

# Algebra Study Guide

Kamala Hunt Diefenthaler

December 11, 2008

## Contents

<b>1</b>	<b>Notes pg 1- 56</b>	<b>4</b>
1.1	Group . . . . .	4
1.2	Group of Units . . . . .	4
1.3	Subgroup . . . . .	4
1.4	Cyclic . . . . .	4
1.5	Cosets . . . . .	4
1.6	Index . . . . .	4
1.7	Normal Subgroup . . . . .	4
1.8	Group Homomorphism . . . . .	4
1.9	Natural Projection Map . . . . .	4
1.10	1st Isomorphism Theorem for Groups . . . . .	4
1.11	2nd Isomorphism Theorem for Groups . . . . .	4
1.12	3rd Isomorphism Theorem for Groups . . . . .	4
1.13	Correspondence Theorem for Groups . . . . .	4
1.14	$D_n$ . . . . .	4
<b>2</b>	<b>Notes pg 57 - 78</b>	<b>4</b>
2.1	G-space (action on G) . . . . .	4
2.2	g equivalence . . . . .	4
2.3	Orbit . . . . .	4
2.4	G-morphism or G-map . . . . .	4
2.5	Stabilizer of $\omega_0$ (isotropy) . . . . .	4
2.6	Conjugate . . . . .	4
2.7	Transitive . . . . .	4
2.8	Homogeneous Space ??? . . . . .	4
2.9	Normalizer of $x$ in $G$ . . . . .	4
2.10	Center . . . . .	4
2.11	Conjugacy Class . . . . .	4
2.12	Class Equation . . . . .	4
2.13	Simple . . . . .	4
2.14	Normalizer of A in G . . . . .	4
<b>3</b>	<b>Notes pg 78 - 100</b>	<b>4</b>
3.1	p-group . . . . .	4
3.2	Cauchy Theorem . . . . .	4
3.3	p-Sylow Subgroups . . . . .	4
3.4	1st Sylow Theorem . . . . .	4
3.5	2nd Sylow Theorem . . . . .	4
3.6	3rd Sylow Theorem . . . . .	4
3.7	Characteristic Subgroup . . . . .	4

<b>4</b>	<b>Notes pg 100 - 113</b>	<b>4</b>
4.1	Alternating Group . . . . .	5
4.2	Even and Odd Permutations . . . . .	5
4.3	k-transitive . . . . .	5
4.4	Invariant under $\beta$ . . . . .	5
4.5	Derived Group . . . . .	5
4.6	Derived Subgroups . . . . .	5
4.7	Solvable Group . . . . .	5
4.8	Central Series . . . . .	6
4.9	Nilpotent Group . . . . .	6
<b>5</b>	<b>Notes pg 114 - 121</b>	<b>6</b>
5.1	Words and Reduced Words . . . . .	6
5.2	Free Group . . . . .	6
5.3	Universal Mapping Property . . . . .	6
<b>6</b>	<b>Notes pg 122 - 128</b>	<b>6</b>
6.1	Ring . . . . .	6
6.2	Ideals . . . . .	7
6.3	Ring Homomorphism . . . . .	7
6.4	Subring . . . . .	7
6.5	Unit (Invertible) Element . . . . .	7
6.6	1st Isomorphism Theorem for Rings . . . . .	8
6.7	2nd Isomorphism Theorem for Rings . . . . .	8
6.8	3rd Isomorphism Theorem for Rings . . . . .	8
6.9	Correspondence Theorem for Rings . . . . .	8
6.10	Unit Ideal . . . . .	8
6.11	Proper Ideal . . . . .	8
6.12	Division Ring and Field . . . . .	8
6.13	Nilpotent Element . . . . .	8
6.14	Null-Radical . . . . .	9
<b>7</b>	<b>Notes pg 129-138</b>	<b>9</b>
7.1	Zero Divisor . . . . .	9
7.2	Integral Domain . . . . .	9
7.3	Cancellation Law . . . . .	9
7.4	Prime Ideal . . . . .	9
7.5	Euclidean Domain . . . . .	9
7.6	Irreducible . . . . .	10
7.7	Associates . . . . .	10
7.8	Principle Ideal . . . . .	10
7.9	Multiplicative Subset . . . . .	10
7.10	Field of Quotients $\mathbb{Q}(R) := S^{-1}R$ . . . . .	11
<b>8</b>	<b>Notes pg 139-148</b>	<b>11</b>
8.1	Partial Ordered Set (Poset) . . . . .	11
8.2	Chain . . . . .	11
8.3	Upper Bound . . . . .	11
8.4	Maximal Element . . . . .	11
8.5	Zorn's Lemma . . . . .	11
8.6	Maximal Ideal . . . . .	12
8.7	Polynomials in x over R ( $R[x]$ ) . . . . .	12
8.8	Evaluation Map . . . . .	12
8.9	Factor into Irreducibles . . . . .	12

<b>9</b>	<b>Notes pg 149-170</b>	<b>12</b>
9.1	Unique Factorization Domain (UFD)	12
9.2	Ascending Chain Condition (ACC)	12
9.3	Greatest Common Divisor	13
9.4	Primitive	13
9.5	Gauss' Lemma	13
9.6	Content of $f(x)$	13
9.7	Reduction of $f(x)$ modulo $I$	13
9.8	Eisenstein's Irreducibility Criterion	14
<b>10</b>	<b>Notes pg 171-185</b>	<b>14</b>
10.1	Chinese Remainder Theorem	14
10.2	Characteristic	15
10.3	Prime Field	15
10.4	Extension Field	15
10.5	Degree (Index) of $\mathbb{K}$ over $\mathbb{F}$	15
10.6	Algebraic	15
10.7	Transcendental	15
10.8	Minimal Polynomial of $\alpha$ over $\mathbb{F}$	15
10.9	Splitting Field	16
10.10	Algebraically Closed	16
10.11	Algebraic Closures	16
10.12	Degree of $\alpha$ over $\mathbb{F}$	16
<b>11</b>	<b>Notes pg 188- 200</b>	<b>17</b>
11.1	R-module	17
11.2	Submodule	17
11.3	Homomorphism of R modules (or Linear Map)	17
11.4	1st Isomorphism Theorem for Modules	17
11.5	2nd Isomorphism Theorem for Modules	17
11.6	3rd Isomorphism Theorem for Modules	17
11.7	Correspondence Theorem for Modules	18
11.8	Simple R module	18
11.9	Schur's Lemma	18
11.10	Annihilator	18
11.11	Primary Decomposition	18
11.12	Similar Linear Maps	18
11.13	Finitely Generated Module	19
11.14	Noetherian Ring	19
11.15	Hilbert Basis Theorem	19
<b>12</b>	<b>Notes pg 200 - 218</b>	<b>19</b>
12.1	Presentation Matrix of a module	19
12.2	Companion Matrix	19
12.3	Invariant Factors	19
12.4	Elementary Divisors	19
12.5	Rational Canonical Form	19
12.6	Jordan Block	19
12.7	Jordan Canonical Form	19

