Dummit & Foote Exercises

Ari Glass

December 2023

Contents

I Group Theory 3

1 Introduction to Groups 4

2 Subgroups 5

3 Quotient Groups and Homomorphisms 6

4 Group Actions 7

5 Direct and Semidirect Products and Abelian Groups 8

6 Durther Topics in Group Theory 9

II Ring Theory 10

7 Introduction to Rings 11
7.1 Basic Definitions and Examples . . . 11
7.2 Examples: Polynomial Rings, Matrix Rings, and Group Rings . . . 12
7.3 Ring Homomorphisms and Quotient Rings . . . 14
7.4 Properties of Ideals . . . 16
7.5 Rings of Fractions . . . 17
7.6 The Chinese Remainder Theorem . . . 17

8 Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains 19
8.1 Euclidean Domains . . . 19
8.2 Principal Ideal Domains . . . 19
8.3 Unique Factorization Domains (U.F.D.s) . . . 21

9 Polynomial Rings 22
9.1 Definitions and Basic Properties . . . 22
9.2 Polynomial Rings Over Fields . . . 23
9.3 Polynomial Rings that are Unique Factorization Domains . . . 24
9.4 Irreducibility Criteria . . . 24
9.5 Polynomial Rings Over Fields II . . . 25

III Modules and Vector Spaces 26

10 Introduction to Module Theory 27
10.1 Basic Definitions and Examples . . . 27
10.2 Quotient Modules and Module Homomorphisms . . . 29
10.3 Generation of Modules, Direct Sums, and Free Modules . . . 30

11 Vector Spaces **33**
11.1 Definitions and Basic Theory 33
11.2 The Matrix of a Linear Transformation 33
11.3 Dual Vector Spaces 34
11.4 Determinants 36

12 Modules over Pricipal Ideal Domains **37**
12.1 The Basic Theory 37
12.2 The Rational Canonical Form 39

13 Field Theory **42**
13.1 Basic Theory of Field Extensions 42
13.2 Algebraic Extensions 42
13.3 Classical Straightedge and Compass Constructions 43
13.4 Splitting Fields and Algebraic Closures 44
13.5 Separable and Inseparable Extensions 44
13.6 Cyclotomic Polynomials and Extensions 45

14 Galois Theory **46**
14.1 Basic Definitions 46
14.2 The Fundamental Theorem of Galois Theory 47
14.3 Finite Fields 48
14.4 Composite Extensions and Simple Extensions 50
14.5 Cyclotomic Extensions and Abelian Extensions Over $\mathbb{Q}$ 50
14.6 Galois Groups of Polynomials 51
14.7 Solvable and Radical Extensions: Insolvability of the Quintic 52

Part I

Group Theory

Chapter 1

Introduction to Groups

Chapter 2

Subgroups

Chapter 3

Quotient Groups and Homomorphisms

Chapter 4

Group Actions

Chapter 5

Direct and Semidirect Products and Abelian Groups

Chapter 6

Durther Topics in Group Theory

Part II

Ring Theory

Chapter 7

Introduction to Rings

7.1 Basic Definitions and Examples

Let R be a ring with identity 1

1. Show that $(-1)^2 = 1$

   Proof.

   $$\begin{aligned} -1+1=0 &\implies 0=(-1+1)^2=(-1)^2-1-1+1^2=(-1)^2-1 \\ &\implies (-1)^2-1+1=1 \\ &\implies (-1)^2=1 \end{aligned}$$

   □

2. Prove that if u is a unit in R, so is $-u$.

   Proof. Let $v \in R$ such that $vu = 1$. Then

   $$\begin{aligned} 0 &= u-u \\ \implies 0 &= v(u-u) = vu + v(-u) = 1 + v(-u) \\ \implies -1 &= v(-u) \\ \implies 1 &= v(-u)v(-u) \end{aligned}$$

   and so the existence of $v(-u)v \in R$ shows that $-u$ is a unit. □

4. Prove that the intersection of any nonempty collection of subrings is a subring.

   Proof. Let $\mathcal{S}$ be a non empty collection of subrings $S_\alpha \subseteq R$ for $\alpha \in J$. We already have that $\bigcap \mathcal{S}$ is a subgroup of R, so we only need to show that $1 \in \bigcap \mathcal{S}$ and that $\bigcap \mathcal{S}$ is closed under multiplication. The first claim is trivial because $1 \in S_\alpha$ for all $\alpha \in J$. The second claim is almost as trivial, for if $r, s \in \bigcap \mathcal{S}$, then $r, s \in S_\alpha$ and hence $rs, sr \in S_\alpha$ for all $\alpha \in J$. □

7. Prove that the center of R is a subring that contains 1. Prove that the center of a division ring is a field.

   Proof. Let Z_R denote the center of R. $1 \cdot r = r = r \cdot 1$, so $1 \in Z_R$ for all $r \in R$. Suppose $y, z \in Z_R$. Then for any $r \in R$, $(yz)r = y(rz) = r(zy) = r(yz)$ so $yz = zy \in Z_R$. Moreover, $(y+z)r = yr + zr = ry + rz = r(y+z)$, so $(y+z) \in Z_R$ and Z_R is a subring.

   If R is a division ring, then its center is clearly a field for a field is simply a commutative division ring and the center of a division ring must also be a division ring. □

8. Describe the center of the real Hamiltonian Quaternions $\mathbb{H}$. Prove that $\{a + bi|a, b \in \mathbb{R}\}$ is a subring of $\mathbb{H}$, which is a field, but is not contained in the center of $\mathbb{H}$.

   Proof. Suppose that $z = a+bi+cj+dk \in Z_{\mathbb{H}}$ for some $a, b, c, d, \in \mathbb{R}$. Then z commutes with all $h \in \mathbb{H}$, so in particular,

$$\begin{aligned}(a + bi + cj + dk)i &= i(a + bi + cj + dk)\\ -b + ai + dj - ck &= -b + ai - dj + ck\\ dj = -dj \qquad &\qquad ck = -ck\\ d = -d \qquad &\qquad c = -c\end{aligned}$$

   and so $c, d = 0$. Similarly, $zj = jz$ shows that $b = 0$. Because that coefficiants of i, j, and k always commute, a can be anything and so $Z_{\mathbb{H}} = \mathbb{R}+0i+0j+0k$. Observe that $\{a+bi|a, b \in \mathbb{R}\}$ is isomorphic to $\mathbb{C}$ and so it is a field, but it is not contained in $Z_{\mathbb{H}}$. □

9. For a fixed element $a \in R$, define the centralizers of a, $C(a) = \{r \in R|ra = ar\}$. Prove that $C(a)$ is a subring of R and that

$$Z_R = \bigcap_{r\in R} C(r)$$

   Proof. Suppose that $c, d \in C(a)$ for some $a \in R$. Then $(c + d)a = ca + da = ac + ad = a(c + d)$ so $(a + c) \in C(a)$. Moreover, $(cd)a = c(da) = c(ad) = (ca)d = (ac)d = a(cd)$, so $cd \in C(a)$ and $C(a)$ is closed under addition and multiplication and is thus a subring of R. As for the other claim:

$$z \in \bigcap_{r\in R} C(r) \iff z \in C(r) \;\; \forall r \in R \iff zr = rz \;\; \forall r \in R \iff z \in Z_R$$

   □

11. Prove that if R is an integral domain and $x^2 = 1$ for some $x \in R$ then $x = \pm 1$.

   Proof. Observe that $(x - 1)(x + 1) = x^2 - 1 = 0$. $(x - 1)$ or $(x + 1)$ has to be 0 by hypothesis that R is an integral domain, which happens if and only if $x = \pm 1$. □

12. Prove that any subring of a field which contains the identity is an integral domain.

   Proof. Suppose that F is a field and S is a subring of F containing 1. Suppose $r, s \in S$ and $rs = 0$. Then $rs = 0$ in F as well, so either $r = 0$ or $s = 0$ and so, because $1 \in S$, S is an integral domain. □

7.2 Examples: Polynomial Rings, Matrix Rings, and Group Rings

Let R be a commutative ring with identity element 1.

6. Let S be a ring with $1 \neq 0$. Let $n \in \mathbb{Z}^+$ and let $A \in M_n(S)$ whose i, j entry is a_{ij}. Let E_{pq} be the element of $M_n(S)$ such that $e_{ij} = 1$ if $i = p$ and $j = q$ and $e_{ij} = 0$ otherwise.

   (a) Prove that $E_{pq}A$ is the matrix whose p^{th} row equals the q^{th} row of A and all other rows are zero.

   Proof. Let $B = E_{pq}A$ with entries b_{ij}. Then

$$b_{ij} = \sum_{k=1}^{n} e_{ik}a_{kj} = \begin{cases} a_{ji} & \text{if } i = q\\ 0 & \text{otherwise}\end{cases}$$

   □

(b) Prove that AE_{rs} is the matrix whose s^{th} column is the r^{th} column of A and all other columns are zero.

Proof. Let $B = AE_{rs}$ with entries b_{ij}. Then

$$b_{ij} = \sum_{k=1}^{n} a_{ik}e_{kj} = \begin{cases} a_{ij} & \text{if } j = r \\ 0 & \text{otherwise} \end{cases}$$

□

(c) Deduce that if $C = E_{pq}AE_{rs}$, then $c_{ij} = a_{qr}$ when $i = p$ and $j = s$ and $c_{ij} = 0$ otherwise.

Proof. Let $B = E_{pq}A$. Then $b_{ij} = a_{ij}$ when $i = q$ and 0 otherwise. $C = BE_{rs}$, so $c_{ij} = b_{ij}$ when $j = r$. Then $c_{ij} = a_{ij}$ when $i = q$ and $j = r$ and is 0 otherwise. □

7. Prove that the center of the ring $M_n(R)$ is the subring of scalar matrices.

Proof. Suppose that $C \in Z_{M_n(R)}$. Then C commutes with all elements of $M_n(R)$, so in particular, $CE_{ij} = E_{ij}C$ for all $i, j \leq n$. Therefore $c_{ij} = c_{ji}$, i.e. C is symmetric. Now let A be the matrix with $a_{ij} = 1$ when $i \leq j$ and 0 otherwise. Then $CA = AC$ implies that for all $i, j \leq n$

$$\sum_{k=1}^{n} c_{ik}a_{kj} = \sum_{k=1}^{n} a_{ik}c_{kj}$$
$$\sum_{k=j}^{n} c_{ik} = \sum_{k=i}^{j} c_{kj}$$

which can only happen if $c_{ij} = 0$ when $i \neq j$, so C is diagonal. Now for any $q, p \leq n$, $B = E_{pq}C = CE_{pq}$, so $c_{pp} = b_{pp} = c_{qq}$ and so C is a scalar matrix. □

10. Consider the following elements of the integral group ring $\mathbb{Z}S_3$:

$$\alpha = 3(1\ 2) - 5(2\ 3) + 14(1\ 2\ 3) \qquad \text{and} \qquad \beta = 6(1) + 2(2\ 3) - 7(1\ 3\ 2)$$

Compute the following elements:

(a) $\alpha + \beta = 6(1) + 3(1\ 2) - 3(2\ 3) + 14(1\ 2\ 3) - 7(1\ 3\ 2)$

(b) $2\alpha - 3\beta = -18(1) + 6(1\ 2) - 16(2\ 3) + 28(1\ 2\ 3) + 21(1\ 3\ 2)$

(c) $\alpha\beta = -108(1) + 81(1\ 2) - 30(2\ 3) - 21(1\ 3) + 90(1\ 2\ 3)$

(d) $\beta\alpha = -108(1) + 18(1\ 2) - 51(2\ 3) + 63(1\ 3) + 84(1\ 2\ 3)$

(e) $\alpha^2 = 34(1) - 70(1\ 2) + 42(2\ 3) - 28(1\ 3) - 15(1\ 2\ 3) + 181(1\ 3\ 2)$

11. Repeat the preceding exercise under the assumption that the coefficients of α and β are in $\mathbb{Z}/3\mathbb{Z}$.

(a) $\alpha + \beta = 2(1\ 2\ 3) + 2(1\ 3\ 2)$

(b) $2\alpha - 3\beta = 2(2\ 3) + 1(1\ 2\ 3)$

(c) $\alpha\beta = 0$

(d) $\beta\alpha = 0$

(e) $\alpha^2 = (1) + 2(1\ 2) + 2(1\ 3) + 1(1\ 3\ 2)$

12. Let $G = \{g_1, ..., g_n\}$ be a finite group. Prove that $N = g_1 + ... + g_n$ is in the center of the group ring RG.

Proof. Any element in RG is given by $M = r_1g_1 + ... + r_ng_n$ for $r_1, ..., r_n \in R$. Then

$$MN = \sum_{i=1}^{n}\sum_{j=1}^{n} r_ig_ig_j = \sum_{i=1}^{n} r_i \sum_{j=1}^{n} g_ig_jg_j^{-1}g_j = \sum_{i=1}^{n}\sum_{j=1}^{n} r_ig_jg_i = NM$$

as desired. □

7.3 Ring Homomorphisms and Quotient Rings

Let R be a ring with identity $1 \neq 0$

1. Prove that $2\mathbb{Z}$ and $3\mathbb{Z}$ are not isomorphic.

   Proof. For the sake of contradiction, suppose that $\varphi : 2\mathbb{Z} \to 3\mathbb{Z}$ is a ring isomorphism. If $x = \varphi(2)$, then $x = 3k$ for some $k \in \mathbb{Z}$. Moreover, $x + x = x^2$, so $6k = 9k^2$ and $3k = 2$, but no such k exists. □

2. Prove that the rings $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$ are not isomorphic.

   Lemma 7.3.1. *Let R be a ring with identity 1_R and let S is a ring with identity 1_S. If $\varphi : R \to S$ is a ring isomorphism, then $\varphi(1_R) = 1_S$.*

   Proof. For any $r \in R$, $\varphi(r) = \varphi(1_R r) = \varphi(1_r)\varphi(r))$. □

   Lemma 7.3.2. *If $\varphi : R \to S$ is a ring isomorphism, than r is a unit in R if and only if $\varphi(r)$ is a unit in S.*

   Proof. Suppose r is a unit in R. Then there is an $s \in R$ such that $rs = 1_R$. Then $\varphi(rs) = 1_S = \varphi(r)\varphi(s)$ and so $\varphi(r)$ is a unit in S. Conversely, if $\varphi(r)$ is a unit in S, there is some $s' \in S$ such that $\varphi(r)s' = 1_S$. φ is surjective, so there is an $s \in R$ such that $\varphi(s) = s'$. Then $\varphi(r)\varphi(s) = \varphi(rs) = 1_S$, so $rs = 1_R$ and r is a unit in R. □

   Proof. The only units in $\mathbb{Z}[x]$ are ± 1, but $\mathbb{Q}[x]$ has many more, e.g. $\frac{1}{2}$. Thus, lemma 7.3.2 shows that there can be no isomorphism between the two rings. □

6. Decide which of the following are ring homomorphisms from $M_2(\mathbb{Z})$ to $\mathbb{Z}$.

   (a)
   $$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a$$

   Not a homomorphism:

   $$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \longmapsto 2 \neq 1 = 1 \times 1$$

   (b)
   $$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a + d$$

   Not a homomorphism:

   $$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix} \longmapsto 2 \neq 1 = 1 \times 1$$

   (c)
   $$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto ad - bc$$

   Not a homomorphism:

   $$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \longmapsto 1 \neq 0 = 0 + 0$$

7. Let

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \middle| a, b, d \in \mathbb{Z} \right\}$$

Prove that the map

$$\varphi : R \to \mathbb{Z} \times \mathbb{Z}, \qquad \varphi \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mapsto (a, d)$$

is a surjective homomorphism. Describe its kernel. For any $a, b, d, e, f, h \in \mathbb{Z}$:

$$\varphi \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} + \varphi \begin{pmatrix} e & f \\ 0 & h \end{pmatrix} = (a, d) + (e, h) = (a + e, d + h) = \varphi \begin{pmatrix} a + e & b + f \\ 0 & d + h \end{pmatrix}$$

and

$$\varphi \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \times \varphi \begin{pmatrix} e & f \\ 0 & h \end{pmatrix} = (a, d) \times (e, h) = (ae, dh) = \varphi \begin{pmatrix} ae & af + bh \\ 0 & dh \end{pmatrix}$$

and thus φ is a homomorphism. Surjectivity is clear. The kernel is givin by:

$$R = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| b \in \mathbb{Z} \right\}$$

8. Decide which of the following are ideals of the ring $\mathbb{Z} \times \mathbb{Z}$:

   (a) $A = \{(a, a) | a \in \mathbb{Z}\}$ is not an ideal because $(1, 0) \cdot (a, a) = (a, 0) \notin A$

   (b) $B = \{(2a, 2b) | a, b \in \mathbb{Z}\}$ is an ideal because for any $a, b, c, d \in \mathbb{Z}$, $(c, d) \cdot (2a, 2b) = (2ac, 2bd) \in B$

   (c) $C = \{(2a, 0) | a \in \mathbb{Z}\}$ is an ideal because for any $a, c, d \in \mathbb{Z}$, $(c, d) \cdot (2a, 0) = (2ac, 0) \in C$

   (d) $D = \{(a, -a) | a \in \mathbb{Z}\}$ is not an ideal because $(1, 0) \cdot (a, -a) = (a, 0) \notin D$

10. Decide which of the following are ideals of the ring $\mathbb{Z}[x]$:

   (a) The set of all polynomials whose constant term is a multiple of 3 is an ideal of $\mathbb{Z}[x]$.

   (b) The set of all polynomials whose second order coefficient is a multiple of 3 is not an ideal of $\mathbb{Z}[x]$. E.g., $(3x^2 + x)(x) = 3x^3 + x^2$.

   (c) The set of all polynomials whose 0^{th}, 1^{st}, and 2^{nd} order coefficients are all 0 is an ideal of $\mathbb{Z}[x]$.

   (d) $\mathbb{Z}[x^2]$ is not an ideal of $\mathbb{Z}[x]$.

