MA377 Rings and modules :: Lecture notes

Lecturer: Dmitriy Rumynin

12th May 2024

Contents

1 Introduction **1**
1.1 Definitions . . . 1
1.2 Chinese remainder theorem . . . 3
1.3 Isomorphism theorems . . . 4

2 Basis **6**
2.1 Free module . . . 6
2.2 Embark on Artin–Wedderburn theory . . . 8
2.3 Algebra . . . 10
2.3.1 Polynomial . . . 12
2.3.2 Noncommutative Nullstellensatz . . . 12

3 Division **13**
3.1 Quaternion . . . 13
3.1.1 Quaternions form a division ring . . . 14
3.1.2 Multiplicative group of quaternions . . . 15
3.1.3 Orthogonal matrix and transformation . . . 16
3.1.4 3D rotation . . . 17
3.1.5 4D scroll . . . 18
3.2 Division algebra over $\mathbb{R}, \mathbb{C}$ . . . 19
3.3 Finite division ring . . . 22
3.3.1 Finite group action . . . 25
3.3.2 Cyclotomic polynomial . . . 27
3.3.3 Unabomber theorem . . . 28
3.4 Laurent series . . . 28

4 Semisimplicity **30**
4.1 Direct sum . . . 30
4.1.1 Peirce decomposition . . . 30

4.1.2 Primary decomposition (example of Peirce decomposition) 32
4.1.3 Primary decomposition on a vector space 32
4.1.4 Peirce decomposition and matrix 33
4.2 Semisimple module 35
4.2.1 Radical 38
4.3 Semisimple ring 40
4.3.1 Artin–Wedderburn theorem 40
4.3.2 Semisimple algebra 41
4.3.3 Maschke's theorem 42
4.4 Jacobson radical 44

Week 1, lecture 1 starts here

1 Introduction

1.1 Definitions

Definition 1.1.1. A *ring* is ...

A ring R is *commutative* if $xy = yx\ \forall x, y \in R$.

R is a *division ring* if $(R\backslash\{0\}, \cdot)$ is a group.

R is a *field* if it's a commutative division ring.

Definition 1.1.2. A *left R-module* is an abelian group M and an action map $R \times M \to M$ such that $1_R m = m,\ (x+y)m = xm + ym,\ x(m+n) = xm + xn,\ x(ym) = (xy)m\ \forall m \in M,\ x, y \in R$. A *right R-module* is similar except the last axiom reads $x(ym) = (yx)m$, also written $(my)x = m(yx)$, with element of R written on the right.

Example 1.1.3. Each R is a left/right module over itself by left/right multiplication, denoted ${}_R R$ and R_R.

$M_n(R)$ is a ring with usual addition and multiplication of matrices. Column/row vectors form a left/right $M_n(R)$-module.

Definition 1.1.4. A *ring homomorphism* is a function $f : R \to S$ such that $f(x + y) = f(x) + f(y),\ f(xy) = f(x)f(y),\ f(1_R) = 1_S$. An *isomorphism* is a bijective homomorphism.

Notation. $R \times S := \{(r, s) : r \in R,\ s \in S\}$. This is a ring with the obvious trivial addition and multiplication.

Example 1.1.5. $i_1 : R \to R \times S : r \mapsto (r, 0)$ is not a homomorphism since $i_1(1_R) = (1_R, 0_S) \neq (1_R, 1_S) = 1_{R\times S}$, but it satisfies the first two conditions.

$\pi_1 : R \times S \to R : (r, s) \mapsto r$ is.

Week 1, lecture 2 starts here

Definition 1.1.6. $A \subseteq R$ is a *subring* of R if A is a ring under the same operations, i.e. $1_R \in A,\ xy, x - y \in A\ \forall x, y \in A$.

Example 1.1.7. Centre of R: $Z(R) := \{x \in R : xy = yx\ \forall y \in R\}$.

Centraliser of $X \subseteq R$ in R: $C_R(X) := \{y \in R : xy = yx\ \forall x \in X\}$.

Definition 1.1.8. A left (or right) *ideal* of R is an additive subgroup $L \leq R$ such that xa (or ax) $\in L\ \forall a \in L, x \in R$, denoted $L \trianglelefteq^l R$ or $L \trianglelefteq^r R$. L is a two-sided ideal (or simply ideal) of R if it's both a left and right ideal, denoted $L \trianglelefteq R$.

If $I \trianglelefteq R$ then $R/I = \{x + I : x \in R\}$ is a ring, called the *quotient ring*, with the following definitions:

$$(x + I) + (y + I) = (x + y) + I$$
$$(x + I)(y + I) = xy + I$$
$$1_{R/I} = 1_R + I$$

Example 1.1.9. For $x_1, \dots, x_n \in R$, one can generated an ideal

$$(x_1, \dots, x_n) = Rx_1R + \cdots + Rx_nR = \{r_1x_1s_1 + \cdots + r_nx_ns_n : r_i, s_i \in R\}.$$

If R is commutative, then

$$(x_1, \dots, x_n) = Rx_1 + \cdots + Rx_n = \{r_1x_1 + \cdots + r_nx_n : r_n \in R\}.$$

Lemma 1.1.10. Let S be a ring and $R = M_n(S)$ with E_{ij}, a matrix with 1 on the i, j position and 0 elsewhere. Then $(E_{ij}) = R$.

Proof. Let $I = (E_{ij})$. One has

$$\begin{aligned} E_{RR} &= E_{Ri}E_{ij}E_{jR} \in I \\ 1_R &= E_{11} + \cdots + E_{nn} \in I \\ x &= x1_R \in I \ \forall x \in R \end{aligned}$$

□

Definition 1.1.11. A *principal ideal domain* is ...

A *unique factorisation domain* is ...

Every PID is a UFD.

Lemma 1.1.12. If R is a UFD and $x_1, \dots, x_n \in R$ with $m = \operatorname{lcm}(x_i)$, then

$$(x_1) \cap \cdots \cap (x_n) = (m).$$

Proof.

$$(x_1) \cap \cdots \cap (x_n) = \{a : x_i \mid a \ \forall i\} = \{a : m \mid a\} = (m).$$

□

Lemma 1.1.13. If R is a PID and $x_1, \dots, x_n \in R$ with $d = \gcd(x_1, \dots, x_n)$, then

$$(x_1) + \cdots + (x_n) = (d).$$

Proof. $\subseteq$: $d \mid x_i \ \forall i \implies d \mid (a_1x_1 + \cdots + a_nx_n)$.

$\supseteq$: Since R is a PID, $\exists z \in R : (x_1) + \cdots + (x_n) = (z)$. We want to show $(z) \supseteq (d) \iff z \mid d$. But $(z) \supseteq (x_i)$, so $z \mid x_i \implies z \mid \gcd(x_i) = d$.

□

Remark. This indeed fails for UFDs. Consider $R = \mathbb{C}[x, y]$, then $\gcd(x, y) = 1$, but $(x) + (y) = (x, y) \neq (1) = R$.

Theorem 1.1.14 (Isomorphism theorems for rings)**.** If $f : R \to S$ is a ring homomorphism, then

1. $\ker f \trianglelefteq R$
2. $\operatorname{im} f \leq S$
3. f decomposes as

$$R \twoheadrightarrow R/\ker f \xrightarrow[\bar{f}]{} \operatorname{im} f \hookrightarrow S$$

Week 1, lecture 3 starts here

1.2 Chinese remainder theorem

Theorem 1.2.1 (Elementary form of Chinese remainder)**.** The system

$$\begin{aligned} x &\equiv k_1 \bmod n_1 \\ &\vdots \\ x &\equiv k_t \bmod n_t \end{aligned}$$

where $n_1, \ldots, n_t \in \mathbb{Z}$ relatively prime and $k_1, \ldots, k_t \in \mathbb{Z}$, has a solution, and any two solutions differ by a multiple of $n_1 \cdots n_t$.