## 1 Notes pg 1- 56

- 1.1 Group
- 1.2 Group of Units
- 1.3 Subgroup
- 1.4 Cyclic
- 1.5 Cosets
- 1.6 Index
- 1.7 Normal Subgroup
- 1.8 Group Homomorphism
- 1.9 Natural Projection Map
- 1.10 1st Isomorphism Theorem for Groups
- 1.11 2nd Isomorphism Theorem for Groups
- 1.12 3rd Isomorphism Theorem for Groups
- 1.13 Correspondence Theorem for Groups
- 1.14  $D_n$

## 2 Notes pg 57 - 78

- 2.1 G-space (action on G)
- 2.2  $G$  equivalence
- 2.3 Orbit
- 2.4 G-morphism or G-map
- 2.5 Stabilizer of  $\omega_0$  (isotropy)
- 2.6 Conjugate
- 2.7 Transitive
- 2.8 Homogeneous Space ???
- 2.9 Normalizer of  $x$  in  $G$
- 2.10 Center
- 2.11 Conjugacy Class
- 2.12 Class Equation
- 2.13 Simple
- 2.14 Normalizer of A in G

## 3 Notes pg 78 - 100

- 3.1 p-group
- 3.2 Cauchy Theorem
- 3.3 p-Sylow Subgroups

Prop: Any element of  $S_n$  can be expressed as a product of transpositions

Prop: The function  $\text{sgn}: S_n \rightarrow \{-1, 1\}$  is a group homomorphism

## 4.1 Alternating Group

Alternating Group  $A_n$  is the  $\text{Ker}(\text{sgn})$ .

Prop: Let  $\sigma \in S_n$  and suppose  $\sigma = \tau_1 \dots \tau_n = s_1 \dots s_m$ . Then  $m \equiv n \pmod{2}$ . (i.e. either both even or both odd)

## 4.2 Even and Odd Permutations

Even if it can be factored into an even number of transpositions; otherwise it is odd. A permutation is even if and only if it is contained in  $A_n$ .

Prop: A  $k$ -cycle is even if and only if  $k$  is odd

$$|A_n| = \frac{|S_n|}{2} = \frac{n!}{2}$$

Prop:  $A_5$  is simple

## 4.3 $k$ -transitive

Let  $G$  act on a set  $\Omega$ . Then  $G$  is  $k$ -transitive on  $\Omega$  if and only if for any 2  $k$ -tuples  $(x_1, \dots, x_k), (y_1, \dots, y_k)$  of distinct elements there is  $\sigma \in G$  with  $\sigma(x_i) = y_i$ .

## 4.4 Invariant under $\beta$

If  $x \in \Omega^\alpha$ , then  $\beta(x) \in \Omega^\alpha$ .

Lemma: Let the group  $G$  be 2-transitive on  $\Omega$  with  $|\Omega| \leq 3$ . Then  $G$  is generated by the subgroups  $G_x = \{a \in G : a(x) = x\}$  for  $x \in \Omega$ .

Theorem:  $A_n$  is simple for  $n \geq 5$ .

Prop: Any simple group of order 60 is isomorphic to  $A_5$ .

## 4.5 Derived Group

Let  $G$  be a group. Then the derived group is  $G' = \langle xyx^{-1}y^{-1} : x, y \in G \rangle$ . (i.e. the subgroup generated by the commutators  $xyx^{-1}y^{-1}$ .)

Prop: The derived group  $G'$  is a characteristic subgroup of  $G$ .

## 4.6 Derived Subgroups

The derived subgroups  $G^{(k)}$  of  $G$  are defined recursively by  $G^{(1)} = G'$  and  $G^{(k+1)} = (G^{(k)})'$ .

Prop: Each  $G^{(k)}$  is a characteristic subgroup of  $G$ .

## 4.7 Solvable Group

The group  $G$  is solvable if and only if  $G^{(n)} = \langle 1 \rangle$  for some  $n$ .

Alternative Definition:  $G$  is solvable if and only if there is a sequence of normal subgroups,  $N_1 = G > N_2 > N_3 > \dots > N_k = \langle 1 \rangle$ , with each  $N_i/N_{i+1}$  is abelian and  $N_i \trianglelefteq G$  for  $i = 1, \dots, k$ .

Prop:  $A_4$  is solvable.

Prop: If  $G$  is a simple group and non abelian, then  $G$  is not solvable.

## 4.8 Central Series

Define central series as follows.

$$Z_0(G) = \langle 1 \rangle$$

$$Z_1(G) = Z(G) \text{ the center of } G$$

$$Z_{k+1}(G) = \pi_k^{-1}[Z(G/Z_k(G))], \text{ where } \pi_k : G \rightarrow G/Z_k(G) \text{ is the natural projection.}$$

Prop: Each  $Z_i$  in the central series is a normal subgroup of  $G$ .

## 4.9 Nilpotent Group

A group  $G$  is nilpotent if and only if  $Z_l(G) = G$  for some  $l$ .

Prop:  $Z_{k+1}(G)/Z_k(G)$  is abelian for all  $k$ .

Prop:  $G$  nilpotent  $\Rightarrow G$  solvable.

Note that  $A_4$  is solvable, but is not nilpotent.

## 5 Notes pg 114 - 121

### 5.1 Words and Reduced Words

??

### 5.2 Free Group

??

### 5.3 Universal Mapping Property

??

## 6 Notes pg 122 - 128

### 6.1 Ring

A ring is a set  $R$  with 2 operations  $+$ ,  $\cdot$  such that for all  $x, y, z \in R$

- Associative:  $(x + y) + z = x + (y + z)$ ,  $(xy)z = x(yz)$
- Distributive:  $x(y + z) = xy + xz$ ,  $(y + z)x = yx + zx$
- Addition Commutes:  $x + y = y + x$
- Identities: There exist  $0, 1 \in R$  such that  $x + 0 = x$ ,  $1x = x1 = x$ , and  $0 \neq 1$

If  $xy = yx$  for all  $x, y \in R$ , then  $R$  is called commutative.

## 6.2 Ideals

Let  $R$  be a ring. Let  $I \subseteq R$  be closed under addition (i.e.  $x, y \in R \Rightarrow x + y \in R$ ). Then

- (a)  $I$  is a left ideal if and only if  $x \in I, r \in R \Rightarrow rx \in I$
- (b)  $I$  is a right ideal if and only if  $x \in I, r \in R \Rightarrow xr \in I$
- (c)  $I$  is a ideal if and only if  $I$  is both a left and a right ideal.

## 6.3 Ring Homomorphism

A map  $\phi : R_1 \rightarrow R_2$  between rings is a homomorphism if and only if

- $\phi(x + y) = \phi(x) + \phi(y)$
- $\phi(xy) = \phi(x)\phi(y)$
- $\phi(1_{R_1}) = 1_{R_2}$

In some settings  $\phi(1_{R_1}) = 1_{R_2}$  is dropped.

Prop: If  $\phi : R_1 \rightarrow R_2$  is a homomorphism of rings, then  $\ker(\phi) := \{x \in R_1 : \phi(x) = 0\}$  is an ideal of  $R_1$ . (This does not require that  $\phi(1_{R_1}) = 1_{R_2}$ )

Prop: If  $R$  is a ring and  $I$  is an ideal, then  $R/I := \{a + I : a \in R\}$  is a ring with operations

- $(a + I) + (b + I) = (a + b) + I$
- $(a + I)(b + I) = (ab) + I$
- $0 + I$  is the zero element
- $1 + I$  is the unity element

Remark: If  $I$  is an ideal in a ring, then we can define for  $x, y \in I$

- $x \equiv y \pmod I$  if and only if  $x - y \in I$ .