   (e) The set of all polynomials whose coefficients sum to 0 is an ideal $\mathbb{Z}[x]$. If $\sum (a_i)_{i \leq n} = 0$, then for any $(b_i)_{i \leq m} \in \mathbb{Z}$, if $C(x) = A(x)B(x)$, then

$$\sum_{i=1}^{n+m} c_i = \sum_{j=1}^{m} \sum_{i=1}^{n} a_i b_j = \sum_{j=1}^{m} b_j \sum_{i=1}^{n} a_i = \sum_{j=1}^{m} b_j \cdot 0 = 0$$

   (f) The set of all polynomials $p(x)$ where $p'(0) = 0$ is not an ideal of $\mathbb{Z}[x]$; e.g., if $p(x) = x^2 + 1$, $p'(x) = 2x$ and $p'(0) = 0$, but if $q(x) = xp(x) = x^3 + x$, then $q'(x) = 3x^2 + 1$ and $q'(0) = 1$.

11. Let R be the ring of all continuous real valued functions on the closed interval $[0, 1]$. Prove that the map $\varphi : R \to \mathbb{R}$ defined by $\varphi(f) = \int_0^1 f(t)dt$ for all $f \in R$ is a homomorphism of additive groups, but is not a ring homomorphism.

Proof. The additive identity is the zero map 0 and $\varpi(0) = 0$. For any $f, g \in R$:

$$\varphi(f + g) = \int_0^1 [f(t) + g(t)]dt = \int_0^1 f(t)dt + \int_0^1 g(t)dt = \varphi(f) + \varphi(g)$$

but

$$\varphi(f \cdot g) = \int_0^1 [f(t) \cdot g(t)]dt \neq \int_0^1 f(t)dt \cdot \int_0^1 g(t)dt = \varphi(f) \cdot \varphi(g)$$

in general. □

19. Prove that if $I_1 \subseteq I_2 \subseteq ...$ are ideals of R, then $\bigcup\{I_n\}_{n\in\mathbb{N}}$ is an ideal of R.

   Proof. Let $S = \bigcup\{I_n\}_{n\in\mathbb{N}}$ and suppose that $s, t \in S$. Then there are N_s, N_t such that $s \in I_{N_s}$ and $t \in I_{N_t}$. Letting $N = \max\{N_s, N_t\}$, $s, t \in I_N$ and so $s + t \in I_N \subseteq S$ as well. Moreover, for any $r \in R$, $rs, sr \in I_N \subseteq S$ and so S is an ideal. □

7.4 Properties of Ideals

Let R be a ring with identity $1 \neq 0$

1. Let L_j be the left ideal of $M_n(R)$ consisting of arbitrary entries in the j^{th} column and zero in all other entries and let E_{ij} be the element of $M_n(R)$ whose i, j entry is 1 and whose other entries are all 0. Prove that $L_j = M_n(R)E_{ij}$ for any i.

   Proof. From exercise 7.2.6, $AE_{i,j}$ is the matrix whose j^th column is any column is the i^th column of A, so $AE_{i,j} \in L_j$. Of course, A can be arbitrarily constructed to have any entries in any column, so for any $\ell \in L_j$ and any $i \leq n$, putting the j^{th} column of ℓ_j in the i^{th} column of A gives $AE_{i,j} = \ell_j$ □

2. Assume that R is commutative. Prove that the augmentation ideal in the group ring RG is generated by $\{g - 1 | g \in G\}$ Prove that if $G = \langle\sigma\rangle$ is cyclic, then augmentation ideal is generated by $\sigma - 1$.

   Remark. *Recall that the augmentation ideal of the group ring RG is the kernel of the ring homomorphism $RG \to R$ given by $\sum r_i g_i \mapsto \sum r_i$; which is to say, it contains the elements $a \in RG$ whose coefficients sum to* 0.

   Proof. Let $S = \{g - 1 | g \in G\}$ and let A be the augmentation ideal of RG. Clearly, $(S) \subseteq A$ because $1 - 1 = 0$ and so $(g - 1) \in A$ for all $g \in G$. As for the other inclusion, suppose that $\alpha = \sum a_i g_i \in A$; that is $\sum a_i = 0$. Then:

$$\begin{aligned}\sum_{i=1}^{n} a_i(g_i - 1) &= \sum_{i=1}^{n}(a_i g_i - a_i) \\ &= \sum_{i=1}^{n} a_i g_i - \sum_{i=1} a_i \\ &= \sum_{i=1}^{n} a_i g_i \\ &= \alpha\end{aligned}$$

   and so $\alpha \in (S)$; that is $A \subseteq (S)$ and hence $A = (S)$.

   In particular, if $G = \langle\sigma\rangle$ is cyclic with $|G| = n$, then $S = \{\sigma^i - 1 | i \leq n\}$, but for any k,

$$(\sigma - 1)\sum_{i=1}^{k-1} \sigma^i = \sigma^k - 1$$

   and so $\sigma^k \in (\sigma - 1)$ for all k. We conclude that $A = (\sigma - 1)$ □

4. Assume that R is commutative. Prove that R is a field if and only if 0 is a maximal ideal.

   Proof. Assume that 0 is a maximal ideal of the commutative ring R. For any $r \in R$, if r is nonzero, then because 0 is maximal, $(r) = R$, so r must be a unit. Because all nonzero elements of R are units and $1 \neq 0$ by hypothesis, R is a field. Conversely, assume that R is a field; i.e., that r is a unit for all nonzero $r \in R$. Then $(r) = R$ and 0 is a maximal ideal. □

5. Prove that if M is an ideal such that R/M is a field, then M is a maximal ideal. (Do not assume that R is commutative).

   Proof. Suppose that N is an ideal of R and that $N \supseteq M$. Then by the Lattice Isomorphism Theorem for Rings, N/M is an ideal of R/M. But by hypothesis, R/M is a field and so its only ideals are 0 and R/M and so $N = 0$ or $N = R$, which is to say, that M is a maximal ideal of R. □

7. Let R be a commutative ring with 1. Prove that the principal ideal generated by x in the polynomial ring $R[x]$ is a prime ideal if and only if R is an integral domain. Prove that (x) is maximal if and only if R is a field.

   Proof. Consider the homomorphism $\varphi : R[x] \to R$ by $p(x) \mapsto a_0$, where a_0 is the constant coefficient of $p(x)$ for any $p(x) \in R[x]$. The kernel of φ is (x), so by the first isomorphism theorem, $R[x]/(x) \cong R$. Then by Proposition 13[1] (x) is a prime ideal if and only if $R \cong R[x]/(x)$ is an integral domain. By Proposition 12[2], (x) is maximal if and only if $R \cong R[x]/(x)$ is a field. □

9. Let R be the ring of all continuous functions on $[0, 1]$ and let I be the collection of functions $f \in R$ with $f(1/2) = f(1/3) = 0$ prove that I is an ideal, but is not a prime ideal.

   Proof. For any $f, g \in I$, $f(1/2) + g(1/2) = f(1/3) + g(1/3) = 0$ and $-f(1/2) = -f(1/3) = 0$, so I is an additive subgroup. Moreover, for any $h \in R$, $h(1/2)f(1/2) = h(1/3)f(1/3) = 0$, so $hf \in I$ and I is an ideal. However, I is not a prime ideal. For example, if $f(x) = x - 1/2$ and $g(x) = x - 1/3$, then $h(x) = f(x)g(x) = (x - 1/2)(x - 1/3)$ and so $h \in I$, but $f, g \notin I$. □

11. Assume R is commutative. Let I and J be ideals of R and assume P is a prime ideal of R that contains IJ. Prove that I or J is contained in P.

    Proof. Suppose that $I \not\subseteq P$; then there is some $a \in I$ such that $a \notin P$. Now $ab \in P$ for all $b \in J$ and P is a prime ideal, so $b \in P$. Thus $J \subseteq P$. Similarly, $J \not\subseteq P$ implies $I \subseteq P$. □

7.5 Rings of Fractions

4. Every subring of $\mathbb{R}$

   Proof. Any subfield of $\mathbb{R}$ contains 1 and so it must also contain $\mathbb{Z}$. $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$ and thus the ”smallest” field containing $\mathbb{Z}$. □

7.6 The Chinese Remainder Theorem

3. Let R and S be rings with identities. Prove that every ideal of $R \times S$ is of the form $I \times J$ where I is an ideal of R and J is an ideal of S.

   Lemma 7.6.1. *If $\varphi : R \to S$ is a surjective ring homomorphism and I is an ideal of R, then $\varphi(I)$ is an ideal of S.*

   Proof. φ is a surjective homomorphism, so its kernel, K is an ideal of R and $R/K \cong S$. Then by the Lattice Isomorphism Theorem for Rings, I/K is an ideal of R/S and so $\varphi(I)$ is an ideal of S. □

[1] Dummit & Foote pg. 255

[2] Dummit & Foote pg. 254

Proof. Let $\pi_R : R \times S \to R$ and $\pi_S : R \times S \to S$ be projection maps; recall that a projection map is a surjective homomorphism. If A is an ideal of $R \times S$, then by the Lemma above, $I = \pi_R(A)$ is an ideal of R and $J = \pi_S(A)$ is an ideal of S. Clearly, $A \subseteq I \times J$. Suppose $(i, j) \in I \times J$, then $(i, s), (r, j) \in A$ for some $r \in R$ and $s \in S$. Because A is an ideal, $(0, 1) \cdot (r, j) = (0, j) \in A$ and $(1, 0) \cdot (i, s) = (i, 0) \in A$, but then $(i, 0) + (0, j) = (i, j) \in A$, so $A = I \times J$. □

6. Let $f_1(x), f_2(x), ..., f_k(x)$ be polynomials with integer coefficients of the same degree d. Let $n_1, n_2, ..., n_k$ be integers which are relatively prime in pairs (i.e., $(n_i, n_j) = 1$ for all $i \neq j$). Use the Chinese Remainder Theorem to prove there exists a polynomial $f(x)$ with integer coefficients anda a degree of d with

$$f(x) \equiv f_1(x) \mod n_1, \qquad f(x) \equiv f_2(x) \mod n_2, \quad ..., \quad f(x) \equiv f_k(x) \mod n_k$$

i.e., the coefficients of $f(x)$ agree with the coefficients of $f_i(x) \mod n_i$. Show that if all the $f_i(x)$ are monic, then $f(x)$ may also be chosen monic.

Proof. By the Chinese Remainder Theorem:

$$\varphi : \mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times ... \times \mathbb{Z}/n_k\mathbb{Z}, \qquad r \mapsto (r + n_1\mathbb{Z}, r + n_2\mathbb{Z}, ..., r + n_k\mathbb{Z})$$

is a surjective homomorphism with kernel $n_1\mathbb{Z} \cap n_2\mathbb{Z} \cap ... \cap n_k\mathbb{Z} = \prod n_i\mathbb{Z}$ by the assumption that all n_i are pairwise coprime. Writing a_{ij} to denote the j^{th} coefficient of $f_i(x)$, we see that there is an a_j such that $\varphi(a_j) = (a_{1j} + n_1\mathbb{Z}, a_{2j} + n_2\mathbb{Z}, ..., a_{kj} + n_k\mathbb{Z})$, which is to say that $a_j \equiv a_{ij} \mod n_i$ for all i. Thus, the desired $f(x)$ exists. Moreover, if each $a_{id} = 1$, $a_d = 1$ works and so $f(x)$ can be chosen monic. □

Chapter 8

Euclidean Domains, Principal Ideal Domains, and Unique Factorization Domains

8.1 Euclidean Domains

3. Let R be a Euclidean Domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of R of norm m is a unit. Deduce that a nonzero element of norm zero (if such anelement exists) is a unit.

   Proof. Let N be a norm on R with $\min\{N(r)|r \in R, r \neq 0\} = m$ and suppose that $N(a) = m$ for some $a \in R$. Because R is a Euclidean domain, there exist $q, r \in R$ such that $1 = qa + r$ and $r = 0$ or $N(r) < N(a) = m$. But there are no nonzero $r \in R$ where $N(r) < m$, so $r = 0$. Thus, $aq = 1$, i.e. a is a unit. Moreover, if there is a nonzero element $x \in R$ with $N(x) = 0$, then $m = 0$ and x is a unit. □

10. Prove that the quotient ring $\mathbb{Z}[i]/I$ is finite for any nonzero ideal I of $\mathbb{Z}[i]$.

    Proof. All ideals of a euclidean domain are principal ideals, so there is some $\alpha \in \mathbb{Z}[i]$ such that $I = (\alpha)$. For any $\beta \in \mathbb{Z}[i]$, there exist $\kappa, \rho \in \mathbb{Z}[i]$ such that $\beta = \kappa\alpha + \rho$ where $|\rho|^2 < |\alpha|^2$. Then $\beta + I = (\kappa\alpha + \rho) + I = \rho + I$ because $\kappa\alpha \in I$. Thus every coset of $\mathbb{Z}[i]/I$ can be represented by some element whose norm is less than the norm of α. Of course, finite such elements exist. □

8.2 Principal Ideal Domains

1. Prove that in a Principal Ideal Domain two ideals (a) and (b) are comaximal if and only if a greatest common divisor of a and b is 1.

   Proof. First, we assume that (a) and (b) are comaximal. Let $d = gcd(a, b)$. Then $a + b \subseteq (d) = R$ by assumption that (a) and (b) are comaximal. Thus we conclude that $d = 1$. Conversely, assume that $\gcd(a, b) = 1$ and suppose that I is an ideal of R with $I \supseteq (a), (b)$. R is a Principal Ideal Domain, so there is a $d \in R$ such that $I = (d)$. Therefore, $d|a$ and $d|b$, so $d = 1$. Then $I = R$ and (a) and (b) are comaximal. □

3. Prove that the quotient of a P.I.D. by a prime ideal is again a P.I.D.

Proof. Let R be a Principal Ideal Domain and P be a prime ideal of R. If $P = 0$, then $R/P \cong R$ and there is nothing left to show. Otherwise, P is maximal because every prime ideal in a Principal Ideal Domain is maximal[1]. It follows that R/P is a field[2] and is therefore a Principal Ideal Domain. □

4. Let R be an integral domain. Prove that the following two conditions are sufficient to show that R is a Principal Ideal Domain:

   (i) Any two nonzero elements a and b in R have a greatest common divisor which can be written in the form $ra + sb$ for some $r, s \in R$.

   (ii) If $a_1, a_2, a_3, ...$ are nonzero elements of R such that $a_{i+1}|a_i$ for all i, then there is a positive integer N such that a_n is a unit times a_N for all $n \geq N$.

   Proof. Let R be an integral domain that satisfies conditions (i) and (ii) and suppose I is an ideal of R. Enumerating the elements of I as r_i, put $a_1 = \gcd(r_1, r_2)$, and then for all $i > 1$, put $a_i = \gcd(a_{i-1}, r_{i+1})$. Observe that $I = (r_1) + (r_2) + (r_3) + ...$ and $(r_i) \subseteq (a_i)$ for all i, so $I \subseteq (a_1) + (a_2) + (a_3) + ...$ Moreover, $a_{i+i}|a_i$ for all i, so $(a_1) \subseteq (a_2) \subseteq (a_3) \subseteq ....$ Now, there is an N such that a_n is a unit, u_n times a_N for all $n \geq N$, so we have $(a_n) = (a_N)$ whenever $n \geq N$. Thus, $I \subseteq (a_1) + (a_2) + (a_3)... = (a_1) + ... + (a_N) = (a_N)$ because $a_N|a_n$ for all $n \leq N$. As I is contained in a principal ideal, it must itself be a principal ideal. □

7. An integral domain R in which every ideal generated by two elements is principal is called a *Bezout Domain.*

   (a) Prove that the integral domain R is a Bezout Domain if and only if every pair of elements a, b of R has a g.c.d. d in R that can be written as an R-linear combination of a and b, i.e., $d = ax + by$ for some $x, y \in R$.

   Proof. Suppose that R is a Bezout domain with $a, b \in R$. Then there is some $d \in R$ such that $(a, b) = (a) + (b) = (d)$. Therefore, there are $x, y \in R$ such that $ax + by = d$ and d is a common divisor of a and b, though not necessarily greatest. If $e \in R$ is a common divisor of a and b, then $a, b \in (e)$ and so $(a, b) = (d) \subseteq (e)$. Thus, we can conclude that $e|d$, i.e. $d = \gcd(a, b)$.

   Conversely, assume that all $a, b \in R$ have a gcd given as an R-linear combination of a and b. Let $a, b, d, x, y \in R$ such that $\gcd(a, b) = d = ax + by$. Then $d \in (a, b)$, so $(d) \subseteq (a, b)$. But also, $d|a, b$, so $(d) \supseteq (a, b)$. Thus we can conclude that $(d) = (a, b)$. □

   (b) Prove that every finitely generated ideal of a Bezout Domain is principal.

   Proof. Let R be a Bezout Domain. We showed in (a) that an ideal generated by two elements of R is principal. Now, assume that all ideals generated by fewer than n elements is principal and let $I = (a_1, ..., a_n)$ be an ideal generated by n elements. By the induction hypothesis, $I' = (a_1, ..., a_{n-1})$ is ideal and thus can be written $I = (d)$ for some $d \in R$. Then $I = (d) + (a_n) = (d, a_n)$ is generated by two elements and is therefore principal, again by (a). By induction, we conclude that all finitely generated ideals of a Bezout Domain are principal. □

   (c) Let F be the fraction field of the Bezout Domain R. Prove that every element of F can be written in the form a/b with $a, b \in R$ and a and b relatively prime.

   Proof. For any $a/b \in F$, let $\gcd(a, b) = d$. Then there are $x, y \in R$ such that $ax + by = d$. There are $a', b' \in R$ such that $a'd = a$ and $b'd = b$, so we can write $a'dx + b'dy = d$. Then $a'x + b'y = 1$, which is to say that a' and b' are relatively prime. Moreover, $ab = ab'd = a'db \implies ab' = a'b \implies a/b = a'/b'$. □

[1] Dummit & Foote 280

[2] Dummit & Foot pg. 254; Proposition 12

8.3 Unique Factorization Domains (U.F.D.s)

2. Let a and b be nonzero elements of the Unique Factorization Domain R. Prove that a and b have a least common multiple and describe it in terms of the prime factorization of a and b in the same manor that Proposition 13 describes their greatest common divisior.