Proof. Consider

$$\begin{aligned} f : \mathbb{Z} &\to \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_t) \\ x &\mapsto (x + (n_1), \ldots, x + (n_t)). \end{aligned}$$

By Lemma 1.1.12, $\ker f = (n_1) \cap \cdots \cap (n_t) = (n_1 \cdots n_t)$. By the isomorphism theorems,

$$\mathbb{Z}/(n_1 \cdots n_t) \xrightarrow[\overline{f}]{} \operatorname{im} f \hookrightarrow \mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_t),$$

but both $\mathbb{Z}/(n_1 \cdots n_t)$ and $\mathbb{Z}/(n_1) \times \cdots \times \mathbb{Z}/(n_t)$ has $|n_1 \cdots n_t|$ elements, so it's an isomorphism. Therefore $\exists x \in \mathbb{Z} : f(x) = (k_1, \ldots, k_t)$.
If y is another solution, then $f(x - y) = f(x) - f(y) = 0$, i.e. $x - y \in \ker f = (n_1 \cdots n_t)$. $\square$

Example 1.2.2. Consider the system

$$\begin{aligned} x &\equiv 1 \bmod 7 \\ x &\equiv 7 \bmod 9 \\ x &\equiv 3 \bmod 11 \end{aligned}$$

Note that by f in the proof,

$$\begin{aligned} 7 \times 9 = 63 &\mapsto (0, 0, 8) \\ 7 \times 11 = 77 &\mapsto (0, 5, 0) \\ 9 \times 11 = 99 &\mapsto (1, 0, 0), \end{aligned}$$

and one needs $f(x) = (1, 7, 3)$, but

$$\begin{aligned} (1, 7, 3) &= (1, 0, 0) + (0, 7, 0) + (0, 0, 3) \\ &= (1, 0, 0) + 5 \times (0, 5, 0) - (0, 0, 8) \\ &= f(99) + 5 \times f(77) - f(63) \\ &= f(99 + 5 \times 77 - 63) \\ &= f(421). \end{aligned}$$

Definition 1.2.3. Let $I, J \trianglelefteq R$. I and J are *coprime* if $I + J = R$.

Lemma 1.2.4. If $I_1, \ldots, I_n \trianglelefteq R$, then

$$\begin{aligned} f : R &\to R/I_1 \times \cdots \times R/I_n \\ x &\mapsto (x + I_1, \ldots, x + I_n) \end{aligned}$$

is a ring homomorphism with kernel $I_1 \cap \cdots \cap I_n$.

Theorem 1.2.5. If $I_1, \dots, I_n$ are pairwise coprime then

$$\overline{f} : R/(I_1 \cap \cdots \cap I_n) \to R/I_1 \times \cdots R/I_n$$

is an isomorphism.

Proof. It suffices to find, for each i, $a_i \in R : f(a_i) = e_i$, since then f would be surjective:

$$\begin{aligned}(x_1 + I_1, \dots, x_n + I_n) &= (x_1 + I_1)e_1 + \cdots + (x_n + I_n)e_n \\ &= f(x_1)f(a_1) + \cdots + f(x_n)f(a_n) = f(x_1a_1 + \cdots + x_na_n).\end{aligned}$$

Let's now find a_i. Note that $\forall j \neq i,\ I_i + I_j = R \ni 1$, so $\exists b_j \in I_i,\ c_j \in I_j : b_j + c_j = 1$. We claim $a_i = \prod_{j \neq i} c_j$. Indeed, $c_j = 0$ in I_j and 1 in I_i. $\square$

Example 1.2.6. In the same example as above, note that $7 \times 9 \times 11 = 693$ and we can write

$$28 - 27 = 45 - 44 = -21 + 22 = 1$$

where $28, -21 \in (7),\ -27, 45 \in (9)$ and $-44, 22 \in (11)$. Hence

$$\begin{aligned}a_1 &= (-27)(22) = -594 \equiv 99 \bmod 693 \\ a_2 &= (28)(-44) = -1232 \equiv 154 \bmod 693 \\ a_3 &= (-21)(45) = -945 \equiv 441 \bmod 693\end{aligned}$$

Week 2, lecture 1 starts here

1.3 Isomorphism theorems

With a left/right R-module we can convert R into its opposite R^{op} by swapping the multiplication. Then a right R-module is a left R^{op}-module, and vice versa.

Definition 1.3.1. For a R-module ${}_RM$, $N \leq M$ is a *submodule* if it's an abelian subgroup and $\forall r \in R, x \in N : rx \in N$.

Note for ${}_RR$ and R_R, submodules are precisely left/right ideals.

Definition 1.3.2. For ${}_RM \geq_R N$, the abelian quotient group M/N is called the *quotient module*, with multiplication defined $r(x + N) = rx + N$. This is well-defined since

$$\begin{aligned}x + N = y + N &\implies x - y \in N \\ &\implies r(x + N) = rx + N = r(y + (x - y))N = ry + r(x - y) + N = ry + N = r(y + N).\end{aligned}$$

Other axioms follow from those for ${}_RM$.

Example 1.3.3. If $L \trianglelefteq R$ then R/L is a left R-module.

Definition 1.3.4. A *homomorphism* of R-modules $\varphi :_R M \to_R N$ is a homomorphism of abelian groups and $\varphi(rm) = r\varphi(m)\ \forall r \in R, m \in M$.

For left R-modules, we write homomorphism on the right: $(rm)\varphi = r(m\varphi) = rm\varphi$ to keep in line with the can-get-rid-of-bracket perspective of associativity. For right R-modules we then simply write $\varphi(mr) = \varphi(m)r = \varphi mr$.

Theorem 1.3.5 (1st isomorphism theorem)**.** If R-modules $\varphi :_R M \to_R N$ is a homomorphism of modules, then

1. $\ker \varphi \leq_R M$
2. $\operatorname{im} \varphi \leq_R N$
3. φ decomposes as

$$\begin{aligned} M \overset{\pi}{\twoheadrightarrow} M/\ker\varphi &\quad \underset{\overline{\varphi}}{\overset{\cong}{\to}} \operatorname{im}\varphi \overset{\iota}{\hookrightarrow} N \\ m \mapsto m + \ker\varphi &\quad \mapsto m\varphi \\ &\qquad\quad x \mapsto x \end{aligned}$$

Proof. All statements hold on the level of abelian groups by isomorphism theorems for groups. It remains to see the R-module structure through.

1. Let $m \in \ker\varphi$, $r \in R$. Then $(rm)\varphi = r(m\varphi) = r0_M = 0_M$, so $rm \in \ker\varphi$, so indeed $\ker\varphi \leq_R M$.
2. Let $x \in \operatorname{im}\varphi$, $r \in R$. Then $\exists m \in M : m\varphi = x$. Then $rx = r(m\varphi) = (rm)\varphi \in \operatorname{im}\varphi$, so indeed $\ker\varphi \leq_R N$.
3. We need to check all 3 maps are homomorphism of R-modules.
   - $(rm)\pi = rm + \ker\varphi = r(m + \ker\varphi) = r(m\pi)$.
   - $(r(m + \ker\varphi))\overline{\varphi} = (rm + \ker\varphi)\overline{\varphi} = (rm)\varphi = r(m\varphi) = r((m + \ker\varphi)\overline{\varphi})$.
   - $(rx)\iota = rx = r(x\iota)$.

□

Proposition 1.3.6 (2nd isomorphism theorem)**.** If ${}_RM, K \leq_R N$ then

$$\frac{M+K}{M} \cong \frac{K}{M \cap K}.$$

Proposition 1.3.7 (3rd isomorphism theorem)**.** If ${}_RK \leq_R M \leq_R N$ then

$$\frac{N/K}{M/K} \cong \frac{N}{M}.$$

Proposition 1.3.8 (Correspondence theorem)**.** Let ${}_RM \leq_R N$. Denote the set of all submodules of N by $S(N)$ and the set of all submodules of N containing M by $S(N, M)$. Then

$$\begin{aligned} \pi : N &\to N/M \\ n &\mapsto n + m \end{aligned}$$

gives a bijection

$$\begin{aligned} S(N, M) &\leftrightarrow S(N/M) \\ {}_RM \leq_R A \leq_R N &\mapsto \pi(A) \\ \pi^{-1}(B) &\leftarrow_R B \leq_R N/M \end{aligned}$$

Notation. $\operatorname{Hom}({}_RM, {}_RN) = \{\text{homomorphisms } \varphi : M \to N\}$. This is an abelian group.

$\operatorname{End}_R M = \{\text{homomorphisms } \varphi : M \to M\}$. This is a ring.

