(u) \to F(v)$ such that $\overline{\sigma}(u) = v$ and $\overline{\sigma}(c) = \sigma(c)$ for all $c \in F$.*

Corollary *If u, v have the same minimal polynomial over F then $F(u) \cong E(v)$.*

Eisenstein's Irreduciblity Theorem

Theorem (Eisenstein's Irreducibility Theorem) *Let R be an integral domain and*

$$f = a_0 + a_1 x + \cdots + a_n x^n \in R[x]$$

where $a_n \neq 0_R$. If there is an irreducible $p \in R$ such that p divides each of $a_0, a_1, \ldots, a_{n-1}$ and $p \nmid a_n$ and $p^2 \nmid a_0$ then f is irreducible in $F_R[x]$.

Section 10.3 - Algebraic Extensions

Definition *Let $F \sqsubseteq K$ be fields. K is an **algebraic extension** of F if every element of K is algebraic over F.*

Theorem (Finite Dim ⇒ Algebraic) *If K is a finite dimensional extension field of F then K is an algebraic extension of F.*

Finitely Generated Extensions

Definition *Let $F \sqsubseteq K$ be fields, $n \in \mathbb{Z}^+$, and $u_1, \ldots, u_n \in K$. Define*

$$F(u_1, \ldots, u_n) = \bigcap_{J \in I} J$$

where $I = \{J : J \text{ is a field and } F \sqsubseteq J \sqsubseteq K \text{ and } u_1, \ldots, u_n \in J\}$, i.e. $F(u_1, \ldots, u_n)$ is the smallest subfield of K that contains F and $u_1, \ldots, u_n$.

*$F(u_1, \ldots, u_n)$ is called the **extension of F generated** by $u_1, \ldots, u_n$ and we say it is a **finitely generated** extension.*

Remark *In the next three theorems let $F \sqsubseteq K$ be fields, $n \in \mathbb{Z}^+$, and $u_1, \ldots, u_n \in K$.*

Theorem *$F(u_1, \ldots, u_n)$ is a field.*

Theorem (Finite Dim⇒Finite Gen) *If K is a finite dimensional extension field of F*

then K is finitely generated.

Theorem $F(u_1, \ldots, u_n) = F(u_1, \ldots, u_{n-1})(u_n)$

Remark *Thus we can "build" a finitely generated extension by a sequence of simple extensions.*

Theorem (Algebraic & Finite Gen⇒Finite Dim) *Let $F \sqsubseteq K$ be fields, $n \in \mathbb{Z}^+$, and $u_1, \ldots, u_n \in K$ be algebraic over F. Then $F(u_1, \ldots, u_n)$ is a finite dimensional algebraic extension of F.*

The Field of Algebraic Numbers

Theorem *Let K be an extension field of F and*

$$E = \{x \in K : x \text{ is algebraic over } F\}$$

Then E is an algebraic extension of F.

Definition *The **field of algebraic numbers** is the extension field of $\mathbb{Q}$ consisting of all $z \in \mathbb{C}$ such that z is algebraic over $\mathbb{Q}$.*

Section 10.4 - Splitting Fields

Definition *Let $F \sqsubseteq K$ be fields and $f \in F[x]$ a nonconstant polynomial. The K is a **splitting field** of f over F if and only if*

1. $f = c(x - u_1)(x - u_2)\cdots(x - u_n)$ in $K[x]$ *(i.e. it splits in $K[x]$)*
2. $K = F(u_1, u_2, \ldots, u_n)$

i.e. K is a smallest field containing all of the roots of f.

Theorem (Splitting Fields Exist) *Let F be a field and $f \in F[x]$ polynomial of degree $n \geq 1$. There exists a splitting field K of f over F with*

$$[K : F] \leq n!$$

Theorem *Let $\sigma : F \to E$ be a field isomorphism, $f \in F[x]$ nonconstant, and σf the corresponding polynomial in $E[x]$. If K is a splitting field of f over F and L is a splitting field of σf over E then σ extends to an isomorphism $K \cong L$.*

Corollary (Splitting Fields are "Unique") *Any two splitting fields of $f \in F[x]$*

over a field F are isomorphic.