   Proof. Let $a = u\prod_{i\leq n} p_i^{e_i}$ and $b = v\prod_{i\leq n} p_i^{f_i}$ be the prime factorizations of a and b where u and v are units and each p_i is a distinct prime. We claim that $c = \prod_{i\leq n} p_i^{\max\{e_i,f_i\}}$ is the least common multiple of a and b. That c is a common multiple of a and b is clear; let $d = x\prod_{i\leq n} p_i^{g_i}$ where $x \in R$ and suppose that d is a multiple of a and b. Then for each i, $g_i \geq e_i$ and $g_i \geq f_i$ so $g_i \geq \max\{e_i, f_i\}$. Then it follows immediately that $c|d$ for all common multiples of a and b, d. Thus, c is the *least* such common multiple. □

11. *(Characterization of Principal Ideal Domains)* Prove that R is a P.I.D. if and only if $\mathbb{R}$ is a *U.F.D* that is also a Bezout Domain.

   Proof. Assume that R is a P.I.D.; then if r is a nonzero element of R which is not a unit. If r is irreducible, we are done. Otherwise we can write $r = r_1r_2$ where r_1 and r_2 are nonzero, non-units of $\mathbb{R}$. If r_1 and r_2 are both irreducible, we are done; otherwise, we can write $r_1 = r_{11}r_{12}$ etc. Continuing this way, we must verify that the process eventually terminates. Observe that $r_1, r_2|r$ and $r_{11}, r_{12}|r_1$, etc. Thus $(r) \subsetneq (r_1) \subsetneq (r_{11}) \subsetneq ... \subsetneq R$ where all containments are proper. We must show that this chain is finite.

   Let $I_1 \subseteq I_2 \subseteq ... \subseteq R$ be an infinite ascending chain of ideals of R whwere containment is not necessarily proper. Let $I = \cup_{i=1}^{\infty} I_i$. Then for every $a \in I$, $a \in I_n$ for some n and so $ra \in I_n \subseteq I$ for all $r \in R$. Therefore, I is an ideal of R. In particular, I is a principal ideal and so there is some $\alpha \in R$ such that $I = (\alpha)$. Then $\alpha \in I_N$ for some N and so $I = (\alpha) \subseteq I_N$. But we already have that $I_N \subseteq I$, so $I_N = I$. Of course, it follows that $I_n = I_N = I$ for all $n \geq N$ and so the chain becomes *stationary* at some finite stage. We can thus conclude that any **properly** ascending chain of ideals must be finite, completing the proof that every Principal Ideal Domain is also a Unique Factorization Domain.

   Conversely, we assume that R is a Unique Factorization Domain and that it is also a Bezout Domain. Let I be any ideal of R and let a be a nonzero element of I with a minimal number of irreducible factors; we know that such an a exists because every element of I has a finite number of factors. We claim that $I = (b)$; to demonstrate this, suppose there is a $b \in I$ such that $b \notin (a)$. Then there is a $d \in I$ such that $(a, b) = (d)$. Then $a \in (d)$, so $d|a$, but a has a minimal numbder of factors, so $a = d$. But this leads to a contradiction, as b was chosen to not be in (a), but $b \in (d) = (a)$.

   Thus, we can conclude that every ideal in R is generated by an element with a minimal number of factors, which is to say that R is a Principal Ideal Domain. □

Chapter 9

Polynomial Rings

9.1 Definitions and Basic Properties

1. Let $p(x,y,z) = 2x^2y - 3xy^3z + 4y^2z^5$ and $q(x,y,z) = 7x^2 + 5x^2y^3z^4 - 3x^2z^3$ be polynomials in $\mathbb{Z}[x,y,z]$

   (a) Write each of p and q as a polynomial in x with coefficients in $\mathbb{Z}[y,z]$.

   $$p(x) = (2y)x^2 - (3y^3z)x + (4y^2z^5) \qquad q(x) = (5y^3z^4 - 3z^3 + 7)x^2$$

   (b) Find the degree of each of p and q. $\deg p = 7$. $\deg q = 9$.

   (c) Find the degree of p and q in each of the three variables, x, y, and z.
   $\deg_x p = 2$, $\deg_y p = 3$, $\deg_z p = 5$, $\deg_x q = 2$, $\deg_y q = 3$, $\deg_z q = 4$.

   (d) Compute pq and find the degree of pq in each of the three variables x, y, and z.

   $$pq(x,y,z) = 14x^4y + 10x^4y^4z^4 - 6x^4yz^3 - 21x^3 - 15x^3y^6z^5 + 9x^3y^3z^4 + 28x^2y^2z^5 + 20x^2y^5z^9 - 12x^2z^8$$

   $\deg_x pq = 4$, $\deg_y pq = 6$, $\deg_z pq = 9$.

   (e) Write pq as a polynomial of the variable z with coefficients in $\mathbb{Z}[x,y]$.

   $$pq(z) =$$

   $$(20x^2y^5)z^9 - (12x^2)z^8 + (28x^2y^2 - 15x^3y^6)z^5 + (10x^4y^4 + 9x^3y^3)z^4 - (6x^4y)z^3 + (14x^4y - 21x^3)$$

4. Prove that the ideals (x) and (x,y) are prime ideals in $\mathbb{Q}[x,y]$, but that only the latter is a maximal ideal.

   Proof. Let $p, q \in \mathbb{Q}[x,y]$. Suppose $pq \in (x)$ and, the sake of contradiction, assume $p, q \notin (x)$. Then we can write $p(x,y) = p'(x,y) + ay^m$ and $q(x,y) = q'(x,y) + by^n$ for some nonzero $a, b \in \mathbb{Q}$ and $mn, \in \mathbb{Z}$. Computing the product, we see that $pq(x,y) = p'q'(x,y) + by^np'(x,y) + ay^mq'(x,y) + aby^{m+n}$, and $ab \neq 0$, which contradicts the assumption that $pq \in (x)$. Thus, either p or q must be in (x), i.e., (x) is a prime ideal. However, $(x) \subseteq (x) + (y) = (x,y) \neq \mathbb{Q}[x,y]$, so (x) is not maximal.

   Let $p, q \in \mathbb{Q}[x,y]$. Suppose $pq \in (x,y)$ and, the sake of contradiction, assume $p, q \notin (x,y)$. Then we can write $p(x,y) = p'(x,y) + a$ and $q(x,y) = q'(x,y) + b$ for some nonzero $a, b \in \mathbb{Q}$. Computing the product, we see that $pq(x,y) = p'q'(x,y) + bp'(x,y) + aq'(x,y) + ab$, and $ab \neq 0$, which contradicts the assumption that $pq \in (x,y)$. Thus, either p or q must be in (x,y), i.e., (x,y) is a prime ideal. Now, let I be an ideal of $\mathbb{Q}[x,y]$ such that $I \supsetneq (x,y)$. Then there is some $p(x,y) \in I$ that can be written $p'(x,y) + a$ where $p'(x,y) \in (x,y)$ and a is a nonzero rational. But then $p'(x,y) \in I$, so $a = p(x,y) - p'(x,y) \in I$ and a is a unit, so $I = \mathbb{Q}[x,y]$. Thus we conclude that (x,y) is maximal. □

5. Prove that (x,y) and $(2,x,y)$ are prime ideals in $\mathbb{Z}[x,y]$, but only the latter is maximal.

Proof. Let $p, q \in \mathbb{Z}[x, y]$. Suppose $pq \in (x, y)$ and, the sake of contradiction, assume $p, q \notin (x, y)$. Then we can write $p(x, y) = p'(x, y) + a$ and $q(x, y) = q'(x, y) + b$ for some nonzero $a, b \in \mathbb{Z}$. Computing the product, we see that $pq(x, y) = p'q'(x, y) + bp'(x, y) + aq'(x, y) + ab$, and $ab \neq 0$, which contradicts the assumption that $pq \in (x, y)$. Thus, either p or q must be in (x, y), i.e., (x, y) is a prime ideal. However, $(x, y) \subseteq (x, y) + (2) = (2, x, y) \neq \mathbb{Z}[x, y]$, so (x, y) is not maximal.

Let $p, q \in \mathbb{Z}[x, y]$. Suppose $pq \in (2, x, y)$ and, the sake of contradiction, assume $p, q \notin (2, x, y)$. Then we can write $p(x, y) = p'(x, y) + 2a + 1$ and $q(x, y) = q'(x, y) + 2b + 1$ for some nonzero $a, b \in \mathbb{Z}$. Computing the product, we see that $pq(x, y) = p'q'(x, y) + 2bp'(x, y) + 2aq'(x, y) + 4ab + 2a + 2b + 1$, which contradicts the assumption that $pq \in (2, x, y)$. Thus, either p or q must be in (x, y), i.e., $(2, x, y)$ is a prime ideal. Now, let I be an ideal of $\mathbb{Z}[x, y]$ such that $I \supsetneq (x, y)$. Then there is some $p(x, y) \in I$ that can be written $p'(x, y) + 2a + 1$ where $p'(x, y) \in (x, y)$ and $a \in \mathbb{Z}$. But then $p'(x, y) \in I$, so $2a + 1 = p(x, y) - p'(x, y) \in I$. Because $2 \in I$, $(2, 2a + 1) \subseteq I$. Of course, $\gcd(2, 2a + 1) = 1$ for all $a \in \mathbb{Z}$, so $(2, 2a + 1) = (1) = \mathbb{Z}[x, y]$. Thus we conclude that $(2, x, y)$ is maximal.

□

6. Prove that (x, y) is not a principal ideal in $\mathbb{Q}[x, y]$.

   Proof. Suppose it were; then there is some nonzero, nonunit $d \in \mathbb{Q}[x, y]$ such that $(d) = (x, y)$. $x, y \in (x, y) = (d)$, so there are $p, q \in \mathbb{Q}[x, y]$ such that $x = dp$ and $y = dq$. In 9.1.4 above, we showed that x and y are prime in $\mathbb{Q}[x, y]$, and d is not a unit, so q and p are both units. But then we have that $(x) = (d) = (y)$, a contradiction. □

7. Let R be a commutative ring with 1 Prove that a polynomial ring over R in more than one variable is not a principal ideal domain.

   Proof. Consider the polynomial ring in more than two variables, $R[x, y, ...]$ and suppose the ideal (x, y) were principal, i.e., there is some nonzero, non-unit $d \in R[x, y, ...]$ such that $(d) = (x, y)$. $x, y \in (x, y) = (d)$, so there are $p, q \in R[x, y, ...]$ such that $x = pd$ and $y = qd$. Now, x and y are both prime in $R[x, y, ...]$, and d is not a unit, so we have that q and p are both units. Then it immediately follows that $(x) = (d) = (y)$, a contradiction. □

9.2 Polynomial Rings Over Fields

Let F be a field and let x be an indeterminate over F.

1. Let $f(x) \in F[x]$ be a polynomial of degree $n \geq 1$ and let bars denote passage to the quotient $F[x]/(f(x))$. Prove that for each $\overline{g(x)}$ there is a unique polynomial $g_0(x)$ of degree $\leq n - 1$ such that $\overline{g(x)} = \overline{g_0(x)}$.

   Proof. $F[x]$ is a Euclidean Domain because F is a field; its norm N is given by the order of the polynomial. Therefore, for every $g \in F[x]$, there are some $q, g_0 \in F[x]$ such that $g = qf + g_0$ and $N(g_0) < N(f)$ or $g_0 = 0$. It follows that $\overline{g} = \overline{qf} + \overline{g_0} = \overline{g_0}$, as desired. □

2. Let F be a finite field of order q and let $f(x)$ be a polynomial in $F[x]$ of degree $n \geq 1$. Prove that $F[x]/(f(x))$ has q^n elements.

   Proof. $F[x]$ is a Euclidean Domain because F is a field; its norm N is given by the order of the polynomial. By the previous exercise, 9.2.1, above, $F[x]/(f(x))$ is an n dimentional vector space over F, so it isomorphic to F^n. F has q elements, so F^n has q^n elements. □

3. Let $f(x)$ be a polynomial in $F[x]$. Prove that $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Proof. Assume that $F[x]/(f(x))$ is a field. Then its only ideals are $\{0\}$ and (1). By the Lattice Isomorphism Theorem for Rings, there are no ideals between $(f(x))$ and $F[x]$, so $f(x)$ is irreducible. Now assume that $f(x)$ is irreducuble, then because $F[x]$ is a Principal Ideal Domain, $(f(x))$ must be maximal. Therefore, the quotient $F[x]/(f(x))$ can only have two ideals, and so it is a field. □

4. Let F be a finite field. Prove that $F[x]$ contains infinitely many primes.

   Proof. For the sake of contradiction, assume that $F[x]$ has finitely many primes $p_1, ..., p_k$. Let $r = p_1 \cdot p_2 \cdot, ..., \cdot p_k$ and $q = r + 1$. Then q is not prime, so there is some prime s, such that $s|q$. There are only finitely many primes and s is one of them, so $s|r$, the product of all primes. But then $s|(q-r) = 1$, and so s is a unit, which is a contradiction, because primes cannot be units. □

6. Describe briefly the ring structure for the following rings:

   (a) $\mathbb{Z}[x]/(2) \cong \mathbb{Z}/2\mathbb{Z}[x]$

   (b) $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$

   (c) $\mathbb{Z}[x]/(x^2) \cong \mathbb{Z}^2$

   (d) $\mathbb{Z}[x,y]/(x^2,y^2,2) \cong \{a + bx + cy + dxy | a,b,c,d \in \mathbb{Z}/2\mathbb{Z}\}$ For any $\alpha = a + bx + cy + dxy \in \mathbb{Z}[x,y]/(2,x^2,y^2)$,

   $$\begin{aligned}(a + bx + cy + dxy)^2 &= a^2 + b^2x^2 + c^2y^2 + dx^2y^2 \\ &\quad + 2abx + 2acy + 2adxy + 2bcxy + 2bdx^2y + 2cdxy^2 \\ &= a^2\end{aligned}$$

   so $\alpha^2 = 0$ when $a = 0$ and $\alpha^2 = 1$ when $a = 1$.

9.3 Polynomial Rings that are Unique Factorization Domains

3. Let F be a field. Prove that the set R of polynomials in $F[x]$ whose coefficient of x is 0 is a subring of $R[x]$, but R is not a U.F.D.

   Proof. Let $r, s \in R$; then $r + s$ has no first degree term, nor does rs. Thus R is a subring of $F[x]$. Observe that x^2 and x^3 are both irreducible in R as each would need to have a first degree factor. But $x^6 = (x^2)^3 = (x^3)^2$, and so x^6 has two distinct factorizations. □

9.4 Irreducibility Criteria

1. Determine whether the following polynomials are irreducible in the rings indicated. For those that are reducible, determine their factorization into irreducibles. The notation $\mathbb{F}_p$ denotes the finite field $\mathbb{Z}/p\mathbb{Z}$.

   (a) $x^2 + x + 1$ in $\mathbb{F}_2[x]$ is irreducible because it has no roots.

   (b) $x^3 + x + 1$ in $\mathbb{F}_3$ is irreducible because it has no roots.

   (c) $x^4 + 1 = x^4 - 4 = (x^2 - 2)(x^2 + 2)$ in $\mathbb{F}_5$.

   (d) $x^4 + 10x^2 + 1$ is irreducible in $\mathbb{Z}[x]$.

7. Prove that $\mathbb{R}[x]/(x^2 + 1)$ is a field which is isomorphic to the complex numbers.

   Proof. First, we notice that $x^2 + 1$ is irreducible in $\mathbb{R}[x]$ because it has no roots in $\mathbb{R}$, and so $C = \mathbb{R}[x]/(x^2 + 1)$ is a field. Observe that under the homomorphism to the quotient ring, $x^2 + 1 \mapsto 0 \implies x^2 \mapsto -1$. Moreover, every polynomial in $\mathbb{R}[x]$ is represented by some polynomial of degree 0 or 1 in the quotient field. For any $a + bx, c + dx \in C$, we see that $(a + bx) + (c + dx) = (a + c) + (b + d)x$ and $(a + bx)(c + dx) = ac + (ad + bc)x + bdx^2 = (ac - bd) + (ad + bc)x$ and so the laws of addition and multiplication for $\mathbb{C}$ hold in C. □

8. Prove that $K_1 = \mathbb{F}_{11}[x]/(x^2+1)$ and $K_2 = \mathbb{F}_{11}[y]/(y^2+2y+2)$ are both fields with 121 elements. Prove that the map which sends the element $p(\bar{x})$ of K_1 to the element $p(\bar{y}+1)$ of K_2 (where p is any polynomial with coefficients in $\mathbb{F}_{11}$) is well defined and gives a ring (hence field) isomorphism from K_1 to K_2.