Example 1.3.9. Let R be a (noncommutative) ring, $A = M_a(R),\ B = M_b(R)$, two rings and $V = R^{a\times b}$, which is just an abelian group. Then ${}_AV$ is a left module and V_B is a right module, and there's no natural choice for V to be a right A-module or a left B-module.

Now consider $E = \mathrm{End}_A V$. Our convention turns V into a right E-module, and there is a ring homomorphism

$$\begin{aligned}\varphi : B &\to E\\ y &\mapsto (\gamma \mapsto \gamma y)\end{aligned}$$

Similarly, if $F = \mathrm{End} V_B$ then V is a left F-module and there is a ring homomorphism $\psi : A \to F$. In fact they are isomorphisms, the proof is left as an exercise.

Lemma 1.3.10 (The $a = b = 1$ special case)**.** $\mathrm{End}_R R \cong R$.

Proof. Consider

$$\begin{aligned}\varphi : R &\to \mathrm{End}_R R\\ x &\mapsto \varphi_x : r \mapsto rx\end{aligned}$$

φ is well-defined since φ_x is well-defined. Also, $(sr)\varphi_x = srx = s(r\varphi_x)$, so indeed $\varphi_x \in \mathrm{End}_R R$. Also, $r\varphi_{x+y} = r(x+y) = rx+ry = r\varphi_x + r\varphi_y = r(\varphi_x + \varphi_y)$, $r\varphi_{xy} = rxy = (r\varphi_x)\varphi_y = r(\varphi_x\varphi_y)$, and $r\varphi_{1_R} = r1 = r = r1_{\mathrm{End}_R R}$, so φ is indeed a homomorphism.

Suppose $\varphi_x = 0$, i.e. $r\varphi_x = 0\ \forall r \in R$. Then for $r = 1,\ 0 = 1\varphi_x = 1x = x$, so $\ker\varphi = \{0\}$, i.e. φ is injective.

Now pick $f \in \mathrm{End}_R R$ and let $x = 1_R f$. Then $\forall r \in R,\ r\varphi_x = rx = r1_R f = rf$. So $f = \varphi_x$, and φ is surjective. $\square$

2 Basis

2.1 Free module

Notation. Let ${}_RM$ be a left module and X a subset of M. Then

$$\mathrm{Fun}(X, M) := \{\text{functions } X \to M\}.$$

This is a left R-module, with a submodule

$$\mathrm{Fun}_f(X, M) := \{f : f(x) = 0\ \forall \text{ but finitely many } x \in X\}.$$

Definition 2.1.1. A subset $X \subseteq_R M$ *spans* M if $\forall m \in M$,

$$\exists f \in \mathrm{Fun}_f(X, R) : m = \sum_{a\in X} f(a)a.$$

X is linearly independent if $\forall f \in \mathrm{Fun}_F(X, R)$,

$$\sum_{a\in X} f(a)a = 0 \implies f(a) = 0 \forall a \in X.$$

X is a *basis* for M if it spans M and is linearly independent.

Definition 2.1.2. ${}_RM$ is *free* if it admits a basis.

Example 2.1.3. 1. Let $R = \mathbb{Z}$ and $M = \mathbb{Z}/n\mathbb{Z}$. Then $\{1 + n\mathbb{Z}\}$ spans M but M is not free, since $nx = 0\ \forall x \in M$.

2. $\varnothing \subseteq M$ is linearly independent for any M, since $\mathrm{Fun}(\varnothing, R)$ only has one element $\widehat{\varnothing}$ which is identically zero, and summing over nothing gives zero.

3. Let R be a ring, $M =_R R$, and $X = \{a\}$. Then

$$X \text{ is linearly independent} \iff (ba = 0 \implies b = 0)$$
$$X \text{ spans } {}_RR \iff (\exists b : ba = 1_R)$$

Week 2, lecture 3 starts here

Lemma 2.1.4. $\forall$ set X and $\forall R$, $\exists$ a free R-module M with a basis of cardinality $|X|$.

Proof. Let $M = \mathrm{Fun}_f(X,_R R)$. Then $\forall a \in X,\ \delta_a \in M$ where $\delta_a(b) := \begin{cases} 1_R & a = b \\ 0_R & a \neq b \end{cases}$. This gives us a basis. Indeed,

- For $f \in M$, list all $x_1, \ldots, x_n \in X : f(x_1) \neq 0_R$. Then
$$f = f(x_1)\delta_{x_1} + \cdots + f(x_n)\delta_{x_n}.$$
So it spans M.
- If $r_1\delta_{x_1} + \cdots + r_n\delta_{x_n} = 0_M$ then
$$0_R = (r_1\delta_{x_1} + \cdots + r_n\delta_{x_n})(x_i) = r_i\delta_{x_i}(x_i) = r_i\ \forall i,$$
so $\{\delta_{x_1}, \ldots, \delta_{x_n}\}$ is linearly independent.

□

Lemma 2.1.5. Every ${}_RM$ is isomorphic to a quotient of a free module.

Proof. Pick $M \subseteq M$ that spans M (e.g. $X = M$). Then

$$\varphi : \mathrm{Fun}_F(X, R) \to M$$
$$f \mapsto \sum_{a \in X} f(a)a$$

is surjective. By lemma above, $\mathrm{Fun}_F(X, R)$ is free, and by 1st isomorphism theorem,

$$M \cong \mathrm{Fun}_f(X, R)/\ker\varphi.$$

□

Definition 2.1.6. A *partially ordered set* (or *poset*) is denoted $(\mathcal{P}, \preceq)$ where $\preceq$ can be viewed as a subset of $\mathcal{P} \times \mathcal{P}$. If $(x, y) \in \preceq$ we denote it as $x \preceq y$. The $\preceq$ satisfies that it's reflexive, antisymmetric ($x \preceq y, y \preceq x \implies x = y$) and transitive.

A partial order $\preceq$ is *linear order* if $\forall x, y \in \mathcal{P}$, either $x \preceq y$ or $y \preceq x$.

A *chain* is a subset $X \subset \mathcal{P}$ such that $(X, \preceq)$ is a linearly ordered set.

$a \in \mathcal{P}$ is a *maximal element* if $\forall b \in P,\ a \preceq b \implies a = b$.

$a \in \mathcal{P}$ is an *upper bound* of a chain X if $\forall b \in X,\ b \preceq a$.

Lemma 2.1.7 (Zorn's)**.** Let $\mathcal{P}$ be a nonempty poset. If every chain in $\mathcal{P}$ has an upper bound then $\mathcal{P}$ contains a maximal element.

Theorem 2.1.8. Let D be a division ring and ${}_DM$ a module. Then

1. M is free
2. $\forall$ linearly independent $X \subseteq M$, $\exists$ basis $B \supseteq X$
3. $\forall$ spanning $Q \subseteq M$, $\exists$ basis $B \subseteq Q$

Proof. 1. This follows from 2 by taking $X = \varnothing$.

2. Consider poset $\mathcal{P} = \{Z \subseteq M : Z \supseteq X$ and Z is linearly independent$\}$ with $\preceq \; = \; \subseteq$. Then $X \in \mathcal{P}$. Pick a chain $C \subseteq \mathcal{P}$ and consider $Z = \bigcup_{Y \in C} Y$. If $Z \in \mathcal{P}$ then it's obviously an upper bound of C. Now by construction, $Z \supseteq X$. Now if $a_1, \dots, a_n \in Z$, clearly $\exists Y \in C : a_i \in Y$, so $r_1a_1 + \cdots + r_na_n = 0_M$ would imply $a_i = 0$. Thus, by Zorn's lemma, there is a maximal element $Z \in \mathcal{P}$. We claim Z spans M, and therefore is a basis. Suppose for contradiction $\exists a \in M : a \notin \operatorname{span}(Z)$. Then $\{a\} \cap Z \supsetneqq Z$ and is linearly independent. Indeed, if
$$ra + \underbrace{r_1a_1 + \cdots r_na_n}_{\in Z} = 0 \text{ and } r \neq 0,$$
then $a \in \operatorname{span}(Z)$, a contradiction, so $r = 0$ and $r_1a_1 + \cdots r_na_n = 0$. Since Z is linearly independent, $a_i = 0$. So $\{a\} \cap Z \in \mathcal{P}$, contradicting maximality of Z.