So if  $x \equiv y \pmod I$  and  $a \equiv b \pmod I$ , then

- $x + a \equiv y + b \pmod I$
- $xa \equiv yb \pmod I$

## 6.4 Subring

$S$  a non-empty subset of  $R$  is a subring if and only if

- $1 \in S$
- Closed Under Addition ( $x, y \in S \Rightarrow x + y \in S$ )
- Closed Under Multiplication ( $x, y \in S \Rightarrow xy \in S$ )
- Closed Under Additive Inverses ( $x \in S \Rightarrow -x \in S$ )

## 6.5 Unit (Invertible) Element

Let  $R$  be a ring. Then  $u \in R$  is a unit if and only if there exists a  $v \in R$  such that  $uv = vu = 1$ .

Prop: If  $R$  is a ring and  $\mathcal{U}(R)$  is the set of units in  $R$ , then  $\mathcal{U}(R)$  is a group under multiplication.

## 6.6 1st Isomorphism Theorem for Rings

Let  $R$  and  $S$  be rings. If  $\phi : R \rightarrow S$  is a ring homomorphism, then  $\ker(\phi)$  is an ideal of  $R$ ,  $\text{Im}(\phi)$  is a subring of  $S$ , and  $R/\ker(\phi) \cong \text{Im}(\phi)$ .

## 6.7 2nd Isomorphism Theorem for Rings

Let  $R$  be a ring, let  $S$  be a subring, and let  $I$  be an ideal of  $R$ . Then  $S + I = \{s + i : s \in S, i \in I\}$  is a subring of  $R$ ,  $I$  is ideal in  $S + I$ ,  $S \cap I$  is an ideal of  $S$  and

$$\frac{S + I}{I} \cong \frac{S}{S \cap I}$$

## 6.8 3rd Isomorphism Theorem for Rings

Let  $R$  be a ring, and let  $I$  and  $J$  be ideals of  $R$  with  $I \subseteq J$ . Then  $J/I$  is an ideal of  $R/I$  and

$$\frac{R/I}{J/I} \cong R/J$$

## 6.9 Correspondence Theorem for Rings

Let  $f : R \rightarrow S$  be a surjective ring homomorphism with  $\ker(f)$  an ideal of  $R$ .  $f$  defines a one-one correspondence (bijection) between the ideals of  $R$  which contain  $\ker(f)$  and the ideals of  $S$ .

Prop: Let  $R$  be a commutative ring. Then any ideal of  $M_{n \times n}(R)$  is of the form  $M_{n \times n}(I)$  where  $I$  is an ideal in  $R$ .

## 6.10 Unit Ideal

The unit ideal of a ring  $R$  is  $I = R$ . Note that  $I$  is the ideal generated by 1.

## 6.11 Proper Ideal

An ideal  $I$  of  $R$  is proper if and only if  $I \neq (0)$  and  $I \neq R$ .

## 6.12 Division Ring and Field

A ring  $R$  is a division ring if and only if every non-zero element of  $R$  has a 2-sided inverse. A commutative division ring is a field.

Theorem: A commutative ring  $R$  is a field if and only if it has no proper ideals.

## 6.13 Nilpotent Element

An element  $a$  of a ring is nilpotent if and only if  $a^n = 0$  for some  $n \in \{1, 2, 3, \dots\}$ .

Prop: If  $a \in R$  is nilpotent, then  $1 + a$  is a unit. Furthermore, if  $R$  is commutative and  $u$  is a unit, then  $u + a$  is also a unit.

## 6.14 Null-Radical

Let  $N$  be the collection of all nilpotent elements in a commutative ring  $R$ . Then  $N$  is the null-radical of  $R$ .

Prop: Let  $R$  be a commutative ring. Let  $N$  be the null-radical of  $R$ . Then  $N$  is an ideal of  $R$  and the ring  $R/N$  has no nilpotent elements.

## 7 Notes pg 129-138

### 7.1 Zero Divisor

Let  $R$  be a commutative ring. Then  $a \in R$  is a zero divisor if and only if there exists  $b \in R$  such that  $b \neq 0$  and  $ab = 0$ .

HW: Find the zero divisors of  $\mathbb{Z}/(12)$ .

### 7.2 Integral Domain

A commutative ring  $R$  is an integral domain if and only if 0 is the only zero divisor of  $R$ . (i.e.  $ab = 0 \Rightarrow a = 0$  or  $b = 0$ )

Prop: In an integral domain *prime*  $\Rightarrow$  *irreducible*

Theorem: A finite integral domain is a field.

Theorem: A finite division ring is a field.

### 7.3 Cancellation Law

Let  $R$  be a ring and  $a, x, y \in R$ . If  $ax = ay$  and  $a \neq 0 \Rightarrow x = y$ , then the cancellation law holds.

Prop: A commutative ring  $R$  is an integral domain if and only if the cancellation law holds.

### 7.4 Prime Ideal

An ideal  $I$  in a commutative ring  $R$  is a prime ideal if and only if  $ab \in I \Rightarrow a \in I$  or  $b \in I$ . Also  $I$  is a prime ideal if and only if  $a \notin I$  and  $ab \in I \Rightarrow b \in I$ .

Theorem: Let  $R$  be a commutative ring and  $I$  an ideal in  $R$ . Then  $I$  is prime if and only if  $R/I$  is an integral domain.

Integral Domains  $\supset$  UFD  $\supset$  PID  $\supset$  Euclidean Domains  $\supset$  Fields

### 7.5 Euclidean Domain

A commutative ring  $R$  is an Euclidean Domain if and only if

- $R$  is an integral domain (i.e. has no zero divisors)
- There exists a function  $\delta : (R \setminus \{0\}) \rightarrow \{0, 1, 2, 3, \dots\}$  such that
  - (a) If  $a, n \in R$  are both non-zero then  $\delta(a) \leq \delta(ab)$ .
  - (b) The division algorithm holds (If  $a, n \in R$  and  $a \neq 0$ , then we can divide  $a$  into  $n$  such that  $a = nq + r$  where  $\delta(r) < \delta(n)$  or  $r = 0$ )

Prop: (Remainder Theorem) If  $x-a$  is divided into  $f(x)$ , then the remainder is  $r = f(a)$ .  $f(a) = 0 \Leftrightarrow (x-a)|f(x)$ .

Prop: The units in  $R := \mathbb{F}[x]$  are the non-zero constant polynomials. Also the associates of  $f(x)$  are  $cf(x)$  where  $c$  is a non-zero element of  $\mathbb{F}$ .

Theorem:  $\mathbb{Z}$  and  $\mathbb{Z}[i]$  with  $\delta(a) := |a|$  are both Euclidean domains.

Theorem: The ring of polynomials  $\mathbb{F}[x]$  over a field  $\mathbb{F}$  with  $\delta(p(x)) := \deg(p(x))$  is a Euclidean domain.

Theorem: (Axiom of Induction) Let  $N := \{0, 1, 2, 3, \dots\}$  be the natural numbers. Then any non-empty subset  $S$  of  $N$  has a smallest element.