Proof. x^2+1 is irreducible in $\mathbb{F}_{11}[x]$ and y^2+2y+2 is irreducible in $\mathbb{F}_{11}[y]$ because they have no roots. Thus, K_1 and K_2 are both fields. K_1 and K_2 are given by the polynomials of order ≤ 1 over $\mathbb{F}_{11}$ and so they have 121 elements. We call the map described above $\varphi : K_1 \to K_2$ and let $p(\bar{x}), q(\bar{x}) \in K_1$. If $p(\bar{x}) = q(\bar{x})$ in K_1, then $p(\bar{x}) - q(\bar{x}) = k(\bar{x}^2+1)$ for some $k \in \mathbb{Z}$. Then

$$\varphi(p(\bar{x}) - \varphi(q(\bar{x})) = \varphi(p(\bar{x}) - q(\bar{x})) = \varphi(k(\bar{x}^2 - 1)) = k(\bar{y}^2 + 2\bar{y} + 2) = 0$$

and so $\varphi(p(\bar{x})) = \varphi(q(\bar{x}))$, i.e., φ is well defined. Moreover, following the above argument backwards shows that φ is injective, and clearly it is a homomorphism. Because K_1 and K_2 both have 121 elements, φ must be surjective as well and hence an isomorphism. □

13. Prove that $p(x) = x^3 + nx + 2$ is irreducible over $\mathbb{Z}[x]$ whenever $n \neq 1, -3, -5$.

Proof. If $p(x)$ is reducible, that it factors into monic polynomials of orders 1 and 2. Therefore, p(x) is reducible if:

$$\begin{aligned} x^3 + nx + 2 &= (x^2 + ax + b)(x + c) \\ &= x^3 + (a+c)x^2 + (b+ac)x + bc \end{aligned}$$

This gives $bc = 2$, so $b \in \{\pm 1, \pm 2\}$. We also have that $a = -c$ and $n = b + ac$.

$$b = 2 \implies c = 1 \implies a = -1 \implies n = 1$$

$$b = 1 \implies c = 2 \implies a = -2 \implies n = -3$$

$$b = -1 \implies c = -2 \implies a = 2 \implies n = -5$$

$$b = -2 \implies c = 1 \implies a = -1 \implies n = -3$$

and so $p(x)$ is reducible when $n \in \{1, -3, -5\}$ and irreducible otherwise. □

9.5 Polynomial Rings Over Fields II

7. Prove that the additive and multiplicative groups of a field are never isomorphic.

Proof. Let F be a field; then, $0 = -1(1-1) = -1 + (-1)^2$, so $(-1)^2 = 1$. If there were an isomorphism between the multiplicative and additive groups of F, then -1 would have to map to an element whose additive inverse is itself, but the only F where such an element exists is $\mathbb{Z}/2\mathbb{Z}$, but in a finite field, the additive and multiplicative groups have different sizes. □

Part III

Modules and Vector Spaces

Chapter 10

Introduction to Module Theory

10.1 Basic Definitions and Examples

Let R be a ring with 1 and M be a left R-module.

1. Prove that $0m = 0$ and $(-1)m = -m$ for all $m \in M$.

   Proof. For any $r \in r$, $rm = (0 + r)m = 0m + rm$, so $0m = 0$. $0 = 0m = (1 - 1)m = m + (-1)m$, so $(-1)m = -m$. □

3. Assume that $rm = 0$ for some $r \in R$ and some $m \in M$ with $m \neq 0$. Prove that r does not have a left inverse.

   Proof. Suppose that there is an $s \in R$ such that $sr = 1$. Then we would have that $m = srm = s(rm) = s(0) = 0$, which contradicts the hypothesis. □

4. Let M be the module R^m described in Example 3 and let $I_1, I_2, ..., I_n$ be left ideals of R. Prove that the following are submodules of M:

   (a) $S = \{(x_1, .x_2, ..., x_n | x_i \in I_i)\}$

   Proof. Clearly, $0 \in S$. For any $(x_1, ..., x_n), (y_1, ..., y_n) \in S$ and $r \in R$, $x_i + y_i \in I_i$ and $rx_i \in I_i$ for all $i \leq n$, so S is a submodule. □

   (b) $S = \{(x_1, x_2, ..., x_n) | x_i \in R \text{ and } x_1 + x_2 + ... + x_n = 0\}$

   Proof. Clearly, $0 \in S$. For any $(x_1, ..., x_n), (y_1, ..., y_n) \in S$ and $r \in R$, $x_1 + ... + x_n + y_1 + ... + y_n = 0$ and $r(x_1 + ... + x_n)$, so S is a submodule. □

5. For any left ideal I of R define

$$IM = \left\{ \sum_{\text{finite}} a_i m_i | a_i \in I, m_i \in M \right\}$$

   to be the collection of all finite sums of elements of the form am where $a \in I$ and $m \in M$. Prove that IM is a submodule of M.

   Proof. Clearly? The empty sum is finite, so $0 \in IM$. The sum of two finite sums is finite, so IM is closed under sums, and for any $r \in R$ $r \sum a_i m_i = \sum r a_i m_i \in IM$ because $ra_i \in I$ for all I, so IM is also closed under action by R. □

6. Show that intesection of any nonempty collection of submodules of an R-module is a submodule.

   Proof. $\{M_\alpha\}_{\alpha \in J}$ be a nonempty collection of R-modules and let $M = \bigcap_{\alpha \in J} M_\alpha$. Then if $m_1, m_2 \in M$ and $r \in R$, $m_1 + m_2 \in M$ and $rm_1 \in M$ since $m_1 + m_2, rm_2 \in M_i$ for all $i \leq J$. □

8. An element of the R-module M is called a *torsion element* if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted

$$\text{Tor}(M) = \{m \in M | rm = 0, r \in R \setminus \{0\}\}$$

   (a) Prove that if R is an integral domain then $\text{Tor}(M)$ is a submodule of M (called the *torsion submodule*).

   Proof. Let $x, y \in \text{Tor}(M)$ and $r, s \in R$ such that $rx = sy = 0$. Then for any arbitrary $t \in R$, if $t = 0$, then $x + ty = x \in \text{Tor}(M)$, and otherwise, $rs \neq 0$, but $rs(x + ty) = s(rx) + rt(sy) = 0$, so $\text{Tor}(M)$ is a submodule. □

   (b) Give an example of a ring R and an R-module M such that $\text{Tor}(M)$ is not a submodule of M.

   Consider $R = \mathcal{M}^{2\times 2}(\mathbb{R})$, the ring of 2×2 matrices over $\mathbb{R}$ as a 1-dimensional module, M. If $x = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $y = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, then $xy = 0$, so $x, y \in \text{Tor}(M)$. However, $x + y = I \notin \text{Tor}(M)$.

   (c) If R has zero divisors, show that every nonzero R-module has nonzero torsion elements.

   Proof. Suppose that $a, b \in R$ are 0-divisors such that $ab = 0$. Then if M is a nonzero R-module and $m \in M$, then $bm \in M$, and $a(bm) = 0$, so $bm \in \text{Tor}(M)$. □

9. If N is a submodule of M, the *annihilator of N in R* is defined to be

$$\text{Ann}_R(N) = \{r \in R | rn = 0 \text{ for all } n \in N\}$$

Prove that the annihilator of N in R is a 2-sided ideal of R.

Proof. $\text{Ann}_R(N)$ is closed under addition since if $r, s \in \text{Ann}_R(N)$, then $(r + s)n = 0 + 0 = 0$. For any $t \in R$, $trn = t0 = 0$, so $\text{Ann}_R(N)$ is a left ideal. Moreover, since N is a submodule and $t \in R$, $tn \in N$, and since r is an annihilator, $r(tn) = rt(n) = 0$, so $\text{Ann}_R(N)$ is also a right ideal. □

15. If M is a finite abelian group then M is naturally a Z-module. Can this action be extended to make M into a $\mathbb{Q}$-module?

Observe that under the natural $\mathbb{Z}$-action, there is a $z \in \mathbb{Z}^+$ such that $zm = 0$ for each $m \in M$. Then by exercise 3, z cannot have a left inverse, so the $\mathbb{Z}$-action cannot be extended to $\mathbb{Q}$.

18. Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$, and let T be the linear transformation from V to V which is rotation clockwise about the origin by $\frac{\pi}{2}$ radians. Show that V and 0 are the only $F[x]$-submodules for this T.

Proof. If U, a submodule of V, has any nontrivial vector v, it also has Tv, which is orthogonal to v. Hence, U has at least two linearly independent vectors and must be all of V. □

19. Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$, and let T be the linear transformation from V to V which is projection onto the y-axis. Show that V, 0, the x-axis, and the y-axis are the only $F[x]$-submodules for this T.

Proof. It is clear that each of these subspaces is indeed a submodule under the action by $F[T]$. If a submodule U contains a u that has nontrivial x and y components, then u along with Tu form a basis for V, so $U = V$. □

20. Let $F = \mathbb{R}$, let $V = \mathbb{R}^2$, and let T be the linear transformation from V to V which is rotation clockwise about the origin by π radians. Show that every subspace of V is an $F[T]$-submodule.

Proof. Let U be a subspace of V. Then $TU = U$, so U is a $F[T]$-submodule. □

21. Let $n \in \mathbb{Z}^+, n > 1$ and let R be a ring of $n \times n$ matrices with entries from a field F. Let M be the set of $n \times n$ matrices with arbitrarty elements of F in the first column and zeros elsewhere. Show that M is a submodule of R when R is considered as a left module over itself, but M is not a submodule when R is considered as a right R-module.

    Proof. Clearly. For any $r \in R$ and $m \in M$, $rm \in M$, but $mr \notin M$. □

10.2 Quotient Modules and Module Homomorphisms

In these exercises R is a ring with 1 and M is a left R-module.

1. Use the submodule criterion to show that kernels and images of R-module homomorphisms are submodules.

    Proof. If $\varphi : M \to N$ is an R-module homomorphism and $x, y \in \ker \varphi$, then for any $r \in R$, $\varphi(x + ry) = \varphi(x) + r\varphi(y) = 0 + r0 = 0$, so $x + ry \in \ker \varphi$ as well. Moreover, if $x, y \in \varphi(M)$, then take any $\bar{x} \in \varphi^{-1}(x)$ and $\bar{y} \in \varphi^{-1}(y)$ and see that $\varphi(\bar{x} + r\bar{y}) = x + ry$. □

2. Show that the relation "is R-module isomorphic to" is an equivalence relation on any set of R-modules.

    Proof. Clearly. □

3. Give an explicit example of a map from one R-module to another which is a group homomorphism but not an R-module homomorphism.

    Let $R = \mathcal{M}_{2\times 2}(\mathbb{R})$, $M = R$, and $N = \mathbb{R}^2$, with the module induced by applying A to x for any $A \in R$ and $x \in N$. Let $\varphi : M \to N$ by $\varphi(A) = (A_{1,1}, A_{2,2})$. φ is clearly a group homomorphism, but

    $$\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right) = (1,0) \neq (0,0) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}(0,0)$$

4. Let A be any $\mathbb{Z}$-module, let a be any element of A and let n be a positive integer. Prove that the map $\varphi_a : \mathbb{Z}/n\mathbb{Z} \to A$ given by $\varphi(\bar{k}) = ka$ is a well defined $\mathbb{Z}$-module homomorphism iff $na = 0$. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$, where $A_n = \{a \in A | na = 0\}$ (so A_n is the annihilator in A of the ideal (n) of $\mathbb{Z}$).

    Proof. Suppose that $k \equiv k' \mod n$, i.e., $k - k' = cn$ for some $c \in \mathbb{Z}$. Then

    $$\varphi(k) = \varphi(k') \iff ka = k'a \iff ka - k'a = 0 \iff cna = 0(\text{ for all } c) \iff na = 0$$

    $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, A) \cong A_n$ because $\varphi_a(1) = a = b = \varphi_b(1)$ iff $a = b$. □

5. Exhibit all $\mathbb{Z}$-module homomorphisms from $\mathbb{Z}/30\mathbb{Z}$ to $\mathbb{Z}/21\mathbb{Z}$.

    By 10.2.4, $\mathrm{Hom}(\mathbb{Z}/30Z, \mathbb{Z}/21\mathbb{Z}) \cong \{a \in \mathbb{Z}/21\mathbb{Z} | 30a = 0\} = \{\varphi_0, \varphi_7, \varphi_{14}\}$.

6. Prove that $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n,m)\mathbb{Z}$.

    Proof. From 10.2.4 we have that $na \equiv_m 0$, so a must be a multiple of $\frac{m}{(n,m)}$. There are (n,m) such unique multiples, mod m. □

7. Let z be a fixed element in the center of R. Prove that the map $m \mapsto zm$ is an R-module homomorphism from M to itself. Show that for a commutative ring R, the map from R to $\mathrm{End}_R(M)$ given by $r \to rI$ is a ring homomorphism (where I is the identity homomorphism).

Proof. For any $x, y \in M$ and $r \in R$,

$$\varphi(x+y) = z(x+y) = zx + zy = \varphi(x) + \varphi(y) \text{ and } \varphi(rx) = zrx = rzx = r\varphi(x).$$

When R is commutative, all such maps are endomorphisms, so $r \to rI$ is clearly a ring homomorphism. □

9. Let R be commutative. Prove that $\text{Hom}_R(R, M)$ and M are isomorphic as left R-modules.

   Proof. Let $\Psi : \text{Hom}_R(R, M) \to M$ by $\Psi(\varphi) = \varphi(1)$. Then for any maps $\varphi, \psi \in \text{Hom}_R(R, M)$ and $r \in R$, $\Psi(\varphi + r\psi) = (\varphi + r\psi)(1) = \varphi(1) + r\psi(1) = \Psi(\varphi) + r\Psi(\psi)$, so Ψ is a module homomorphism.

   To see that Ψ is an isomorphism, consider the map $\Theta : M \to \text{Hom}_R(R, M)$ defined by $\Theta(m) = r \mapsto rm$. For any $m, n \in M$ and $r \in R$, $\Theta(m + rn) = s \mapsto (m + rn)s = s \mapsto sm + rsn = \Theta(m) + r\Theta(n)$. Now for any $\varphi : R \to M$ and $m \in M$,

   $$(\Theta \circ \Psi(\varphi))(r) = \Theta(\varphi(1))(r) = (s \mapsto s\varphi(1))(r) = r\varphi(1) = \varphi(r)$$

   and

   $$(\Psi \circ \Theta)(m) = \Psi(s \mapsto sm) = 1m = m.$$

   Thus, Ψ and Θ are inverses and Ψ is an isomorphism. □

10. Let R be commutative. Prove that $\text{Hom}_R(R, R)$ and R are isomorphic as rings.

    Proof. This is just an immediate corollary of 4.1.9. □

11. Let $A_1, ..., A_n$ be R-modules and let B_i be a submodule of A_i. Prove that

    $$(A_1 \times ... \times A_n)/(B_1 \times ... \times B_n) \cong (A_1/B_1) \times ... \times (A_n/B_n).$$

    Proof. We prove the claim for $n = 2$ and then the result follows for all n by induction. Let

    $$\begin{aligned} \varphi : (A_1 \times A_2) &\to (A_1/B_1) \times (A_2/B_2) \\ (x_1, x_2) &\mapsto (x_1 + B_1, x_2 + B_2) \end{aligned}$$

    For any $x_1, y_1 \in A_1$, $x_2, y_2 \in A_2$, and $r \in R$,

    $$\begin{aligned} \varphi((x_1 + ry_1, x_2 + ry_2)) &= (x_1 + ry_1 + B_1, x_2 + ry_2 + B_2) \\ &= (x_1 + B_1, x_2 + B_2) + r(y_1 + B_1, y_2 + B_2) = \varphi(x_1, x_2) + r\varphi(y_1, y_2) \end{aligned}$$

    so φ is a module homomorphism. $(x_1, x_2) \in \ker\varphi$ iff $(x_1 + B_1, x_2 + B_2) = (B_1, B_2)$ iff $(x_1, x_2) \in (B_1, B_2)$, so $\ker\varphi = (B_1, B_2)$. Surjectivity is clear, so the claim follows from the first isomorphism theorem. □

10.3 Generation of Modules, Direct Sums, and Free Modules

In these execises R is a ring with 1 and M is a left R-module.

1. Prove that if A and B are sets of the same cardinality, then the free modules $F(A)$ and $F(B)$ are isomorphic.

   Proof. Let $\alpha : A \to B$ be a bijection, $\iota_A : A \hookrightarrow F(A)$, and $\iota_B : B \hookrightarrow F(B)$, then $\iota_B \circ \alpha$ is a map $A \to F(B)$. Thus, by the universal property, there is a map $\varphi : F(A) \to F(B)$ such that $\varphi \circ \iota_A = \iota_B \circ \alpha$. Similarly, there is a map $\psi : F(B) \to F(A)$ such that $\psi \circ \iota_B = \iota_A \circ \alpha^{-1}$. For any $a \in A$, $\psi \circ \varphi(a) = \psi(\alpha(a)) = \alpha^{-1}(\alpha(a)) = b$. Similarly, $\varphi \circ \psi(b) = b$ for any $b \in B$. □

3. Show that the $F[x]$-modules in 10.1.18 and 10.1.19 are both cyclic.

   Proof. In the case of 10.1.18, $T : V \to V$ is the linear transformation that is a clockwise rotation of $\frac{\pi}{2}$ radians. Then $V = \mathbb{R}^2 = \mathbb{R}[T](0,1)$ because $T(0,1) = (1,0)$.

   In the case of 10.1.19, $T : V \to V$ is projection onto the y-axis. Then $V = \mathbb{R}^2 = \mathbb{R}[T](1,1)$ because $T(1,1) = (0,1)$. □

4. An R-module M is called a torsion module if for each $m \in M$ there is a nonzero element $r \in R$ such that $rm = 0$, where r may depend on m. Prove that every finite abelian group is a torsion $\mathbb{Z}$-module. Give an example of an infinite abelian group that is a torsion $\mathbb{Z}$-module.

   Proof. For any finite abelia group A, $|A|a = 0$ for all $a \in A$, so A is a torsion $\mathbb{Z}$-module. $\mathbb{Q}$ is an example of an infinite abelian group is a torsion $\mathbb{Z}$-module. □

5. Let R be an integral domain. Prove that every finitely generated torsion R-module has a nonzero annihilator. Give an example of an R-module whose annihilator is the zero ideal.

   Proof. Let M be a finitely generated torsion R-module with generators $\{x_1, ..., x_n\}$. Since M is torsion, there are nonzero $\{r_1, ..., r_m\}$ such that $r_i x_i = 0$ for all $i \leq n$. Let $r = \text{lcm}(\{r_1, ..., r_n\})$. $r \neq 0$ becausse R is an integral domain. To each r_i, there is a k_i such that $k_i r_i = r$, so $r x_i = k_i r_i x_i = 0$. For an arbitrary $m \in M$, we can write $m = a_1 x_1 + ... + a_n x_n$. Then $rm = r a_1 x_1 + ... + r a_n x_n = a_1 r x_1 + ... + a_n r x_n = 0$, so (r) annihilates M. □

   $\text{Ann}(\mathbb{Q}) = (0)$.