Week 3, lecture 1 starts here

3. Consider poset $\mathcal{P} = \{Z \subseteq M : Z \subseteq Q$ and Z is linear independent$\}$ with $\preceq \; = \; \subseteq$. It's nonempty since $\varnothing \in \mathcal{P}$. Similarly to above, a chain C in $\mathcal{P}$ has an upper bound $X = \bigcup_{A \in C} A$, which spans M by the same argument.

$\square$

2.2 Embark on Artin–Wedderburn theory

Definition 2.2.1. ${}_RM$ is *simple* if $M \neq 0$ and $\forall {}_RN \leq {}_RM$, either $N = 0$ or $N = M$. i.e. Simple modules have exactly two submodules.

Example 2.2.2. 1. $\mathbb{Z}/m\mathbb{Z}$ as a $\mathbb{Z}$-module is simple iff m is prime.

2. ${}_RR$ is simple iff R is a division ring.

Proof. $\Leftarrow$: Let ${}_RL \leq {}_RR$ such that ${}_RL \neq 0$. Then $\forall 0 \neq x \in L$, $1_R = x^{-1}x \in L$, so $r = r \cdot 1_R \in L \; \forall r \in R$, i.e. $L = R$.

$\implies$: Let $x \in R$, $x \neq 0$. Then $Rx = \{rx : r \in R\} \trianglelefteq^l R$, so ${}_RRx \leq {}_RR$, and since $Rx \neq 0$ and ${}_RR$ is simple, one has $Rx = R$, and since $1_R \in R$, $\exists y \in R : yx = 1$. Similarly, $Ry = R$ so $\exists z \in R : zy = 1$, so $x = (zy)x = z(yx) = z$ and y is both left and right inverse of x.

$\square$

Notation. $\mathcal{L}(R) = \{L : L \trianglelefteq^l R\}$. This is a poset under $\subseteq$. Maximal left ideal is then a maximal element in $(\mathcal{L}(R)\backslash\{R\})$ and minimal left ideal is a minimal element in $(\mathcal{L}(R)\backslash\{0\})$.

Lemma 2.2.3. $L \trianglelefteq^l R$ is maximal iff R/L is a simple left R-module.

Proof. By correspondence theorem,

$$\{L, R\} = \{M : L \subsetneq M \trianglelefteq^l R\} \leftrightarrow \text{nonzero submodules of } R/L.$$

□

Remark. Given ${}_RM \ni m$, we have a homomorphism of R-modules $\varphi_m : {}_RR \to M : r \mapsto rm$. Indeed, $\varphi_m(sr) = srm = s\varphi_m(r)$. We call the kernel $\ker \varphi_m = \{x \in R : xm = 0\}$ the *annihilator* of m, denoted $\operatorname{Ann}(m)$. 1st isomorphism theorem says $\operatorname{Ann}(m) \trianglelefteq^l R$, and $\operatorname{im} \varphi_m = Rm \cong R/\operatorname{Ann}(m)$.

Lemma 2.2.4. If ${}_RM$ is simple with $x \in M,\ x \neq 0$, then $\operatorname{Ann}(x)$ is a maximal left ideal and $M \cong R/\operatorname{Ann}(x)$.

Proof. One has $x \in \operatorname{im} \varphi_x$, so $\operatorname{im} \varphi_x \neq 0$. By simplicity of M, $\operatorname{im} \varphi_x = M$. $M \cong R/\operatorname{Ann}(x)$ then follows from 1st isomorphism theorem. Maximality of $\operatorname{Ann}(x)$ follows from correspondence theorem. □

Week 3, lecture 2 starts here

Theorem 2.2.5. A nonzero ring has a maximal left ideal.

Proof. Let R be a nonzero ring and consider poset $\mathcal{P} = \{L \triangleleft^l R : L \neq R\}$ with $\preceq\ =\ \subseteq$. One has $0 \in \mathcal{P}$ so $\mathcal{P} \neq \varnothing$. Let $C \subseteq \mathcal{P}$ be a chain. Define $I = \bigcup_{L \in C} L$. Clearly I is an additive abelian subgroup, since for $x, y \in I$ then $x \in L_1$ and $y \in L_2$, but C is chain so WLOG $L_1 \supseteq L_2$, so $x, y \in L_1 \implies x - y \in L_1 \implies x - y \in I$. We claim I is in fact a left ideal. Indeed, for $x \in I$, one knows $x \in L \in C$, and $\forall r \in R,\ rx \in L$, so $rx \in I$. Note that $I \neq R$ since $1_R \notin L\ \forall L \in C$. Therefore I is an upper bound for C, and by Zorn's lemma $\mathcal{P}$ has a maximal element J, which by definition is a maximal left ideal. □

Corollary 2.2.6. A nonzero ring admits a simple module.

Proof. Let $I \triangleleft^l R$ be a maximal ideal of a nonzero ring R, which is guaranteed by theorem above. Then R/I is a simple R-module by 2.2.3. □

Proposition 2.2.7 (Schur lemma I)**.** If $\varphi : {}_RM \to {}_RN$ is a homomorphism of simple modules, then either $\varphi = 0$ or φ is an isomorphism.

Proof. Note $\ker \varphi \leq {}_RM$ and $\operatorname{im} \varphi \leq {}_RN$. By simplicity, $\ker \varphi \in \{0, M\}$ and $\operatorname{im} \varphi \in \{0, N\}$, i.e. there are 4 possible cases.

$(0, 0)$ This is impossible, since $\operatorname{im} \varphi = 0 \implies \ker \varphi = M$.

$(0, N)$ This implies precisely φ is an isomorphism.

$(M, 0)$ It follows $\varphi = 0$.

(M, N) This is impossible, since $\ker \varphi = M \implies \operatorname{im} \varphi = 0$.

□

Corollary 2.2.8 (Schur lemma II)**.** If ${}_RM$ is simple then $\mathrm{End}_R M$ is a division ring.

Proof. By Schur lemma I, if ${}_RM$ is simple then every $\varphi \in \mathrm{End}_R M = \{\text{homomorphisms } \varphi : {}_RM \to {}_RM\}$ either is 0 or has an inverse. □

Example 2.2.9. $R = \mathbb{R}[x],\ M = \mathbb{R}^2,\ X = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$. M is an R-module with $f(x)v := f(X)v$. Consider a submodule $N \leq M$, then for $\forall \alpha \in R,\ \alpha 1 \in R$, so $\alpha N \subseteq N$, hence N is a vector subspace. But $\dim N = 1$ is impossible, so M is simple. Suppose it is, then $\forall v \in N : v \neq 0,\ xv = \alpha v$, i.e. v is an eigenvector of X, which has no real eigenvalues, an absurdity. Now we have $\mathrm{End}_R M$ is a division ring, and note that

$$\begin{aligned}\mathrm{End}_R M &= \{f : M \to M : f(xv) = xf(v)\} = \{Y \in M_2(\mathbb{R}) : XY = YX\} = C_{M_2(\mathbb{R})}(X) \\ &= \left\{aI + \frac{1}{2}bX^2 : a, b \in \mathbb{R}\right\} \cong \mathbb{C} \text{ via } X \mapsto 1 + i.\end{aligned}$$

Theorem 2.2.10 (baby Artin–Wedderburn)**.** The following are equivalent for a nonzero ring R.

1. Every left R-module is free.
2. R is a division ring.

Proof. 2⇒1: This is Theorem 2.1.8.1.

1⇒2: By Corollary 2.2.6, $\exists$ a simple R-module M, which is free by assumption, i.e. admits a basis $B \subseteq M$. Pick $x \in B$, then $Rx \leq M$ by simplicity has to be M, so $M = Rx \cong R/\mathrm{Ann}(x)$ by Lemma 2.2.4. But $rx = 0_M \implies r = 0_R$ since x is in a basis, so $\mathrm{Ann}(x) = 0$, hence by Lemma 1.3.10, $M \cong R \cong \mathrm{End}_R R \cong \mathrm{End}_R M$ which is a division ring by 2.2.8.

