Rings and Modules

by Dr. Charudatta Hajarnavis

University of Warwick

Lectures in the module

Contents

((the first lecturer))

1.1 Rings

Definitions 1.1.1. Let R be a non-empty set that has two laws of compo-sition defined on it. (We call these laws *addition* and *multiplication* and use the familian notatation.) We say that R is a *ring* (with respect to the given addition and multiplication) if the following hold:

(i) $a + b$ and $ab \quad R$ for all $a, b \quad R$;

(ii) $a + b = b + a$ for all $a, b \quad R$;

(iii) $a + (b + c) = (a + b) + c$ for all $a, b, c \quad R$;

(iv) there exists an element $0 \quad R$ such that $a + 0 = a$ for all $a \quad R$;

(v) given $a \quad R$ there exists an element $-a \quad R$ such that $a + (-a) = 0$;

(vi) $a(bc) = (ab)c$ for all $a, b, c \quad R$;

(vii) $(a + b)c = ac + bc$ for all $a, b, c \quad R$;

(viii) $a(b + c) = ab + ac$ for all $a, b, c \quad R$.

Thus, a ring is an additive Abelian group on which an operation of mul-tiplication is defined, this operation being associative and distributive (on both sides) with respect to the addition.

R is called a *commutative ring* if, in addition, it satisfies $ab = ba$ for all $a, b \; R$. The term *non-commutative ring* can be a little ambiguous. When applied to a particular example it clearly means that the ring is not com-mutative. However, when we discuss a class of “non-commutative rings” we mean “not necessarily commutative rings”, and it is usually not intended to exclude the commutative rings in that class.

If there is an element $1 \; R$ such that $1a = a1 = a$ for all $a \; R$ we say R has an *identity*.

1.2 Examples of Rings

Example 1.2.1. The integers Z, the rational numbers Q, the real numbers R, the complex numbers C all with the usual operations.

Example 1.2.2. $R[x]$, the *polynomial ring* in an indeterminate x with coefficients in R, with $xr = rx$ for all $r \in R$.

Example 1.2.3. $M_n(R) := \{n \times n$ matrices over the ring $R\}$.

Example 1.2.4. $T_n(R) := \{n \times n$ upper-triangular matrices over the ring $R\}$.

Example 1.2.5. $U_n(R) := \{n \times n$ strictly upper-triangular matrices over the ring $R\}$.

Example 1.2.6. $F\langle x_1, \ldots, x_n \rangle$, the *free algebra* over a field F with generators $x_1, \ldots, x_n$. The generators do not commute, so $x_1x_2x_1x_3 = x_1^2x_2x_3$.

Example 1.2.7. $A_1(\mathbb{C})$, the *first Weyl algebra*, which is the ring of poly-nomials in x and y with coe cients in C, where x, y do not commute but $xy - yx = 1$.

Example 1.2.8. Subrings of the above, such as $J := \{a + ib | a, b \in \mathbb{Z}\}$.

1.3 Properties of Addition and Multiplication

We typically write $a - b$ for $a + (-b)$.

Proposition 1.3.1. *The following hold for any ring R:*

(i) *the element* $0 \in R$ *is unique;*

(ii) *given* $a \in R$, $-a$ *is unique;*

(iii) $-(-a) = a$ *for all* $a \in R$;

(iv) *for any* $a, b, c \in R$, $a + b = a + c \Rightarrow b = c$;

(v) *given* $a, b \in R$, *the equation* $x + a = b$ *has a unique solution* $x = b - a$;

(vi) $-(a + b) = -a - b$ *for all* $a, b \in R$;

(vii) $-(a-b) = -a + b$ *for all* $a, b \in R$;

(viii) $a0 = 0a = 0$ *for all* $a \in R$;

(ix) $a(-b) = (-a)b = -(ab)$ *for all* $a, b \in R$;

(x) $(-a)(-b) = ab$ *for all* $a, b \in R$;

(xi) $a(b-c) = ab - ac$ *for all* $a, b, c \in R$.

1.4 Subrings and Ideals

Definition 1.4.1. A subset S of a ring R is called a *subring* of R if S is itself a ring with respect to the laws of composition of R.

Proposition 1.4.2. *A non-empty subset* S *of a ring* R *is a subring of* R *if and only if* $a - b \in S$ *and* $ab \in S$ *whenever* $a, b \in S$.

Proof. If S is a subring then obviously the given condition is satisfied. Conversly, suppose that the condition holds. Take any $a \in S$: $a - a = 0 \in S$. For any $x \in S$, $0 - x = -x \in S$. So, if $a, b \in S$, $a - (-b) = a + b \in S$. So S is closed with respect to both addition and multiplication. Thus S is a subring since all the other axioms are automatically satisfied. □

Examples 1.4.3. (i) $2\mathbb{Z}$, the subset of even integers, is a subring of $\mathbb{Z}$.

(ii) $\mathbb{Z}$ is a subring of the polynomial ring $\mathbb{Z}[x]$.

Definition 1.4.4. A subset I of a ring R is called an *ideal* if

(i) I is a subring of R;

(ii) for all $a \in I$ and $r \in R$, $ar \in I$ and $ra \in I$. If I is an ideal of R we denote this fact by $I \trianglelefteq R$.

Examples 1.4.5. (i) Let R be a non-zero ring. Then R has at least two ideals, namely R and $\{0\}$. We often write 0 for $\{0\}$.

(ii) $2\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Proposition 1.4.6. *Let* I *be a non-empty subset of a ring* R. *Then* $I \trianglelefteq R$ *if and only if for all* $a, b \in I$ *and* $r \in R$, $a - b \in I$, $ar \in I$, $ra \in I$.

Proof. Exercise. □

1.5 Cosets and Homomorphisms

Definition 1.5.1. Let I be an ideal of a ring R and $x \in R$. Then the set of elements $x + I := \{x + i | i \in I\}$ is the *coset* of x in R with respect to I.

When dealing with cosets, it is important to realise that, in general, a given coset can be represented in more than one way. The next lemma shows for the coset representatives are related.

Lemma 1.5.2. *Let R be a ring with an ideal I and $x, y \in R$. Then $x + I = y + I \Leftrightarrow x - y \in I$.*

Proof. Exercise. □

We denote the set of all cosets of R with respect to I by $\frac{R}{I}$. We can give $\frac{R}{I}$ the structure of a ring as follows: define

$$(x + I) + (y + I) := (x + y) + I$$

and

$$(x + I)(y + I) := xy + I$$

for $x, y \in R$. The key point here is that the sum and product on $\frac{R}{I}$ are well-defined; that is, they are independent of the coset representatives chosen. Check this and make sure that you understand why the fact that I is an ideal is crucial to the proof.

Definition 1.5.3. $\frac{R}{I}$ is called the *residue class ring* (or *quotient ring* or *factor ring*) of R with respect to I.

The zero element of $\frac{R}{I}$ is $0 + I = i + I$ for any $i \in I$.

If $I \subseteq S \subseteq R$ we denote by $\frac{S}{I}$ the subset $\{s + I | s \in S\}$ of $\frac{R}{I}$.

(i) *every ideal of the ring $\frac{R}{I}$ is of the form $\frac{K}{I}$ where $K \subseteq R$ and $K \supseteq I$. Conversely, $K \subseteq R$, $K \supseteq I \Rightarrow \frac{K}{I} \subseteq \frac{R}{I}$;*

(ii) *there is a one-to-one correspondence between the ideals of $\frac{R}{I}$ and the ideals of R containing I.*

Proof. (i) If $K \frac{R}{I}$ then define $K := \{x \in R | x + I \in K\}$. Then $K \subseteq R$, $K \supseteq I$ and $\frac{K}{I} = K$.

(ii) The correspondence is given by $K \leftrightarrow \frac{K}{I}$, where $I \subseteq K \subseteq R$. □

Definitions 1.5.5. A map of rings $\theta : R \to S$ is a (*ring*) *homomorphism* if $\theta(x + y) = \theta(x) + \theta(y)$ and $\theta(xy) = \theta(x)\theta(y)$ for all $x, y \in R$. θ defined by $\theta(r) = 0$ for all $r \in R$ is a homomorphism; it is called the *zero homomorphism*.
φ defined by $\varphi(r) = r$ for all $r \in R$ is also a homomorphism; it is called the *identity homomorphism*. Let $I \subseteq R$. Then $\sigma : R \to \frac{R}{I}$ defined by $\sigma(x) = x + I$ for $x \in R$ is a homomorphism of R onto $\frac{R}{I}$; it is called the *natural* (or *canonical*) *homomorphism* (of R onto $\frac{R}{I}$).

Proposition 1.5.6. *Let R, S be rings and $\theta : R \to S$ a homomorphism. Then*

(i) $\theta(0_R) = 0_S$;

(ii) $\theta(-r) = -\theta(r)$ *for all* $r \in R$;

(iii) the kernel $\ker \theta := \{x \in R | \theta(x) = 0_S\}$ *is an ideal of* R;

(iv) the image $\theta(R) := \{\theta(r) | r \in R\}$ *is a subring of* S.

Proof. Exercise. □

Definitions 1.5.7. Let $\theta : R \to S$ be a ring homomorphism. Then θ is called an *isomorphism* if θ is a bijection. We say that R and S are *isomorphic* rings

=

(The second lecture))

1.6 The Isomorphism Theorems

Theorem 1.6.1. (The First Isomorphism Theorem.) *Let $\theta : R \to S$ be a homomorphism of rings. Then*

$$\theta(R) \quad \frac{R}{\ker \theta}.$$

Proof. Let $I := \ker \theta$ and define $\sigma : \frac{R}{I} \to \theta(R)$ by $\sigma(x + I) := \theta(x)$ for $x \ R$. The map σ is well-defined since for $x, y \ R$,

$$x + I = y + I \qquad x - y \quad I = \ker \theta \qquad \theta(x - y) = 0 \qquad \theta(x) = \theta(y).$$

σ is easily seen to be the required isomorphism. □

Theorem 1.6.2. (The Second Isomorphism Theorem.) *Let I be an ideal and L a subring of R. Then*

$$\frac{L}{L \cap I} \quad \frac{L + I}{I}.$$

Proof. Let σ be the natural homomorphism $R \to \frac{R}{I}$. Restrict σ to the ring L. We have $\sigma(L) = \frac{L+I}{I}$, a subring of $\frac{R}{I}$. The kernel of σ restricted to L is $L \cap I$. Now apply Theorem 1.6.1. □

Theorem 1.6.3. (The Third Isomorphism Theorem.) *Let $I , K \ R$ be such that $I \ K$. Then*

$$\frac{R/I}{K/I} \quad \frac{R}{K}.$$

Proof. $\frac{K}{I} \quad \frac{R}{I}$ and so $\frac{R/I}{K/I}$ is defined. Define a map $\gamma : \frac{R}{I} \to \frac{R}{K}$ by $\gamma(x + I) := x + K$ for all $x \ R$. The map γ is easily seen to be well-defined and a homomorphism onto $\frac{R}{K}$. Further,

$$\gamma(x + I) = Kx + K = K$$
$$x \quad K$$
$$K$$
$$x + I \qquad \frac{K}{I} \text{ since } K \quad I$$

Therefore, $\ker \gamma = \frac{K}{I}$. Now apply Theorem 1.6.1. □

1.7 Direct Sums

Definitions 1.7.1. Let $\{I_\lambda\}_{\lambda \ \Lambda}$ be a collection of ideals of a ring R. We define their (*internal*) *sum* to be

$$\sum_{\lambda \ \Lambda} I_\lambda := x \quad R \quad x = \sum_{i=1}^{k} x_i, \ x_i \quad I_{\lambda i} , \ k \quad \mathbb{N} \ ,$$

the set of all finite sums of elements of the I_λ's. We say that the sum of the I_λ's is *direct* if each element of $\sum_{\lambda\in\Lambda} I_\lambda$ is uniquely expressible as $x_1 + \cdots + x_k$ with $x_i \in I_{\lambda_i}$, $\lambda_i \neq \lambda_j$ if $i \neq j$. In this case we denote the sum as $\sum_{\lambda\in\Lambda} I_\lambda$, or $I_1 + \cdots + I_n$ if Λ is finite.

Proposition 1.7.2. *The sum* $\sum_{\lambda\in\Lambda} I_\lambda$ *is direct if and only if* $I_\mu \cap \sum_{\lambda\in\Lambda\setminus\{\mu\}} I_\lambda = 0$ *for all* $\mu \in \Lambda$.

Proof. Exercise. □

Definition 1.7.3. Let $R_1, \ldots, R_n$ be rings. We define their *external direct sum* S to be the set of all n-tuples $\{(r_1, \ldots, r_n) | r_i \, R_i\}$. On S we define addition and multiplication componentwise, thus making S into a ring. We write $S = R_1 \cdots R_n$.

The set $(0, \ldots, 0, R_j, 0, \ldots, 0)$ is an ideal of S. Clearly S is the inter-nal direct sum of the ideals $(0, \ldots, 0, R_j, 0, \ldots, 0)$ for $j = 1, \ldots, n$. But

$$j \qquad = \quad j$$

which the R_j are ideals and S is their internal direct sum. Also, in Defini-tions 1.7.1 we can consider $I_1 \cdots I_n$ to be the external direct sum of the rings I_j. Hence, in practice, we do not need to distinguish between external and internal direct sums.

1.8 Division Rings

Definition 1.8.1. Let R be a ring with 1. An element $u \; U$ is a *unit* (or an *invertible element*) if there is a $v \; R$ such that $uv = vu = 1$. The element v is called the *inverse* of u and is denoted u^{-1}.

Definitions 1.8.2. A ring D with at least two elements is called a *division ring* (or a *skew field*) if D has an identity and every non-zero element of D has an inverse in D. A division ring in which the multiplication is commutative is called a *field*.

Example 1.8.3. (The Quaternions.) Let H be the set of all symbols $a_0 + a_1 i + a_2 j + a_3 k$ where a_i R. Two such symbols $a_0 + a_1 i + a_2 j + a_3 k$ and $b_0 + b_1 i + b_2 j + b_3 k$ are considered to be equal if and only if $a_i = b_i$ for i = 0, 1, 2, 3.

We make H into a ring as follows: addition is componentwise and two elements of H are multiplied term-by-term using the relations $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$ and $ki = -ik = j$. Then H is a non-commutative ring with zero $0 := 0 + 0i + 0j + 0k$ and identity $1 := 1 + 0i + 0j + 0k$.