Normal Extensions

Definition *An algebraic extension field K of a field F is* ***normal*** *if and only if for all irreducible polynomials $p \in F[x]$, if p has a root in K then p splits in K (i.e. its normal iff whenever an irreducible polynomial has one root, it has them all)*

Theorem *A field K is a splitting field over a field F of some polynomial in $F[x]$ if and only if K is a finite dimensional normal extension of f.*

Algebraic Closure

Definition *A field F is* ***algebraically closed*** *if and only if every nonconstant polynomial $f \in F[x]$ splits in $F[x]$, i.e. iff the only irreducible polynomials are of degree 1. The* ***algebraic closure*** *of a field F is an algebraic extension field K of F which is algebraically closed.*

Theorem *Every field has an algebraic closure.*

Section 10.5 - Separable Extensions

Definition *Let F be a field, $f \in F[x]$, $\deg(f) = n$, K a splitting field of f over F and $f = c(x-u_1)(x-u_2)\cdots(x-u_n)$ where $c \in F$ and $u_1, u_2, \ldots, u_n \in K$. If $u_i = u_j$ for some $i \neq j$ then we say u_i is a* ***repeated root****. If f has no repeated roots, we say f is* ***separable.***

Definition *Let K be any extension field of a field F and $u \in K$. We say u is* ***separable*** *over F if and only if*

1. *u is algebraic over F and*
2. *the minimal polynomial of u is separable*

We say K is ***separable*** *over F (or a* ***separable extension*** *of F) if and only if every element of K is separable over F.*

Definition *Let F be a field and $f = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \in F[x]$. The* ***algebraic derivative*** *of f is*

$$f' = a_1 + 2a_2x + 3a_3x^2 + \cdots + na_nx^{n-1}$$

Remark *In the previous definition, the numerical coefficients* $2, 3, \ldots$ *etc are additive notation for power in a group, i.e.* $3a_3$ *means* $a_3 + a_3 + a_3$. *(Equivalently we can consider the* 3 *to be* $1_F + 1_F + 1_F$ *in* F*)*

Theorem *Let* F *be a field and* $f, g \in F[x]$. *Then*

$$(f+g)' = f' + g'$$
$$(fg)' = fg' + gf'$$

Lemma *Let* F *be a field and* $f \in F[x]$. *If* $\gcd(f, f') = 1_{F[x]}$ *then* f *is separable.*

Definition *Let* F *be a field.* F *has* ***characteristic*** 0 *if and only if* $\forall n \in \mathbb{N}^{+}, n1_F \neq 0_F$.

Theorem (Alg & Char 0 ⇒ separable) *If* F *has characteristic* 0 *then every irreducible polynomial in* $F[x]$ *is separable and every algebraic extension of* F *is separable.*

Theorem (Fin Gen & Separable⇒Simple) *Every finitely generated separable extension of a field simple.*

Section 10.6 - Classification of Finite Fields

Definition *Let* R *be a ring with identity. We say* R *has* ***characteristic*** 0 *if* $m1_R \neq 0_R$ *for any* $m \in \mathbb{Z}^{+}$. *We say* R *has* ***characteristic*** n *if* $n1_R = 0_R$ *and* $m1_R \neq 0_R$ *for any* $1 \leq m < n$. *We denote the characteristic of* R *by* $char(R)$.

Lemma *If* R *is an integral domain then* $char(R) = 0$ *or* $char(R)$ *is a positive prime integer.*

Lemma *If* $char(R) = n > 0$ *then*

$$k1_R = 0_R \Leftrightarrow n \mid k$$

The Prime Subfield

Theorem *Let* R *be a ring with identity. Then*

1. $P = \{k1_R : k \in \mathbb{Z}\}$ *is a subring of* R
2. $char(R) = 0 \Rightarrow P \cong \mathbb{Z}$

3. $char(R) = n > 0 \Rightarrow P \cong \mathbb{Z}_n$

Corollary *If $char(R) = 0$ then R is infinite.*

Corollary *Every finite field has characteristic p for some prime p.*

Definition *Let K be a finite field of characteristic p. The subfield P in the previous theorem is called the **prime subfield** of K.*

Remark *Every finite field contains a subfield isomorphic to $\mathbb{Z}_p$, i.e. it is an extension field of $\mathbb{Z}_p$.*

The order of finite fields

Definition *The number of elements in a finite field is called its **order**.*

Theorem *Every finite field K has order p^n where $p = char(K)$ and $n = [K : \mathbb{Z}_p]$.*

Classification of all Finite Fields

Lemma (The Freshman's Dream) *Let p be a prime and R a commutative ring with identity and $char(R) = p$. Then $\forall a, b \in R, \forall n \in \mathbb{N}^+$,*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

Theorem (Classification of Finite Fields) *Let K be an extension field of $\mathbb{Z}_p$ and $n \in \mathbb{N}^+$.*

$$|K| = p^n \Leftrightarrow K \text{ is a splitting of } x^{p^n} - x \text{ over } \mathbb{Z}_p$$

Corollary *For each positive prime p and each $n \in \mathbb{N}^+$, there exists a field of order p^n.*