□

Week 3, lecture 3 starts here

2.3 Algebra

Definition 2.3.1. An *algebra* is a pair $(A, \mathbb{F})$ where A is a ring and a $\mathbb{F}$-vector space such that

1. $\underbrace{x + y}_{\text{in ring}} = \underbrace{x + y}_{\text{in vector space}} \quad \forall x, y \in A$
2. $(\alpha x)y = \alpha(xy) = x(\alpha y)\ \forall x, y \in A, \alpha \in \mathbb{F}$

Remark. Notions about a ring are extended to algebras like so:

- An ideal of $(A, \mathbb{F})$ is an ideal of A that is also an $\mathbb{F}$-vector subspace
- A subalgebra of $(A, \mathbb{F})$ is a subring of R that is also an $\mathbb{F}$-vector subspace
- A homomorphism $(A, \mathbb{F}) \to (B, \mathbb{F})$ is a ring homomorphism $A \to B$ with $\mathbb{F}$-linearity
- A module over $(A, \mathbb{F})$ is a module over A with the action being $\mathbb{F}$-linear

- A submodule of a module over $(A, \mathbb{F})$ is a submodule of the module over A and a $\mathbb{F}$-vector subspace
- A homomorphism of modules over $(A, \mathbb{F})$ is a module homomorphism with $\mathbb{F}$-linearity

Lemma 2.3.2. Let R be a ring and $\mathbb{F}$ a field. Then there is a bijection

$$\{\text{algebras } (R, \mathbb{F})\} \leftrightarrow \{\text{ring homomorphisms } \mathbb{F} \to Z(R)\}.$$

Proof. For an algebra $(R, \mathbb{F})$, define $\varphi : \mathbb{F} \to Z(R) : \alpha \mapsto \alpha 1_R$. (Verify this is indeed a ring homomorphism.) Then by definition, $(\alpha 1_R)x = \alpha x = \alpha(x1) = x(\alpha 1_R)\ \forall x \in R$, so $\operatorname{im} \varphi \subseteq Z(R)$.

For a ring homomorphism $\varphi : \mathbb{F} \to Z(R)$, define $\mathbb{F} \times R \to R : (\alpha, x) \mapsto \varphi(\alpha)x =: \alpha x$. Then $(\alpha\beta)(x) = \varphi(\alpha\beta)x = \varphi(\alpha)(\varphi(\beta)x) = \alpha(\beta x)$ (verify similar statements for $(\alpha+\beta)(x)$ and $\alpha(x+y)$) and $\alpha(xy) = \varphi(\alpha)xy = (\varphi(\alpha)x)y = (\alpha x)y$ and since $\varphi(\alpha) \in Z(R)$ it's also $x(\alpha y)$.

It remains to verify they are indeed inverse bijections:

$$\begin{aligned} &(R, \mathbb{F}) \\ &\to \varphi : \mathbb{F} \to Z(R) : \alpha \mapsto \alpha 1_R \\ &\to \alpha x := \varphi(\alpha)x = \alpha 1_R x = \alpha x \end{aligned}$$

and

$$\begin{aligned} &\varphi : \mathbb{F} \to Z(R) \\ &\to \alpha x := \varphi(\alpha)x \\ &\to \varphi(\alpha) = \alpha 1_R = \varphi(\alpha) \cdot 1 = \varphi(\alpha). \end{aligned}$$

□

Remark.
1. By the structure of a field, the following ring things are automatically algebra things: ideals, modules, submodules, module homomorphisms (ingredients in 1st isomorphism theorem). e.g. Suppose M is a module over algebra $(A, \mathbb{F})$ and N is a submodule of M for the ring A. Then $\forall \alpha \in \mathbb{F},\ n \in N,\ \alpha n = (\alpha 1_A)n \in N$ since $\alpha 1_A \in Z(A)$. So N is a subspace and hence a submodule of the algebra $(A, \mathbb{F})$.
2. Subrings and ring homomorphisms are different. Consider the algebra $(\mathbb{C}, \mathbb{Q})$, then $\mathbb{Z}[i] \leq \mathbb{C}$ is not a subalgebra. Also, for the algebra $A = (\mathbb{C}, \mathbb{C})$, $\varphi : A \to A : x \mapsto \overline{x}$ is a ring homomorphism $\mathbb{C} \to \mathbb{C}$ but not an algebra homomorphism since it's not $\mathbb{C}$-linear.

Definition 2.3.3. Let $(A, \mathbb{F})$ be an algebra with a $\mathbb{F}$-basis of A $e_1, \dots, e_n$. Then one can write $\forall i, j = 1, \dots, n$

$$e_i \cdot e_j = \sum_k c_{ij}^k e_k,$$

where $c_{ij}^k \in \mathbb{F}$, called *structure constants*, determine and are determined by the algebra structure of $(A, \mathbb{F})$.

Example 2.3.4. The quaternions $\mathbb{H} = \mathbb{R}^4$ with basis $1, i, j, k$ has the structure constants table:

Week 4, lecture 1 starts here

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

2.3.1 Polynomial

The video recording was completely black! See notes given by Dmitriy. The following is the best I can manage:

Proposition 2.3.5. If $n \geq 1$ then $\dim_{\mathbb{F}} \mathbb{F}\langle x_1, \dots, x_n \rangle$ is countable.

Proposition 2.3.6 (Universal property)**.** Let $(A, \mathbb{F})$ be an algebra. Then $\forall a_1, \dots, a_n \in A$, $\exists!$ homomorphism of algebras $\varphi : \mathbb{F}\langle x_1, \dots, x_n \rangle \to A : \varphi(x_i) = a_i \ \forall i$.

Proof. Define φ by $x_1 \cdots x_n \mapsto a_1 \cdots a_n$ and extend by $\mathbb{F}$-linearity, so that it's an algebra homomorphism. Suppose $\psi : \mathbb{F}\langle x_1, \dots, x_n \rangle \to A$ is another such homomorphism, then $\varphi(x_i) = \psi(x_i) = a_i$ and by properties of homomorphism and linearity they must then be the same map. $\square$

2.3.2 Noncommutative Nullstellensatz

Definition 2.3.7. Let $(A, \mathbb{F})$ be an algebra with $\alpha \in A$. Consider the algebra homomorphism $\varphi_\alpha : \mathbb{F}[x] \to A : x \mapsto \alpha$. Since $\mathbb{F}[x]$ is a PID, $\ker f$ is generated by one element $\mu_\alpha(x)$, called the *minimal polynomial* of α. One says α is *transcendental* if $\mu_\alpha \equiv 0$ and *algebraic* if $\mu_\alpha \not\equiv 0$.

Example 2.3.8. $A = M_n(\mathbb{F}) \ni \alpha$, then all α are algebraic by Cayley–Hamilton theorem.
If $\dim_{\mathbb{F}} A < \infty$ then $1, \alpha, \alpha^2, \dots$ are linearly dependent, so all α are algebraic.

Lemma 2.3.9. If $(D, \mathbb{F})$ is a division algebra, then $\forall \alpha \in D \backslash \{0\}$, $\mu_\alpha(x) \in \mathbb{F}[x]$ is irreducible.

Proof. Suppose $\mu_\alpha(x) = g(x)h(x)$ with $0 < \deg g < \deg \mu_\alpha$, but then since $\mu_\alpha(\alpha) = 0$ and D is a division ring, WLOG $g(\alpha) = 0$, contradicting minimality of μ_α. $\square$

Week 4, lecture 2 starts here

Theorem 2.3.10 (Amitsur–Schur lemma)**.** If $(A, \mathbb{F})$ is an algebra with $\dim_{\mathbb{F}} A < |\mathbb{F}|$ and M is simple A-module, then any $d \in D = \mathrm{End}_A M$ (also an $\mathbb{F}$ algebra) is algebraic over $\mathbb{F}$.