Theorem: Let  $R$  be a Euclidean domain. Then every ideal in  $R$  is principle. Moreover, if  $I$  is a non-trivial ideal of  $R$  and  $(a) = (b) = I$ , then  $a = ub$  for some unit  $u \in R$  ( $a$  and  $b$  are associates).

Theorem: Let  $R$  be a Euclidean domain and let  $a$  and  $b$  be nonzero elements of  $R$ . Then  $a$  and  $b$  have at least one gcd. Also, if  $c$  and  $d$  are both gcd's of  $a$  and  $b$ , then  $d = cu$  for some unit  $u \in R$ . Finally, if  $c$  is any gcd of  $a$  and  $b$ , then  $\exists x, y \in R$  such that  $ax + by = c$ .

Prop: In a Euclidean domain, *prime*  $\Leftrightarrow$  *irreducible*

Corollary: If  $p$  is prime in the Euclidean domain  $R$  and  $p|a_1a_2\dots a_n$ , then  $p$  divides at least one of  $a_1, a_2, \dots, a_n$ .

Prop: Let  $R$  be a Euclidean domain. Then a nonzero element  $a \in R$  is a unit if and only if  $\delta(a) = \delta(1)$ .

Prop: Let  $R$  be a Euclidean domain and nonzero elements  $a, b \in R$ . If  $\delta(ab) = \delta(a)$ , then  $b$  is a unit.

Theorem: (Fundamental Theorem of Arithmetic) Let  $a$  be a nonzero, non-unit element in the Euclidean domain  $R$ . Then  $a$  is a product of primes ( $a = p_1p_2\dots p_n$ ). Furthermore, the product is unique up to multiplication by a unit. (i.e. If  $a = p_1p_2\dots p_n = q_1q_2\dots q_m$ , then  $m = n$  and after reordering there are units  $u_1, u_2, \dots, u_n$  so that  $q_i = u_i p_i$  for  $i = 1, \dots, n$ ).

## 7.6 Irreducible

Let  $R$  be a commutative ring. Let  $r$  be a non-zero and non-constant element of  $R$ . Then  $r$  is irreducible if and only if  $ab|r \Rightarrow$  either  $a$  or  $b$  is a unit.

## 7.7 Associates

Let  $R$  be a commutative ring. Then  $a, b \in R$  are associates if and only if there is a unit  $u \in R$  with  $a = ub$ .

## 7.8 Principle Ideal

If  $R$  is a commutative ring and  $a \in R$ , then  $(a) := \{ra : r \in R\}$  is the principle ideal generated by  $a$ .

## 7.9 Multiplicative Subset

Let  $R$  be a commutative ring. Then a subset  $S \subseteq R$  is a multiplicative subset if and only if

- $1 \in S$
- $s_1, s_2 \in S \Rightarrow s_1s_2 \in S$
- $0 \notin S$  and  $S$  contains no zero divisors.

$$(r_1, s_1) \sim (r_2, s_2) \Leftrightarrow r_1s_2 = r_2s_1$$

$\frac{r}{s} :=$  equivalence class of  $(r, s) \in R \times S$ .

$S^{-1}R$  is the set of equivalence classes.

Prop:  $S^{-1}R$  is a ring. The set  $\bar{R} = \{\frac{r}{1} : r \in R\} \subseteq S^{-1}R$  is a subring of  $S^{-1}R$  isomorphic to  $R$ .

Prop:  $S \subseteq R \subseteq S^{-1}R$ . Each element of  $S$  has an inverse in  $S^{-1}R$ . So we have added to  $R$  the inverses of  $S$ .

## 7.10 Field of Quotients $\mathbb{Q}(R) := S^{-1}R$

Let  $R$  be an integral domain. Then  $S := R \setminus \{0\}$  is a multiplicative subset of  $R$  and  $\mathbb{Q}(R) := S^{-1}R$  is the field of quotients of  $R$  that has  $R$  as a subring.

Prop: Let  $R$  be an integral domain and  $\mathbb{Q}(R)$  the field of quotients of  $R$ . Let  $\mathbb{F}$  be a field and  $\phi : R \rightarrow \mathbb{F}$  an injective homomorphism. Then  $\phi$  extends to an injective homomorphism  $\bar{\phi} : \mathbb{Q}(R) \rightarrow \mathbb{F}$ .

## 8 Notes pg 139-148

### 8.1 Partial Ordered Set (Poset)

A partial ordered set is a pair  $(P, \leq)$  where  $P$  is a set and  $\leq$  is a binary operation on  $P$  such that for  $x, y, z \in P$

- $x \leq x$
- $x \leq y$  and  $y \leq x \Rightarrow x = y$
- $x \leq y$  and  $y \leq z \Rightarrow x \leq z$ .

Remark: It is not assured that elements are necessarily comparable. There may be elements  $x$  and  $y$  such that neither  $x \leq y$  nor  $y \leq x$  holds.

### 8.2 Chain

If  $(P, \leq)$  is a partial ordered set then  $\mathcal{C} \subseteq P$  is a chain if and only if for all  $x, y \in \mathcal{C}$  either  $x \leq y$  or  $y \leq x$ . (i.e. any 2 elements of  $\mathcal{C}$  are comparable)

Prop: Let  $R$  be a ring and  $\mathcal{C}$  a chain of ideals in  $R$ . Then  $\bigcup \mathcal{C} = \bigcup_{I \in \mathcal{C}} I$  is an ideal in  $R$ . (The union of a chain of ideals is an ideal)

Note that not all unions of ideals are ideals.

### 8.3 Upper Bound

If  $(P, \leq)$  is a partial ordered set and  $S \subseteq P$ , then  $x \in P$  is an upper bound for  $S$  if and only if  $s \leq x$  for all  $s \in S$ .

### 8.4 Maximal Element

If  $(P, \leq)$  is a partial ordered set, then  $x \in P$  is a maximal element of  $P$  if and only if  $x \leq y \Rightarrow y = x$ .

A poset can have many maximal elements.

### 8.5 Zorn's Lemma

Let  $(P, \leq)$  be a partial ordered set where every chain has an upper bound. Then  $(P, \leq)$  has a maximal element.

## 8.6 Maximal Ideal

Let  $R$  be a commutative ring. Then an ideal  $I$  of  $R$  is a maximal ideal if and only if  $I$  is a proper ideal of  $R$  and if  $J$  is any proper ideal of  $R$  with  $I \subseteq J$ , then  $I = J$ . (i.e. all ideals  $J$  of  $R$  with  $I \subseteq J$ , either  $I = J$  or  $J = R$ ).

Theorem: Let  $R$  be a commutative ring. Then any proper ideal is contained in a maximal ideal of  $R$ .

Corollary: Every nonzero ring has a maximal ideal.

Theorem: Let  $R$  be a commutative ring and  $S \subseteq R$  a subset such that  $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$ . Let  $I$  be an ideal of  $R$  such that  $I \cap S = \emptyset$ . Then there is a prime ideal  $P$  of  $R$  with  $I \subseteq P$  and  $P \cap S = \emptyset$

Theorem: Let  $R$  be a commutative ring. Let  $N$  be the null radical of  $R$ . Then  $N = \bigcap \{P : P \text{ is a prime ideal of } R\}$ .