6. Prove that if M is a finitely generated R-module that is generated by n elements then every quotient of M may be generated by n (or fewer) elements.

   Proof. Let M be generated by $\{m_1, ..., m_n\}$ and let N be a submodule of M. For any $x \in M$, we can write $x = a_1 m_1 + ... + a_n m_n$. Thus, for any $x + N \in N/M$, we can write

   $$x + N = a_1 m_1 + ... + a_n m_n + N = a_1 m_1 + N + ... + a_n m_n + N$$

   so $\{m_1 + N, ..., m_n + N\}$ generates M/N. Some of these terms may be trivial. By this result, quotients of cyclic modules can have at most 1 generator and hence are also cyclic. □

7. Let N be a submodule of M. Prove that if both M/N and N are finitely generated, then so is M.

   Proof. Let M N be generated by $\{a_1 + N, ..., a_m + N\}$ and let N be generated by $\{b_1, ..., b_n\}$. For any $x \in M$, $x + N = r_1 a_1 + ... + r_m a_m + N$ for some $r_1, ..., r_m \in R$. Let $\bar{x} = r_1 a_1 + ... + r_m a_m$ such that $x - \bar{x} = s_1 b_1 + ... + s_n b_n \in N$ for some $s_1, ..., s_n \in R$. Then $x = r_1 a_1 + ... + r_m a_m + s_1 b_1 + ... + s_n b_n$, so $\{a_1, ..., a_m, b_1, ..., b_n\}$ is a (not necessarily minimal) generating set. □

9. An R-module M is called *irreducible* if $M \neq 0$ and if 0 and M are its only submodules. Show that M is irreducible iff $M \neq 0$ and M is a cyclic module with any nonzero element as its generator.

   Proof. If M is irreducible and x and y are nonzero generators of M, then $Rx = Ry = M$, so $x = y$. Thus, M is cyclic. The other way is clear. The irreducible $\mathbb{Z}$ modules must then be given by $\mathbb{Z}/p\mathbb{Z}$ for any prime p. □

10. Assume R is commutative. Show that an R-module M is irreducible iff M is isomorphic to R/I where I is a maximal ideal of R.

Proof. Assume M is irreducible and define $\varphi : R \to M$ by $\varphi(r) = rm$ for some nonzero $m \in M$. $\ker \varphi$ must be maximal because M has no nontrivial quotients and φ is surjective by 10.3.9. Conversely, if $M \cong R/I$ for some maximal ideal I, then R/I is cyclic and so M is irreducible by 10.3.9. □

11. Show that if M_1 and M_2 are irreducible R-modules, then any nonzero R-module homomorphism from M_1 to M_2 is an isomorphism. Deduce that if M is irreducible then $\text{End}_R(M)$ is a division ring.

    Proof. Let m_1 be a nonzero element of M_1 and let $\varphi : M_1 \to M_2$ be a nontrivial homomorphism so that $\varphi(m_1) \neq 0$. Then $\varphi(m_1)$ must generate M_2 because M_2 was assumed to be irreducible. Any map that takes a generator of a cyclic module to a generator of another cyclic module is an isomorphsim. Thus, every morphism in $\text{End}_R(M)$ is invertible or 0. Thus, $\text{End}_R(M)$ is a division ring. □

Chapter 11

Vector Spaces

11.1 Definitions and Basic Theory

4. Prove that the space of real-valued functions on the closed interval $[a, b]$ is an infinite dimensional vector space over $\mathbb{R}$.

   Proof. For any two functions $f, g : [a, b] \to \mathbb{R}$ and any $\lambda \in \mathbb{R}$, $f + \lambda g$ is also a function $[a, b] \to \mathbb{R}$. Observe that the set of monic monomials, $\mathcal{B} = \{1, x, x^2, ...\}$, is linearly independent, so $\mathcal{F}(\mathbb{R})$ cannot be finitely spanned. □

5. Prove that the space of continuous real-valued functions on the closed interval $[a, b]$ is an infinited dimensional vector space over $\mathbb{R}$.

   Proof. See 11.1.4. □

6. Let V be a vector space of finite dimension. If φ is any linear transformation from V to V prove there is an integer m such that $\varphi^m(V) \cap \ker\varphi = 0$.

   Proof. Let $U_n = \varphi^n(V)$. For any n, $\dim U_{n-1} = \dim U_n + \dim(\ker\varphi \cap U_{n-1})$. If $\dim(\ker\varphi \cap U_{n-1}) = 0$, there is nothing to show. Otherwise, $\dim U_n < \dim U_{n-1}$, and this process must eventually terminate. □

11.2 The Matrix of a Linear Transformation

9. If W is a subspace of the vector space V stable under the linear transformation φ, show that φ induces linear transformations $\varphi|_W$ on W and $\tilde{\varphi}$ on V/W. If $\varphi|_W$ and $\tilde{\varphi}$ are nonsingular, prove that φ is nonsingular. Prove that the converse holds if V has finite dimension and give a counterexample when V is infinite dimensional.

   Proof. That $\varphi|_W$ is a linear transformation on W it is immediate that $\varphi|_W : W \to W$ is linear from the fact that φ stabilizes W. Let $\tilde{\varphi} : V/W \to V/W$ by $\tilde{\varphi}(x + W) = \varphi(x) + W$. $\tilde{\varphi}$ is clearly well defined since $x + W = y + W$ iff $x - y \in W$ iff $\varphi(x - y) \in W$ iff $\varphi(x) + W = \varphi(y) + W$.

   If $\varphi|_W$ and $\tilde{\varphi}$ are nonsingular, then they have inverses $\varphi|_W^{-1}$ and $\tilde{\varphi}^{-1}$. Let $\bar{\varphi} : V \to V$ be defined by $\bar{\varphi}(x + w) = \tilde{\varphi}^{-1}(x) + \varphi|_W^{-1}(w)$ for any $w \in W$ and $x \in V/W$. Then for any $x \in V$, and $w \in W$,

   $$\bar{\varphi} \circ \varphi(x + w) = \bar{\varphi}(\tilde{\varphi}(x) + \varphi|_W(x)) = x + w$$

   so $\bar{\varphi}$ is an inverse for φ. When V is finite-dimensional, nonsingularity is equivalent to invertibility, so φ^{-1} can be split as described above, giving rise to inverses for $\tilde{\varphi}$ and $\varphi|_W$. However, if V is infinite dimensional, φ may not be invertible. For example, consider the infinite dimensional vector space $\mathbb{R}[x]$ and the map $\varphi : p(x) \mapsto xp(x)$. Observe that φ is nonsingular and stabilizes $x\mathbb{R}[x]$. However, in this case $\tilde{\varphi} : \mathbb{R} \to \mathbb{R}$ is the 0 map. □

11. Let φ be a linear transformation from the finite dimensional vector space V to itself such that $\varphi^2 = \varphi$.

    (a) Prove that $\operatorname{im}\varphi \cap \ker\varphi = 0$.

    Proof. If $v \in \operatorname{im}\varphi$, then $\varphi(v) = v$, so if $v \in \ker\varphi$ as well, then $v = 0$. □

    (b) Prove that $V = \operatorname{im}\varphi \oplus \ker\varphi$.

    Proof. For any $v \in V$, let $x = v - \varphi(v)$. Then $\varphi(x) = \varphi(v) - \varphi^2(v) = 0$, so $x \in \ker\varphi$ and $v \in \operatorname{im}\varphi \oplus \ker\varphi$. The claim follows since we showed that $\ker\varphi$ and $\operatorname{im}\varphi$ intersect trivially in (a). □

    (c) Prove that there is a basis of V such that the matrix of φ with respect to this basis is a diagonal matrix whose entries are all 0 or 1.

    Proof. Any basis for $\operatorname{im}\varphi$ and $\ker\varphi$, put together should do the trick. □

12. Let $V = \mathbb{R}^2$, $v_1 = (1, 0), v_2 = (0, 1)$, so that v_1, v_2 are a basis for V. Let $\varphi : V \to V$ be defined by the matrix $\begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$. Prove that if W is the subspace generated by v_1 then W is stable under action of φ. Prove that there is no subspace W' invariant under φ so that $V = W \oplus W'$.

    Proof. For any $\lambda \in \mathbb{R}$, $\varphi(\lambda v_1) = \lambda\varphi(v_1) = 2\lambda v_1$ so $\varphi(W) = W$. If $V = W \oplus W'$, then $\dim W' = 1$, so $W' = \{\lambda w | \lambda \in \mathbb{R}\}$ for some $w \in V$. We right $w = \alpha v_1 + \beta v_2$, since v_1, v_2 form a basis for V. Since $\varphi(v_2) = (1, 2) = v_1 + 2v_2$, $\varphi(w) = \alpha\varphi(v_1) + \beta\varphi(v_2) = (2\alpha + \beta)v_1 + 2\beta v_2$. Therefore, W' is only invariant under action by φ if $\beta = 1$, but then $V \neq W \oplus W'$. □

38. Let $A \in M^{m\times m}$ and $B \in M^{n\times n}$ be square matrices. Prove that the trace of their Kronecker product is the product of their traces: $\operatorname{tr}(A \otimes B) = \operatorname{tr}(A)\operatorname{tr}(B)$.

    Proof. Let $A = (a_{ij})$ and $B = (b_{kl})$. Then

$$\operatorname{tr}(A \otimes B) = \sum_{i\leq m} a_{ii}\operatorname{tr}(B) = \operatorname{tr}(A)\operatorname{tr}(B)$$

□

11.3 Dual Vector Spaces

2. Let V be the collection of polynomials with coefficients in $\mathbb{Q}$ in the variable x of degree at most 5 with $1, x, x^2, ..., x^5$ as a basis. Prove that the following are elements of the dual space of V and express them as linear combinations of the dual basis: Let $v_i : V \to \mathbb{Q}$ by $v_i(x^j) = 1$ if $i = j$ and zero otherwise.

    (a) $E : V \to \mathbb{Q}$ defined by $E(p(x)) = p(3)$.

$$E = \sum_{0\leq i\leq 5} 3^i v_i$$

    (b) $\varphi : V \to \mathbb{Q}$ defined by $\varphi(p(x)) = \int_0^1 p(t)dt$.

$$\varphi = \sum_{0\leq i\leq 5} \frac{v_i}{i+1}$$

(c) $\varphi : V \to \mathbb{Q}$ defined by $\varphi(p(x)) = \int_0^1 t^2 p(t)dt$.

$$\varphi = \sum_{0\leq i\leq 5} \frac{v_i}{i+3}$$

(d) $\varphi : V \to \mathbb{Q}$ defined by $\varphi(p(x)) = p'(5)$.

$$\varphi = \sum_{1\leq i\leq 5} iv_{i-1}$$

3. Let S be any subset of V^* for some finite dimensional space V. Define $\text{Ann}(S) = \{v \in V | f(v) = 0 \text{ for all } f \in S\}$ called the *annihilator of* S in V.

(a) Prove that $\text{Ann}(S)$ is a subspace of V.

Proof. For any $v, w \in \text{Ann}(S)$, $f \in S$, and any $\lambda \in K$ (the ground field of V),

$$f(v + \lambda w) = f(v) + \lambda f(w) = 0$$

so $\text{Ann}(S)$ is indeed a subspace of V. □

(b) Let W_1 and W_2 be subspaces of V^*. Prove that $\text{Ann}(W_1 + W_2) = \text{Ann}(W_1) \cap \text{Ann}(W_2)$ and $\text{Ann}(W_1 \cap W_2) = \text{Ann}(W_1) + \text{Ann}(W_2)$.

Proof. Clearly. □

(c) Let W_1 and W_2 be subspaces of V^*. Prove that $W_1 = W_2$ iff $\text{Ann}(W_1) = \text{Ann}(W_2)$.

Proof. Immediate from (d). □

(d) Prove that the annihilator of S is the same as the annihilator of the subspace of V^* spanned by S.

Proof. Let $W = \operatorname{span} S$. That $\text{Ann}(W) \subseteq \text{Ann}(S)$ is trivial. Conversely, let $w \sum \lambda_i s_i \in W$ where each $s_i \in S$ and $\lambda_i \in K$. Then for any $v \in \text{Ann}(S)$,

$$w(v) = \sum \lambda s_i(v) = 0$$

so $v \in \text{Ann}(W)$ as well. □

(e) Assume V is finite dimensional with basis $v_1, ..., v_n$. Prove that if $S = \{v_1^*, ..., v_k^*\}$ for some $k \leq n$, then $\text{Ann}(S) = \text{span}\{v_{k+1}, ..., v_n\}$.

Proof.

$$v \in \text{Ann}(S) \iff v_i^*(v) = 0 \text{ for all } i \leq k \iff v \in \text{span}\{v_{k+1}^*, ..., v_n^*\}.$$

□

(f) Assume V is finite dimensional. Prove that if W^* is any subspace of V^* then $\dim \text{Ann}(W^*) = \dim V - \dim W^*$.

Proof. Pick a basis $v_1^*, ..., v_k^*$ for W^* and extend it to a basis $v_1^*, ..., v_n^*$ for V^*. Then the claim follows immediately from (e). □

4. If V is infinite dimensional with basis $\mathcal{A}$, prove that $\mathcal{A}^* = \{v^* | v \in \mathcal{A}\}$ does *not* span V^*.

Proof. Define $f : V \to K$ by

$$f\left(\sum_{v_n\in\mathcal{A}} \alpha_n v_n\right) = \sum_{v_n\in\mathcal{A}} \alpha_n$$

Note that f is well defined since $v \in V$ will always be a finite sum of components of $\mathcal{A}$. However, f can clearly not be written as a finite sum of components of $\mathcal{A}^*$. □

11.4 Determinants

3. Let R be any commutative ring with 1, let V be an R-module and let $x = (x_i)_{i \leq n} \in V$. Assume that for some $A \in M_{n \times n}(R)$, $Ax = 0$. Prove that $(\det A)x_i = 0$ for all $i \leq n$.

   Proof. If $\det A = 0$, the claim is trivial. Otherwise, note that $B = \sum x_i A_i = Ax = 0$ where A_i are the columns of A. Then by Cramer's Rule, $x_i \det A = \det(A_1, ..., A_{i-1}, 0, A_{i+1}, ..., A_n) = 0$. □

Chapter 12

Modules over Pricipal Ideal Domains

12.1 The Basic Theory

1. Let M be a module over the integral domain R.

   (a) Suppose x is a nonzero torsion element in M. Show that x and 0 are "linearly dependent." Conclude that the rank of $\operatorname{Tor}(M)$ is 0, so that in particular any torsion R-module has free rank 0.

   Proof. If $x \in \operatorname{Tor}(M)$, there is a nonzero $r \in R$ such that $rx = rx + 0 = 0$, so it is immediate that x and 0 are linearly dependent. Moreover, if $y \in \operatorname{Tor}(M)$ as well with annihilator s, then $rx + sy = 0$, so there are no linearly independent torsion elements of $\operatorname{Tor}(M)$. □

   (b) Show that the rank of M is the same as the rank of the (torsion free) quotient $M/\operatorname{Tor}(M)$.

   Proof. $\operatorname{rank} M/\operatorname{Tor}(M) = \operatorname{rank} M - \operatorname{rank}\operatorname{Tor}(M) = \operatorname{rank} M$. □

2. Let M be a module over the integral domain R.

   (a) Suppose that M has a rank n and that $x_1, ..., x_n$ is any maximal set of linearly independent elements of M. Let $N = Rx_1 + ... + Rx_n$ be the submodule generated by $x_1, ..., x_n$. Prove that N is isomorphic to R^n and that the quotient M/N is a torsion R-module (equivalently, the elements $x_1, ..., x_n$ are linearly independent and for any $y \in M$ there is a nonzero $r \in R$ such that ry can be written as a linear combination $r_1x_1 + ... + r_nx_n$ of the x_i).

   Proof. Note that N has n linearly independent elements, so it has rank n, as it is a submodule of M, a rank n R-module. Moreover, N must be torsion free, as it is generated entrirely by non-torsion elements. Hence $N \cong R^n$. It follows that $\operatorname{rank} M/N = \operatorname{rank} M - \operatorname{rank} N = 0$, so M/N is torsion. □

   (b) Prove conversely that if M contains a submodule N that is free of rank n such that the quotient M/N is torsion, then M has rank n.

   Proof. Let $y_1, ..., y_{n+1}$ be any $n+1$ elements of M and let $x_1, ..., x_n$ be a basis for N. Since M/N is torsion, there is an $r_i \in R$ to each y_i such that $r_iy_i = a_1x_1 + ... + a_nx_n$ for some $a_i \in R$. Thus, it is clear that the r_iy_i are linearly independent, and so too are the y_i. □

5. Let $R = \mathbb{Z}[x]$ and let $M = (2, x)$ be the ideal generated by 2 and x, considered as a submodule of R. Show that $\{2, x\}$ is not a basis for M. Show that the rank of M is 1, but its free rank is not 1.

Proof. Observe that $2 \in M$ and $-x \in M$, so 2 and x are linearly dependent since $-x(2) + 2(x) = 0$.

Let $x_1 = \alpha_1(2)+\beta_1(x)$ and $x_2 = \alpha_2(2)+\beta_2(x)$, where $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{Z}$. Similarly, for any $a, b \in M\backslash\{0\}$, $b(a) - a(b) = 0$, so no two nontrivial elements are linearly independent. However, for any $m, n \in M$,

$ma + n0 = 0$ iff $m = 0$, so nontrivial vectors are linearly independent form 0, hence rank $M = 1$. If M had a free rank of 1, it would be isomorphic to R, i.e., $M = aR$ for some $a \in R$. If so, then we have $ar = 2$ for some $r \in R$. Thus, $a \in \{\pm 1, \pm 2\}$, but clearly, $a \neq \pm 1$, since $M \neq R$. However if $a = 2$, then $x = 2r$ for some $r \in R$, but no such r exists. Thus, M does not have free rank 1. □

6. Show that if R is an integral domain and M is any nonprincipal ideal of R then M is torsion free of rank 1 but is not a free R-module.