Let $a_0 + a_1 i + a_2 j + a_3 k$ be a non-zero element of H, so not all the a_i are zero. We have

$$(a_0 + a_1 i + a_2 j + a_3 k)(a_0 - a_1 i - a_2 j - a_3 k) = a^2_0 + a^2_1 + a^2_2 + a^2_3 = 0.$$

So, letting $n := a_0^2 + a_1^2 + a_2^2 + a_3^2$, the element $\frac{a_0}{n} - \frac{a_1}{n} i - \frac{a_2}{n} - \frac{a_3}{n}$ is the inverse of $a_0 + a_1 i + a_2 j + a_3 k$.

Thus, H is a division ring. It is called the division ring of *real quaternions*. *Rational quaternions* can be defined similarly where the coe cients are from Q.

1.9 Matrix Rings

Definition 1.9.1. Let R be a ring with 1. Define E_{ij} $M_n(R)$ to be the matrix with 1 in the (i, j)th position and 0 elsewhere. The E_{ij} are called *matrix units*.

If (a_{ij}) $M_n(R)$ is arbitrary then clearly $(a_{ij}) =$ $\sum_{i,j=1}^{n} a_{ij} E_{ij}$, a_{ij} R,

and this expression is unique. We also have

$$E_{ij} E_k = \begin{cases} E & \text{if } j = k \\ 0^i & \text{otherwise.} \end{cases}$$

Theorem 1.9.2. *Let R be a ring with* 1*. Then*

(i) I $RM_n(I)$ $M_n(R)$*;*

(ii) conversely, every ideal of $M_n(R)$ *is of the form* $M_n(I)$ *for some* IR*.*

Proof. (i) Trivial.

(ii) Let $XM_n(R)$. We need an IR such that $X = M_n(I)$. Let $A = (a_{ij}) =$ $\sum_{i,j} a_{ij} E_{ij}$ X. Consider fixed α, β, $1\alpha, \beta$ n. We have

$$a_{\alpha\beta} E_{11} \quad X, \tag{1.9.1}$$

that is, the matrix with $a_{\alpha\beta}$ in the (1, 1) position and 0 elsewhere belongs to X .

Now let I be the set of all elements of R that occur in the (1, 1) position of some matrix in X. We show that I R and $X = M_n(I)$.

Let a, b I. Then a, b occur in the (1, 1) positions of matrices A, B X. So $a - b = (A - B)_{11}$ I. Let a I, r R. Let a be the (1, 1) entry of

$A \quad X$. Then $A = (a_{ij}) = \quad _{i,j} a_{ij} E_{ij}$ with $a_{11} = a$. Then $E_{11}A(rE_{11}) \quad X$ since $XM_n(R)$. So $a_{11} \quad rE_{11}X$, so arI. Similarly, raI. Thus $I \quad R$.

$$c \; E$$

Now let $C = (c_{ij}) = \quad _{i,j} \; _{ij} \; _{ij} \; X$, $c_{ij} \quad R$. By (1.9.1), $c_{ij} \quad I$. So $CM_n(I)$. So $XM_n(I)$. Finally, let $D = \quad (d_{ij}) = \quad _{i,j} d_{ij} E_{ij}$, $d_{ij} \quad I$. By the definition of I, for each (i, j), $d_{ij} E_{11} \quad X$. Therefore, $E_{i1}(d_{ij} E_{11})E_{1j} \quad X$. So $d_{ij} E_{ij} \quad X$ for each $1 \leq i, j \leq n$. Since X is an ideal, we have $D = \quad _{i,j} d_{ij} E_{ij} \quad X$. So $M_n(I) \quad X$, so $M_n(I) = X$. □

Remark 1.9.3. The above does not hold for right ideals, e.g.

$$\begin{matrix} Z & Z \\ & r \; M_2(Z). \\ 0 & 0 \end{matrix}$$

Definition 1.9.4. A ring R is said to be *simple* if 0 and R are the only ideals of R.

Theorem 1.9.5. *Let R be a ring with* 1*. If R is simple then so is the ring $M_n(R)$.*

Proof. 0 and R are the only ideals of R and so $M_n(0)$ and $M_n(R)$ are the only ideals of $M_n(R)$. So $M_n(R)$ is simple as well. □

Corollary 1.9.6. *Let D be a division ring. Then the ring $M_n(D)$ is a simple ring.*

Proof. The only ideals of D are 0 and D. □

((The Third lecture))

1.10 The Field of Fractions

Definition 1.10.1. A (commutative) ring R is called an *integral domain* if $ab = 0$ $a = 0$ or $b = 0$.

Example 1.10.2. Z; $F[x]$, where F is a field.

Beware – non-commutative integral domains exist in advanced ring the-ory.

Definition 1.10.3. Let R be a (commutative) integral domain that is a K is subring of a field K. Then of the *field of fractions* of R if every element $b = 0$, K is expressible as ab^{-1}, $a, b \; R$. *We write* $K = \text{Frac}(R)$.

We now show that every commutative integral domain has a field of fractions that is in some sense unique.

Example 1.10.4. Q = Frac(Z). Note that Z R, C as well, but R, C = Frac(Z).

Let R be a commutative integral domain, $R := R\backslash\{0\}$. Let $S = \{(a, b) | a \in R, b \in R\}$. Define a relation on S by

$$(a_1, b_1) \quad (a_2, b_2) \quad a_1b_2 = a_2b_1.$$

Lemma 1.10.5. *is an equivalence relation on S.*

Proof. Let (a_i, b_i) S, $i = 1, 2, 3$.

Reflexivity: (a_1, b_1) (a_1, b_1) since $a_1b_1 = a_1b_1$.

Symmetry:

$$(a_1, b_1) \qquad (a_2, b_2) \qquad a_1b_2 = a_2b_1$$
$$a_2b_1 = a_1b_2$$
$$(a_2, b_2) \quad (a_1, b_1)$$

Transitivity:

(a_1, b_1) (a_2, b_2) (a_3, b_3) $a_1b_2 = a_2b_1$, $a_2b_3 = a_3b_2$

$$a_1b_2b_3 = a_2b_1b_3$$
$$a_1b_2b_3 = b_1a_3b_2$$
$$(a_1b_3 - a_3b_1)b_2 = 0$$
$$a_1b_3 = a_3b_1$$

since $b_2 = 0$ and R is an integral domain

$$(a_1, b_1) \qquad (a_3, b_3)$$

□

Theorem 1.10.6. *Every (commutative) integral domain with* 1 *has a field of fractions.*

Proof. Let R be an integral domain. Consider the equivalence relation as above. Denote the equivalence class of (a, b) by $\frac{a}{b}$. Let K be the set of all such equivalence classes. Define addition and multiplication in K by

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}$$

and

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

for $\frac{a}{b}, \frac{c}{d} \in K$. We first make sure that these definitions are well-defined. Let $\frac{a}{b} = \frac{a'}{b'}, \frac{c}{d} = \frac{c'}{d'}$. Then $(a, b) \sim (a', b')$ and $(c, d) \sim (c', d')$, so $ab' = ba'$, $cd' = dc'$. Hence

$$\begin{aligned}(ad + bc)b'd' &= adbd' + bcb'd' \\ &= a'bdd' + bb'cd' \\ &= (a'd' + b'c')bd\end{aligned}$$

So $(ad + bc, bd) \sim (a'd' + b'c', b'd')$. So + is well-defined. Similarly for multiplication.

Note that $\frac{0}{b} = \frac{0}{d}$ for any $b, d \in R$, since $0d = b0 = 0$.

It can be checked that K is a commutative ring under these operations. $\frac{0}{b}$, for any $b \in R$, is the zero element of K; $\frac{-x}{y}$ is the additive inverse of $\frac{x}{y}$; the commutative, associative and distributive laws can be easily verified.

$\frac{1}{1} = \frac{b}{b}$ for any $b \in R$ is clearly the multiplicative identity in K. The multiplication is clearly commutative. Let $\frac{x}{y} \in K$, so $x \neq 0$, so $xy \neq 0$. So $\frac{y}{x}$ exists and

$$\frac{x}{y} \cdot \frac{y}{x} = \frac{xy}{xy} = \frac{1}{1} = 1_K$$

Thus every non-zero element of K has an inverse in K, so K is a field.

There is also a clear injective homomorphic embedding of R in K by $\theta : r \to \frac{r}{1}$ for $r \in R$. Now we truly have K as a field of fractions for

= □

Remark 1.10.7. There is no fundamental problem if R is without 1, since we can still have $1_K = \frac{b}{b}$ for any $b \in R$. Now embed $R \to K$ by $r \to \frac{rb}{b}$.

Lemma 1.10.8. *Let R, R be commutative integral domains with fields of fractions K, K respectively. Then $R = R$ $K = K$.*

Proof. Let $\theta : R \to R$ be an isomorphism. We have $K = \{ab^{-1} \mid (a, b) \in R \times R\}$. Define a map $\Theta : K \to K$ by $\Theta(ab^{-1}) := \theta(a)\theta(b)^{-1}$.

Θ is well-defined: suppose that $ab^{-1} = cd^{-1}$, $(a, b), (c, d) \in R \times R$. Then $ad = bc$, so $\theta(ad) = \theta(bc)$, so $\theta(a)\theta(d) = \theta(b)\theta(c)$, so $\theta(a)\theta(b)^{-1} = \theta(c)\theta(d)^{-1}$, so $\Theta(ab^{-1}) = \Theta(cd^{-1})$.

Θ is a homomorphism: let $ab^{-1}, cd^{-1} \in K$. Then

$$\begin{aligned}\Theta(ab^{-1} + cd^{-1}) &= \Theta((ad + bc)b^{-1}d^{-1}) \\ &= \theta(ad + bc)\theta(bd)^{-1} \\ &= (\theta(a)\theta(d) + \theta(b)\theta(c))\theta(b)^{-1}\theta(d)^{-1} \\ &= \theta(a)\theta(b)^{-1} + \theta(c)\theta(d)^{-1} \\ &= \Theta(ab^{-1}) + \Theta(cd^{-1}).\end{aligned}$$

Similarly, $\Theta((ab^{-1})(cd^{-1})) = \Theta(ab^{-1})\Theta(cd^{-1})$.

Θ is surjective: every element of K is expressible as $a b^{-1}$, $(a, b) \in R \times R$. But θ is an isomorphism, so $a = \theta(a)$ for some $a \in R$, and $b = \theta(b)$ for some $b \in R$. So $ab = \theta(a)\theta(b)^{-1} = \Theta(ab^{-1})$.

It is easy to check that Θ is injective. □

Corollary 1.10.9. *Let R be a commutative integral domain. Then its field of fractions is essentially unique, in that any two such fields of fractions are isomorphic.*

Proof. Take $R = R$, $\theta = \mathrm{id}_R$ in the above. □

2 Modules

2.1 Modules

Definitions 2.1.1. Let R be a ring. A set M is called a *right R-module* if

(i) M is an Abelian additive group;

(ii) a law of composition $M \times R \to M : (m, r) \to mr$ is defined that satisfies, for all $x, y \in M$ and $r, s \in R$,

$$(x + y)r = xr + yr,$$
$$x(r + s) = xr + xs,$$
$$x(rs) = (xr)s.$$

A *left R-module* is defined analagously. Here the composition law goes $R \times M \to M$ and is denoted rm.

Examples 2.1.2. (i) R and $\{0\}$ are both left and right R-modules.

(ii) Let V be a vector space over a field F. Then V is left (alternatively, a right) F-module. The module axioms are part of the vector space axioms.

(iii) Any Abelian group A can be considered as a left Z-module: for $g \in A$, $k \in Z$, define

$$kg := \begin{cases} g + \ldots + g & k \text{ times} \quad k > 0 \\ (-g) + \ldots + (-g) & k \text{ times} \quad k < 0 \\ 0_A & k = 0 \end{cases}$$

(iv) Let R be a ring. Then $M_n(R)$ becomes a left R-module under the action $r(x_{ij}) := (rx_{ij})$. Clearly, we can also make a similar right R-module action.

For technical reasons, it is easier to work with right modules in the theory of semi-simple Artinian rings.

Let R be a ring. The symbol M_R will denote M, a right R-module; similarly, ${}_RM$ will denote M, a left R-module.

Proposition 2.1.3. *Let M be a right R-module. Then*

(i) $0_M r = 0_M$ *for all* $r \in R$;

(ii) $m0_R = 0_M$ *for all* $m \in M$;

(iii) $(-m)r = m(-r) = -(mr)$ *for all* $m \in M$, $r \in R$.

Proof. (i), (ii). Exercises.

(iii) By (ii),

$$mr + m(-r) = m(r + (-r)) = m0_R = 0_M .$$

So $m(-r) = -(mr)$ by the uniqueness of $-(mr)$ in the Abelian group M. Similarly $(-m)r = -(mr)$. □

Definition 2.1.4. Let $K \subseteq M_R$. Then K is a *right R-submodule* (or just *submodule*) if K is also a right R-module under the law of composition for M.

Proposition 2.1.5. *Let $\varnothing \neq K \subseteq M_R$. Then K is a submodule of M if and only if for all $x, y \in K$, $r \in R$, $x - y \in K$ and $xr \in K$.*

Proof. Exercise. □

Definitions 2.1.6. Submodules of the module R_R are called *right ideals*. Submodules of ${}_RR$ are called *left ideals*.

2.2 Factor Modules and Homomorphisms

Let K be a submodule of M_R. Consider the factor group $\frac{M}{K}$. $\frac{M}{K}$ Elements of are cosets of the form $m + K$ for $m \in M$. We can make $\frac{M}{K}$ R- into a right module by defining, for $m \in M$, $r \in R$,

$$[m + K]r := [mr + K].$$

Check that this action is well-defined and that the module axioms are satis-fied.

Definition 2.2.1. $\frac{M}{K}$ with this action is called the *factor* (or *quotient*) *module* of M by K.

Example 2.2.2. Let n Z, $n \geq 2$. Then $_n\frac{Z}{Z}$ is a natural Z-module.

Definitions 2.2.3. Let M, M be right R-modules. A map $\theta : M \to M$ is an *R-homomorphism* if

(i) $\theta(x + y) = \theta(x) + \theta(y)$ for all x, y M ;

(ii) $\theta(xr) = \theta(x)r$ for all x M , r R.