## 8.7 Polynomials in $x$ over $R$ ( $R[x]$ )

Let  $R$  be a commutative ring and  $x$  is a variable. Then  $R[x]$  is the ring for polynomials over  $R$ .  $R[x] = a_0 + \dots + a_n x^n : n \geq 0, a_0, \dots, a_n \in R$ .

## 8.8 Evaluation Map

Let  $a_1, \dots, a_n \in R$ . Then there is a unique homomorphism  $\varepsilon : R[x_1, \dots, x_n] \rightarrow R$  such that  $\varepsilon(x_i) = a_i$ . This is the evaluation map.

## 8.9 Factor into Irreducibles

Let  $R$  be a ring. Then we say that elements of  $R$  factor into irreducibles if and only if the process of factoring  $a \in R$  stops after a finite number of steps with  $a = b_1 b_2 \dots b_n$  with each  $b_j$  irreducible.

# 9 Notes pg 149-170

## 9.1 Unique Factorization Domain (UFD)

A commutative ring  $R$  is a unique factorization domain if and only if

- Every element of  $R$  factors into a finite number of irreducibles.
- Factorization into irreducibles is unique in the sense that if  $a = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$  are factorizations into irreducibles, then  $n = m$  and after reordering  $p_i$  and  $q_i$  are associates for  $i = 1, \dots, n$ .

Theorem: Any Euclidean Domain is a UFD.

Prop: In a UFD *prime*  $\Leftrightarrow$  *irreducible*

## 9.2 Ascending Chain Condition (ACC)

A ring  $R$  satisfies the ascending chain condition on principal ideals if and only if any chain of principle ideals  $(a_1) \subseteq (a_2) \subseteq \dots$  eventually stabilizes. (i.e. There is an  $n$  such that  $(a_n) = (a_{n+1})$ )

Prop: Let  $R$  be an integral domain. Then every element of  $R$  factors into irreducibles if and only if there is no infinite increasing sequence of principle ideals  $(a_1)$  (i.e. ACC holds for principle ideals).

Prop: Let  $R$  be an integral domain, where elements factor into irreducibles. Then  $R$  is a UFD if and only if each irreducible is prime.

### 9.3 Greatest Common Divisor

If  $R$  is a commutative ring and  $a, b \in R$ , then  $d$  is a gcd of  $a$  and  $b$  if and only if  $d \mid a$  and  $d \mid b$  and if  $c$  is common divisor of  $a$  and  $b$ , then  $c \mid d$ .

Prop: If  $R$  is a UFD, then any 2 elements  $a, b \in R$  have a gcd  $d$ . If  $d_1$  and  $d_2$  are both gcd( $a, b$ )'s, then  $d_1$  and  $d_2$  are associates.

Prop: If  $D$  is a an integral domain, then  $D[x]$  is also an integral domain.

### 9.4 Primitive

Let  $R$  be a UFD. Then  $f(x) \in R[x]$  is primitive if and only if  $\gcd(a_0, a_1, \dots, a_n) = 1$  where  $f(x) = a_n x^n + \dots + a_0$ . (i.e. The gcd of the coefficients of  $f$  is 1.)

### 9.5 Gauss' Lemma

If  $f(x), g(x) \in R[x]$  are both primitive, then the product  $f(x)g(x)$  is also primitive.

### 9.6 Content of $f(x)$

Let  $R$  be a UFD and  $\mathbb{F}$  the field of quotients of  $R$ . Then for  $f(x) \in \mathbb{F}[x]$ , and if  $f(x) = cf_0(x)$  where  $f_0(x) \in R[x]$  is primitive and  $c \in \mathbb{F}[x]$ , then  $c$  is the content of  $f(x)$ .

Content is not quite well-defined. It is defined up to multiplication by units of  $R$ .

Prop: If  $f(x), g(x) \in \mathbb{F}[x]$ , then  $\text{content}(f(x)g(x)) = \text{content}(f(x))\text{content}(g(x))$ .

Prop: Let  $R$  be a UFD and  $\mathbb{F}$  the field of quotients of  $R$ . Also let  $f(x), g(x) \in R[x]$  be primitive. Assume  $f(x) \mid g(x)$  in  $\mathbb{F}[x]$ . Then  $f(x) \mid g(x)$  in  $R[x]$ .

Prop: Let  $R$  be a UFD and  $\mathbb{F}$  its quotient field. Let  $f(x) \in R[x]$  be primitive. Then  $f(x)$  is irreducible in  $R[x]$  if and only if it is irreducible in  $\mathbb{F}[x]$ . Logic Question pg 160 in Notes

Theorem: If  $R$  is a UFD, then so is  $R[x]$ . The primes of  $R[x]$  are the primes of  $R$  (view as constants) and the irreducible primitive polynomials in  $R[x]$ .

Prop: If  $\mathbb{F}$  is a field, then  $\mathbb{F}[x], \mathbb{F}[x_1, x_2], \dots, \mathbb{F}[x_1, \dots, x_n]$  are UFD's.

Corollary: If  $R$  is a UFD then  $R[x_1, \dots, x_n]$  is also a UFD.

Prop: Let  $a, b \in \mathbb{F}$  a field and  $a \neq 0$ . Then a polynomial  $f(x) \in \mathbb{F}[x]$  is irreducible if and only if  $f(ax + b)$  is irreducible.

Prop: Let  $f, g \in \mathbb{C}[x, y]$ . Then if  $f$  and  $g$  have a common factor in  $\mathbb{C}(x)[y]$ , then they also have a common factor in  $\mathbb{C}[x, y]$ .

Prop: Let  $f(x), g(x) \in \mathbb{Z}[x]$ . Then  $f(x)$  and  $g(x)$  are relatively prime in  $\mathbb{Q}[x]$  if and only if the ideal generated by  $f(x)$  and  $g(x)$  in  $\mathbb{Z}[x]$  contains an integer.

Prop: Let  $\phi : R \rightarrow \bar{R}$  be a homomorphism of commutative rings. Then  $\phi$  induces a homomorphism  $\bar{\phi} : R[x] \rightarrow \bar{R}[x]$  given by  $\bar{\phi}(a_n x^n + \dots + a_0) = \phi(a_n) x^n + \dots + \phi(a_0)$ .

### 9.7 Reduction of $f(x)$ modulo $I$

$\bar{R} = R/I$  for ideal  $I$  in  $R$ . Then  $\bar{a}$  is the image of  $a$  in  $R/I$  under the natural projection. If  $f(x) = a_n x^n + \dots + a_0$  we call  $\bar{f}(x) = \bar{a}_n x^n + \dots + \bar{a}_0$  the reduction of  $f(x)$  modulo  $I$ .

Note that  $\overline{f(x) + g(x)} = \bar{f}(x) + \bar{g}(x)$  and  $\overline{f(x)g(x)} = \bar{f}(x)\bar{g}(x)$ .

Prop: Let  $R$  be a UFD and  $f(x) = a_n x^n + \dots + a_0 \in R[x]$  be primitive with  $n \geq 1$ . Let  $P$  be a prime ideal. If  $\bar{R} = R/P$  and  $\bar{f}(x)$  is irreducible in  $\bar{R}[x]$  and  $a_n \notin P$ , then  $f(x)$  is irreducible in  $R[x]$ .