   Proof. This is just a generalization of exercise 5. □

7. Let R be any ring, let $A_1, ..., A_m$ be R-modules and let B_i be a submodule of A_i, $1 \leq i \leq m$. Prove that
$$(A_1 \oplus ... \oplus A_m)/(B_1 \oplus ... \oplus B_m) \cong (A_1/B_1) \oplus ... \oplus (A_m/B_m).$$

   Proof. For convenience, let $\mathcal{A} = A_1 \oplus ... \oplus A_m$, $\mathcal{B} = B_1 \oplus ... \oplus B_m$, and $\mathcal{Q} = (A_1/B_1) \oplus ... \oplus (A_m/B_m)$. We define
$$\varphi : \mathcal{A}/\mathcal{B} \to \mathcal{Q} \text{ by } \varphi : (a_1, ..., a_m) + \mathcal{B} \mapsto (a_1 + B_1, ..., a_m + B_m)$$
□

   Suppose that $\alpha + \mathcal{B} = (a_1, ..., a_m) + \mathcal{B} = \alpha' + B = (a'_1, ..., a'_m) + B$. Then there is a $\beta = (b_1, ..., b_m) \in \mathcal{B}$ such that $\alpha - \alpha' = \beta$. Then for each i $a_i - a'_i = b_i \in B_i$, so $\varphi(\alpha + \mathcal{B}) = \varphi(\alpha' + \mathcal{B})$, i.e., φ is well defined. Reversing this argument shows that φ is injective, and clearly φ is surjective.

9. Give an example of an integral domain R and a nonzero torsion R-module M such that $\text{Ann}(M) = 0$. Prove that if N is any finitely generated torsion R-module, then $\text{Ann}(N) \neq 0$.

   Proof. Consider $\mathbb{Q}/\mathbb{Z}$ as a $\mathbb{Z}$-module. $\text{Ann}(\mathbb{Q}/\mathbb{Z}) = 0$ since for any $r \in \mathbb{Z}$, simply pick s, corime to r, and see that $rs \neq 0$.

   When N is a finitely generated torsion R-module, simply let $r = r_1...r_m$ where $r_i a_i = 0$ for each generator a_i. Then $ra_i = 0$ for all a_i, and hence $r \in \text{Ann}(N)$. □

13. If M is a finitely generated module over the P.I.D. R, describe the structure of $M/\operatorname{Tor}(M)$.

    $M/\operatorname{Tor}(M)$ will be a free R-module with the same rank as the free rank of M.

15. Prove that if R is a Noetherian ring then R^n is a Noetherian R-module.

    Proof. We proceed by induction on n. In the base case, when $n = 1$, the claim is trivial. Assume that R^n is a Noetherian module for some $n \geq 1$. Consider the set $N = \{(x_1, ..., x_n) | (x_1, ..., x_n, a) \in M \text{ for some } a \in R\}$. It is easy to see that $N \subseteq R^n$ is a submodule since $r(x_1, ..., x_n, a) = (rx_1, ..., rx_n, ra) \in M$. Since R^n is Noetherian, N is finitely generated by $m_1, ..., m_k$. We abuse notation and append a 0 as the last coordinate of each m_i, so we can think of m_i as an element of R^{n+1}.

    Let $A = \{(0, ..., 0, a) | (x_1, ..., x_n, a) \in M \text{ for some } x_1, ..., x_n \in R\}$ and note that A can be thought of as a submodule of R if we ignore the leading zeros. Hence, A is also finitely generated by some $a_1, ..., a_l$. Now note that $M \subseteq N + A$, so every $m \in M$ can be written as an R-linear combination of m_i's and a_j's. Thus, M is finitely generated, and so R^{n+1} is a Noetherian module. Hence, by induction, R^n is a Noetherian module for any n. □

12.2 The Rational Canonical Form

1. Prove that similar linear transformations of V (or $n \times n$ matrices) have the same characteristic and the same minimal polynomial.

   Proof. If $\sigma, \tau : V \to V$ are similar, they have the same eigenvalues and multiplicities. Since the characteristic polynomial of a linear transformation is that which has the eigenvalues with their respective multiplicities at roots, σ and τ must have the same characteristic polynomial. If the similarity between σ and τ is witnessed by $\varphi : V \to V$, so that $\varphi\sigma\varphi^{-1} = \tau$, then for any $k \in \mathbb{Z}$ and $\alpha \in F$, $\alpha(\varphi\sigma\varphi^{-1})^k = \varphi(\alpha\sigma^k)\varphi^{-1}$. Therefore, if $m_\sigma(x)$ is the minimal polynomial for σ, then by linearity,

   $$m_\sigma(\tau) = m_\sigma(\varphi\sigma\varphi^{-1}) = \varphi m_\sigma(\sigma)\varphi^{-1} = 0$$

   and since $m_\sigma(x)$ is irreducible, it must be the minimal polynomial for τ as well. □

3. Prove that two 2×2 matrices over F which are not scalar matrices are similar if and only if they have the same characteristic polynomial.

   Proof. We have already showed that if A and B are similar, their minimal and characteristic polynomials are equal. Conversely, if $c_A(x) = c_B(x)$ and A and B are not scalar, then $c_A(x)$ and $c_B(x)$ must have two invariant factors. That is, $m_A(x) = m_B(x) = c_A(x) = c_B(x)$, and so A and B share a rational canonical form (and are both similar to it). □

4. Prove that two 3×3 matrices are similar if and only if they have the same characteristic and same minimal polynomials.

   Proof. We have already showed that if A and B are similar, their minimal and characteristic polynomials are equal. Conversely, if $c_A(x) = c_B(x)$ and A and B are not scalar, then $c_A(x)$ and $c_B(x)$ must have two or three invariant factors. Either way, the rational canonical form is fully determined, and A and B are both similar to it.

   If A and B are 4×4, this does not necessarily hold. For example, if

   $$A = \begin{pmatrix} \lambda & & & \\ & \lambda & & \\ & & 0 & -\lambda^2 \\ & & 1 & 2\lambda \end{pmatrix} \text{ and } \begin{pmatrix} 0 & -\lambda^2 & & \\ 1 & 2\lambda & & \\ & & 0 & -\lambda^2 \\ & & 1 & 2\lambda \end{pmatrix}$$

   then $m_A(x) = m_B(x) = (x - \lambda)^2$ and $c_A(x) = c_B(x) = (1 - \lambda)^4$, but these matrices are already in rational canonical form, and so it is easy to see they are not similar. □

5. Prove directly from the fact that the collection of *all* linear transformartions of an n dimensional vector space V over F to itself form a vector space over F of dimension n^2 that the minimal polynomial of a linear transformation T has degree at most n^2.

   Proof. Notice that the collection $\{T^0, T^1, ..., T^{n^2}\} \subseteq \text{End}(V)$ has $n^2 + 1$ elements and so they must be F-linearly *dependent*. Thus, there are $a_0, ..., a_{n^2} \in F$ such that $a_{n^2}T^{n^2} + ... + a_0 = 0$. Now we can easily see that the polynomial $f(x) = a_{n^2}x^{n^2} + ... + a_0$ annihilates T, so that it is an upper bound for $m_T(x)$ (in terms of degree). □

6. Prove that the constant term in the characteristic polynomial of the $n \times n$ matrix A is $(-1)^n \det A$ and that the coefficient of x^{n-1} is the negative of the sum of the diagonal entries of A (called the *trace*). Prove that $\det A$ is the product of the eigenvalues of A and that the trace of A is the sum of the eigenvalues of A.

Proof. The constant term of any polynomial is given by its evaluation at 0. Hence

$$a_0 = c_A(0) = \det(0I - A) = (-1)^n \det A.$$

Since $c_A(x) = c'_A(x)$ if A and A' are similar, we need only consider the case in which A is in rational canonical form. In that case, if $\alpha_i(x) = a_{i,n}a^n + a_{i,n-1}a^{n-1} + ... + a_{i,0}$ for $i \in \{1, ..., k\}$ are the invariant factors, the only non-zero terms on the diagonal of A will be the $a_{i,n-1}$ for each i. Moreover, since $c_A(x) = \prod_{i \leq k} \alpha_i(x)$, we have that the $n - 1^{th}$ coefficient of $c_A(x)$ is given by $\sum_{i \leq k} a_{i,n-1} = \operatorname{tr} A$. Eigenvalues are the roots of the characteristic polynomial c_A, so it is clear that their sum is the $n - 1^{th}$ coefficient and their product the 0^{th}. □

11. Find all similarity classes of 6×6 matrices over $\mathbb{C}$ with the characteristic polynomial $(x^4 - 1)(x^2 - 1)$.

Proof. Note that $(x^4 - 1)(x^2 - 1) = (x - 1)^2(x + 1)^2(x + i)(x - i)$. The highest multiplicity is 2, so each class can have at most 2 invariant factors. The following options are possible:

(i) $a_1(x) = (x - 1)(x + 1)$, $a_2(x) = x^4 - 1$ in which case the similarity class is represented by:

$$\begin{pmatrix} 0 & 1 & & & & \\ 1 & 0 & & & & \\ & & 0 & 0 & 0 & 1 \\ & & 1 & 0 & 0 & 0 \\ & & 0 & 1 & 0 & 0 \\ & & 0 & 0 & 1 & 0 \end{pmatrix}$$

(ii) $a_1(x) = (x - 1)$, $a_2(x) = (x + 1)(x^4 - 1) = x^5 + x^4 - x - 1$ in which case the similarity class is represented by:

$$\begin{pmatrix} 1 & & & & & \\ & 0 & 0 & 0 & 0 & 1 \\ & 1 & 0 & 0 & 0 & 1 \\ & 0 & 1 & 0 & 0 & 0 \\ & 0 & 0 & 1 & 0 & 0 \\ & 0 & 0 & 0 & 1 & -1 \end{pmatrix}$$

(iii) $a_1(x) = (x + 1)$, $a_2(x) = (x - 1)(x^4 - 1) = x^5 - x^4 - x + 1$ in which case the similarity class is represented by:

$$\begin{pmatrix} -1 & & & & & \\ & 0 & 0 & 0 & 0 & -1 \\ & 1 & 0 & 0 & 0 & 1 \\ & 0 & 1 & 0 & 0 & 0 \\ & 0 & 0 & 1 & 0 & 0 \\ & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

(iv) $a_1(x) = (x^2 - 1)(x^4 - 1) = x^6 - x^4 - x^2 + 1$ in which case the similarity class is represented by:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

□

17. Determine the representatives for the conjugacy classes for $\mathrm{GL}_3(\mathbb{F}_2)$.

    Matrices will be determined by the characteristic and minimal polynomial. There are four degree 3 polynomials over $\mathbb{F}_2$ which do not vanish at 0. $(x+1)^3$ can have itself as a minimal polynomial or $x+1$ or x^2+1. The others, x^3+1, x^3+x^2+1, and x^3+x+1 must each also be the minimal polynomial when they are the characteristic polynomial.

18. Let V be a finite dimensional vector space over $\mathbb{Q}$ and suppose T is a nonsingular linear transformation of V such that $T^{-1} = T^2 + T$. Prove that the dimension of V is divisible by 3. If the dimension is precisely 3, prove that all such tranformations T are similar.

    Proof. Multiplying both sides by T, we get that $T^3 + T^2 - 1 = 0$. $x^3 + x^2 - 1$ is irreducible over $\mathbb{Q}$, so it is the minimal polynomial $m_T(x)$. $m_T(x)$ must divide the characterisitic polynomial $c_T(x)$ and $c_T(x)$ can have no factors that do not divide $m_T(x)$, so its only factor is $m_T(x)$. If the dimension of V is exactly 3, then $m_T(x) = c_T(x)$ and linear transformations in three-dimensional spaces are determined by their minimal and characteristic polynomials. □

Chapter 13

Field Theory

13.1 Basic Theory of Field Extensions

3. Show that $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and let θ be a root. Compute the powers of θ in $\mathbb{F}_2(\theta)$.

   Proof. Since the polynomial is degree three, it is irreducible only if it has a root. F_2 has only 0 and 1 as elements, so it is easy enough to show that neither is a root. There is no simplification for θ or θ^2. $\theta^3 = 1 + \theta$. $\theta^4 = \theta + \theta^2$. $\theta^5 = 1 + \theta + \theta^2$. $\theta^6 = 1 + \theta^2$. $\theta^7 = \theta^0 = 1$. □

5. Suppose α is a rational root of a monic polynomial f in $\mathbb{Z}[x]$. Prove that α is an integer.

   Proof. Let $\alpha = \frac{p}{q}$ for some $p, q \in \mathbb{Z}$ with $(p, q) = 1$. Then

$$\begin{aligned} f(\alpha) = \left(\frac{p}{q}\right)^n + c_{n-1}\left(\frac{p}{q}\right)^{n-1} + ... + c_1\frac{p}{q} + c_0 = 0 \\ p^n + qc_{n-1}p^{n-1} + ... + q^{n-1}c_1 p + c_0 q^n = 0 \end{aligned}$$

   So q divides p, but since $(p, q) = 1$, q is 1. □

7. Prove that $f(x) = x^3 - nx + 2$ is irreducible over $\mathbb{Z}$ for $n \neq -1, 3, 5$.

   Proof. If $f(x)$ is reducible, then it has a root. If $f(\alpha) = 0$, then $\alpha(n - \alpha^2) = 2$, so α divides 2. If $\alpha = -1$, then $n = -1$. If $\alpha = 1$, then $n = 3$. If $\alpha = 2$, then $n = 5$. If $\alpha = -2$, then $n = 3$. These are the only cases in which f has roots. □

13.2 Algebraic Extensions

3. Determine the minimal polynomial over $\mathbb{Q}$ for the element $\alpha = 1 + i$.

   Proof. We want $x = 1 + i$, so $x - 1 = i$ and $(x - 1)^2 = -1$, so $m_\alpha(x) = x^2 - 2x + 1$. □

4. Determine the degree over $\mathbb{Q}$ of $\alpha = 2 + \sqrt{3}$ and of $\beta = 1 + \sqrt[3]{2} + \sqrt[3]{4}$. In the case of α, we want $x = 2 + \sqrt{3}$ to be a root, so $(x - 2)^2 = 3$ and $m_\alpha(x) = x^2 - 4x + 1$, so α is degree 2. We notice that

$$\beta = 1 + \sqrt[3]{2} + \sqrt[3]{4} = \frac{(1 - \sqrt[3]{2})(1 + \sqrt[3]{2} + \sqrt[3]{2}^2)}{1 - \sqrt[3]{2}} = \frac{1}{\sqrt[3]{2} - 1}$$

   so we can see that $m_{\beta^{-1}}(x) = x^3 + 3x^2 + 3x - 1$. Since β and β^{-1} have the same degree, the degree of β is 3.

5. Let $F = \mathbb{Q}(i)$. Prove that $x^3 - 2$ and $x^3 - 3$ are irreducible over F.

   Proof. Both of these polynomials are irreducible over $\mathbb{Q}$ by Eisentstein's Criterion. The extension $\mathbb{Q}(\alpha)$, for α a root of either, would be degree 3. Since $\mathbb{Q}(i)$ is degree 2, $\mathbb{Q}(\alpha) \cap \mathbb{Q}(i) = \mathbb{Q}$ when considered as subfields of $\mathbb{C}$. Thus, the polynomials do not have roots in $\mathbb{Q}(i)$ and so are irreducible. □

10. Determine the degree of the extension $\mathbb{Q}(\sqrt{3+2\sqrt{2}})$ over $\mathbb{Q}$.

    We notice that $\sqrt{3+2\sqrt{2}} = \sqrt{2+2\sqrt{2}+1} = \sqrt{(\sqrt{2}+1)^2} = \sqrt{2}+1$, so the extension is of degree 2.

12. Suppose the dergee of the extension K/F is a prime p. Show that any subfield E of K containing F is either K or F.

    Proof. We have $p = [K : F] = [K : E][E : F]$, so $[K : E] = 1$ or $[E : F] = 1$. □

13. Suppose $F = \mathbb{Q}(\alpha_1, ..., \alpha_n)$, where $\alpha_i^2 \in \mathbb{Q}$ for each i. Prove that $\sqrt[3]{2} \notin F$.

    Proof. $[F : \mathbb{Q}]$ must be even, but $\sqrt[3]{2}$ is of odd degree. □

14. Prove that if $[F(\alpha) : F]$ is odd then $F(\alpha) = F(\alpha^2)$.

    Proof. Suppose not. Then $[F(\alpha) : F(\alpha^2)] = 2$ and $[F(\alpha) : F] = [F(\alpha) : F(\alpha^2)][F(\alpha^2) : F]$, but this contradicts that $[F(\alpha) : F]$ is odd. □

16. Let K/F be an algebraic extension and let R be a ring contained in K and containing F. Show that R is a subfield of K.

    Proof. Let $\alpha \in R$. Then α is a root of some polynomial $f(x) = a_n x^n + ... + a_0$ with coefficients in F. Then $\alpha^{-1} = \frac{-1}{a_0}(a_n \alpha^{n-1} + ... + a_1) \in K$. But $\frac{-1}{a_0} \in R$ because $F \subseteq R$ and $\alpha^k \in R$ for any k because $\alpha \in R$. Therefore, $\alpha^{-1} \in R$ as well; *i.e.*, R is a field. □

19. Let K be an extension of F of degree n.

    (a) For any $\alpha \in K$ prove that α acting by multiplication on K is an F-linear trasnformation of K.

    Proof. We consider K as an n-dimensional vector space over F. Then for any $x, y \in K$ and $\lambda \in F$, $\alpha(x + \lambda y) = \alpha x + \alpha \lambda y$, so multiplication by α is a linear transformation. □

    (b) Prove that K is isomorphic to a subfield of the ring of $n \times n$ matrices over F, so the ring of $n \times n$ matrices over F contains an isomorphic copy of *every* extension of F of degree $\leq n$.