(Similarly for left R-modules.) If K is a submodule of M_R then the map $\sigma : M \to \frac{M}{K}$ defined by $\sigma(m) = [m + K]$ is an R-homomorphism of M onto $\frac{M}{K}$. It is called the *canonical* (or *natural*) *R-homomorphism*.

Proposition 2.2.4. *Let $\theta : M_R \to M_R$ be an R-homomorphism. Then*

(i) $\theta(0_M) = 0_M$ *;*

(ii) the kernel $\ker \theta := \{x \quad M \mid \theta(x) = 0_M \}$ *is a submodule of M ;*

(iii) the image $\theta(M) := \{\theta(m) \mid m \quad M\}$ *is a submodule of M ;*

(iv) θ is injective if and only if $\ker \theta = \{0_M\}$.

Definition 2.2.5. Let $\theta : M_R \to M_R$ be an R-homomorphism. If θ is

=

((Fourth lecture))

2.3 The Isomorphism Theorems

These are similar to those for rings and have similar proofs. Theorem

2.3.1. *Let $\theta : M_R \to M_R$ be an R-homomorphism. Then*

$$\theta(M) \quad \frac{M}{\ker \theta}.$$

Theorem 2.3.2. *If K, L are submodules of M_R then*

$$\frac{L + K}{K} = \frac{L}{L \cap K}.$$

Theorem $_M$ 2.3.3. *If K, L are submodules of M $_R$ and* K L *then* $\frac{L}{K}$ *is a submodule of* $\frac{M}{K}$ *and*

$$\frac{M/K}{L/K} = \frac{M}{L}.$$

When K is a submodule of M_R and $L \subseteq K$ a submodule of M, then $\frac{L}{K}$ is a submodule of $\frac{M}{K}$. Conversely, every submodule of $\frac{M}{K}$ is $\frac{L}{K}$ for L a submodule of M containing K. Thus

$$\text{submodules of } \frac{M}{K} \leftrightarrow \{\text{submodules of } M \text{ containing } K\}.$$

2.4 Direct Sums of Modules

Definition 2.4.1. Let $M_1, \ldots, M_n$ be right R-modules. The set of all n-tuples $\{(m_1, \ldots, m_n) | m_i \, M_i\}$ becomes a right R-module if we define

$$(m_1, \ldots, m_n) + (m_1, \ldots, m_n) := (m_1 + m_1, \ldots, m_n + m_n),$$
$$(m_1, \ldots, m_n)r := (m_1 r, \ldots, m_n r),$$

for $m_i, m_i \, n \quad M_i, r \quad R$. This is the *external direct sum* of the M_i, which we denote $\bigoplus_{i=1}^{} M_i$ or $M_1 \cdot \cdot \cdot M_n$.

Definition 2.4.2. Let $\{M_\lambda\}_{\lambda \, \Lambda}$ be a collection of subsets of M_R. We define their (*internal*) *sum* by

$$M_\lambda := \{m_{\lambda 1} + \cdot \cdot \cdot + m_{\lambda k} \mid m_{\lambda i} \quad M_{\lambda i} \quad \text{for finite subsets } \{\lambda_1, \ldots, \lambda_k\} \ \Lambda\}.$$

Thus $\lambda \ \Lambda M_\lambda$ is the set of all finite sums of elements from the M_λ. It is easy to see that $\lambda \ \Lambda M_\lambda$ is a submodule of M.

Definition 2.4.3. $\lambda \ \Lambda M_\lambda$ is *direct* if each m for some m_λ $\lambda \ \Lambda M_\lambda$ has a unique representation as $m = m_{\lambda 1} + \ldots$

We can show that $\lambda \ \Lambda M_\lambda$ is direct if and only if

$$M_\mu \cap \sum_{\lambda \ \Lambda \setminus \{\mu\}} M_\lambda = \{0\}$$

for all $\mu \quad \Lambda$. If the sum is direct we use the same notation as above.

As before with rings, there really is no di erence between (finite) internal and external direct sums of modules.

Definition 2.4.4. Let R be a ring with 1. M_R is *unital* if $m1 = m$ for all $m \in M$. Similarly for ${}_RM$.

Exercise 2.4.5. Let R be a ring with 1, M a right R-module. Show that M has submodules M_1 and M_2 such that $M = M_1 \oplus M_2$ with M_1 unital and $m_2 r = 0$ for all $m_2 \in M_2$, $r \in R$.

Since modules like M_2 give us no information about R, whenever R has 1 we assume that all R-modules are unital.

2.5 Products of Subsets

Let K, S be non-empty subsets of M_R and R respectively. Define their prod-uct KS to be

$$KS := \sum_{i=1}^{n} k_i s_i \mid k_i \in K, s_i \in S, n \in \mathbb{N}.$$

I.e., KS consists of all finite sums of elements of type ks If $= $ for $k \in K, s \in S$. $K \subseteq M$, $S \subseteq R$, then KS is a submodule of M – to make this we need finiteness work.

This definition applies, in particular, with $M = R$. Thus, if $= S \subseteq R$,

$$S^2 := \sum_{i=1}^{n} s_i t_i \mid s_i, t_i \in S, n \in \mathbb{N}.$$

Extending this inductively, S^n consists of all finite sums of elements of type $s_1 s_2 \ldots s_n$, $s_i \in S$. Note that $S \subseteq R$ $S^n \subseteq R$.

3 Zorn's Lemma

3.1 Definitions and Zorn's Lemma

Definition 3.1.1. A non-empty set S is said to be *partially ordered* if there is a binary relation $\leq$ on S, defined for certain pairs of elements, such that for all $a, b, c \in S$,

(i) $a \leq a$;

(ii) $a \leq b$ and $b \leq c \Rightarrow a \leq c$;

(iii) $a \leq b$ and $a \leq b \Rightarrow a = b$.

Definition 3.1.2. Let S be a partially ordered set, a non-empty subset T is said to be *totally ordered* if for all $a, b \in T$, $a \leq b$ or $b \leq a$.

Definitions 3.1.3. Let S be a partially ordered set. An element $x \in S$ is called *maximal* if $x \leq y$ and $y \in S \Rightarrow x = y$. Similarly for *minimal*.

Definition 3.1.4. Let T be a totally ordered subset of a partially ordered set S. We say T has an *upper bound (in S)* if $c \in S$ such that $x \leq c$ for all $x \in T$.

Axiom 3.1.5. (Zorn's Lemma.) If a partially ordered set S has the property that every totally ordered subset of S has an upper bound then S contains a maximal element.

Remark 3.1.6. There may in fact be several maximal elements. Zorn's Lemma guarantees the existence of at least one such element.

3.2 The Well-Ordering Principle

Definition 3.2.1. A non-empty set S is said to be *well-ordered* if it is totally ordered and every non-empty subset of S has a minimal element.

Axiom 3.2.2. (The Well-Ordering Principle.) Any non-empty set can be well-ordered.

3.3 The Axiom of Choice

Axiom 3.3.1. (The Axiom of Choice.) Given a class of non-empty sets there exists a "choice function", i.e. a function that assigns to each of the sets one of its elements.

It can shown that

Axiom of Choice Zorn's Lemma Well-Ordering Principle.

3.4 Applications

Definitions 3.4.1. let M be a right ideal of a ring R. M is said to be a *maximal right ideal* if $M = R$ and $M\ M_r\ R\ M$ *maximal* $= R$, Similarly for *left ideal* and *maximal two-sided ideal*.

Theorem 3.4.2. *Let R be a ring with* 1*. Let $I = R$ be a (right) ideal of R. Then R contains a maximal (right) ideal M such that $I \quad M$.*

Proof. We prove this for $I_r R$. Consider $S := \{X_r R | X \ I\ , X = R\}$. S = since I S. Partially order S by inclusion. Let $T := \{X_\alpha\}_{\alpha\ \Lambda}$ be a totally ordered subset of S.

Consider $X :=$ $_{\alpha\ \Lambda} X_\alpha$. If $x_1, x_2 \quad X$ then $x_1 \quad \alpha_1 \quad 2 \quad \alpha_2$ for some $\alpha_1, \alpha_2 \quad \Lambda$. Since T is totally ordered, we can assume that $X_{\alpha 1} X_{\alpha 2}$. So $x_1, x_2 \quad X_{\alpha 2}$, so $x_1 - x_2 \quad X_{\alpha 2} \quad X$. Clearly, also $x \quad X$, and $r \quad RXr$ X. Thus $X \quad_r \quad R$. Also $X = R$ since

$$X = R1 \quad X$$
$$1 \quad X_\alpha \text{ for some } \alpha$$
$$X_\alpha = R,$$

S

which is a contradiction. Trivially, $X\ I$ so X . Also clearly, $X_\alpha\ X$ for all $\alpha\ \Lambda$.

$$S \quad T$$

Thus, X is an upper bound in for . So Zorn's Lemma applies and hence S contains a maximal element M . Clearly M is a maximal right ideal of R and contains I.

The proof is similar for left ideals and two-sided ideals. □

Remark 3.4.3. This result is false if R is without 1.

Corollary 3.4.4. *A ring with* 1 *contains a maximal (right) ideal.*

Proof. Take $I = \{0\}$ in the above. □

Note that pZ is a maximal ideal of Z for each prime p.

Theorem 3.4.5. *Every vector space has a basis.*

Proof. Exercise. Hint: Apply Zorn's Lemma to obtain a maximal set of linearly independent vectors. Note that a set of vectors is defined to be linearly independent if every finite subset is linearly independent. □

Exercises 3.4.6. Let R be a commutative ring with 1. Show that

(i) if R is a finite integral domain then R is a field;

(ii) if $M \quad R$ and $M = R$ then M is maximal if and only if $\frac{R}{M}$ is a field.

((Fifth lecture))

4 Completely Reducible Modules

4.1 Irreducible Modules

Definition 4.1.1. A right R-module M is *irreducible* if

(i) $MR = 0$;

(ii) M has no submodules other than 0 and M.

If R has 1 and M is unital then (i) can be replaced by $M = 0$.

Examples 4.1.2. (i) Let p be a prime; then $\mathbb{Z}/p\mathbb{Z}$ is an irreducible $\mathbb{Z}$-module.

(ii) Every ring R with 1 has an irreducible right R-module. By Theorem 3.4.2, R has a maximal right ideal M; R/M is an irreducible right R-module.

(iii) Let V be a vector space over a field F. Then any 1-dimensional sub-space of V is an irreducible F-module.

The vector space V has the following interesting property: V is a sum of 1-dimensional irreducible submodules/subspaces, i.e. has a basis; this sum is direct. Not all modules over arbitrary rings have this property. Consider $\mathbb{Z}/4\mathbb{Z}$ as a $\mathbb{Z}$-module. $2\mathbb{Z}/4\mathbb{Z}$ is the only (irreducible) submodule of $\mathbb{Z}/4\mathbb{Z}$. So $\mathbb{Z}/4\mathbb{Z}$ is not expressed as a sum of irreducible submodules.

4.2 Completely Reducible Modules

Definition 4.2.1. M_R is said to be *completely reducible* if M is expressible as a sum of irreducible submodules.

Examples 4.2.2. (i) Let F be a field. Then every F-module is completely reducible, i.e. every vector space has a basis.

(ii) $\mathbb{Z}/6\mathbb{Z}$ is completely reducible as a $\mathbb{Z}$-module: $\mathbb{Z}/6\mathbb{Z} = 2\mathbb{Z}/6\mathbb{Z} + 3\mathbb{Z}/6\mathbb{Z}$.

Definition 4.2.3. Let $\{M_\lambda\}_{\lambda \in \Lambda}$ be a family of submodules of M_R. The family is *independent* if the sum $\sum_{\lambda \in \Lambda} M_\lambda$ is direct. Thus $\{M_\lambda\}_{\lambda \in \Lambda}$ is inde-

pendent if and only if $M_\mu \cap \sum_{\lambda \in \Lambda \setminus \{\mu\}} M_\lambda = 0$ for all $\mu \in \Lambda$.

Lemma 4.2.4. *Suppose* $\{M_\lambda\}_{\lambda \in \Lambda}$ *is a family of irreducible submodules of* M_R *and let* $M := \sum_{\lambda \in \Lambda} M_\lambda$. *Let* K *be a submodule of* M. *Then there is an independent subfamily* $\{M_\lambda\}_{\lambda \in \Lambda}$ *such that* $M = K \oplus \sum_{\mu \in \Lambda} M_\mu$.

Proof. We apply Zorn's Lemma to the independent families of the form $\{K\} \cup \{M_\mu\}_{\mu \in X}$, $X \subseteq \Lambda$.

Partially order the set S of all such families by inclusion. Let T be a to-tally ordered subset of S, C the union of all the families in T. Each member of T has the form $\{K\} \cup \{M_\mu\}_{\mu \in X}$, $X \subseteq \Lambda$, so we have the same form for C.

We need to show that $C \in S$, i.e. C is an independent family. Let I be any submodule in C and suppose Σ is the sum of all other submodules in C. Let $x \in I \cap \Sigma$. Then $x = x_1 + \cdots + x_n$, $x_j \in I_j$, I_j a submodule in C for $j = 1, \ldots, n$.

Now $I, I_1, \ldots, I_n$ are all in C so each comes from some family in T. But T is totally ordered, so $I, I_1, \ldots, I_n$ lie in some one family in T. But this family is independent, so $x = x_1 = \cdots = x_n = 0$. So $I \cap \Sigma = 0$.

So C is independent. Also C has the form $\{K\} \cup \{M_\mu\}_{\mu \in X}$, $X \subseteq \Lambda$, so $C \in S$. Clearly C is an upper bound for T. So, by Zorn's Lemma, S contains a maximal element, say $\{K\} \cup \{M_\mu\}_{\mu \in \Lambda}$, $\Lambda \subseteq \Lambda$. ( ).

We claim $M = K_{\mu \wedge} M_{\mu}$. Suppose $\alpha \in \Lambda$ such that $M_\alpha \cap K_{\mu \wedge} M_{\mu} \neq M_\alpha$. Then $\{K_{\mu \wedge} M_{\mu}, M_\alpha\}$ would be an independent family, contradicting ( ). Thus $M_\alpha \cap K_{\mu \wedge} M_{\mu} = M_\alpha$ for all $\alpha \in \Lambda$, since M_α is irreducible and $M_\alpha \cap K_{\mu \wedge} M_{\mu}$ is a submodule of M_α. So $M_\alpha \subseteq K_{\mu \wedge} M_{\mu}$ for each $\alpha \in \Lambda$. As $M = \sum_{\lambda \in \Lambda} M_\lambda$, $M = K_{\mu \wedge} M_{\mu}$.