Proof. Note that $\dim_{\mathbb{F}} D \leq \dim_{\mathbb{F}} M \leq \dim_{\mathbb{F}} A < |\mathbb{F}|$. Indeed, since M is simple, $\forall m \in M, m \neq 0$, $M \cong A/\mathrm{Ann}(m)$ (Lemma 2.2.4), so $\dim_{\mathbb{F}} M \leq \dim_{\mathbb{F}} A$; now pick $m \in M, m \neq 0$ and consider $\alpha_m : D \to M : x \mapsto mx$. This is injective: suppose $\alpha_m(x) = 0$, but $M = Am$ by simplicity, so $\forall \widetilde{m} \in M$, $\exists a \in A : \widetilde{m} = am$. Then $\widetilde{m}x = a(mx) = a\alpha_m(x) = 0$, so $x = 0_D$.
Now let $d \in D$. Note $\mathbb{F} = \mathbb{F}1_D \leq Z(D)$, and if $d \in \mathbb{F}$ then $d = \alpha 1_D$ for some $\alpha \in \mathbb{F}$, so minimal polynomial of d is simply $z - \alpha$, hence algebraic. Suppose now $d \notin \mathbb{F}$. Then $d - \alpha \notin \mathbb{F}\ \forall \alpha \in \mathbb{F}$. This implies $(d - \alpha) = \frac{1}{d-\alpha}$ are linearly dependent over $\mathbb{F}$, hence $\exists \gamma_1, \dots, \gamma_n$ all $\neq 0$ such that

$$\gamma_1 \frac{1}{d - \alpha_1} + \cdots + \gamma_n \frac{1}{d - \alpha_n} = 0.$$

Now note that $\alpha_i \in \mathbb{F}$, so all $(d-\alpha_i)$ commute, hence $(d-\alpha_i)^{-1}$ commute as well, since

$$xy = yx \implies y = x^{-1}xy = x^{-1}yx \implies yx^{-1} = x^{-1}yxx^{-1} = x^{-1}y$$

and doing the same trick for y one yields $x^{-1}y^{-1} = y^{-1}x^{-1}$. We can therefore multiply $(d-\alpha_1)(d-\alpha_2)\cdots(d-\alpha_n)$ on both sides and get

$$\gamma_1(d-\alpha_2)\cdots(d-\alpha_n) + \gamma_2(d-\alpha_1)(d-\alpha_3)\cdots(d-\alpha_n) + \cdots + \gamma_n(d-\alpha_1)\cdots(d-\alpha_{n-1}) = 0.$$

In other words, if we let

$$f(z) = \sum_{i=1}^{n} \gamma_i \frac{\prod_{k=1}^{n}(z-\alpha_k)}{z-\alpha_i}$$

then $f(d) = 0$. One has d is algebraic as long as $f \neq 0$. And indeed $f \neq 0$, since

$$f(\alpha_1) = \gamma_1(\alpha_1-\alpha_2)(\alpha_1-\alpha_3)\cdots(\alpha_1-\alpha_n) \neq 0.$$

□

Corollary 2.3.11 (Noncommutative Nullstellensatz)**.** If $(A, \mathbb{C})$ is an algebra with A finitely generated and M is a simple A-module, then $\mathrm{End}_A M = \mathbb{C}$.

Proof. Suppose A is generated by $a_1, \ldots, a_n$. Then $\mathbb{C}\langle x_1, \ldots, x_n\rangle \to A : x_i \mapsto a_i$ is surjective. By 2.3.5, $\dim_{\mathbb{C}} A$ is at most countable, so by theorem above, any $d \in \mathrm{End}_A M$ is algebraic over $\mathbb{C}$ and let $f_d(z) \in \mathbb{C}[z]$ be its minimal polynomial. By 2.3.9, it's irreducible, but since $\mathbb{C}$ is algebraically closed, $f_d(z)$ must be of the form $\alpha z - \beta$ where $\alpha \neq 0$. It follows that $d \in \mathbb{C}$. □

Corollary 2.3.12 (Weak Nullstellensatz)**.** Let $I \lhd \mathbb{C}[x_1, \ldots, x_n]$ be a proper ideal. Then $\exists (a_i) \in \mathbb{C}^n : \forall f \in I,\ f(a_1, \ldots, a_n) = 0$.

Proof. Adapt proof of Theorem 2.2.5 with $\mathcal{P}$ now being the poset of all left ideals $J \trianglelefteq R$ such that $J \supseteq I$ and $J \neq R$. The maximal element L the argument produces gives a simple $\mathbb{C}[x_1, \ldots, x_n]$-module $M = \mathbb{C}[x_1, \ldots, x_n]/L$ (2.2.3). Now each x_i defines $\widehat{x_i} : f+L \mapsto x_i f + L \in \mathrm{End}_{\mathbb{C}[x_1,\ldots,x_n]} M$, and by corollary above, $\mathrm{End}_{\mathbb{C}[x_1,\ldots,x_n]} M = \mathbb{C}$, so let $\widehat{x_i} = a_i \in \mathbb{C}$. Let $h(x_1, \ldots, x_n) \in I \subseteq L$ and consider $\widehat{h} : f + L \mapsto hf + L$. Since $h \in L$, $\widehat{h}$ is identically zero, i.e. $\widehat{h} = 0$, but on the other hand,

$$\widehat{h} = h(\widehat{x_1}, \ldots, \widehat{x_n}) = h(a_1, \ldots, a_n) \in \mathbb{C},$$

the desired is thus proven. □

Week 4, lecture 3 starts here

3 Division

3.1 Quaternion

By writing down the fundamental formula for quaternions $i^2 = j^2 = k^2 = ijk = -1$, Sir William Rowan Hamilton defined, in modern language, the quotient algebra

$$\mathbb{H} = \mathbb{R}\langle x_1, x_2, x_3\rangle / I \text{ where } I = \left(1 + x_1^2, 1 + x_2^2, 1 + x_3^2, 1 + x_1x_2x_3\right),$$

and i, j, k are then $x_1 + I,\ x_2 + I,\ x_3 + I$.

Proposition 3.1.1. Products of i, j, k are as the table in 2.3.4.

Proof. The diagonal is immediate from the formula. Now

$$\begin{aligned} -i = -iijk = -jk &\quad\implies\quad jk = i \\ -k = ijkk = -ij &\quad\implies\quad ij = k \end{aligned}$$

and similarly for the rest. $\square$

Proposition 3.1.2. $1, i, j, k$ is a basis for $(\mathbb{H}, \mathbb{R})$.

Proof. Clearly $1, i, j, k$ generate $\mathbb{H}$ and any product is a linear combination of $1, i, j, k$. It remains to show they are linearly independent. Consider an algebra homomorphism $f : \mathbb{R}\langle x_1, x_2, x_3\rangle \to M_2(\mathbb{C})$ given by

$$\begin{aligned} x_1 &\mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = A_1 \\ x_2 &\mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = A_2 \\ x_3 &\mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = A_3. \end{aligned}$$

We claim $I \subseteq \ker f$. Indeed $A_1^2 = A_2^2 = A_3^2 = -1_{M_2(\mathbb{C})}$ so $1 + x_i^2 \in \ker f$, and $A_1A_2A_3 = -1_{M_2(\mathbb{C})}$ so $1 + x_1x_2x_3 \in \ker f$. Hence $\overline{f} : \mathbb{H} \to M_2(\mathbb{C})$ given by $i \mapsto A_1, j \mapsto A_2, k \mapsto A_3$ is a well-defined algebra homomorphism. Since I, A_1, A_2, A_3 are linearly independent over $\mathbb{R}$, so are $1, i, j, k$. $\square$

3.1.1 Quaternions form a division ring

Definition 3.1.3. Similar to complex numbers, quaternions can be divided into their *real part* and *imaginary part*, i.e. one can write $X = \alpha + x$ where $\alpha \in \mathbb{R}$ and $x \in \operatorname{span}(i, j, k) = \mathbb{H}_0$. *Conjugation* is defined similarly as well: $X^* := \alpha - x$, e.g. $(3 + 5i - 77j)^* = 3 - 5i + 77j$. One also has

$$\Re X = \frac{q + q^*}{2}, \qquad \Im X = \frac{q - q^*}{2}.$$

Define and notate the *norm* as $q(X) = XX^*$. Notate the usual Euclidean distance by $||x|| = \sqrt{q(x)}$.