Prop: Let  $\mathbb{F}$  be a field. If  $f(x) \in \mathbb{F}[x]$  and  $\deg(f(x)) = 2$  or  $\deg(f(x)) = 3$ , then  $f(x)$  is irreducible in  $\mathbb{F}[x]$  if and only if  $f(x)$  has no root in  $\mathbb{F}[x]$ .

## 9.8 Eisenstein's Irreducibility Criterion

Let  $R$  be a UFD,  $p$  a prime of  $R$  and  $f(x) = a_n x^n + \dots + a_0 \in R[x]$  be primitive such that

- $p \nmid a_n$
- $p \mid a_j \quad n-1 \geq j \geq 0$
- $p^2 \nmid a_0$ .

Then  $f(x)$  is irreducible in  $R[x]$ .

## 10 Notes pg 171-185

Let  $R$  be a commutative ring, and  $I, J$  ideals in  $R$ . Then  $I + J$  and  $IJ$  as defined below are ideals.

- $I + J = \{i + j : i \in I, j \in J\}$
- $IJ = \text{Set of all finite sums of the form } \sum_{\alpha} i_{\alpha} j_{\alpha} \text{ with } i_{\alpha} \in I \text{ and } j_{\alpha} \in J.$
- $I \cap J = \{x : x \in I \text{ and } x \in J\}$

Prop: Let  $R$  be a PID and  $I = (a), J = (b)$  be ideals in  $R$ . Then

- $I + J = (\gcd(a, b))$     gcd of the ideals  $I$  and  $J$
- $IJ = (ab)$     product of  $I$  and  $J$
- $I \cap J = (\text{lcm}(a, b))$     lcm of  $I$  and  $J$

Think of  $I + J = R$  as meaning the ideals  $I$  and  $J$  are relatively prime.

If  $a \in R$ , then the ideal generated by  $a$  and  $I$  is  $(a, I) = \{ar + i : r \in R, i \in I\}$ .

Prop: If  $I, J$  are ideals in the commutative ring  $R$ , then  $IJ \subseteq I \cap J$ .

Prop: Let  $I, J$  be ideals in the commutative ring  $R$ , with  $I + J = R$ . Then  $IJ = I \cap J$ .

Prop: Let  $I_1, \dots, I_n$  be ideals in the commutative ring  $R$ . Then their product is an ideal in  $R$ .  
 $I_1 I_2 \cdots I_n = \text{Set of all finite sums, } \sum_{\alpha} i_{1\alpha} i_{2\alpha} \cdots i_{n\alpha} \text{ with } i_{k\alpha} \in I_k.$

Lemma: Let  $J, I_1, \dots, I_n$  be ideals in the commutative ring  $R$  and  $J + I_i = R$  for  $i = 1, 2, \dots, n$ .  
 Then  $J + I_1 I_2 I_3 \cdots I_n = R$ .

## 10.1 Chinese Remainder Theorem

Let  $R$  be a commutative ring and  $I_1, \dots, I_n$  ideals of  $R$  such that  $I_i + I_j = R$  for  $i \neq j$ .  
 Then  $R/(I_1 \cap \cdots \cap I_n) \cong (R/I_1) \oplus \cdots \oplus (R/I_n)$ .

Prop: Let  $n_1, \dots, n_m \in \mathbb{Z}$  be positive integers with  $\gcd(n_i, n_j) = 1$  for  $i \neq j$ . And let  $a_1, \dots, a_m \in \mathbb{Z}$ . Then there is a solution to the system of congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_m \pmod{n_m} \end{aligned}$$

## 10.2 Characteristic

Let  $R$  be a ring. For  $n \in \mathbb{Z}$  and  $n \geq 1$ , the characteristic of  $R$  (i.e.  $\text{char}(R) = \min\{n : n = 0 \text{ in } R\}$ ). If  $n \neq 0$  for all  $n \geq 1$ , then  $\text{char}(R) = 0$ .

Prop: If  $R$  is an integral domain, then either  $\text{char}(R) = 0$  or  $\text{char}(R) = p$ , where  $p$  is prime.

Prop: Let  $R$  be an integral domain. If  $\text{char}(R) = 0$ , then  $R$  contains a subring isomorphic to  $\mathbb{Z}$ . And if  $\text{char}(R) = p$ , then  $R$  contains a subring isomorphic to  $\mathbb{Z}/(p)$ .

Prop: Let  $\mathbb{F}$  be a field. If  $\text{char}(\mathbb{F}) = 0$ , then  $\mathbb{F}$  contains a subfield isomorphic to  $\mathbb{Q}$ .

## 10.3 Prime Field

Let  $\mathbb{F}$  be a field. The prime field of  $\mathbb{F}$  is

- $\mathbb{Q}$  if  $\text{char}(\mathbb{F}) = 0$ .
- $\mathbb{Z}/(p)$  if  $\text{char}(\mathbb{F}) = p$ .

The prime field is the smallest subfield of  $\mathbb{F}$ .

## 10.4 Extension Field

If  $\mathbb{F}$  is a subfield of  $\mathbb{K}$ , then  $\mathbb{K}$  is an extension field of  $\mathbb{F}$ .

## 10.5 Degree (Index) of $\mathbb{K}$ over $\mathbb{F}$

If  $\mathbb{F}$  is a subfield of  $\mathbb{K}$ , then the degree of  $\mathbb{K}$  over  $\mathbb{F}$  is  $[\mathbb{K} : \mathbb{F}] = \dim_{\mathbb{F}} \mathbb{K}$ .

Prop: If  $\mathbb{F}$  is a subfield of  $\mathbb{K}$ ,  $\mathbb{K}$  is a subfield of  $\mathbb{L}$ , and  $[\mathbb{K} : \mathbb{F}] < \infty$ ,  $[\mathbb{L} : \mathbb{K}] < \infty$ . Then  $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}] < \infty$ .

Prop: If  $R$  is a PID and  $p \in R$  is prime, the  $(p)$  is a maximal ideal of  $R$  and thus  $R/(p)$  is a field.

Prop: Let  $\mathbb{F}$  be a field and  $f(x) \in \mathbb{F}[x]$  an irreducible polynomial. Then  $\mathbb{F}$  has an extension field  $\mathbb{K}$  such that  $[\mathbb{K} : \mathbb{F}] = \deg(f(x))$ . Also, there is an element  $\alpha \in \mathbb{K}$  with  $f(\alpha) = 0$  (i.e.  $\alpha$  is a root of  $f(x)$  in  $\mathbb{K}$ ), and  $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$  is a basis of  $\mathbb{K}$  as a vector space over  $\mathbb{F}$ .

Similar Prop: Let  $\mathbb{F}$  be a field and  $f(x) \in \mathbb{F}[x]$  a non-constant polynomial. Then  $\mathbb{F}$  has an extension field  $\mathbb{K}$  such that  $[\mathbb{K} : \mathbb{F}] \leq \deg(f(x))$ . Also,  $f(x)$  has a root in  $\mathbb{K}$ .

## 10.6 Algebraic

Let  $\mathbb{F}$  be a subfield of  $\mathbb{K}$ . Then an element  $\alpha \in \mathbb{K}$  is algebraic over  $\mathbb{F}$  if and only if there is a non-constant polynomial  $f(x) \in \mathbb{F}[x]$  such that  $f(\alpha) = 0$ .

(i.e.  $\alpha \in \mathbb{K}$  is algebraic over  $\mathbb{F}$  if and only if  $\alpha$  is a root of some polynomial with coefficients in  $\mathbb{F}$ ).