□

Lemma 4.2.5. (Dedekind Modular Law.) *Let A, B, C be submodules of M_R such that $B \subseteq A$. Then $A \cap (B + C) = B + A \cap C$.*

Proof. Elementary. □

Theorem 4.2.6. *Let M be a non-zero right R-module. The following are equivalent:*

(i) M is completely reducible;

(ii) M is a direct sum of irreducible submodules;

(iii) mR = 0, *m M m* = 0 *and every submodule of M is a direct summand of M .*

Proof. (i) (ii). Take $K = 0$ in Lemma 4.2.4 above.

(ii) (iii). Suppose that $mR = 0$ for some m M. Let $M =$ $\lambda \wedge M_\lambda$, M_λ irreducible. Then $m = m_1 + \cdots + m_k$ for some m_i $M_{\lambda i}$.

$$mr = 0,\ r \quad R \quad m_1 r + \cdots + m_k r = 0$$
$$m_i r = 0 \text{ for all } i,$$

since the sum of the M_λ is direct.

Define $K_j := \{x\ M_{\lambda j} \mid xR = 0\}$ for $j = 1, \ldots, k$. Then K_j is a submod-ule of $M_{\lambda j}$. So $K_j = 0$ or $M_{\lambda j}$ since $M_{\lambda j}$ is irreducible. But $K_j = M_{\lambda j}$ since $M_{\lambda j} R = 0$ by definition of irreducible submodule. So $K_j = 0$ for $j = 1, \ldots, k$. Thus $m_j = 0$ for $j = 1, \ldots, k$, so $m = 0$. The second part follows from Lemma 4.2.4.

(iii) (i). Our first aim is to show that M has an irreducible submodule.

Note that by the Dedekind Modular Law the hypothesis on M is inher-ited by every submodule of M.

Let $0 = y\ M$. Let S be the set of all submodules K of M such that $y\ K$. $S =$ since $\{0\}$ S. Partially order S by inclusion; let T be a totally ordered subset of S. Let C be the union of all the submodules in T. Then $y\ C$ and C is a submodule of M. So $C\ S$ and C is an upper bound for T. By Zorn's Lemma, S has a maximal element B. $y\ B$ so $B = M$. Hence, by hypothesis, there is a $B = 0$ such that $B\ B = M$. We claim

that B is irreducible.

$B\ R = 0$ by hypothesis. Suppose B contains a proper submodule $B_1 = 0$. Then there is a submodule $B_2 = 0$ such that $B = B_1\ B_2$. Now $y\ B_1\ B_2$ by the maximality of $B\ S$. So $y\ (B\ B_1) \cap (B\ B_2) = B$, a contradic-tion. So B is irreducible, and thus M has an irreducible. Let K be the sum of all these.

If $K = M$ there is a non-zero submodule L of M such that $M = K\ L$. But the above applied to L gives an irreducible in L, a contradiction since K contains all the irreducible submodules of M and $K \cap L = 0$. Thus $K = M$ and M is completely reducible. □

Remark 4.2.7. The first part of condition (iii) holds automatically when R has 1 and M is unital.

4.3 Examples of Completely Reducible Modules

Example 4.3.1. Let D be a division ring and $R := M_n(D)$. Then both ${}_RR$ and R_R are completely reducible.

Proof. Let

$$\begin{matrix} 0 & \cdots & 0 \\ \vdots & \ddots & \vdots \end{matrix}$$

$$I_j := \begin{matrix} D & \dots & D \\ \vdots & \dots & \vdots \end{matrix} \leftarrow j\text{th row}$$

$$= a_{j1} \ \dots \ a_{jn} \begin{matrix} 0 & \dots & 0 \\ \vdots & & \vdots \end{matrix} \quad a_{jk} \quad D$$

$$\begin{matrix} \vdots & \ddots & \vdots \\ \vdots & & \vdots \end{matrix}$$

I_j is the set of all matrices in $M_n(D)$ where all rows except the jth are zero.
Then $I_j \quad _r R$ and $I_j = E_{jj} R$, where E_{jj} is the (j, j) matrix unit.

We claim that each I_j is an irreducible R-module.

Suppose that $0 \; X \; I_j$, $X \; _r \; R$. Then X contains a non-zero matrix $A = (a_{\alpha\beta})$. A must have a non-zero entry, and since $A \; I_j$, $a_{jk} = 0$ for some k. Let B be he matrix with $\bar{a}_{jk}^{1}$ in the (k, j)th place and 0 elsewhere. Then $AB = E_{jj}$. So $E_{jj} \; X$, since $A \; X \; _r \; R$. So $E_{jj} \; R \; X$ since $X \; _r \; R$. Thus $I_j = X$. Since R has 1, $I_j \; R = 0$, each I_j is an irreducible right R-module.

It is clear that $R = I_1 \cdot \cdot \cdot I_n$, so R_R is completely reducible. Similarly for $_R R$. □

Example 4.3.2. Let $R := R_1 \cdot \cdot \cdot R_m$ be a direct sum of rings, where $R_i := M_{ni}$ (D_i), D_i division rings, n_i N. Again $_R R$ and R_R are completely reducible.

Proof. Since each $R_i \; R$, each R_i can be viewed as an R_i-module or an R-module. Further, the R_i-submodules and R-submodules coincide. Note that $R_i R_j = 0$ for $i = j$.

By the previous example, each R_i is a sum of irreducible R_i-submodules. So each R_i is a sum of irreducible R-submodules. So R is a sum of irreducible R-submodules. Hence $_R R$ and R_R are completely reducible.

The significance of this example is that we now aim to show that if R is a ring with 1 and R_R is completely reducible then it is necessarily a ring of the type given in the second example above. As a consequence we shall have R_R completely reducible $_R R$ completely reducible.

((Sixth lecture))

5 Chain Conditions

5.1 Cyclic and Finitely Generated Modules

Definitions 5.1.1. Let = T M_R. By the *submodule of M generated by* T we mean the intersection of all submodules of M that contain T . We de-note this by (T). Thus (T) is the "smallest" submodule of M that contains T .

When T consists of a single element a M we have

(a) = {$ar + \lambda a | r$ R, λ Z}

since the RHS

(i) is a submodule of M ;

(ii) contains a;

(iii) lies inside any submodule of M containing a. If

R has 1 and M is unital then (a) = aR.

If M = (a) for some a M then M is said to be a *cyclic module generated by a*. A module M is said to be *finitely generated* if $M = (a_1) + \cdots + (a_k)$ for some finite collection $\{a_1, \ldots, a_k\}$ M . The a_i are *generators* of M

If R has 1 and M_R is unital then M_R finitely generated $M = a_1R +$ $\cdots + a_k R$ for some a_i M .

A cyclic submodule of R_R (respectively $_RR$) is called a *principal right* (respectively *left*) *ideal* of R. Thus aZ Z is principal.

5.2 Chain Conditions

Definition 5.2.1. A set A is called an *algebra* over a field F if

(i) A is a vector space over F ;

(ii) A is a ring with the same addition as in (i);

(iii) the ring and vector space products satisfy

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

for all $a, b \quad A$ and $\lambda \quad F$.

Example 5.2.2. $M_n(F)$ is an n^2-dimensional algebra over the field F.

Substructures, homomorphisms etc. for algebras can be defined in the usual ways. Thus

Definition 5.2.3. $I \quad A$ is an *(algebra) right ideal* if

(i) $I \quad_r A$ as rings;

(ii) I is a subspace of the vector space A.

If A has identity 1 then the vector space structure is automatically preserved.

Example 5.2.4. Let $I \; _r A$, $K \; A$. Then for $\lambda \; F$, $x \; I$, $\lambda x = \lambda(x1) = x(\lambda 1) \; I$, since I is a right ideal of the ring A and $\lambda 1 \; A$. Similarly, for $\lambda \quad F$, $y \; K$, $\lambda y = \lambda(1y) = (\lambda 1)y \; K$. In general, if A is an algebra over a field F and $\lambda \; F$ we cannot immediately say that $\lambda \; A$.

However, if A has 1 we can overcome this problem: define

$$\overline{F} := \{\lambda 1 | \lambda \quad F\}.$$

Clearly $\overline{F}$ is a subalgebra of A and a field isomorphic to F. If we identify $\overline{F} \quad F$ we can assume $F \quad A$.

Example 5.2.5. For $M_n(F)$,

$$F \quad \lambda \leftrightarrow \begin{pmatrix} \lambda & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \lambda \end{pmatrix} \quad F \; .$$

Now let A be an n-dimensional algebra with 1. Let $I_1 \; I_2 \; \dots$ be an ascending chain of right ideals in A. Since each I_j is a subspace of A we have

$$\dim I_j = \dim I_{j+1} \qquad I_j = I_{j+1}.$$

Hence, the chain can have at most $n + 1$ terms. Similarly for descending chains. Many properties of algebras can be deduced from these facts alone. Moreover, there are rings (for example, Z) that are not algebras but that still satisfy something like the above property.

Definitions 5.2.6. (i) A module M_R has the *ascending chain condition* on submodules if every ascending chain of submodules $M_1 \quad M_2 \quad \ldots$ has equal terms after a finite number of steps. Similarly for the *descending chain condition*.

(ii) M_R has the *maximum condition* if every non-empty set S of submodules of M contains a maximal element with respect to inclusion. Similarly for the *minimum condition*.

Remark 5.2.7. The ascending chain condition or descending chain condi-tion alone does not imply that all chains stop after a fixed n terms. For example, $\mathbb{Z}$ has the ascending chain condition (it's a principal ideal domain) but ascending chains of arbitrary length can be constructed:

$$2^k\mathbb{Z} \quad 2^{k-1}\mathbb{Z} \quad \cdots \quad 2\mathbb{Z} \quad \mathbb{Z}.$$

However, if we have both the ascending chain condition and descending chain condition then such a "global" n does exist. This follows from the theory of composition series.

Theorem 5.2.8. *Let M_R be a right R-module. The following are equivalent*

(i) M has the maximum condition on submodules;

(ii) M has the ascending chain condition on submodules;

(iii) every submodule of M is finitely generated.

Proof. (i) (iii). Suppose that K is a submodule of M that is not finitely generated. Choose $x_1 \ K$ and let $K_1 := (x_1)$. Then $K = K_1$. So $x_2 \ K$ with $x_2 \ K_1$. Let $K_2 := (x_1) + (x_2)$. Then $K_2 = K$. So $x_3 \ K$ such that $x_3 \ K_2$. $K_3 := (x_1) + (x_2) + (x_3)$. Define K_i inductively like this for positive integers i. Let $S := \{K_i | i \ \mathbb{N}\}$; S has no maximal element. So, by the contrapositive, if M has the maximum condition on submodules then every submodule is finitely generated.

(iii) (ii). Let $K_1 \quad K_2 \quad \ldots$ be an ascending chain of submodules of M. Let $K := {}_{i=1} K_i$; then K is a submodule of M and K is finitely generated, generated by $x_1, \ldots, x_n \ K$, say. Then $t \ \mathbb{N}$ such that $x_1, \ldots, x_n \ K_t$. So $K = (x_1) + \cdots + (x_n) \ K_t$. Hence $K_t = K_{t+j}$ for all $j \geq 0$.

(ii) (i). Let S be a non-empty collection of submodules of M , Choose K_1 S. If K_1 is not maximal in S, K_2 S such that K_1 K_2. If K_2 is not maximal K_3 S such that K_2 K_3. So, by the Axiom of Choice, we obtain an ascending chain K_1 K_2 K_3 . . . of submodules of M . □

Theorem 5.2.9. *Let M_R be a right R-module. The following are equivalent*

(i) M has the minimum condition on submodules;

(ii) M has the descending chain condition on submodules;

Proof. Similar to the above. □

Examples 5.2.10. (i) A finite ring has both the ascending chain condi-tion and descending chain condition on right and left ideals.

(ii) A finite-dimensional algebra with 1 has both the ascending chain condition and descending chain condition on right and left ideals.

(iii) A commutative principal ideal domain has the ascending chain condition on ideals. Z, F [x] and J are commutative principal ideal domains. So, in particular, these have the ascending chain condition on ideals; they do not have the descending chain condition on ideals.

Theorem 5.2.11. *Let K be a submodule of a module M_R. Then M has the ascending chain condition (respectively the descending chain condition) on submodules if and only if $\frac{M}{K}$ has the ascending chain condition (respectively the descending chain condition) on submodules.*

Proof. ( ). Easy.

( ). Let M_1 M_2 . . . be an ascending chain of submodules of M . Consider the chains

$$M_1 \cap K \quad M_2 \cap K \quad \ldots,$$
$$M_1 + K \quad M_2 + K \quad \ldots.$$

The first chain consists of submodules of K, so j N such that $M_j \cap K = \cap K$ for all $i \geq 0$. The second chain consists of submodules of M

$\frac{M}{M_{j+i}}$

containing K. These are in one-to-one correspondence with submodules of

$\frac{M}{K}$. So $k \in \mathbb{N}$ such that $M_k + K = M_{k+i} + K$ for all $i \geq 0$. Let $n = \max\{j, k\}$. Now

$$\begin{aligned} M_{n+i} &= M_{n+i} \cap (M_{n+i} \cap K) \\ &= M_{n+i} \cap (M_n + K) \\ &= M_n + (M_{n+i} \cap K) \text{ by the Dedekind Modular Law} \\ &= M_n + (M_n \cap K) \\ &= M_n \end{aligned}$$

So M has the ascending chain condition on submodules. Similarly for the descending chain condition. □

Corollary 5.2.12. *Let $M_1, \ldots, M_n$ be submodules of M_R. If each M_i has the ascending chain condition (respectively, the descending chain condition) on submodules then so does $K := M_1 + \cdots + M_n$.*

Proof. Let $K_1 := M_1 + M_2$. Then by the Second Isomorphism Theorem,

$$\frac{K_1}{M_1} = \frac{M_1 + M_2}{M_1} = \frac{M_2}{M_1 \cap M_2}.$$

Now $\frac{M_2}{M_1 \cap M_2}$ has the ascending chain condition on submodules, since it is a factor of M_2. So $\frac{K_1}{M_1}$ has the ascending chain condition on submodules. Thus M_1 and $\frac{K_1}{M_1}$ have the ascending chain condition on submodules. So, by Theorem 5.2.11, K_1 has the ascending chain condition on submodules. Extend to K by induction.