    Proof. Fix a basis for K and let $\varphi : K \to \mathcal{M}^{n \times n}(F)$ by taking to α to the matrix representation of its linear transformation. φ is injective since $\varphi(\alpha) = 0$ iff $\alpha = 0$. Therefore, $\varphi(K) \cong K$ is a subfield of $\mathcal{M}^{n \times n}(F)$. □

13.3 Classical Straightedge and Compass Constructions

4. The construction of a regular 7-gon amounts to the constructibility of $\zeta = \cos(\frac{2\pi}{7})$. We shall see later that $\cos(\frac{2\pi}{7})$ satisfies the equation $x^3 + x^2 - 2x - 1 = 0$. Use this to prove that the reqular 7-gon is not constructible by compass and straightedge.

   Proof. It is enough to show that $f(x) = x^3 + x^2 - 2x - 1$ is irreducible over $\mathbb{Q}$ since elements of $\mathbb{R}$ with degree 3 over $\mathbb{Q}$ are not contructible by compass and straightedge. If f has no zeros in $\mathbb{Z}$, then it has no zeros in $\mathbb{Q}$. It is easy to see that $f(x)$ is increasing outside of $(-2, 2)$, so its only possible integer roots are ± 1 or 0, but it can be easily varified that these are not zeros. □

5. Use the fact that $\alpha = 2\cos(\frac{2\pi}{5})$ satisfies the equation $x^2 + x - 1 = 0$ to conclude that the regular 5-gon is constructible.

   Proof. Recall that the interior angle of an n-gon is given by $\frac{n-2}{n}\pi$, so it is enough to construct the point $(\cos(\frac{2\pi}{5}), \sin(\frac{2\pi}{5}))$. As α is degree 2, it is constructible. Furthermore, $\sin(\frac{2\pi}{5}) = \sqrt{1-\alpha^2}$, so it is constructible as well. □

13.4 Splitting Fields and Algebraic Closures

1. Determine the splitting field and its degree over $\mathbb{Q}$ for $f(x) = x^4 - 2$.
   $\mathbb{Q}(\sqrt[4]{2}, i)$ has degree 8 over $\mathbb{Q}$.

2. Determine the splitting field and its degree over $\mathbb{Q}$ for $f(x) = x^4 + 2$.
   $\mathbb{Q}(\sqrt[4]{2}, i)$ has degree 8 over $\mathbb{Q}$.

3. Determine the splitting field and its degree over $\mathbb{Q}$ for $f(x) = x^4 + x^2 + 1$.
   $f(x) = u^2 + u + 1$ where $u = x^2$. $u = \frac{-1\pm\sqrt{-3}}{2} = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i = e^{\frac{2\pi i}{3}}, e^{\frac{4\pi i}{3}}$. $x = \pm e^{\frac{\pi i}{3}}, \pm e^{\frac{2\pi i}{3}} \in \mathbb{Q}(\sqrt{-3})$ has degree 2.

4. Determine the splitting field and its degree over $\mathbb{Q}$ for $f(x) = x^6 - 4$.
   Let $\omega = e^{\frac{\pi i}{3}}$. $\mathbb{Q}(\sqrt[3]{2}, \omega)$ has degree 6.

13.5 Separable and Inseparable Extensions

3. Prove that d divides n if and only if $x^d - 1$ divides $x^n - 1$.

   Proof. If $n = ad$ for some $a \in \mathbb{Z}_{\geq 0}$, then

$$x^n - 1 = (x-1)\sum_{0<j<n} x^j = \sum_{0<q<a} x^{qd} \sum_{0<r<d} x^r = (x^d - 1)\sum_{0<q<a} x^{qd}$$

   Conversely, if $n = qd + r$ for some $0 < r < d$, then $x^n - 1 = (x^n - x^r) + (x^r - 1) = x^r(x^{qd} - 1) + (x^r - 1)$. By the previous argument, $x^d - 1$ divides $x^r(x^{qd} - 1)$, but it does not divide $x^r + 1$ because $r < d$. Therefore $x^d - 1$ does not divide $x^n - 1$ □

6. Prove that

$$x^{p^n - 1} - 1 = \prod_{\alpha \in \mathbb{F}_{p^n}^\times} (x - \alpha)$$

   so the product of the nonzero elements of a finite field is $+1$ if $p = 2$ and -1 otherwise. For p odd and $n = 1$ derive *Wilson's Theorem:* $(p-1)! \equiv_p -1$.

   Proof. Every $\alpha \in \mathbb{F}_{p^n}^\times$ is a root for $x^{p^n-1} - 1$ since $\alpha^{p^n} = \alpha$. Since $x^{p^n-1} - 1$ has at degree $p^n - 1$, each α is a root with multiplicity 1. Therefore, for any p prime,

$$(p-1)! = \prod_{\alpha \in \mathbb{F}_p^\times} (0 - \alpha) = 0^{p^n-1} - 1 = -1$$

   and we note that $-1 = +1$ when $p = 2$. □

9. Show that the binomial coefficient $\binom{pn}{pi}$ is the coefficient of x^{pi} in the expansion of $(1+x)^{pn}$. Working over $\mathbb{F}_p$ show that this is the coefficient of $(x^p)^i$ in $(1+x^p)^n$ and hence $pnchoosepi \equiv_p \binom{n}{i}$.

   Proof. This is a trivial corollary of the binomial theorem. □

13.6 Cyclotomic Polynomials and Extensions

1. Suppose m and n are relatively prime positive integers. Let ζ_m be a primitive m^{th} root of unity and let ζ_n be a primitive n^{th} root of unity. Prove that $\zeta_m\zeta_n$ is a primitive mn^{th} root of unity.

   Proof. Note that $(\zeta_m\zeta_n)^d = 1$ if and only if d is a common multiple of m and n. Since m and n are coprime, mn is the least common multiple of m and n. Therefore, $\zeta_m\zeta_n$ is not a root of $\Phi_d(x)$ for any $d|, n$, where $d < mn$. Since $\zeta_m\zeta_n$ is clearly an mn^{th} root of unity, it therefore must be a root of $\Phi_{mn}(x)$. *I.e.,* it is primitive. □

2. Let ζ_n be a primitive n^{th} root of unity and let d be a divisor of n. Prove that ζ_n^d is a primitive $(\frac{n}{d})^{th}$ root of unity.

   Proof. Let a be any divisor of $\frac{n}{d}$. Then $(\zeta_n^d)^a = \zeta_n^{da} = 1$ if and only if $a = \frac{n}{d}$ since ζ_n is primitive. Therefore, ζ_n^d is a primitive $(\frac{n}{d})^{th}$ root of unity. □

3. Prove that if a field F contains the n^{th} roots of unity for n odd then it also contains the $2n^{th}$ roots of unity.

   Proof. Let ζ_n be an n^{th} root of unity. Then $(-\zeta_n)^m = 1$ iff $m \equiv 0 \pmod{2n}$. Since negation is bijective, and n^{th} roots of unity are also $2n^{th}$ roots of unity, F contains all $2n$ such roots. □

4. Prove that if $n = p^k m$ where p is prime and m is relatively prime to p then there are precicely m distinct n^{th} roots of unity over a field of characteristic p.

   Proof. If $n = p^k m$, we have
   $$x^n - 1 = (x^m)^{p^k} - 1^{p^k} = (x^m - 1)^{p^k}$$
   in a field of characteristic p, so any n^{th} root of unity must also be an m^{th} root. As such, there are *at most* m of them. Now we notice that $D_x(x^m - 1) = mx^{m-1}$, which has only 0 as its roots. Therefore, $x^m - 1$ has no multiple roots and so there are exactly m m^{th} roots of unity. □

6. Prove that for n odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$.

   Proof. ζ_n is a primitive n^{th} root of unity iff $-\zeta_n$ is a primitive $2n^{th}$ root of unity (see 13.6.3). Thus, α is a root of $\Phi_{2n}(x)$ if and only if α is a root of $\Phi_n(-x)$. Since both of these polynomials are monic and separable, they must be equal. □

9. Suppose A is an $n \times n$ matrix over $\mathbb{C}$ for which $A^k = I$ for some integer $k \geq 1$. Show that A can be diagonolized.

   Proof. Observe that the polynomial $f(x) = x^k - 1$ sends A to the zero matrix, and so it must be divisible by $m_A(x)$, the minimal polynomial for A. Therefore $m_A(x)$ is seperable, and so by Corollary 25 *[Dummit & Foote pg. 494]*, A is diagonalizable. □

10. Let φ denote the Frobenius map $x \mapsto x^p$. Prove that φ is an automorphism of $\mathbb{F}_{p^n}$ and that $\varphi^n = 1$.

    Proof. We already have that φ is an injective homomorphism of fields. Any injection on a finite set is bijective. Recall that the multiplicative group $\mathbb{F}_{p^n}^{\times}$ is cyclic; let α be a generator. be a generator. Then $\alpha^{pk} = \alpha$ iff $k \equiv 0 \bmod n$. □

Chapter 14

Galois Theory

14.1 Basic Definitions

2. Let $\tau : \mathbb{C} \to \mathbb{C}$ by $\tau(a+bi) = a - bi$ (*complex conjugation*). Prove that $\tau \in \mathrm{Aut}(\mathbb{C})$.

   Proof. Complex conjugation is an automorphism of $\mathbb{C}$ when considered as a vector space over $\mathbb{R}$. For $a+bi, c+di \in \mathbb{C}$,

   $\tau((a+bi)(c+di)) = \tau(ac - bd + adi + bci) = ac - bd - (ad+bc)i = (a-bi)(c-di) = \tau(a+bi)\tau(b+ci)$

   □

3. Determine the fixed field of complex conjugation.

   Clearly, it is just $\mathbb{R} \subseteq \mathbb{C}$.

4. Prove that $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$ are not isomorphic.

   Proof. Suppose that $\sigma : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{3})$ is an isomorphism. Since $\sigma(1) = 1$, $\sigma(2) = 2 = \sigma((\sqrt{2})^2)$ so $\mathbb{Q}(\sqrt{3})$ has a square root of 2. Of course, this can't be, since we would need $\sqrt{2} = a + b\sqrt{3}$ for some $a, b \in \mathbb{Q}$, which would imply $2 = a^2 + 2ab\sqrt{3} + b^2$, but $\sqrt{3}$ is not rational. □

6. Let k be a field.

   (a) Show that the mapping $\varphi : k[t] \to k[t]$ defined by $\varphi(f(t)) = f(at+b)$ for fixed $a, b \in k$, $a \neq 0$ is an automorphism of $k[t]$ that fixes k.

   Proof. Clearly this is a homomorphism. It fixes k tautologically, and so it is injective. It is surjective since for any $f \in k[t]$, $\varphi(\frac{f}{a} - b) = f$. □

   (b) Conversely, let $\varphi \in \mathrm{Aut}(k[t])$ that fixes k. Prove that there exist $a, b \in k$ with $a \neq 0$ such that $\varphi(f(t)) = f(at+b)$.

   Proof. Isomorphisms preserve the degree of a polynomial, so if $f(x) = x$, then $\varphi(x) = ax + b$ for some $a, b \in k$. Then for an arbitrary polynomial $g(x) = a_n x^n + ... + a_0$,

   $$\varphi(g(x)) = a_n \varphi(x)^n + ... + \varphi(a_n) = a_n(ax+b)^n + ... + a_0 = g(ax+b)$$

   since φ fixes k. □

7. This exercise determines $\mathrm{Aut}(\mathbb{R}/\mathbb{Q})$.

(a) Prove that any $\sigma \in \text{Aut}(\mathbb{R}/\mathbb{Q})$ takes squares to squares and takes positive reals to positive reals. Conclude that $\sigma(a) < \sigma(b)$ for $a < b \in \mathbb{R}$.

Proof. For $x \in \mathbb{R}$, $\sigma(x^2) = \sigma(x)^2$ so σ takes squares to squares. Since every positive real is a square, σ takes positives to positives. Therefore, if $a < b$, $\varphi(b-a) > 0$ and so $\varphi(b) > \varphi(a)$. □

(b) Prove that $-\frac{1}{m} < a - b < \frac{1}{m}$ implies $\frac{1}{m} < \sigma(a) - \alpha(b) < \frac{1}{m}$ for any positive $m \in \mathbb{Z}$. Conclude that σ is continuous on $\mathbb{R}$.

Proof. This is immediate from the monotonicity proved in (a), since σ fixes $-\frac{1}{m}$ and $\frac{1}{m}$. □

(c) Prove that any continuous map which is the identity on $\mathbb{Q}$ is the identity map. *I.e.*, $\text{Aut}(\mathbb{R}/\mathbb{Q}) = 1$.

Proof. For every $x \in \mathbb{R}$ there is a sequence $(a_n)_{n\in\omega} \subseteq \mathbb{Q}$ converging to x. If $\sigma : \mathbb{R} \to \mathbb{R}$ is continuous and fixes $\mathbb{Q}$, then

$$\sigma(x) = \lim_{n\to\infty} \sigma(a_n) = \lim_{n\to\infty} a_n = x.$$

□

10. Let K be an extension of the field F. Let $\varphi : K \to K'$ be an isomorphism of K with a field K' which maps F to the subfield F' of K'. Prove that the map $\Phi : \sigma \mapsto \varphi\sigma\varphi^{-1}$ defines a group isomorphism $\text{Aut}(K/F) \to \text{Aut}(K'/F')$.

Proof. For $\sigma, \tau \in \text{Aut}(K/F)$,

$$\Phi(\sigma\tau) = \varphi\sigma\tau\varphi^{-1} = \varphi\sigma\varphi^{-1}\varphi\tau\varphi^{-1} = \Phi(\sigma)\Phi(\tau)$$

so Φ is a homomorphism. To see that Φ is an isomorphism, we simply notice that $\Psi : \text{Aut}(K'/F') \to \text{Aut}(K/F)$ by $\Psi(\tau) = \varphi^{-1}\tau\varphi$ is an inverse for Φ. □

14.2 The Fundamental Theorem of Galois Theory

1. Determine the minimal polynomial over $\mathbb{Q}$ for the element $\sqrt{2} + \sqrt{5}$.

$$\begin{aligned} x &= \sqrt{2} + \sqrt{5} \\ x^2 &= 2 + 2\sqrt{10} + 5 \\ (x^2 - 7)^2 &= 40 \\ x^4 - 14x^2 + 9 &= m(x) \end{aligned}$$

4. Let p be prime. Determine the elements of the Galois group of $x^p - 2$.

Proof. $x^p - 2$ has as roots $\sqrt[p]{2}\zeta_p^i$ for $0 \leq i < p$ where ζ_p is a primitive p^{th} root of unity. Since the splitting field contains all of these roots, it contains $\sqrt[p]{2}$, and so it also contains each ζ_p^i. Thus, the splitting field is $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$. Note that $[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p-1)$ since p and $p-1$ are relatively prime.

Any automorphism will defined by its action on the two generators of the splitting field, and so can be contstructed by compositions of the following two automorphisms:

$$\sigma : \begin{cases} \sqrt[p]{2}\zeta_p^i & \mapsto \sqrt[p]{2}\zeta_p^{i+1} \\ \zeta_p & \mapsto \zeta_p \end{cases} \text{ and } \tau : \begin{cases} \sqrt[p]{2} & \mapsto \sqrt[p]{2} \\ \zeta_p^i & \mapsto \zeta_p^{2i} \end{cases}$$

Where multiplication and addition are mod p. Note that $\sigma\tau = \tau\sigma^{\frac{p+1}{2}}$, so we have the following presentation of the Galois group:

$$\langle \sigma, \tau | \sigma^p = \tau^{p-1} = 1, \sigma\tau = \tau\sigma^{\frac{p+1}{2}} \rangle.$$

□

5. Prove that the Galois group of $x^p - 2$ for p a prime is isomorphic to the group of matrices $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where $a, b \in \mathbb{F}_p$ and $a \neq 0$.

   Proof. Let the Galois group be written as in 14.2.4 and define the following map:

$$\Phi(\sigma) = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \text{ and } \Phi(\tau) = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$$

   Then $\Phi(\sigma)^p = \Phi(\tau)^{p-1} = I$ and

$$\Phi(\sigma)\Phi(\tau) = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{p+1}{2} \\ 0 & 1 \end{pmatrix} = \Phi(\tau)\Phi(\sigma)^{\frac{p+1}{2}}$$

   So Φ is a homomorphism. Clearly, it is injective and it is surjective since both groups have the same size. □

8. Suppose K is a Galois extension of F of degree p^n for some prime p and some $n \geq 1$. Show there are Galois extensions of F contained in K of degrees p and p^{n-1}.

   Proof. Let $G = \text{Aut}(K/F)$, so that $|G| = p^n$. Recall that a group of order p^n has a normal subgroup of order p^k for all $0 \leq k \leq n$. In particular, there is a normal subgroup H of order p and another, I of order p^{n-1}. From the fundamental theorem of Galois theory, there are fields L and J such that $F \subseteq L \subseteq K$ and $F \subseteq J \subseteq K$ with $\text{Aut}(K/L) = H$ and $\text{Aut}(K/J) = I$. Moreover, L and J are Galois over F, since H and I are normal in G. □

11. Suppose $f(x) \in \mathbb{Z}[x]$ is an irreducible quartic whose splitting field L has Galois group S_4 over $\mathbb{Q}$. Let θ be a root of $f(x)$ and such that $K = \mathbb{Q}(\theta)$. Prove that K is an extension of $\mathbb{Q}$ of degree 4 which has no proper subfields. Are there Galois extensions of $\mathbb{Q}$ of degree 4 with no proper subfields?

    Proof. We have that $[L : K] = |H| = 6$ where $H \leq S_4$ fixes K. If there were a subfield $F \subseteq E \subseteq K$, the corrseponding subgroup H' would need to contain H. Hovever, the only larger proper subgroup of S_4 is A_4 and A_4 has no subgroup of order 6.