The field  $\mathbb{K}$  is algebraic over  $\mathbb{F}$  if and only if every element of  $\mathbb{K}$  is algebraic over  $\mathbb{F}$ .

## 10.7 Transcendental

If  $\alpha \in \mathbb{K}$  is not algebraic over  $\mathbb{F}$ , then  $\alpha$  is transcendental over  $\mathbb{F}$ .

## 10.8 Minimal Polynomial of $\alpha$ over $\mathbb{F}$

Let  $\mathbb{F}$  be a subfield of  $\mathbb{K}$  and let  $\alpha \in \mathbb{K}$  be algebraic over  $\mathbb{F}$ . Then the minimal polynomial of  $\alpha$  over  $\mathbb{F}$  ( $\min_{\alpha}(x)$ ) is  $f(x) \in \mathbb{F}[x]$ . Where

- $f(x)$  is a unique monic polynomial of minimal degree

- $f(\alpha) = 0$
- If  $g(x) \in \mathbb{F}[x]$  with  $g(\alpha) = 0$ , then  $f(x)|g(x)$ .

Prop: Let  $\mathbb{F}$  be a subfield of  $\mathbb{K}$  and let  $\alpha \in \mathbb{K}$  be algebraic over  $\mathbb{F}$ . Then there is a minimal polynomial of  $\alpha$  over  $\mathbb{F}$ , and  $\mathbb{F}[\alpha] \cong \mathbb{F}[x]/(f(x))$ .

Prop: Let  $\mathbb{F}$  be a finite field. Then there is an irreducible monic quadratic polynomial  $f(x) = x^2 + ax + b$  in  $\mathbb{F}[x]$ .

Prop: Let  $\mathbb{F}$  be a finite field. Then there exists a finite field  $\mathbb{K}$  with  $|\mathbb{K}| = |\mathbb{F}|^2$ .

## 10.9 Splitting Field

Let  $\mathbb{F}$  be a field and let  $f(x) = a_0 + a_1x + \dots + a_nx^n$  be a polynomial in  $\mathbb{F}[x]$  of degree  $n > 0$ . An extension field  $\mathbb{K}$  of  $\mathbb{F}$  is called a splitting field for  $f(x)$  over  $\mathbb{F}$  if there exist elements  $r_1, r_2, \dots, r_n \in \mathbb{K}$  such that

- $f(x) = a_n(x - r_1)(x - r_2)\dots(x - r_n)$ , and
- $\mathbb{K} = \mathbb{F}(r_1, r_2, \dots, r_n)$

Prop: Let  $f(x)$  be a polynomial in  $\mathbb{F}[x]$  of degree  $n > 0$ . Then there exists a splitting field  $\mathbb{K}$  for  $f(x)$  over  $\mathbb{F}$ .

Theorem: Let  $p$  be a prime, and  $q = p^n$  for some  $n$ . Then there is a finite field  $\mathbb{F}_q$  with  $|\mathbb{F}_q| = q$ . (This is unique up to isomorphism.)

## 10.10 Algebraically Closed

The field  $\mathbb{F}$  is algebraically closed if and only if every non-constant polynomial  $f(x) \in \mathbb{F}[x]$  has a root in  $\mathbb{F}[x]$ .

Theorem: The complex number are algebraic closed.

## 10.11 Algebraic Closures

Let  $\mathbb{F}$  be a field. Then  $\mathbb{F}$  has an extension field  $\mathbb{K}$  such that

- $\mathbb{K}$  is algebraic over  $\mathbb{F}$
- $\mathbb{K}$  is algebraically closed

$\mathbb{K}$  is unique up to isomorphism fixing  $\mathbb{F}$

Prop: If  $f(x) \in \mathbb{F}[x]$  and  $\mathbb{F}[x]$  is a field, then  $f(r) = 0$  if and only if  $(x - r)|f(x)$

Prop: Let  $f(x) \in \mathbb{F}[x]$  with  $\mathbb{F}[x]$  a field. Then  $f(x)$  has at most  $n = \deg(f(x))$  roots in  $\mathbb{F}[x]$ .

Prop: Let  $\mathbb{F}$  be a finite field. Then the multiplicative group  $\mathbb{F}^* = \{a \in \mathbb{F} : a \neq 0\}$  is cyclic.

## 10.12 Degree of $\alpha$ over $\mathbb{F}$

The degree of  $\alpha$  over  $\mathbb{F}$  is the degree of the minimal polynomial of  $\alpha$  over  $\mathbb{F}$ .

Prop: Let  $\mathbb{K}$  be an extension field of  $\mathbb{F}$  and  $[\mathbb{K} : \mathbb{F}] = n < \infty$ . Then every  $\alpha \in \mathbb{K}$  is algebraic over  $\mathbb{F}$  and degree of  $\alpha$  over  $\mathbb{F}$  is less than or equal to  $n$ .

Prop: If  $[\mathbb{K} : \mathbb{F}] = n < \infty$  and  $\alpha$  is algebraic over  $\mathbb{K}$  with degree  $m$ , then  $\alpha$  is also algebraic over  $\mathbb{F}$  with degree less than or equal to  $mn$ . (i.e. algebraic over the large one  $\Rightarrow$  algebraic over the small one.)

Theorem: Let  $a, b$  be algebraic over  $\mathbb{F}$  and  $b \neq 0$ . Then  $a + b, a - b, ab$ , and  $\frac{a}{b}$  are also algebraic over  $\mathbb{F}$ .

## 11 Notes pg 188- 200

### 11.1 R-module

Let  $R$  be a commutative ring. Then  $V$  is a module over  $R$  if and only if  $V$  is an abelian group under  $+$ , and there is a multiplication of elements  $r \in R$  with  $v \in V$  such that

- $r_1(r_2v) = r_1r_2v$
- $r(v_1 + v_2) = rv_1 + rv_2$
- $(r_1 + r_2)v = r_1v + r_2v$
- $1v = v$

IMPORTANT: Let  $V$  be an abelian group. Then  $V$  is a  $\mathbb{Z}$  module with operation  $n \cdot v = v + v + \dots + v$  ( $n$  times). Thus abelian groups are just  $\mathbb{Z}$  modules.

IMPORTANT: Let  $V$  be a vector space over  $\mathbb{F}$  and  $A : V \rightarrow V$  a linear map. Then  $V$  is a  $\mathbb{F}[x]$  module with operation  $f(x) \cdot v = f(A) \cdot v$ .

### 11.2 Submodule

If  $V$  is an  $R$  module, then  $W \subseteq V$  is a submodule of  $V$  if and only if  $W \neq 0$  and  $W$  is closed under addition in  $W$  and multiplication by  $R$ . (Similar to an ideal)

### 11.3 Homomorphism of R modules (or Linear Map)

A homomorphism of  $R$  modules is a map  $\phi : V \rightarrow W$  such that

- $\phi(v_1 + v_2) = \phi(v_1) + \phi(v_2)$
- $\phi(rv) = r\phi(v)$

### 11.4 1st Isomorphism Theorem for Modules

Let  $V$  and  $W$  be  $R$  modules. If  $\phi : V \rightarrow W$  is a  $R$  module homomorphism, then  $\ker(\phi)$  is a submodule of  $V$ ,  $\text{Im}(\phi)$  is a submodule of  $W$ , and  $V/\ker(\phi) \cong \text{Im}(\phi)$ .