Analagously for the descending chain condition. □

Corollary 5.2.13. *Let R have 1 and the ascending chain condition (respectively, the descending chain condition) on ideals. Let M_R be a (unital) finitely generated R-module. Then M has the ascending chain condition (respectively, the descending chain condition) on submodules.*

Proof. Since M_R is unital and finitely generated, there exist $m_1, \ldots, m_k \in M$ such that $M = m_1R + \cdots + m_k R$. By Corollary 5.2.12, it is enough to show that each m_iR has the ascending chain condition on submodules. Let $\theta_i : R_R \to m_iR : r \to m_ir$. Then θ_i is an R-homomorphism onto m_iR. So each m_iR is a factor module of R_R. Since R_R has the ascending chain con-dition on submodules it follows that m_iR has the ascending chain condition

on submodules.

Similarly for the descending chain condition. □

Remark 5.2.14. For the ascending chain condition the above result is still true even if R does not have 1; for the descending chain condition the result is false.

Corollary 5.2.15. *If R has the ascending chain condition (respectively, the descending chain condition) on right ideals then so does the ring $M_n(R)$.*

Proof. Consider $M_n(R)$ as a right R-module in the natural way. Let $T_{ij} := \{(r_k) \in M_n(R) \mid r_k = 0 \text{ if } k = i, = j\}$. Then each T_{ij} is an R-submodule of $M_n(R)$ that is isomorphic to R_R. So each T_{ij} has the ascending chain condition on R-submodules. But $M_n(R) = \sum_{i,j=1}^{n} T_{ij}$. So by Corollary 5.2.12, $M_n(R)$ has the ascending chain condition on R-submodules. Clearly, however, a right ideal of $M_n(R)$ is also an R-submodule of $M_n(R)$. So $M_n(R)$ has the ascending chain condition on right ideals.

Similarly for the descending chain condition. □

Example 5.2.16. Let D be a division ring. Then $M_n(D)$ has both the ascending chain condition and descending chain condition on right ideals, since 0 and D are the only (right) ideals of D.

Exercise 5.2.17. Let S be a subring of $M_n(\mathbb{Z})$ such that S contains the identity of $M_n(\mathbb{Z})$. Show that S is a ring with the ascending chain condition on right ideals.

Definitions 5.2.18. A module with the ascending chain condition on submodules is called a *Noetherian*[1] *module*. A module with the descending chain condition on submodules is called an *Artinian*[2] *module*. A ring with the ascending chain condition on right ideals is called a *right Noetherian ring*. A ring with the descending chain condition on right ideals is called a *right Artinian ring*. Similarly for *left Noetherian ring* and *left Artinian ring*.

Theorem 5.2.19. (The Hilbert Basis Theorem.) *If R is a right Noetherian ring then so is the polynomial ring $R[x]$.*

---

1 Amalie (Emmy) Noether (1883–1935)

2 Emil Artin (1898–1962)

((Seventh lecture))

6 Semi-Simple Artinian Rings

6.1 Nil and Nilpotent Subsets

Definitions 6.1.1. Let R be a ring.

(i) $x \in R$ is *nilpotent* if $x^n = 0$ for some $n \geq 1$.

(ii) A subset $S \subseteq R$ is a *nil subset* if every element of S is nilpotent. Thus S nil, $\forall x \in S\ n(x) \in \mathbb{N}$ such that $x^{n(x)} = 0$.

(iii) S is a *nilpotent subset* if $S^n = 0$ for some $n \geq 1$. Recall that

$$S^n = \{ s_1 s_2 \ldots s_n \mid s_i \in S \}.$$

finite

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

Examples 6.1.2. (i) In $M_2(\mathbb{Z})$, $\begin{matrix} 0 & 1 \\ 0 & 0 \end{matrix}$ is a nilpotent element.
(ii) In $\frac{\mathbb{Z}}{4\mathbb{Z}}$, $\frac{2\mathbb{Z}}{4\mathbb{Z}}$ is a nilpotent ideal.

Lemma 6.1.3. *(i) If I, K are nilpotent right ideals than so are $I + K$ and RI.*

(ii) Every nilpotent right ideal is contained in a nilpotent ideal.

Proof. (i) There are positive integers r, s such that $I^r = K^s = 0$. Con-sider $(I + K)^{r+s-1} = (I + K)(I + K) \ldots (I + K)$. This, when expanded, has 2^{r+s-1} terms, each of which has the form $T = A_1 A_2 \ldots A_{r+s-1}$, where each $A_i = I$ or K. So in a typical term either I occurs $\geq r$ times or K occurs $\geq s$ times.

Suppose I occurs $\geq r$ times. Then $T = K^i I^k$ where $i \geq 0$, $k \geq r$, with the convention $K^0 I = I$. We have used the fact that $I K I$. So $T = 0$. So every term in the expansion of $(I + K)^{r+s-1}$ vanishes. So $I + K$ is nilpotent.

$$(RI)^r = (RI)(RI) \ldots (RI) = R(I R) \ldots (I R)I \qquad RI^r = 0.$$

(ii) Let $I \triangleleft_r R$. If I is nilpotent then so is $I + RI$ by (i). Clearly $I + RI \triangleleft R$ and $I \subseteq I + RI$. □

Definition 6.1.4. The sum of all nilpotent ideals of R is calles the *nilpotent radical* of R, usually denoted $N(R)$.

It follows from Lemma 6.1.3 that

$N(R)$ = nilpotent right ideals = nilpotent left ideals.

Clearly $N(R)$ is a nil ideal. It is not, in general, nilpotent.

Exercise 6.1.5. Let R be a commutative ring. Show that $N(R)$ = the set of all nilpotent elements of R. (Hint: use the Binomial Theorem.) Give an example to show that this is false in general for non-commutative rings.

Example 6.1.6. (A Zassenhaus Algebra.) Let F be a field, I the interval $(0, 1)$, R the vector space over F with basis $\{x_i | i \in I\}$. Define multiplication on R by extending the following product on basis elements:

$$x_i x_j := \begin{cases} x_{i+j} & \text{if } i + j < 1, \\ 0 & \text{if } i + j \geq 1. \end{cases}$$

Thus every element of R can be written uniquely in the form $\sum_i a_i x_i$, with $a_i \in F$, with $a_i = 0$ for all but a finite number of indices i. Check that R is nil but not nilpotent and that $N(R) = R$.

6.2 Idempotent Elements

Definition 6.2.1. An element $e \in R$ is *idempotent* if $e = e^2$.

Examples 6.2.2. (i) In any ring, 0 is an idempotent element. If 1 exists, it is idempotent.

(ii) In $M_2(\mathbb{Z})$, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$ are idempotents.

Lemma 6.2.3. *Let e be an idempotent in a ring R. Then $R = eR \oplus K$, where $K = \{x - ex | x \in R\} \lhd_r R$.*

Proof. Clearly $K \lhd_r R$. Now $x \in R$ $x = ex + (x - ex) \in eR + K$. If $z \in eR \cap K$ then $z = ea = eb - b$ for some $a, b \in R$. Then

$$e^2 a = e^2 b - eb = eb - eb = 0$$

and

$$e^2 a = ea = 0.$$

So $z = 0$. So $R = eR \oplus K$ □

Corollary 6.2.4. (Peirce Decomposition.) *Let R be a ring with* 1 *and e R an idempotent. Then* $R = eR \ (1 - e)R$

Proof. $K = (1 - e)R$ in the above if R has 1. □

Remark 6.2.5. e is idempotent $1 - e$ is idempotent.

Exercise 6.2.6. Take an idempotent in $M_2(\mathbb{Z})$ and write down a Peirce decomposition.

Proposition 6.2.7. *Let R be a ring with* 1*. Suppose* $R = \sum_{j=1}^{n} I_j$, *a direct sum of right ideals. Then we can write* $1 = e_1 + \cdots + e_n$ *with* $e_j \in I_j$ *having the following properties:*

(i) each e_j is an idempotent;

(ii) $e_i e_j = 0$ for all $i \neq j$;

(iii) $I_j = e_j R$ for $j = 1, \ldots, n$;

(iv) $R = Re_1 \oplus \cdots \oplus Re_n$, a direct sum of left ideals.

Proof. (i) and (ii). For each j we have

$$e_j = 1e_j = e_1e_j + \cdots + e_{j-1}e_j + e_j^2 + e_{j+1}e_j + \cdots + e_ne_j .$$

So

$$e_j - e_j^2 = e_1e_j + \cdots + e_{j-1}e_j + e_{j+1}e_j + \cdots + e_ne_j \in I_j \cap \sum_{s \neq j} I_s = 0$$

by directness. So $e_j = e_j^2$ and $\sum_{s \neq j} e_s e_j = 0$. Since the sum of the I_j is direct, we have $e_i e_j = 0$ for all $i \neq j$.

(iii), (iv). Exercises. □ Example 6.2.8. Take $R = M_n(\mathbb{Z})$, $e_j = E_{jj}$ matrix unit. Then $1 = e_1 + \cdots + e_n$ and $R = e_1R \oplus \cdots \oplus e_nR = Re_1 \oplus \cdots \oplus Re_n$.

Definition 6.2.9. Let R be a ring. The *centre* of R is

$$C(R) := \{x \in R \mid r \in R, xr = rx\}.$$

$C(R)$ is a subring of R but not, in general, an ideal.

Exercise 6.2.10. Let F be a field. Find $C(M_n(F))$. Show that $C(M_n(F)) = F$ as rings.

Proposition 6.2.11. *Let R be a ring with* 1, *with $R = A_1 \oplus \cdots \oplus A_k$ a direct sum of ideals. Let* $1 = e_1 + \cdots + e_k$, $e_j \in A_j$. *Then*

(i) $e_j \in C(R)$ *for* $j = 1, \ldots, k$;

(ii) $e_j^2 = e_j$ *for all* j; $e_i e_j = 0$ *for* $i \neq j$;

(iii) $A_j = e_j R = R e_j$;

(iv) e_j *is the identity of the ring* A_j.

Proof. (ii) follows from Proposition 6.2.7.

(iii) $A_j = e_j R = R e_j$ as in Proposition 6.2.7 since $A_j \trianglelefteq_r R$ and $A_j \trianglelefteq R$.

(iv) Let $x \in A_j$. Then $x = e_j t_1 = t_2 e_j$ for some t_1, t_2. Then $e_j x = e_j^2 t_1 = e_j t_1 = x$ and $x e_j = t_2 e_j^2 = t_2 e_j = x$. Thus $x e_j = e_j x = x$ for all $x \in A_j$. Since $e_j \in A_j$, it follows that e_j is the identity of the ring A_j.

(i) Let $x \in R$. Then $e_j x = e_j^2 x = e_j (e_j x) = (e_j x) e_j$ since $e_j x \in A_j$ and e_j is the identity of A_j. Also $x e_j = x e_j^2 = (x e_j) e_j = e_j (x e_j)$ similarly. By associativity, $e_j x = x e_j$ for all $x \in R$, so $e_j \in C(R)$. □

Definition 6.2.12. Such an $e_j \in C(R)$ is called a *central idempotent*.

6.3 Annihilators and Minimal Right Ideals

Definitions 6.3.1. Let $S \subseteq M_R$. We define the *right annihilator* of S to be $r(S) := \{r \in R \mid Sr = 0\}$. Clearly, $r(S) \trianglelefteq_r R$. When S is a submodule of M, $r(S) \trianglelefteq R$. $\ell(S)$, the *left annihilator* of S, is defined analagously when M is a left R-module.

In most applications, $S \trianglelefteq R$ itself, and so we can consider both $r(S)$ and $\ell(S)$.

Definition 6.3.2. A non-zero right ideal M of a ring R is a *minimal right ideal* if whenever $M' \subseteq M$, $M' \trianglelefteq_r R$, it follows that $M' = 0$.

If R has 1 then the minimal right ideals of R are precisely the irreducible submodules of R_R.

Lemma 6.3.3. *Let M be a minimal right ideal of a ring R. Then either $M^2 = 0$ or $M = eR$ from some $e = e^2 \in M$.*

Proof. Suppose $M^2 = 0$. Then $a \in M$ such that $aM = 0$. $aM \leq_r R$ and $aM \subseteq M$ since $a \in M$. So $aM = M$. Thus $e \in M$ such that $a = ae$. $a = 0 \Rightarrow e = 0$. Also $a = ae = ae^2$. So $a(e - e^2) = 0$.

Now consider $M \cap r(a)$. $M \cap r(a) \leq_r R$ and $M \cap r(a) \subseteq M$. So $M \cap r(a) = 0$ or M. Suppose for a contradiction that $M \cap r(a) = M$. So $M \subseteq r(a)$, so $aM = 0$. Thus $M \cap r(a) = 0$.

But $e - e^2 \in M \cap r(a) = 0$, so $e = e^2$. Now $0 = e^2 \in eR$. So $eR = 0$. But $eR \leq_r R$ and $eR \subseteq M$ since $e \in M$. Thus $eR = M$ as required. □

Example 6.3.4. Take $R := \begin{pmatrix} Q & Q \\ 0 & Q \end{pmatrix}$. Consider $M_1 := \begin{pmatrix} 0 & Q \\ 0 & 0 \end{pmatrix}$, $M_2 := \begin{pmatrix} 0 & 0 \\ 0 & Q \end{pmatrix}$. Both M_1, M_2 are minimal right ideals. Now $M_1^2 = 0$, $M_2 = eR$ where $e := \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$.

Definition 6.3.5. A ring with no non-zero nilpotent ideal and the descending chain condition on right ideals is called a *semi-simple Artinian ring*.

Note that by Lemma 6.1.3(ii) and symmetry such a ring has no non-zero nilpotent right or left ideals.

Remarks 6.3.6. (i) The left-right symmetry of semi-simple Artinian rings will be established later.

(ii) We will justify the term "Artinian" by showing the existence of an identity.

(iii) We shall not define "semi-simple" on its own, but in this context it can be thought of as meaning a direct sum of simple rings.

Proposition 6.3.7. *Let R be a semi-simple Artinian ring and $I \leq_r R$. Then $I = eR$ for some $e = e^2 \in I$.*

Proof. By the minimum condition every non-zero right ideal of R con-tains a minimal right ideal. Hence, by Lemma 6.3.3, since R contains non non-zero nilpotent right ideal, every non-zero right ideal of R contains a non-zero idempotent.