    If K/F is a degree 4 Galois extension, then its Galois group has order 4, and so it has at least 1 proper subgroup of degree 2. Hence, K has a proper subfield containing F. □

13. Prove that if the Galois group of the splitting field of a cubic $f(x)$ over $\mathbb{Q}$ is the cyclic group of order 3 then all the roots of the cubic are real.

    Proof. Assume not, so that $f(x)$ has a complex root z. Then $\bar{x}$ is also a root of f, so the complex conjugate map $\tau \in \text{Aut}(K/\mathbb{Q})$. However, τ has order 2, contradicting the hypothesis that $\text{Aut}(K/\mathbb{Q})$ is cyclic of order 3. □

14.3 Finite Fields

1. Factor $x^8 - x$ into irreducibles in $\mathbb{Z}[x]$ and $\mathbb{F}_2[x]$.

   In $\mathbb{Z}[x]$, we have

$$x^8 - x = x\Phi_1(x)\Phi_7(x) = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

   In $\mathbb{F}_2[x]$

$$x^8 - x = x(x-1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1) = x(x-1)(x^3 + x^2 + 1)(x^3 + x + 1)$$

3. Prove that an algebraically closed field must be infinite.

Proof. Let F be an algebraically closed field and for the sake of contradiction, suppose it is finite with n elements. Then $f(x) = (x - x_1)...(x - x_n) + 1$ has no roots in F since $f(x) = 1$ for all $x \in F$. This contradicts the assumption that F is algebraically closed. □

7. Prove that one of $2, 3$, or 6 is a square in $\mathbb{F}_p$ for every prime p. Conclude that the polynomial

$$f(x) = x^6 - 11x^4 + 36x^2 - 36 = (x^2 - 2)(x^2 - 3)(x^2 - 6)$$

has a root mod p for every prime p but has no root in $\mathbb{Z}$.

Proof. If 2 or 3 are squares in $\mathbb{F}_p$, there is nothing to show. Otherwise, recall that $\mathbb{F}^\times$ is cyclic–let $\alpha \in \mathbb{F}_p^\times$ be a generator. Every element in $\mathbb{F}_p^\times$ can be written as a power of α and even powers of α are squares, so $2 = \alpha^m$ and $3 = \alpha^n$ for m and n both odd. But then $6 = \alpha^{m+n}$ and $m + n$ is even, so 6 is a square. □

8. Determine the splitting field of the polynomial $f(x) = x^p - x - a$ over $\mathbb{F}_p$ where $a \neq 0$. Show explicitly that the Galois group is cyclic. Such an extension is called an *Artin-Schreier extension.*

Proof. Let α be a root of $f(x)$. For all $x \in \mathbb{F}_p$, $x^p - x = 0$, so

$$f(\alpha) + x^p - x = \alpha^p + x^p - \alpha - x - a = (x + \alpha)^p - (x + \alpha) - a = f(x + \alpha) = 0$$

i.e., $x + \alpha$ is also a root. Therefore, $\mathbb{F}_p(\alpha)$ contains all p roots of f, and so it is the splitting field. Let $\sigma : \mathbb{F}_p(\alpha) \to \mathbb{F}_p(\alpha)$ by $\sigma : \alpha \mapsto \alpha+1$. It is easy to see that σ is an automorphism on $\mathbb{F}_p(\alpha)/\mathbb{F}_p$. Moreover, any automorphism of $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ can be defined by where it takes α, so $\langle\sigma\rangle = \mathrm{Aut}(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$. □

9. Let $q = p^m$ be a power of the prime p and let $\mathbb{F}_q = \mathbb{F}_{p^m}$ be the finite field with q elements. Let $\sigma_q = \sigma_p^m$ be the m^{th} power of the Frobenius automorphism σ_p, called the q-Frobenius automorphism.

   (a) Prove that σ_q fixes $\mathbb{F}_q$.

   Proof. For any $x \in \mathbb{F}_q$, $\sigma_p^m(x) = x^{p^m} = x$. □

   (b) Prove that every finite extension of $\mathbb{F}_q$ of degree n is the splitting field of $x^{q^n} - x$ over $\mathbb{F}_q$, hence is unique.

   Proof. Every finite extension of $\mathbb{F}_q$ of degree n is an extension of $\mathbb{F}_p$ of degree mn. Thus, it is the splitting field of $x^{p^{nm}} - x = x^{q^n} - x$ over $\mathbb{F}_p$, which is a subfield of $\mathbb{F}_q$. □

   (c) Prove that every finite extension of $\mathbb{F}_q$ of degree n is cyclic with σ_q as a generator.

   Proof. Let $K/\mathbb{F}_q$ be an extension of degree n. K is also an extension of F_p of degree mn and its Galois group is generated by σ_p. Since $\mathrm{Aut}(K/\mathbb{F}_q) \leq \mathrm{Aut}(K/\mathbb{F}_p)$, it must also be cyclic. σ_q fixes $\mathbb{F}_q$ and has the right order to be a generator. □

   (d) Prove that the subfields of the unique extension of $\mathbb{F}_q$ of degree n are in bijective correspondence with the divisors d of n.

   Proof. This is immediate from the Fundamental Theorem of Galois Theory and the fact that $\mathrm{Aut}(K/\mathbb{F}_q)$ is cyclic. □

10. Prove that n divides $\varphi(p^n - 1)$.

Proof. Recall that $\varphi(p^n - 1) = |\,\mathrm{Aut}(\langle\zeta_{p^n-1}\rangle)|$ where $\langle\zeta_{p^n-1}\rangle$ is the cyclic group of order $p^n - 1$. Recall further that $\langle\zeta_{p^n-1}\rangle \cong \mathbb{F}_{p^n}^\times$. Thus, there is a subgroup isomorphic to $\mathrm{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p)$, which has order n. The claim follows from Lagrange's Theorem. □

14.4 Composite Extensions and Simple Extensions

1. Determine the Galois closure of the field $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ over $\mathbb{Q}$.

   To find the minimal polynomial

$$\begin{aligned} x &= \sqrt{1+\sqrt{2}} \\ x^2-1 &= \sqrt{2} \\ m(x) &= x^4-2x^2-1 \\ &= (x^2-1+\sqrt{2})(x^2-1-\sqrt{2}) \\ &= \left(x+\sqrt{1+\sqrt{2}}\right)\left(x-\sqrt{1+\sqrt{2}}\right)\left(x+i\sqrt{-1+\sqrt{2}}\right)\left(x-i\sqrt{-1+\sqrt{2}}\right) \end{aligned}$$

   We can see that the splitting field is $\mathbb{Q}(\sqrt{1+\sqrt{2}}, i\sqrt{-1+\sqrt{2}})$ as those are the two generators.

3. Let F be a field contained in the ring of $n \times n$ matrices over $\mathbb{Q}$. Prove that $[F:\mathbb{Q}] \leq n$.

   Proof. Since $\mathbb{Q}$ has characterisitic 0, all of its extensions are separable. Therefore, by the primitive element theorem, $F = \mathbb{Q}(\alpha)$ for some $\alpha \in F$. The minimal polynomial $m_\alpha(x)$ divides the characteristic polynomial $\chi_\alpha(x)$ since $\chi_\alpha(\alpha) = 0$. Recalling that $\deg \chi_\alpha(x) = n$, the claim follows. □

14.5 Cyclotomic Extensions and Abelian Extensions Over $\mathbb{Q}$

4. Let $\sigma_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ denote the automorphism of the cyclotomic field of n^{th} roots of unity which maps $\zeta_n \mapsto \zeta_n^a$ where $(a,n) = 1$ and ζ_n is a primitive n^{th} root of unity. Show that $\sigma_a(\zeta) = \zeta^a$ for *every* n^{th} root of unity.

   Proof. For any n^{th} root of unity ζ, $\zeta = \zeta_n^k$ for some $0 \leq k < n$. Then $\sigma_a(\zeta) = \sigma_a(\zeta_n^k) = \zeta_n^{ak} = \zeta^a$. □

5. Let p be a prime and let $\epsilon_1, \epsilon_2, ..., \epsilon_{p-1}$ denote the primitive p^{th} roots of unity. Set $p_n = \epsilon_1^n + \epsilon_2^n + ... + \epsilon_{p-1}^n$, the sum of the n^{th} powers of the ϵ_i. Prove that $p_n = -1$ if p does not divide n and that $p_n = p-1$ if p does divide n.

   Proof. Note that

$$1 + \epsilon_1 + ... + \epsilon_{p-1} = \zeta^{p-1} + ... + \zeta + 1 = 0$$

   where ζ is *any* primitive p^{th} root of unity. When p does not divide n, ζ^n is still a primitive p^{th} root of unity, and so $p_n = -1$. Otherwise, $\zeta^n = 1$, and so $p_n = p-1$. □

7. Show that complex conjugation restricts to the automorphism $\sigma_{-1} \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of the cyclotomic field of n^{th} roots of unity. Show that the field $K^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ is the subfield of real elements in $K = \mathbb{Q}(\zeta_n)$, called the *maximal real subfield of* K.

   Proof. This is a trivial property of roots of unity. In case it is not plain to see, simply write $\zeta_n = e^{\frac{2ki\pi}{n}}$ where k and n are coprime and see that $\operatorname{im} \zeta_n^{-1} = \sin(\frac{-2\pi}{n}) = -\sin(\frac{2\pi}{n}) = -\operatorname{im} \zeta_n$. The subfield of real elements of $\mathbb{Q}(\zeta_n)$ is precisely the subfield fixed by $\langle \sigma_{-1} \rangle$ and so it must have degree 2. Therefore, there can be no possible extensions betweeen $K^+/\mathbb{Q}$ and $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. □

10. Prove that $\mathbb{Q}(\sqrt[3]{2})$ is not a subfield of any cyclotomic field over $\mathbb{Q}$.

    Proof. $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = S_3$, which is not abelian. Hence, it cannot be a subgroup of an abelian group, let alone a cyclic one. Therefore, $\mathbb{Q}(\sqrt[3]{2})$ cannot be extended further to a cyclotomic field. □

12. Let σ_p denote the Frobenius automorphism $x \mapsto x^p$ of the finite field $\mathbb{F}_q$ of $q = p^n$ elements. Viewing $\mathbb{F}_q$ as a vector space V of dimension n over $\mathbb{F}_p$ we can consider σ_p as a linear transformation of V to V. Determine the characteristic polynomial of σ_p and prove that σ_p is diagonalizable over $\mathbb{F}_p$ iff n divides $p-1$, and is diagonalizable over the algebraic closure of $\mathbb{F}_p$ iff $(n,p)=1$.

    Proof. $\sigma_q = \sigma_p^n$ fixes $\mathbb{F}_q$, so $\chi_{\sigma_p}(x) = x^n - 1$ is the charactersitic polynomial form σ_p. σ_n is diagonalizable iff χ_{σ_p} factors linearly over p, which happens iff $n|p-1$ (since $\mathbb{F}_p$ has n n^{th} roots of unity in that case). Similarly, the cyclotomic polynomial Φ_n is irreducible over $\mathbb{F}_p$ iff $(p,n)=1$, in which case the splitting field has degree n over $\mathbb{F}_p$. □

14.6 Galois Groups of Polynomials

2. Determine the Galois groups of the following polynomials:

    (a) $x^3 - x^2 - 4 = (x-2)(x^2+x+2)$. Since the quadratic is irreducible over $\mathbb{Q}$, the Galois group is $\mathbb{Z}/2\mathbb{Z}$.

    (b) $x^3 - 2x + 4 = (x+2)(x^2-2x+2)$, so the Galois group is $\mathbb{Z}/2\mathbb{Z}$.

    (c) $x^3 - x + 1$ is irreducible. $D = -4 - 27 = -23$, which is not a square, so the Galois group is S_3.

    (d) $x^3 + x^2 - 2x - 1 = (x - 2\cos(\frac{2\pi}{7}))(x - 2\cos(\frac{4\pi}{7}))(x - 2\cos(\frac{6\pi}{7}))$ is also irreducible over $\mathbb{Q}$. The Galois group is $\mathbb{Z}/3\mathbb{Z}$.

3. Prove that for any $a, b \in \mathbb{F}_{p^n}$ that if $x^3 + ax + b$ is irreducible then $-4a^3 - 27b^2$ is a square in $\mathbb{F}_{p^n}$. Note that the descriminant $D = -4a^3 - 27b^2$ in this case. Since the Galois group of the extension of a finite group must be cyclic, this means that the Galois group is Z_3 and so D is a square.

4. Determine the Galois group of $f(x) = x^4 - 25$.

    $f(x) = (x^2+5)(x^2-5)$, so the Galois group is $\mathbb{Z}/4\mathbb{Z}$.

11. Let F be an extension of $\mathbb{Q}$ of degree 4 that is not Galois over $\mathbb{Q}$. Prove that the Galois closure of F has Galois group either S_4 or A_4 or D_8. Prove that the Galois group is dihedral if and only if F contains a quadratic extension of $\mathbb{Q}$.

    Proof. F is a finite extension of $\mathbb{Q}$, so it is simple, generated by some α. Then the minimal polynomial $f(x)$ over α has degree 4 by hypothesis and the splitting field K over F will be the Galois closure. Therefore, $\mathrm{Gal}(K/\mathbb{Q})$ is $S_4, A_4, D_8, V_4, or Z_4$, but $\mathrm{Gal}(K/\mathbb{Q})$ must have a non-normal subgroup H of index 4, so it cannot be V_4 or Z_4. F contains a quadratic extension of $\mathbb{Q}$ iff H sits inside a subgroup of index 2. A_4 has no subgroups of index 2 and so K can't be S_4 or A_4. On the other hand, every subgroup of index 4 of D_8 sits inside of the Klein-4 group. □

17. Find the Galois group of $f(x) = x^4 - 7$ over $\mathbb{Q}$ explicitly as a permutation group on the roots.

    Proof. The roots of $f(x)$ are $\pm\sqrt[4]{7}$ and $\pm i\sqrt[4]{7}$, so the splitting field is given by $\mathbb{Q}(\sqrt[4]{7}, i)$. This extension is of degree 8 and its Galois group is determined by the automorphisms σ, which takes i to i and $\sqrt[4]{7}$ to $i\sqrt[4]{7}$ and τ, the complex conjugation map. Thus the Galois group is isomorphic to D_8. □

44. Let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be the roots of a quartic polynomial $f(x)$ over $\mathbb{Q}$. Show that the quantities $\gamma_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4, \gamma_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4$, and $\gamma_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3$ are permuted by the Galois group of $f(x)$. Conclude that these elements are the roots of a cubic polynomial with coefficients in $\mathbb{Q}$.

Proof. Let $G \leq S_4$ be the Galois group of $f(x)$. Note that any transposition fixes one of the γ_i and transposes the other 2. *E.g.* $(1\,2)$ fixes γ_1 and swaps γ_2 with γ_3. Since the transpositions generate S_4, every element in S_4 and hence G permutes the γs. Let

$$g(x) = (x-\gamma_1)(x-\gamma_2)(x-\gamma_3) = x^3 - (\gamma_1+\gamma_2+\gamma_3)x^2 + (\gamma_1\gamma_2+\gamma_2\gamma_3+\gamma_1\gamma_3)x - \gamma_1\gamma_2\gamma_3$$

Note that $\gamma_1+\gamma_2+\gamma_3$, $\gamma_1\gamma_2+\gamma_2\gamma_3+\gamma_1\gamma_3$, and $\gamma_1\gamma_2\gamma_3$ are all symmetric in $\alpha_1, \alpha_2, \alpha_3$, and α_4, and so they are all fixed by G. Thus, $g(x)$ has coefficients in $\mathbb{Q}$. □

46. Prove that every finite group occurs as the Galois group of a field extension of the form $F(x_1, x_2, ..., x_n)/E$ Let G be a finite group with n elements, so that we can think of G as a subgroup of S_n via the Cayley representation. S_n is the Galois group for $F(x_1, ..., x_n)$, and since $G \leq S_n$, there is an extension E/F such that G fixes E and $G = \text{Gal}(F(x_1, ..., x_n), E)$.

14.7 Solvable and Radical Extensions: Insolvability of the Quintic

10. Let $K = \mathbb{Q}(\zeta_p)$ be the cyclotomic field of p^{th} roots of unity for the prime p and let $G = \text{Gal}(K/\mathbb{Q})$. Let ζ denote any p^{th} root of unity. Prove that $\sum_{\sigma \in G} \sigma(\zeta)$ (the trace from K to $\mathbb{Q}$ of ζ) is -1 or $p-1$ depending on whether ζ is primitive or not.

Proof. Recall that cyclotomic extensions are cyclic, so $G = Z_{p-1}$. If ζ is not primitive, then $\zeta = 1$ since p is prime, and so $\sigma(\zeta) = 1$ for all $\sigma \in G$. In that case, $\sum_{\sigma \in G} \sigma(\zeta) = p-1$. Otherise, $\sum_{\sigma \in G} \sigma(\zeta) = \sum_{1 \leq k < p} \zeta^k = -1$. □

12. Let L be the Galois closure of the finite extension $\mathbb{Q}(\alpha)$ of $\mathbb{Q}$. For any prime p dividing the order of $\text{Gal}(L/\mathbb{Q})$ prove there is a subfield F of L with $[L : F] = p$ and $L = F(\alpha)$.

Proof. Let $G = \text{Gal}(L/\mathbb{Q})$ and let $n = |G|$. By Cauchy's theorem, if $p|n$, then G has a cyclic subgroup H of order p. By the Fundamental Theorem of Galois Theory, there is an extension $F'/\mathbb{Q}$ such that $[K : F'] = p$. There must be some $\sigma \in G$ such that $\sigma(\alpha) \notin F'$, since otherwise G fixes F, which contradicts that $K \neq F'$. Let $F = \sigma(F')$, so that $[K : F] = p$ and $\alpha \notin F$. Then $F(\alpha)$ properly contains F, so $F(\alpha) = K$ since there cannot be any extensions lying between F and K. □