Theorem 3.1.4. If $\alpha, \beta \in \mathbb{R}$ and $x, y \in \mathbb{H}_0$ then

$$(\alpha + x)(\beta + y) = \underbrace{\alpha\beta - x \cdot y}_{\in\mathbb{R}} + \underbrace{\alpha y + \beta x + x \times y}_{\in\mathbb{H}_0}.$$

Proof. One has

$$(\alpha + x)(\beta + y) = \alpha\beta + \alpha y + \beta x + xy,$$

so it remains to show $xy = x \times y - x \cdot y$. Write $x = \alpha i + \beta j + \gamma k$ and $y = \widehat{\alpha} i + \widehat{\beta} j + \widehat{\gamma} k$, then

$$\begin{aligned} xy &= -(\alpha\widehat{\alpha} + \beta\widehat{\beta} + \gamma\widehat{\gamma}) + (\beta\widehat{\gamma} - \widehat{\beta}\gamma)i + (\gamma\widehat{\alpha} - \alpha\widehat{\gamma})j + (\alpha\widehat{\beta} - \beta\widehat{\alpha})k \\ &= -x \cdot y + x \times y. \end{aligned}$$

$\square$

Corollary 3.1.5. $q(X) = q(\alpha + \beta i + \gamma j + \delta k) = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$.

Proof. Write $X = \alpha + \nu$. Then by definition,

$$q(X) = (\alpha + \nu)(\alpha - \nu) = \alpha^2 - \nu \cdot (-\nu) - \alpha\nu + \alpha\nu - \nu \times \nu = \alpha^2 + \nu \cdot \nu,$$

which is what's desired. $\square$

Corollary 3.1.6. $(qp)^* = p^* q^*$.

Proof. Write $p = \alpha + x$ and $q = \beta + y$. Then

$$(qp)^* = (\alpha\beta - x \cdot y + \beta x + \alpha y + y \times x)^* = \alpha\beta - x \cdot y - \beta x - \alpha y - y \times x$$

and

$$(\alpha - x)(\beta - y) = \alpha\beta - (-x) \cdot (-y) - \alpha y - \beta x + (-x) \times (-y),$$

the desired then follows from $(-x) \times (-y) = -y \times x = x \times y$ (the other parts don't care about orders). $\square$

Corollary 3.1.7. $||pq|| = ||p||||q||$.

Proof. $||pq|| = (pq)(pq)^* = pqq^*p^* = p||q||p^* = pp^*||q|| = ||p||||q||$. $\square$

Proposition 3.1.8. $\mathbb{H}$ is a division algebra.

Proof. Let $q \in \mathbb{H},\ q \neq 0$. Then $||q|| \neq 0$, and since $qq^* = ||q||$, one has $q^{-1} = \frac{1}{||q||} q^*$. $\square$

Week 5, lecture 1 starts here

3.1.2 Multiplicative group of quaternions

The group $\mathbb{H}^\times = (\mathbb{H} \backslash \{0\}, \cdot)$ has subgroups $\mathbb{R}_+^\times = \{\alpha : \alpha > 0\}$ and $U(\mathbb{H}) = \{x \in \mathbb{H} : ||x|| = 1\}$ (the 3-sphere).

Proposition 3.1.9 (Polar representation of quaternions)**.** $\mathbb{H}^\times \cong \mathbb{R}_+^\times \times U(\mathbb{H})$.

Proof. Define $f(\alpha, X) = \alpha X$. This is a group homomorphism:

$$f((\alpha, X), (\beta, Y)) = f(\alpha\beta, XY) = \alpha\beta XY = \alpha X \beta Y = f(\alpha, X) f(\beta, Y).$$

f is injective: indeed, let $(\alpha, X) \in \ker f$. Then $\alpha X = 1$ and $X = \alpha^{-1} \in \mathbb{R}$, and since $||x|| = 1,\ x = \pm 1$, but $\alpha > 0$, so $(\alpha, X) = (1, 1)$.
f is surjective: indeed, pick $X \in \mathbb{H}^\times$ and one can write $X = ||X|| \cdot ||X||^{-1} X$ where $||X|| \in \mathbb{R}_+$ and $||||X||^{-1} X|| = ||X||^{-1} ||X|| = 1$, i.e. $||X||^{-1} X \in U(\mathbb{H})$. $\square$

Proposition 3.1.10. For $X \in \mathbb{H}^\times$, the following hold:

1. $X^2 \in \mathbb{R} \iff X \in \mathbb{R} \cup \mathbb{H}_0$
2. $X^2 \in \mathbb{R}_{>0} \iff X \in \mathbb{R}$
3. $X^2 \in \mathbb{R}_{<0} \iff X \in \mathbb{H}_0$

4. $|X| = 2 \iff X = -1$
5. $|X| = 4 \iff X \in \mathbb{H}_0$ and $||X|| = 1$

Proof. 1. Write $X = \alpha + x$. Then $X^2 = (\alpha^2 - x \cdot x) + 2\alpha x + \underbrace{x \times x}_{0}$, hence $\Im X = 2\alpha x$, so $\Im X = 0 \iff \alpha = 0$ or $x = 0 \iff X \in \mathbb{H}_0$ or $X \in \mathbb{R}$.

2, 3. Now suppose $X \in \mathbb{R} \cup \mathbb{H}_0$, then $X^2 = \alpha^2 - x \cdot x$. Note $\alpha = 0$ or $x = 0$. So $X^2 > 0 \iff x = 0 \iff X \in \mathbb{R}$ and $X^2 < 0 \iff \alpha = 0 \iff X \in \mathbb{H}_0$.

4. $X^2 = 1 \iff x = 0$ and $\alpha^2 = 1$, so $\alpha = \pm 1$, but $|1| = 1$ so $\alpha = -1$.

5. By above, $|X| = 4 \implies X^2 = -1$ and this is equivalent to $\alpha = 0$ and $||x|| = 1$.

□

Proposition 3.1.11 (Quaternionic Euler formula)**.** Write $X = \alpha + \beta x$ where $\alpha, \beta \in \mathbb{R}$ and $x \in U(\mathbb{H}) \cap \mathbb{H}_0$. Then

$$e^X = e^\alpha(\cos\beta + x \sin\beta).$$

Proposition 3.1.12 (de Moivre's formula)**.** If $x \in \mathbb{H}_0 \cap U(\mathbb{H})$ and $n \in \mathbb{N}$ then

$$(\cos\alpha + x\sin\alpha)^n = \cos n\alpha + x \sin n\alpha$$

Proof. $(e^{\alpha x})^n = e^{n\alpha x}$. □

3.1.3 Orthogonal matrix and transformation

Recall that for $\begin{pmatrix} c_1 & \cdots & c_n \end{pmatrix} = A \in \mathbb{R}^{n\times n}$, the following are equivalent:

1. $A^T A = I_n$
2. $c_1, \dots, c_n$ is an orthonormal basis
3. $x \mapsto Ax$ preserves dot product, i.e. $(Ax) \cdot (Ay) = x \cdot y \ \forall x, y \in \mathbb{R}^n$
4. $x \mapsto Ax$ preserves distances, i.e. $||Ax|| = ||x|| \ \forall x \in \mathbb{R}^n$

We are going to see that $\mathbb{C}$ gives nice description of orthogonal transformations on $\mathbb{R}^2$ and $\mathbb{H}$ gives these of those on $\mathbb{R}^3$ and $\mathbb{R}^4$. Specifically, a unit vector $v_\alpha = \begin{pmatrix} \cos\alpha \\ \sin\alpha \end{pmatrix}$ (which can also be described as a complex number) determines two orthogonal transformations of $\mathbb{R}^2$: $R_\alpha = \begin{pmatrix} v_\alpha & v_{\alpha+\pi/2} \end{pmatrix} = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ and $S_\alpha = \begin{pmatrix} v_\alpha & v_{\alpha-\pi/2} \end{pmatrix} = \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$ which have determinants ± 1 respectively.

Proposition 3.1.13. $\{S_\alpha, R_\alpha : \alpha \in \mathbb{R}\}$ is precisely the set of 2×2 orthogonal matrices.

Proposition 3.1.14. Rotations on $\mathbb{R}^2$ are given by left multiplication of $z \in \mathbb{C}$, $||z|| = 1$.

Proof. This is clear by writing such z as $\cos\alpha + i \sin\alpha$. □

3.1.4 3D rotation

To specify a 3D rotation, we need a directional axis and an angle and use Euler's angle-axis notation $R_{(\alpha,v)}$.