Now if $I = 0$ then the result is trivial with $e = 0$, so assume that $I = 0$. Let E be the set of all non-zero idempotents in I. By the above, $E =$. We claim that there is an idempotent $e \in E$ such that $I \cap r(e) = 0$.

Suppose not. Let $I \cap r(z)$ be minimal in the set $S := \{I \cap r(x) | x \in E\}$. By assumption, $I \cap r(z) = 0$. So $I \cap r(z)$ contains a non-zero idempotent z . So $(z)^2 = z$, $zz = 0$. Consider $z_1 = z + z - z\,z$. $z_1 \in I$ since $z, z \in I$. We have

$$z_1 z = (z + z - z\,z)z = z + z\,z - z\,z = z.$$

So, in particular, $z_1 = 0$.

$$z_1 z = (z + z - z\,z)z = (z)^2 = z,$$

so

$$z_1^2 = z_1(z = z - z\,z) = z + z - z\,z = z_1.$$

Thus $z_1 \in E$. We shall now show that

$$r(z_1) \cap I \subseteq r(z) \cap I \tag{6.3.1}$$

t $r(z_1) \cap I z_1 t = 0 z z_1 t = 0 z t = 0$, since $z z_1 = z t \in r(z) \cap I$.

Also, $z \in r(z_1) \cap I$ but $z \notin r(z) \cap I$ since $z_1 z = z = 0$. This establishes (6.3.1). But (6.3.1) contradicts the minimality of $r(z) \cap I$. This proves our claim. So there is an $e \in E$ such that $I \cap r(e) = 0$.

Now define $K := \{x - ex | x \in I\}$. Then $K \subseteq_r R$, $K \subseteq I$, and $eK = 0$. So $K \subseteq I \cap r(e) = 0$. Thus $x = ex$ for all $x \in I$. Hence $I \subseteq eR$. But clearly $eR \subseteq I$ since $e \in I$ and $I \subseteq_r R$. So $I = eR$ as required. □

Corollary 6.3.8. *Let R be a semi-simple Artinian ring and $A \subseteq R$. Then there is an $e = e^2 \in A$ such that $A = eR = Re$.*

Proof. By Proposition 6.3.7, $A = eR$ for some $e = e^2 \in A$, since $A \subseteq_r R$. Let $K := \{x - xe | x \in A\}$. Then $K \subseteq R$, since $A \subseteq R$. Also, $Ke = 0$, so

$KeR = 0$ and $K^2 = 0$ since $KA = eR$. So $K = 0$ as R has no non-zero nilpotent left ideal. Thus $x = xe$ for all $x \in A$. So $A \subseteq Re$. But $Re \subseteq A$ since $e \in A$ and $A \subseteq R$. Thus $A = eR = Re$. □

Corollary 6.3.9. *A semi-simple Artinian ring has identity.*

Proof. Take $A = R$ in Corollary 6.3.8. □

Theorem 6.3.10. *The following are equivalent for any ring R:*

(i) R is semi-simple Artinian ring;

(ii) R has 1 *and* R_R *is completely reducible.*

Proof. (i) (ii). By Corollary 6.3.9 R has 1. Let $I \subseteq_r R$. By Proposition 6.3.7 $I = eR$ for some $e = e^2 \in I$. By Peirce Decomposition, Corollary 6.2.4, I is a direct summand of R. So every submodule of R_R is a direct summand of R_R. So by Theorem 4.2.6, R_R is completely reducible.

(ii) (i). We have $R = \sum_{\lambda \in \Lambda} I_\lambda$, I_λ an irreducible submodule of R_R. Then $1 = x_1 + \cdots + x_n$ for some $x_i \in I_{\lambda_i}$. Now for any $x \in R$,

$$x = 1x = x_1x + \cdots + x_nx \in I_{\lambda_1} + \cdots + I_{\lambda_n},$$

so $R = I_{\lambda_1} + \cdots + I_{\lambda_n}$ and $|\Lambda| < \infty$. So by Corollary 5.2.12, R_R has the descending chain condition on R-submodules, i.e. R has the descending chain condition on right ideals. Now let T be a nilpotent right ideal of R. Then $R = T + K$ for some $K \subseteq_r R$ by Theorem 4.2.6. We have $1 = t + k$ for some $t \in T$, $k \in K$, t nilpotent so $t^n = 0$ for some $n \geq 1$. Thus $(1 - k)^n = 0$. So $1 - nk + \cdots \pm k^n = 0$, $1 = nk - \cdots - k^n \in K$. So $K = R$, so $T = 0$ as required. □

Remark 6.3.11. Note that we have shown $R = I_1 + \cdots + I_n$, a finite direct sum of minimal right ideals, when R is semi-simple Artinian.

Corollary 6.3.12. *A direct sum of matrix rings over division rings is a semi-simple Artinian ring.*

Proof. It was shown in Theorem 4.2.6 that for such a ring R_R is com-pletely reducible. □

((Eighth lecture))

6.4 Ideals in Semi-Simple Artinian Rings

Proposition 6.4.1. *Let R be a semi-simple Artinian ring:*

(i) Every ideal of R is generated by an idempotent lying in the centre of R.

(ii) There is a 1-1 *correspondence between ideals of R and idempotents in C*(*R*)*.*

Proof. (i) See proofs of of Corollary 6.3.8 and Proposition 6.2.11.

(ii) For each e $C(R)$ define $f(e) := eR$ R. Check that f is the required 1-1 correspondence. □

Definition 6.4.2. I R is a *minimal ideal* if $I = 0$, I I, I R $I = 0$.

Theorem 6.4.3. *Let R be a semi-simple Artinian ring. Then R has a finite number of minimal ideals, their sum is direct, and is R.*

Proof. Note that at least one minimal ideal exists since R has the descending chain condition on right ideals . Let S_1 be a minimal ideal of R. Then by Proposition 6.4.1, $S_1 = e_1R = Re_1$, $e_1 = e_1^2$ $C(R)$. Note that $(1 - e_1)^2 = 1 - e_1$, $1 - e_1$ $C(R)$, and we have a direct sum of ideals
$R = S_1$ T_1, $T_1 := (1 - e_1)R = R(1 - e_1)$. (Note that T_1 is two-sided.)

If $T_1 = 0$, T_1 contains a minimal S_2 R. As above, $R = S_2$ K, K R. Now

$$T_1 = T_1 \cap R = T_1 \cap (S_2 \quad K) = S_2 \qquad (T_1 \cap K) = S_2\, T_2$$

by the Dedekind Modular Law. We have $R = S_1$ $T_1 = S_1$ S_2 T_2. If $T_2 = 0$ proceed inductively.

We have T_1 T_2 T_3 . . . , so by descending chain condition this pro-cess must terminate. It can only stop when some $T_m = 0$. At this stage we have $R = S_1 \cdot \cdot \cdot S_m$, a finite direct sum of minimal ideals.

Now let S be a minimal ideal of R. We have $SR = 0$ since R has 1. So $SS_j = 0$ for some j, $1 \le j \le m$. Now SS_j R and SS_j S, SS_j S_j . Since both S and S_j are minimal, we have $S = SS_j = S_j$. □

6.5 Simple Artinian Rings

Let R be a simple ring. Consider R^2. R^2 R so $R^2 = 0$ or R. Suppose $R^2 = 0$. Then $xy = 0$ for all x, y R. So any additive subgroup of R is an ideal of R. Thus R has no additive subgroups other than 0 and R. Thus the additive group of R must be cyclic of prime order p; the ring structure of

R is completely determined: $R = \{0, 1, \ldots, p - 1\}$ with addition modulo p, multiplication identically 0.

Thus, when studying simple rings, we assume that $R^2 = R$. Therefore, in this case, $N(R) = 0$.

Note that a simple Artinian ring is semi-simple Artinian.

Lemma 6.5.1. *Let R be a semi-simple Artinian ring and* $0 = I$ R. *Then*

I *itself is a semi-simple Artinian ring. In particular, when I is a minimal ideal, I is a simple Artinian ring.*

Proof. We claim that K $_r$ I K $_r$ R.

We have $I = eR = Re$ where $e = e^2$ I by Corollary 6.3.8. Now k K, r E $kr = (ke)r$ since e is the identity of I and k I. So $kr = k(er)$ K since er $eR = I$. This proves the claim.

It follows that I considered as a ring has the descending chain condition on right ideals and no non-zero nilpotent ideal.

If I is minimal then by the above it must be a simple Artinian ring. (Note that $I^2 = I$ since $I^2 = 0$ – i.e., I is a simple ring of the type that we are considering. □

Theorem 6.5.2. *Let R be a semi-simple Artinian ring. Then R is a direct sum of simple Artinian rings and this representation is unique.*

Proof. By Theorem 6.4.3 and Lemma 6.5.1 above we have $R = S_1$ $\cdots$ S_m, where the S_i are minimal ideals of R, hence simple Artinian rings. The uniqueness follows from the fact that the S_i are precisely the minimal ideals of R. □

6.6 Modules over Semi-Simple Artinian Rings

Proposition 6.6.1. *Let R be a semi-simple Artinian ring. Let M_R be unital and irreducible. Then $M = I$ as R-modules, where I R.*

Proof. $M = \frac{K}{R}$, K a maximal right ideal of R, by Exercise Sheet 3. By Corollary 6.2.4 and Proposition 6.3.7 (or by Theorem 6.3.10 and Theorem

k K, x I unique; consider r x). So $M = \overline{R} = I$ as R-modules. □

Theorem 6.6.2. *Every non-zero unital module over a semi-simple Artinian ring is completely reducible.*

Proof. Let R be semi-simple Artinian. We have $R = I_1 \cdot \cdot \cdot I_n$, a direct sum of minimal right ideals of R (see Remark 6.3.11). Let $0 = M_R$ be unital and let m M . Then $m = m1$ $mI_1 + \cdot \cdot \cdot + mI_n$. We claim that each mI_j is either irreducible or 0.

Consider the map $\theta : I_j \to mI_j$ given by $\theta(x) = mx$ for x I_j . Clearly θ is an R-homomorphism onto mI_j . ker θ is a submodule of $(I_j)_R$. So ker $\theta = 0$ or I_j . This implies that either θ is an isomorphism or the zero map. This proves the claim.

Thus, m irreducible submodules. So $M =$ irreducible submodules. So is completely reducible. □

6.7 The Artin-Wedderburn Theorem

Definitions 6.7.1. Let M be a right R-module. An R-homomorphism θ : M $\to M$ is called an *R-endomorphism*. The set of all R-endomorphisms of M is denoted by $E_R(M)$ or simply $E(M)$. On $E_R(M)$ we define a sum and product as follows. Let θ, φ $E_R(M)$. Define $\theta + \varphi$ and $\theta\varphi$ by

$$(\theta + \varphi)(m) := \theta(m) + \varphi(m)$$
$$(\theta\varphi)(m) := \theta(\varphi(m))$$

for m M . Check that $(\theta + \varphi)$, $(\theta\varphi)$ $E_R(M)$. It is routine to check that $E_R(M)$ is a ring under these operations.

Exercise 6.7.2. Show that if $M^1 = M^2$ as R-modules then $(M^1) = E_R(M_2)$ as rings.

More generally,

Definitions 6.7.3. For right R-modules X and Y denote the set of all R-homomorphisms $X \to Y$ by $\mathrm{Hom}_R(X, Y)$. For $\alpha, \beta \in \mathrm{Hom}_R(X, Y)$ define $\alpha + \beta$ as above. $\mathrm{Hom}_R(X, Y)$ is easily seen to be an Abelian group.

Definitions 6.7.4. Let $V = V_1 \cdot \cdot \cdot V_n$, $W = W_1 \cdot \cdot \cdot W_m$ be right R-modules. Let $\varepsilon_j : V_j \to V$ be the *injection map* $\varepsilon_j(v_j) := (0, \ldots, 0, v_j, 0, \ldots, 0)$ for $v_j \in V_j$ (the v_j is in the jth place).

Let $\pi_i : W \to W_i$ be the *projection map*, $\pi_i(w_1, \ldots, w_m) = w_i$, $w_k \in W_k$.

For a module M, write $M^{(n)}$ for $M \oplus \cdots \oplus M$ (n times).

Lemma 6.7.5. *Let $V = V_1 \oplus \cdots \oplus V_n$, $W = W_1 \oplus \cdots \oplus W_m$ be right R-modules.*

(i) If $\varphi_{ij} \in \mathrm{Hom}_R(V_j, W_i)$ are given for each $1 \le i \le m$, $1 \le j \le n$, then we can define $\varphi \in \mathrm{Hom}_R(V, W)$ by

$$\varphi(v_1, \ldots, v_n) := \begin{pmatrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \vdots \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

$$= (\varphi_{11}v_1 + \cdots + \varphi_{1n}v_n, \ldots, \varphi_{m1}v_1 + \cdots + \varphi_{mn}v_n).$$

(ii)

$$\mathrm{Hom}_R(V, W) = \begin{pmatrix} \mathrm{Hom}_R(V_1, W_1) & \cdots & \mathrm{Hom}_R(V_n, W_1) \\ \vdots & & \vdots \\ \mathrm{Hom}_R(V_1, W_m) & \cdots & \mathrm{Hom}_R(V_n, W_m) \end{pmatrix}$$

as Abelian groups.

(iii) In particular, for a right R-module M we have

$$E_R(M^{(n)}) = \begin{pmatrix} E_R(M) & \cdots & E_R(M) \\ \vdots & & \vdots \\ E_R(M) & \cdots & E_R(M) \end{pmatrix}$$

as rings.

Proof. (i) Easy to see that φ as defined above does indeed belong to $\mathrm{Hom}_R(V, W)$.