Corollary *Any two finite fields of the same order are isomorphic.*

Definition *Let p be a positive prime and $n \in \mathbb{N}^+$. The unique field of order p^n is called the **Galois field** of order p^n and is denoted $\mathbb{F}_{p^n}$.*

The Simplicity of Finite Field Extensions

Theorem *Let K be a finite field and F a subfield. Then K is a simple extension of F.*

Corollary *Let p be a prime. For each $n \in \mathbb{N}^+$, there exists an irreducible polynomial of degree n in $\mathbb{Z}_p[x]$.*

Section 11.1 - The Galois Group

Solving Polynomial Equations

Q: Let $f \in \mathbb{R}[x]$. When can we solve $\overline{f}(x) = 0$, i.e. when can we find the roots of f?

Degree 0

A: If $f = a \in \mathbb{R} - \{0\}$ then there are no roots of f.

Degree 1

A: If $f = ax + b$ and $a \neq 0$ then the root of f is $-b/a$.

Degree 2 (the quadratic formula)

A: If $f = ax^2 + bx + c$ and $a \neq 0$ then the roots of f are

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Degree 3 (the cubic formula)

A: If $f = ax^3 + bx^2 + cx + d$ and $a \neq 0$, define $p = b/a$, $q = c/a$, and $r = d/a$ so that the roots of f are the same as the roots of $x^3 + px^2 + qx + r$. Define

$$\alpha = \frac{1}{3}(3q - p^2)$$

$$\beta = \frac{1}{27}(2p^3 - 9pq + 27r)$$

$$A = \sqrt[3]{-\frac{\beta}{2} + \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}$$

$$B = \sqrt[3]{-\frac{\beta}{2} - \sqrt{\frac{\beta^2}{4} + \frac{\alpha^3}{27}}}$$

Then the roots of f are

$$A+B-\frac{p}{3}$$
$$-\frac{A+B}{2}-\frac{p}{3}+\frac{A-B}{2}\sqrt{-3}$$
$$-\frac{A+B}{2}-\frac{p}{3}-\frac{A-B}{2}\sqrt{-3}$$

Degree 4 (the quartic formula)

A: If $f = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ and $a_4 \neq 0$, define $a = a_3/a_4$, $b = a_2/a_4$, $c = a_1/a_4$, and $d = a_0/a_4$, so that the roots of f are the same as the roots of $x^4 + ax^3 + bx^2 + cx + d$.

Let y be any root of $x^3 - bx^2 + (ac - 4d)x + (4bd - a^2d - c^2)$ and define

$$R = \sqrt{\frac{a^2}{4} - b + y}$$

If $R = 0$ define

$$D = \sqrt{\frac{3a^2}{4} - 2b + 2\sqrt{y^2 - 4d}}$$
$$E = \sqrt{\frac{3a^2}{4} - 2b - 2\sqrt{y^2 - 4d}}$$

If $R \neq 0$ define

$$D = \sqrt{\frac{3a^2}{4} - R^2 - 2b + \frac{4ab - 8c - a^3}{4R}}$$
$$E = \sqrt{\frac{3a^2}{4} - R^2 - 2b - \frac{4ab - 8c - a^3}{4R}}$$

Then the roots of f are

$$-\frac{a}{4} + \frac{R}{2} \pm \frac{D}{2}$$
$$-\frac{a}{4} - \frac{R}{2} \pm \frac{E}{2}$$

Degree 5 ???

Galois Theory

The Galois Group

Definition *Let $F \sqsubseteq K$ be fields. A map $\sigma : K \to K$ is an **F-automorphism** iff*

1. σ is a field isomorphism

2. $\forall x \in F,\ \sigma(x) = x$

Definition *The set of all F-automorphisms of K over F is called the **Galois group** of K over F and is denoted $Gal_F(K)$*

Theorem $(Gal_F(K), \circ)$ *is a group.*

The Action of the Galois Group on Roots

Theorem *Let* K *be an extension field of* F *and* $f \in F[x]$. *If* $u \in K$ *is a root of* f *and* $\sigma \in Gal_F(K)$ *then* $\sigma(u)$ *is also a root of* f.

Theorem *Let* K *be the splitting field of* $f \in F[x]$ *and* $u, v \in K$. *Then* $\sigma(u) = v$ *for some* $\sigma \in Gal_F(K)$ *if and only if* u, v *have the same minimal polynomial.*

Theorem *Let* $K = F(u_1, \ldots, u_n)$ *be an algebraic extension of* F *and* $\sigma, \tau \in Gal_F(K)$. *If* $\sigma(u_i) = \tau(u_i)$ *for all* $1 \leq i \leq n$ *then* $\sigma = \tau$.