### 11.5 2nd Isomorphism Theorem for Modules

Let  $V$  be an  $R$  module, let  $W$  and  $U$  be submodules of  $V$ . Then  $W + U = \{w + u : w \in W, u \in U\}$  is a submodule of  $V$ ,  $U$  is a submodule of  $W + U$ ,  $W \cap U$  is a submodule of  $W$  and

$$\frac{W + U}{U} \cong \frac{W}{W \cap U}$$

.

### 11.6 3rd Isomorphism Theorem for Modules

Let  $V$  be an  $R$  module, and let  $W$  and  $U$  be submodules of  $V$  with  $U \subseteq W$ . Then  $W/U$  is a submodule of  $V/U$  and

$$\frac{V/U}{W/U} \cong V/W$$

.

## 11.7 Correspondence Theorem for Modules

Let  $N$  be a submodule of the  $R$ -module  $M$ . The map  $S \rightarrow S/N$  sets up a one-to-one correspondence between the set of all submodules of  $M$  containing  $N$  and the set of all submodules of  $M/N$ . The inverse of the map is  $T \rightarrow \pi^{-1}(T)$ , where  $\phi$  is the canonical map  $M \rightarrow M/N$ .

## 11.8 Simple $R$ module

A module  $V$  is simple if and only if the only submodules of  $V$  are  $0$  and  $V$ .

## 11.9 Schur's Lemma

Let  $\phi : V \rightarrow W$  be an  $R$  module homomorphism. Then

- If  $V$  is simple, then  $\phi$  is  $0$  or injective.
- If  $W$  is simple, then  $\phi$  is  $0$  or surjective.
- If  $V$  and  $W$  are simple and  $\phi \neq 0$ , then  $\phi$  is an isomorphism.

Prop:  $\text{Hom}_R(V, W)$  is an  $R$  module with the following operations.

- $(\phi + \psi)(v) = \phi(v) + \psi(v)$
- $(r\phi)(v) = r(\phi(v))$

## 11.10 Annihilator

Let  $V$  be a module over the commutative ring  $R$ . Let  $S \subseteq V$ , and  $S \neq 0$ . Then  $\text{Ann}(S) = \{r \in R : rs = 0 \text{ for all } s \in S\}$ .

Prop:  $\text{Ann}(S)$  is an ideal in  $R$ .

Prop: Let  $V$  be a vector space over a field  $\mathbb{F}$  and  $A : V \rightarrow V$  a linear map. Make  $V$  into a  $\mathbb{F}[x]$  module by  $f(x)v = f(A)v$ .

- Then  $W \subseteq V$  is a submodule of  $V$  if and only if  $W$  is a subspace of  $V$  invariant under  $A$  (that is  $w \in W \Rightarrow Aw \in W$ ).
- If  $v$  is an eigenvector of  $A$  ( $Av = \lambda v$  with  $\lambda \in \mathbb{F}$ ) then  $f(x)v = f(A)v = f(\lambda)v$ .

## 11.11 Primary Decomposition

Let  $R$  be a PID and  $V$  an  $R$  module so that  $\text{Ann}(V) = (f) \neq 0$ . Then  $V = V_1 \oplus \cdots \oplus V_n$  where  $\text{Ann}(V_j) = p_j^{a_j}$  (prime powers of  $f$ ). This is the primary decomposition of  $V$ , and is unique up to ???.

Prop: Let  $V$  be a module over the commutative ring  $R$ . Let  $I$  be an ideal of  $R$  with  $I \subseteq \text{Ann}(V)$ , and set  $\bar{R} = R/I$ . Then  $V$  is also an  $\bar{R}$  module by  $(r + I)v = rv$ .

## 11.12 Similar Linear Maps

Let  $A : V \rightarrow V$  and  $B : W \rightarrow W$  be linear maps. Then  $A$  and  $B$  are similar if and only if there is an invertible linear map  $S : V \rightarrow W$  such that  $S^{-1}BS = A$ .

Theorem Let  $V$  and  $W$  be vector spaces over  $\mathbb{F}$ . Define  $f(x)v = f(A)v$  and  $f(x)w = f(B)w$  so  $V$  and  $W$  are  $\mathbb{F}[x]$  modules. Then  $V$  and  $W$  are isomorphic as  $\mathbb{F}$  modules if and only if  $A$  and  $B$  are similar.

### 11.13 Finitely Generated Module

A module  $V$  over  $R$  is finitely generated if and only if there are  $v_1, \dots, v_n \in V$  such that  $V = (v_1, \dots, v_n) = \{r_1v_1 + \dots + r_nv_n : r_1, \dots, r_n \in R\}$ .

### 11.14 Neotherian Ring

A commutative ring  $R$  is Neotherian if and only if each ideal of  $R$  is finitely generated. (This is the same as satisfying the ACC)

Prop: Every PID is Neotherian, as every ideal is generated by a simple element.

### 11.15 Hilbert Basis Theorem

If  $R$  is Neotherian, then the polynomial ring  $R[x]$  is also Neotherian.

Prop: Repeated use of the Hilbert Basis Theorem shows that  $\mathbb{F}[x_1, \dots, x_n]$  is Neotherian.

Theorem: Let  $V$  be finitely generated module over the Neotherian ring  $R$ . Then every submodule of  $V$  is also finitely generated.

## 12 Notes pg 200 - 218

### 12.1 Presentation Matrix of a module

Theorem: If  $V$  is a finitely generated module over a Neotherian ring  $R$ , then there are  $m, n$  and  $A \in M_{n \times m}(R)$  such that  $V \cong R^n / AR^m$

$A$  is a presentation matrix of  $V$ .

Theorem: Let  $R$  be a commutative ring, and  $A, B \in M_{n \times m}(R)$  such that there are matrices  $P \in M_{n \times n}(R)$  and  $Q \in M_{m \times m}(R)$  such that  $B = PAQ^{-1}$ . Then  $R^n / AR^m \cong R^n / BR^m$ .

Theorem: Let  $V$  be a finitely generated module over a PID  $R$ . Then  $V$  is a direct sum of cyclic  $R$  modules.

### 12.2 Companion Matrix

If  $g(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ , then the companion matrix of  $g(x)$  is given by 
$$\begin{bmatrix} 0 & 0 & 0 & -a_0 \\ 1 & 0 & 0 & -a_1 \\ 0 & 1 & 0 & -a_2 \\ 0 & 0 & 1 & -a_3 \end{bmatrix}$$

Theorem:  $A, B \in M_{n \times n}(\mathbb{F})$  are similar if and only if the matrices  $xI - A$  and  $xI - B \in M_{n \times n}(\mathbb{F}[x])$  have the same Smith Normal Form (SNF).

Theorem: Let  $A, B \in M_{n \times n}(\mathbb{F})$ .  $A$  and  $B$  are similar if and only if they have the same invariant factors.

### 12.3 Invariant Factors

The invariant factors of  $A$  are the  $f_i(x)$ 's of the SNF of  $xI - A$ .

### 12.4 Elementary Divisors

### 12.5 Rational Canonical Form

### 12.6 Jordan Block

### 12.7 Jordan Canonical Form