(ii) Let $\psi \in \mathrm{Hom}_R(V, W)$. Define $\psi_{ij} := \pi_i \psi \varepsilon_j$. Then $\psi_{ij} \in \mathrm{Hom}_R(V_j, W_i)$. Define a map

$$\Theta : \mathrm{Hom}_R(V, W) \to \begin{matrix} \mathrm{Hom}_R(V_1, W_1) & \cdots & \mathrm{Hom}_R(V_n, W_1) \\ \vdots & & \vdots \\ \mathrm{Hom}_R(V_1, W_m) & \cdots & \mathrm{Hom}_R(V_n, W_m) \end{matrix}$$

by $\Theta(\psi) := (\psi_{ij})$. It is easy to see that Θ is an additive group homomorphism.
Θ is injective:

$$\psi_{ij} = 0 \ \forall i, j \qquad \pi_i \psi \varepsilon_j = 0 \text{ for all } i, j$$
$$\psi \varepsilon_j = 0 \text{ for all } j$$
$$\psi = 0$$

Θ is surjective: let (θ_{ij}) be given with $\theta_{ij} \in \mathrm{Hom}_R(V_j, W_i)$. Define $\theta : V \to W$ by

$$\varphi(v_1, \ldots, v_m) := \begin{matrix} \varphi_{11} & \cdots & \varphi_{1n} \\ \vdots & & \vdots \\ \varphi_{m1} & \cdots & \varphi_{mn} \end{matrix} \begin{matrix} v_1 \\ \vdots \\ v_n \end{matrix}$$

Then $\theta \in \mathrm{Hom}_R(V, W)$ by part (i). For $v_j \in V_j$ we have

$$\begin{aligned} \pi_i \theta \varepsilon_j (v_j) &= \pi_i \theta(0, \ldots, 0, v_j, 0, \ldots, 0) \\ &= \pi_i(\theta_{1j}(v_j), \ldots, \theta_{mj}(v_j)) \\ &= \theta_{ij}(v_j) \end{aligned}$$

So $\pi_i \theta \varepsilon_j = \theta_{ij}$. Hence Θ is an isomorphism.

(iii) We must check that when $V = W = M^{(n)}$ then Θ defined above is a

ring homomorphism. Let $\theta, \varphi \quad E_R(M^{(n)})$. We have

$$
\begin{aligned}
(\theta\varphi)_{ij} &= \pi_i(\theta\varphi)\varepsilon_j \\
&= \pi_i\theta \, \mathrm{id}_{M^{(n)}} \varphi\varepsilon_j \\
&= \pi_i\theta \sum_{k=1}^{n} \varepsilon_k \pi_k \varphi\varepsilon_j \\
&= \sum_{k=1}^{n} (\pi_i\theta\varepsilon_k)(\pi_k \varphi\varepsilon_j) \\
&= \sum_{k=1}^{n} (\theta_{ik})(\varphi_{kj}) \\
((\theta\varphi)_{ij}) &= (\theta_{ik})(\varphi_{kj}) \\
\Theta(\theta\varphi) &= \Theta(\theta)\Theta(\varphi)
\end{aligned}
$$

So Θ is a ring homomorphism. □

Note that if $\theta : M_R \to K_R$ is an isomorphism then the inverse map exists and is an isomorphism from K onto M.

Corollary 6.7.6. (Schur's Lemma.) *Let R be a ring and M_R an irreducible module. Then $E_R(M)$ is a division ring.*

Proof. Let $0 = \theta \; E_R(M)$. We must show that θ is an isomorphism. θ is injective since $\ker \theta$ is a submodule of M, so $\ker \theta = 0$ or M. But $\ker \theta = M$ $\theta = 0$, a contradiction, so $\ker \theta = 0$ and θ is injective.

θ is surjective since $\theta(M)$ is a submodule of M. As above, $\theta(M) = 0$, so $\theta(M) = M$ and θ is surjective.

Thus θ is an isomorphism. Thus every non-zero element of $E_R(M)$ has an inverse, and so $E_R(M)$ is a division ring. □

Lemma 6.7.7. *Let R be a simple ring with $R^2 = R$. Then any two minimal right ideals of R are isomorphic as R-modules.*

Proof. Let I_1, I_2 be two minimal right ideals of R. Then $r(I_1)$ R and $r(I_1) = R$. So $r(I_1) = 0$, so $I_1 I_2 = 0$. So x I_1 such that $xI_2 = 0$. xI_2 $_r$ R

and $xI_2 \; I_1$ since $I_1 \; _r \; R$. So $xI_2 = I_1$. Now define a map $\theta : I_2 \to I_1$ by $\theta(r) = xr$ for $r \; I_2$. Check that $\ker \theta = 0$ so that θ is an isomorphism from I_2 onto $xI_2 = I_1$. □

Lemma 6.7.8. *Let R be a ring with* 1*. Then* $R \quad = \quad R \quad R \quad {}^{E}(R \;)$ *as rings.*

Proof. Let $x \; R$. Define $\rho_x \; E_R(R_R)$ by $\rho_x(r) = xr$ for $r \; R$. Fopr $r, \; s \; R$,

$$\rho_x(r + s) = x(r + s) = xr + xs = \rho_x \; (r) + \rho_x(s)$$

and

$$\rho_x(rt) = x(rt) = (xr)t = \rho_x(r)t.$$

So we do indeed have that $\rho_x \qquad E_R(R_R)$.

Now define $\Theta : R \to E_R(R_R)$ by $\Theta(x) = \rho_x$ for $x \; R$. We claim that Θ is an isomorphism of rings. Let $x_1, \; x_2 \; R$. Then for any $r \; R$,

$$\rho_{x1+x2} \; (r) + (x_1 + x_2)r = x_1r + x_2r = \rho_{x1} \; (r) + \rho_{x2} \; (r) = (\rho_{x1} + \rho_{x2} \;)(r),$$

so $\rho_{x1+x2} = \rho_{x1} + \rho_{x2}$, and hence $\Theta(x_1 + x_2) = \Theta(x_1) + \Theta(x_2)$. Also

$$\rho_{x1x2} \; (r) + (x_1x_2)r = x_1(x_2r) = \rho_{x1} \; (\rho_{x2} \; (r)) = (\rho_{x1} \; \rho_{x2} \;)(r),$$

so $\Theta(x_1x_2) = \Theta(x_1)\Theta(x_2)$. Θ is injective since $\rho_x = 0 \; \rho_x(1) = x1 = 0 \; x = 0$. Θ is surjective: let $\varphi \; E_R(R_R)$. Let $y := \varphi(1) \; R$. Then $\varphi(r) = \varphi(1r) = yr = \rho_y \; (r)$, for all $r \; R$. So $\varphi = \rho_y$. Thus Θ is an isomorphism of rings. □

Remark 6.7.9. If we work with left modules then we would have to define $\rho_x(r) = rx$. But then we get an anti-isomorphism between R and $E_R(R_R)$: $\Theta(xy) = \Theta(y)\Theta(x)$. To get an isomorphsim we need to write our maps on the right.

Theorem 6.7.10. (The Artin-Wedderburn Theorem.) *R is semi-simple Artinian if and only if $R = S^{1} \cdots \; S^{m}$, where $S^{i} = M^{n_i} \; (D^{i})$ for some integers n_i and division rings D_i.*

Proof. $R = S_1 \; \cdot \cdot \cdot \; S_m$, S_i simple Artinian by Theorem 6.5.2. $S_i = I_1 \; \cdot \cdot \cdot \; I_{ni}$, a direct sum of minimal right ideal, for some integer n_i, by Remark

6.3.11. But $I^j = I^k$ for all j, k, by Lemma 6.7.7. Thus $S_i = I^1 \oplus \cdots \oplus I^1$ (n_i summands). Thus,

$$\begin{aligned} S_i &= \underset{E_{S_i}}{\cdots} ((S_i)_{S_i}) \text{ by Lemma 6.7.8} \\ &= I^{(n_i)} \\ &= M_{n_i}(E_{S_i}(I_1)) \text{ by Lemma 6.7.5} \\ &= M_{n_i}(D_i), \end{aligned}$$

where $D_i := E_{S_i}(I_1)$ is a division ring by Schur's Lemma. □

Theorem 6.7.11. *A semi-simple Artinian ring is left-right symmetric.*

Proof. Right-hand conditions R is a direct sum of matrix rings over division rings left-hand conditions.

For another proof, see Exercise Sheet 5, Question 7. □

((The ninth lecture))

Wedderburn's Theorem on Finite Division Rings

In this chapter we prove that every finite division ring is a field.

Our strategy is to let D be a finite division ring. We show that $|D| = q^n$ for some $q \geq 2$, $n > 1$. If we set $D := D\backslash\{0\}$ then D is not an Abelian group. Counting elements in each conjugacy class of D we get an equation

$$q^n - 1 = q - 1 + \sum_{n(a)|n, n(a)=n} \frac{q^n - 1}{q^{n(a)} - 1}.$$

We then show that such an equation is impossible on number theoretic grounds.

7.1 Roots of Unity

Definitions 7.1.1. (i) θ is called a *primitive nth root of unity* if $\theta^n = 1$ and $\theta^m = 1$ for all $m < n$, where m and n are integers.

(ii) $\Phi_n(x) := \prod (x - \theta)$, where the product is taken over all primitive nth roots of

We note that the primitive nth roots of unity exist because of $y = e^{2\pi ki/n}$ C. Thus

$$\Phi_1(x) = x - 1$$
$$\Phi_2(x) = x + 1$$
$$\Phi_3(x) = x^2 + x + 1$$
$$\Phi_4(x) = x^2 + 1$$

Lemma 7.1.2. *Every cyclotomic polynomial is monic with integer coe - cients.*

Proof. First note that

$$x^n - 1 = \prod_{d|n} \Phi_d(x). \qquad (7.1.1)$$

Now we prove our claim by induction on n. If $n = 1$, $\Phi_1(x) = x - 1$. So, assume all $\Phi_k(x)$ monic with integer coefficients for $k < n$. Now we can write

$$x^n - 1 = \Phi_n(x) \prod_{d|n, d=n} \Phi_d(x).$$

By the induction hypothesis we can write $x^n - 1 = \Phi_n(x) f(x)$, where $f(x)$ is monic with coefficients in $\mathbb{Z}$. Therefore, we may assume that

$$f(x) = x^{} + a_{-1}x^{-1} + \cdots + a_1 x + a_0,$$

a_i $\mathbb{Z}$, and

$$\Phi_n(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x +$$

b_0, b_i $\mathbb{C}$. We see that

$$x^n - 1 = b_m x^{m+} + (b_{m-1} + b_m a_{-1})x^{m+-1} + \cdots + a_0 b_0.$$

Comparing these two polynomials, we have $b_m = 1$, so Φ_n is monic; $m+ = n$; $b_{m-1} + b_m a_{-1} = 0$, so $b_{m-1} = -1 \cdot a_{-1}$ $\mathbb{Z}$. By continuing this method, we see that b_i $\mathbb{Z}$ for $0 \le i \le m$. □

Lemma 7.1.3. *If $d|n$ and $d = n$ then*

$$\Phi_n(x) \qquad \frac{x^n - 1}{x^d - 1}$$

in the sense that the quotient is polynomial with integer coefficients.

Proof. By (7.1.1) we can write

$$\frac{x^d - 1}{x^n - 1} = \prod_{k|d, d \neq n} \Phi_k(x).$$

Because every divisor of d is a divisor of n, we have

$$\frac{x^n - 1}{x^d - 1} = \Phi_n(x) \prod_{d||n, d \neq d} \Phi_d(x)$$

and so $\frac{x^n}{x^d - 1} = \Phi_n(x) f(x)$, where

$$f(x) = \prod_{n,d \neq d} \Phi_d(x).$$

So $f(x)$ is a monic polynomial in $Z[x]$ by the previous lemma. So

$$\Phi_n(x) \qquad \frac{x^n - 1}{x^d - 1}$$

□

Lemma 7.1.4. *Let q, n, m be positive integers, $q > 1$. Then*

$$q^m - 1 | q^n - 1 \; m | n.$$

Proof. ( ). Evident.

( ). We may assume that $n > m$. Then $n = km + r$, $0 \le r < m$, $k > 0$. Now

$$\begin{aligned} \frac{q^n - 1}{q^m - 1} &= \frac{q^{km} q^r - 1}{q^m - 1} \\ &= \frac{q^{km} q^r q^r + q^r - 1}{q^m - 1} \\ &= q^r \frac{((q^m)^k - 1}{q^m - 1} + \frac{q^r - 1}{q^m - 1} \end{aligned}$$

By our assumption, the LHS is an integer, and $\frac{q^r((q^m)^k - 1}{q^m - 1}$ Z, so $\frac{q^r - 1}{q^m - 1}$ Z, so $r = 0$. Thus $m | n$. □

7.2 Group Theory

Definitions 7.2.1. Let G be a group. We say that x, y G are *conjugate* if a G such that $x = a^{-1} y a$, and so we can define an equivalence relation of conjugacy, and the corresponding *conjugacy classes*: $x^G := \{a^{-1} x a | a \; G\}$. We define

$C(x) = \{a \quad G | ax = xa\}$ to be the *centralizer* of x in G. The *centre* of G is

$$Z(G) := \{g \quad G | \; h \quad G, \; gh = hg\}.$$

Proposition 7.2.2. *For G a group, x G, $C(x)$ is a subgroup of G.*

Theorem 7.2.3. *Let G be a finite group. Then $|x^G| = |G : C(x)|$.*

Proof. Let a, b G. Then

$$a^{-1}xa = b^{-1}xb \qquad xab^{-1} = ab^{-1}x$$
$$(ab^{-1}) \quad C(x)$$
$$C(x)a = C(x)b$$

So there are as many elements in x^G as there are cosets of $C(x)$. □

7.3 Finite Division Rings

Lemma 7.3.1. *Let K be a non-zero subring of a finite division ring D. Then K is also a division ring.*

Proof. Exercise. Need 1_D K and x^{-1} K for x K, $x = 0$. □

Corollary 7.3.2. *The centre of a finite division ring is a field.*

Lemma 7.3.3. *Let D be a finite division ring with centre C. Then $|D| = q^n$ where $q = |C| > 1$ and n is some positive integer.*

Proof. C is a field. We can view D as a vector space over C. Let $n = \dim_C D$, with $d_1, \ldots, d_n$ a basis for D over C. So every element of D is uniquely expressible as $c_1d_1 + \cdots + c_nd_n$ with c_i C. So we have $|D| = q^n$. □

Theorem 7.3.4. (Wedderburn 1905.) *A finite division ring is necessarily a field.*

Proof. Let D be a finite division ring with centre C, $|C| = q$. Then $|D| = q^n$, $q \geq 2$, $n \geq 1$, by Lemma 7.3.3. We want to show that $D = C$, or, equivalently, that $n = 1$.