Corollary *If* K *is the splitting field of a separable polynomial* $f \in F[x]$ *and* $deg(f) = n$ *then* $Gal_F(K)$ *is isomorphic to a subgroup of* S_n.

Intermediate Fields

Definition *Let* $F \sqsubseteq E \sqsubseteq K$ *be fields.* E *is called* ***an intermediate field*** *of the extension* $F \sqsubseteq K$.

Theorem *If* $F \sqsubseteq E \sqsubseteq K$ *are fields then* $Gal_E(K) \sqsubseteq Gal_F(K)$.

Theorem *Let* $F \sqsubseteq K$ *be fields and* $H \sqsubseteq Gal_F(K)$. *Define*

$$E_H = \{\alpha \in K : \sigma(\alpha) = \alpha \text{ for every } \sigma \in H\}$$

Then E_H *is an intermediate field of the extension, i.e.* $F \sqsubseteq E_H \sqsubseteq K$.

Definition *In the previous theorem,* E_H *is called the fixed field of the subgroup* H.

Section 11.2 - The Fundamental Theorem of Galois Theory

The Galois Correspondence

Definition *Let* $F \sqsubseteq E \sqsubseteq K$ *fields and* $[K : F]$ *finite. Define*

$$\theta(E) = Gal_E(K)$$

Then θ *is called the* ***Galois correspondence*** *between the intermediate fields of the extension* $F \sqsubseteq K$ *and the subgroups of* $Gal_F(K)$.

Notation $\begin{array}{c} K \\ {}_n\uparrow \\ F \end{array}$ means K is an extension field of F and $[K : F] = n$.

$\begin{array}{c} H \\ {}_n\downarrow \\ G \end{array}$ means H is a subgroup of G and $[G : H] = n$.

Q: Is θ surjective? injective? Does it have an inverse?

Surjective

Theorem *Let K be a finite dimensional extension field of F and H a subgroup of $\mathrm{Gal}_F(K)$. Then $\theta(E_H) = H$ and $[K : E_H] = |H|$.*

Corollary *θ is surjective.*

Injective

Definition *We say K is a **Galois extension** of F (or **Galois over** F) iff K is a finite dimensional normal separable extension field of F.*

Theorem *Let K be a finite dimensional extension field of F and H a subgroup of $\mathrm{Gal}_F(K)$. Then K is Galois over E_H and K is a simple extension of E_H.*

Theorem *If K is a Galois extension of F and $F \sqsubseteq E \sqsubseteq K$ then $E = E_{\mathrm{Gal}_E(K)}$.*

Corollary *θ is injective for Galois extensions.*

Corollary *Let K be a finite dimensional extension field of F.*

$$K \text{ is Galois over } F \Leftrightarrow F = E_{\mathrm{Gal}_F(K)}$$

The Fundamental Theorem

Theorem (Fundamental Theorem of Galois Theory) *Let K be Galois over F. Define*

$$S = \{E : F \sqsubseteq E \sqsubseteq K\}$$

and

$$T = \{H : H \sqsubseteq Gal_F(K)\}$$

and $\theta : S \to T$ *by* $\theta(E) = Gal_E(K)$. *Then*

1. θ *is a bijection*
2. $[K : E] = |\theta(E)|$ *and* $[E : F] = [\theta(F) : \theta(E)]$
3. E *is a normal extension of* $F \Leftrightarrow \theta(E)$ *is a normal subgroup of* $\theta(F)$. *In this situation* $Gal_F(E) \cong Gal_F(K)/Gal_E(K)$.

(clip here)..

Galois cheet sheet

Types of Field Extensions	
finite dimensional	has a finite basis as a vector space
algebraic	every element is a root of a polynomial
finitely generated	the smallest extension containing finitely many additional elements
simple	finitely generated by one element
splitting field	the smallest extension in which a particular nonconstant polynomial splits
separable	algebraic and no minimal polynomial of an element has repeated roots
normal	every irreducible polynomial that has a root splits
Galois	finite dimensional, normal, and separable

Implications
simple $\Rightarrow$ finitely generated
finite dimensional $\Leftrightarrow$ algebraic & finitely generated
separable $\Rightarrow$ algebraic
algebraic & characteristic 0 $\Rightarrow$ separable
finitely generated & separable $\Rightarrow$ simple
splitting field $\Rightarrow$ finitely generated & algebraic & finite dimensional
splitting field $\Leftrightarrow$ finite dimensional & normal
Galois $\Rightarrow$ finite dim, normal, separable, algebraic, finitely gen, simple

(clip here)..