Assume that $n > 1$. Let a D, $C(a) := \{x \; D \mid xa = ax\}$. Then $C(a)$ is a subring of D. By Lemma 7.3.1, it is a division ring with $C(A)$ C. So $|C(a)| = q^{n(a)}$ for some $n(a) \geq 1$. $C(a) := C(a) \backslash \{0\}$ is a multiplicative subgroup of D. We have $|C(a)| = q^{n(a)} - 1$, $|D| = q^n - 1$. By Lagrange's Theorem, $q^{n(a)} - 1 | q^n - 1$. Lemma 7.1.4 implies that $n(a) | n$. Theorem 7.2.3 applied to D implies that the number of elements conjugate to a = the index of $C(a)$ in D = $\frac{q^n - 1}{q^{n(a)} - 1}$. Now a $C(a)$ $n(a) = n$. By counting elements of D :

$$q^n - 1 = q - \sum_{n(a)|n,\, n(a)=n} \frac{q^n - 1}{q^{n(a)} - 1}, \qquad (7.3.1)$$

where the sum is carried out for one a in each conjugacy class for elements not in the centre. Now $\Phi_n(q) = q^n - 1$ by Lemma 7.1.2; $n(a) = n$ by Lemma 7.1.3. By (7.3.1),

$$\Phi_n(q) \mid \frac{q^n - 1}{q^{n(a)} - 1}$$

$$\Phi_n(q) = q - 1. \tag{7.3.2}$$

We have $\Phi_n(q) = \prod (q - \theta)$, θ a primitive nth root of 1. So $|\Phi_n(q)| = |q - \theta| > q - 1$ since $n > 1$. This contradicts (7.3.2). So the assumption $n > 1$ is false, and $D = C$ is a field. □

To answer the question of what finite fields look like, we need Galois Theory.

((tenth lecture))

8 Some Elementary Homological Algebra

In this section all rings have 1 and all modules are unital.

8.1 Free Modules

Definitions 8.1.1. A right R-module F is *free* if

(i) F is generated by a subset S F;

(ii) $_i s_i r_i = 0$ $r_i = 0$ for all such finite sums with s_i S, r_i R.

We say that *free basis* for F. (Convention: $\{0\}$ is the free module generated by .)

An element of F has a unique epression as $s_1 r_1 + \cdots + s_k r_k$. A typical free module is isomorphic to $(R \cdots R \ldots)_R$. F_R free and finitely generated $F^R = (R \cdots R)^R$ (a finite direct sum).

The Z-module $\frac{Z}{nZ}$, $n > 1$, cannot be free: for suppose that $a^- = a + nZ$ is

an element of a free basis. Then $an^- = 0$, with $n = 0$, a contradiction.

8.2 The Canonical Free Module

Definition 8.2.1. Let A be a set indexed by Λ. Let F_A be the set of all formal sums

$$\sum_{a_\lambda r_\lambda} a_\lambda \qquad \text{many } r_\lambda = 0 \text{ for } a, r_\lambda \in R, \text{ finitely}$$

with $a_\lambda r_\lambda = a_\lambda s_\lambda$ $r_\lambda = s_\lambda$ for all $\lambda \in \Lambda$. We make F_A into the

canonical free right R-module by defining

$$a_\lambda r_\lambda + a_\lambda s_\lambda := a_\lambda (r_\lambda + s_\lambda)$$

and

$$a_\lambda r_\lambda \quad r := \qquad a_\lambda (r_\lambda r)$$

A is a free basis for F_A; we identify $a \qquad A$ with $a1 \qquad F_A$.

Proposition 8.2.2. *Every right R-module is the homomorphic image of a free right R-module.*

Proof. Let M be a free right R-module. Index the elements of M and form the free module F_M, considering M merely as a set. Elements of F_M are formal sums of the form $(m_i)r_i$, $m_i \in M$, $r_i \in R$. Define $\theta : F_M \to M : (m_i)r_i \to m_i r_i \in M$. This map is well-defined and is an R-homomorphism by the definition of F_M □

8.3 Exact Sequences

Definitions 8.3.1. Let M_i be a sequence of right R-modules and f_i a sequence of R-homomorphisms $M_i \to M_{i-1}$. The sequence (which may be finite or infinite)

$$\cdots \xrightarrow{f_{i+2}} M_{i+1} \xrightarrow{f_{i+1}} M_i \xrightarrow{f_i} M_{i-1} \xrightarrow{f_{i-1}} \cdots$$

is said to be *exact* if $\operatorname{im} f_{i+1} = \ker f_i$ for all i. A *short exact sequence* is an exact sequence of the form

$$0 \longrightarrow M \xrightarrow{f} M \xrightarrow{g} M \longrightarrow 0.$$

In a short exact sequence, since $0 \longrightarrow M \xrightarrow{f} M$ is exact, $\ker f = 0$ and so f is a monomorphism (an injective homomorphism). Since $M \xrightarrow{g} M \longrightarrow 0$ is exact, $\operatorname{im} g = M$ and g is an epimorphism (a surjective homomorphism).

Also $M = \operatorname{im} f = f(M) \in M$, so M is isomorphic to a submodule of M.

$$M = \frac{M}{\ker g} = \frac{M}{\operatorname{im} f}.$$

Given modules A and B we can construct the short exact sequence

$$0 \longrightarrow B \xrightarrow{i} A \xrightarrow{\pi} \frac{A}{B} \longrightarrow 0,$$

where i is the inclusion map and π the natural projection.

Proposition 8.3.2. *Given a short exact sequence*

$$0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$$

of right R-modules the following are equivalent:

(i) im α *is a direct summand of* B*;*

(ii) an R*-homomorphism* $\gamma : C \to B$ *with* $\beta\gamma = \mathrm{id}_C$ *;*

(iii) an R*-homomorphism* $\delta : B \to A$ *with* $\delta\alpha = \mathrm{id}_A$*.*

Proof. (i) (ii). Let $B = \mathrm{im}\ \alpha\ B_1$, B_1 a submodule of B. So $B = \ker\ \beta\ B_1$. Let $\beta_1 := \beta|_{B1}$. We have

$$C = \beta(B) = \beta(\ker\ \beta \quad B_1) = \beta B_1 \ = \beta_1 B_1,$$

so β_1 is an epimorphism. Also $\ker\ \beta_1 \ker\ \beta \cap B_1 = 0$. Thus β_1 is an isomorphism of B_1 onto C. Define $\gamma := \beta_1^{-1} : C \to B$. Then $\beta\gamma = \mathrm{id}_C$.

(ii) (i). We shall show that $B = \ker\ \beta\ \gamma\beta(B)$. If $b\ B$, $b = (b - \gamma\beta b) + \gamma\beta(b)$. $b - \gamma\beta(b) \ker\ \beta$ since

$$\beta(b - \gamma\beta(b)) = \beta(b) - \beta\gamma\beta(b) = \beta(b) - \mathrm{id}_C\ \beta(b) = \beta(b) - \beta(b) = 0,$$

and if z $\ker\ \beta \cap \gamma\beta(B)$ then $z = \gamma\beta(b)$ for some b B, and $\beta(z) = 0$. Thus

$$0 = \beta(z) = \beta\gamma\beta(b) = \beta(b),$$

so $z = 0$, $B = \ker\ \beta$ $\gamma\beta(B) = \mathrm{im}\ \alpha$ $\gamma\beta(B)$.

Similarly, we can show the equivalence of (i) and (iii). □

Definition 8.3.3. We say that the short exact sequence

$$0 \xrightarrow{\alpha} A \xrightarrow{\beta} B \longrightarrow C \longrightarrow 0$$

splits if any one (and hence all) of the above conditions holds.

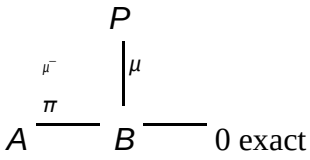
Note that if the above sequence splits then $B = \mathrm{im}\ \alpha$ $\overset{1}{B}, B^{1} = C$; i.e., =

8.4 Projective Modules

Definition 8.4.1. A right R-module P is said to be *projective* if given any diagram of the form

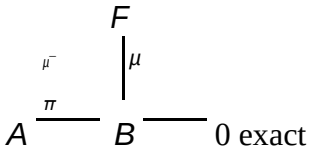
$$\begin{array}{ccccc} & & P & & \\ & & \downarrow \mu & & \\ A & \xrightarrow{\pi} & B & \longrightarrow & 0 \text{ exact} \end{array}$$

there is an R-homomorphism $\mu^- : P \to A$ such that $\mu = \pi\mu^-$, i.e. $\mu(x) = \pi(\mu^-(x))$ for all $x \in P$.



Lemma 8.4.2. *A free module is projective.*

Proof. Let F be a free module with a free basis $\{e_\alpha\}$. Consider



Let $b_\alpha := \mu(e_\alpha)$. As π is an epimorphism we can choose $a_\alpha \in A$ such that $b_\alpha = \pi(a_\alpha)$. Define $\mu^- : F \to A$ by $\mu^-(\sum_\alpha e_\alpha r_\alpha) := \sum_\alpha a_\alpha r_\alpha$, $r_\alpha \in R$. Then μ^- is an R-homomorphism $F \to A$ and

$$\pi\mu^-\left(\sum_\alpha e_\alpha r_\alpha\right) = \pi\left(\sum_\alpha a_\alpha r_\alpha\right)$$

$$= \sum_\alpha \pi(a_\alpha) r_\alpha$$

$$= \sum_\alpha b_\alpha r_\alpha$$

$$= \sum_\alpha \mu(e_\alpha) r_\alpha$$

$$= \mu\left(\sum_\alpha e_\alpha r_\alpha\right).$$

So $\pi\mu^- = \mu$. □

We shall see that a projective module need not be free.

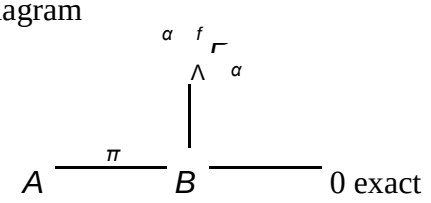
Lemma 8.4.3. *Let P_α, $\alpha \in \Lambda$, be right R-modules. Then $\sum_{\alpha \in \Lambda} P_\alpha$ is pro-jective if and only if all P_α are projective.*

$P \to P$.

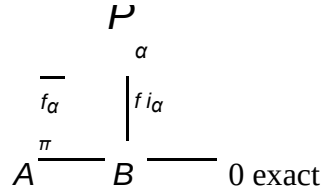
jection map $\alpha \wedge \alpha \beta \to \alpha \wedge$

Proof. Let i_β be the inclusion map P_β P_α; let p_β be the pro-

( ) Consider the diagram



This gives rise to diagrams



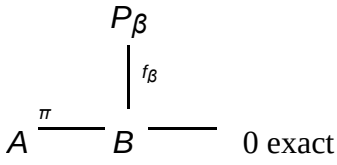
Since each P_α is projective there are R-homomorphisms $f_\alpha : P_\alpha \to A$ such

that $f i_\alpha = \pi f_\alpha$. Define f: $\alpha \wedge \alpha \alpha$ $\alpha \wedge f_\alpha p_\alpha$. (This makes

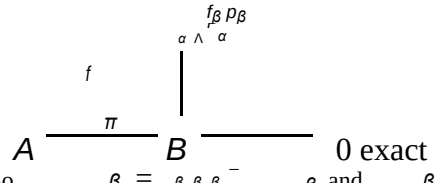
sense: for any z P we have $p(z) = 0$ for all except a finite number

of α's.) We have $= \alpha \wedge \alpha \alpha$ $\alpha \wedge \alpha \alpha$ as required.

( ) For any $\beta \Lambda$ consider



This gives rise to



such Since P_α is projective, there is an R-homomorphism f: $\beta \beta$. So $\beta = \beta \beta \beta$ β and β $P \to A$

that $\alpha \wedge$ $\pi f = f p$ $\pi f i$ $f p i$ f $f i$ $P \to A$. Thus

P_β is projective. □

Proposition 8.4.4. *The following are equivalent:*

(i) P is a projective module;

(ii) P is a direct summand of a free module;

(iii) every short exact sequence $0 \to M \to M \to P \to 0$ *splits.*

Proof. (iii) (ii). Consider the short exact sequence

$$0 \longrightarrow K_P \longrightarrow F_P \longrightarrow P \to 0,$$

where K_P is the kernel of the canonical map $F_P \to P$. Since this short exact sequence splits we have $F_P = P \oplus K_P$.

(ii) (i). Follows from Lemma 8.4.2 and Lemma 8.4.3.

(i) (iii). Consider

$$\begin{array}{ccccccccc} & & & & & & P & & \\ & & & & & \overset{\mu^-}{\swarrow} & \downarrow{\scriptstyle \mathrm{id}_P} & & \\ 0 & \longrightarrow & M & \overset{f}{\longrightarrow} & M & \overset{g}{\longrightarrow} & P & \longrightarrow & 0 \text{ exact} \end{array}$$

Since P is projective, there is an R-homomorphism $\mu^- : P \to M$ such that $g\mu^- = \mathrm{id}_P$. Thus the given short exact sequence splits. □

Theorem 8.4.5. *The following are equivalent:*

(i) R is semi-simple Artinian;

(ii) every unital right R-module is projective.

Proof. (i) (ii). Let M be a right R-module. By Theorem 6.6.2, $M = \sum_\lambda \oplus M_\lambda$, each M_λ irreducible. Proposition 6.6.1 implies that each M_λ is isomorphic to a right ideal of R. A right ideal of R is a direct sum-mand of R since R_R is completely reducible. So, by Lemma 8.4.2 and Lemma 8.4.3, right ideals of R are projective. So M is projective by Lemma 8.4.3.

(ii) (i). Let $I \leq_r R$. Consider the short exact sequence

$$0 \longrightarrow I \xrightarrow{i} R \xrightarrow{\pi} \frac{R}{I} \longrightarrow 0.$$

This short exact sequence splits since $\frac{R}{I}$ is a projective R-module. So $R = I \oplus K$, $K \leq R$. Thus I is a direct summand of R. So R_R is completely

reducible and thus R is semi-simple Artinian. □

If R is a ring with 1, then all right R-modules are free if and only if R is a division ring (Exercise Sheet 5, Question 8).

Example 8.4.6. Projective free. Let $R = {}_{6}\mathbb{Z}_{\mathbb{Z}}$, $A = {}_{\overline{2}_6}\mathbb{Z}_{\mathbb{Z}}$, $B = {}_{\overline{3}_6}\mathbb{Z}_{\mathbb{Z}}$. Then $R = A \oplus B$, and A and B are projective by Lemma 8.4.2 and Lemma 8.4.3. A, B cannot be free since they have fewer elements than R.