Week 5, lecture 2 starts here

Lemma 3.1.15. If $f \in \mathbb{R}[x]$ is monic and irreducible, then either $f(x) - x - \alpha$ or $x^2 + \alpha x + \beta$ with $\mathcal{D} = \alpha^2 - 4\beta < 0$.

Proof. One has $\exists \lambda \in \mathbb{C} : f(\lambda) = 0$. If $\lambda \in \mathbb{R}$, then $(x - \lambda) \mid f$ so $f = x - \lambda$ by irreducibility. If $\lambda \notin \mathbb{R}$, then $f(\overline{\lambda}) = 0$ and $(x - \lambda)(x - \overline{\lambda}) \mid f(x)$ where $(x - \lambda)(x - \overline{\lambda}) = x^2 + \alpha x + \beta$ with $\mathcal{D} < 0$ and again by irreducibility $f(x) = x^2 + \alpha x + \beta$. $\square$

Corollary 3.1.16. Let $V_{\mathbb{R}}$ be a vector space with $\dim_{\mathbb{R}} V$ odd and $L : V \to V$ a linear operator. Then L admits a real eigenvalue.

Proof. Write the characteristic polynomial $\chi_L(z)$ of L as $\pm f_1, \ldots, f_n$ where f_i are all monic and irreducible, but $\deg \chi$ is odd, so there must be one $f_i = x - \alpha$, where α is the desired eigenvalue. $\square$

Recall Sylvester's theorem from MA251.

Lemma 3.1.17. If $L : \mathbb{R}^3 \to \mathbb{R}^3$ is special orthogonal ($\det L = 1$), then $\exists$ orthonormal basis in which the matrix of L is

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos\alpha & -\sin\alpha \\ 0 & \sin\alpha & \cos\alpha \end{pmatrix}.$$

Proof. L admits eigenvalue $\alpha \in \mathbb{R}$ by previous lemma, so $Lx = \alpha x$ for some $x \in \mathbb{R}^3 \backslash \{0\}$. Since $||x|| = ||Lx|| = |a|||x||$, $\alpha = \pm 1$. Now $Lx^\perp \subseteq x^\perp$. Indeed, let $y \in x^\perp$, then $x \cdot y = 0$, and $0 = x \cdot y = Lx \cdot Ly = \pm x \cdot Ly$, so $Ly \in x^\perp$. Consider the two cases.

1. $\alpha = 1$, then $L|_{x^\perp} : x^\perp \to x^\perp$ is orthogonal of $\det = 1$, so $L|_{x^\perp} = R_\alpha$ and in an orthonormal basis $\frac{1}{||x||}x, y, z,$ L has the desired form.

2. $\alpha = -1$, then $L|_{x^\perp} : x^\perp \to x^\perp$ is orthogonal of $\det = -1$, so $L|_{x^\perp}$ is reflection $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ and one has orthonormal basis $y, \frac{1}{||x||}x, z$ such that

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

where $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = R_\pi$.

$\square$

We now bring quaternions in by identifying $\mathbb{R}^3 \cong \mathbb{H}_0 \ni x$ and rotation as $R_{x,\alpha}$.

Lemma 3.1.18. $\forall w \in \mathbb{H}_0$,

$$R_{x,\alpha}(w) = e^{\frac{\alpha}{2}x} w e^{-\frac{\alpha}{2}x}.$$

Proof. Pick any $y : x \cdot y = 0$ and $||y|| = 1$. Define $z := x \times y$. Then x, y, z behave exactly like i, j, k, so it suffices to check the lemma on the basis x, y, z. Now a priori one has

$$R_{x,\alpha}(x) = x, \quad R_{x,\alpha}(y) = y\cos\alpha + z\sin\alpha, \quad R_{x,\alpha}(z) = -y\sin\alpha + z\cos\alpha,$$

and let's check the case for z:

$$\begin{aligned} e^{\frac{\alpha}{2}x} z e^{-\frac{\alpha}{2}x} &= \left(\cos\frac{\alpha}{2} + x\sin\frac{\alpha}{2}\right) z \left(\cos\frac{\alpha}{2} - x\sin\frac{\alpha}{2}\right) \\ &= \left(z\cos\frac{\alpha}{2} - y\sin\frac{\alpha}{2}\right)\left(\cos\frac{\alpha}{2} - x\sin\frac{\alpha}{2}\right) \\ &= z\cos^2\frac{\alpha}{2} - y\cos\frac{\alpha}{2}\sin\frac{\alpha}{2} - y\sin\frac{\alpha}{2}\cos\frac{\alpha}{2} - z\sin^2\frac{\alpha}{2} \\ &= z\left(\cos^2\frac{\alpha}{2} - \sin^2\frac{\alpha}{2}\right) - 2y\cos\frac{\alpha}{2}\sin\frac{\alpha}{2} \\ &= z\cos\alpha - y\sin\alpha. \end{aligned}$$

The remaining two are left as enjoyment. □

Theorem 3.1.19.

$$\begin{aligned} \varphi : U(\mathbb{H}) &\to SO(\mathbb{H}_0) \cong SO_3(\mathbb{R}) \\ x &\mapsto (z \mapsto xzx^{-1}) \end{aligned}$$

is a surjective 2-to-1 group homomorphism.

Proof. Check φ is indeed a group homomorphism:

- $\varphi(x) \in SO(\mathbb{H}_0)$ since $||xzx^{-1}|| = ||x||||z||||x^{-1}|| = ||z|| \ \forall z \in \mathbb{H}_0$.
- $\varphi(xy)(z) = (xy)z(xy)^{-1} = x(yzy^{-1})x^{-1} = \varphi(x)(\varphi(y)(z))$.

Now 3.1.17 says $L = R_{x,\alpha}$ and 3.1.18 says $L = \varphi\left(e^{\frac{\alpha}{2}x}\right) \in \operatorname{im}\varphi$, so φ is surjective.
If $x \in \ker\varphi$ then $xzx^{-1} = z$, i.e. $z \in Z(\mathbb{H}) = \mathbb{R}$ so $z = \pm 1$, hence in particular $|\ker\varphi| = 2$. □

Week 5, lecture 3 starts here

3.1.5 4D scroll

Rotations in 4D can be understood by identifying $\mathbb{R}^4 \cong \mathbb{H}$. For $x \in U(\mathbb{H})$, define $L_x : z \mapsto xz$ and $R_x : z \mapsto zx$, called *left scroll* and *right scroll*, which are clearly orthogonal. They are also special orthogonal (see Lemma 3.1.19 in Dmitriy's notes). Analogously,

Theorem 3.1.20.

$$\begin{aligned} \varphi : U(\mathbb{H}) \times U(\mathbb{H}) &\to SO(\mathbb{H}) \cong SO_4(\mathbb{R}) \\ (x, y) &\mapsto L_x R_{y^{-1}} \end{aligned}$$

is a surjective 2-to-1 group homomorphism.

Example 3.1.21. Consider $f : 1 \mapsto i \mapsto j \mapsto k \mapsto -1 \in SO(\mathbb{H})$. Write it in the form as in previous theorem:

1. We need to fix 1 by

$$L_{-i}f : 1 \mapsto (-i)i = 1,\ i \mapsto (-i)j = -k,\ j \mapsto (-i)k = j,\ k \mapsto (-i)(-1) = i.$$

2. Identify the axis of $L_{-i}f|_{\mathbb{H}_0}$, i.e. the vector that's fixed, which in this case is j.

3. Find the angle: let $(k, i, j) \cong (x, y, z)$ be the positively oriented basis in $\mathbb{R}^3$ and one can see it's a rotation by $\pi/2$, hence

$$L_{-i}f(w) = e^{\frac{\pi}{4}j} w e^{-\frac{\pi}{4}j}, \quad \text{i.e. } L_{-i}f = L_{e^{\frac{\pi}{4}j}} R_{e^{-\frac{\pi}{4}j}}$$

4. Assemble:

$$f = L_i L_{e^{\frac{\pi}{4}j}} R_{e^{-\frac{\pi}{4}j}} = L_{ie^{\frac{\pi}{4}j}} R_{e^{-\frac{\pi}{4}j}},$$

where $ie^{\frac{\pi}{4}j} = i\left(\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}j\right) = \frac{1}{\sqrt{2}}i + \frac{1}{\sqrt{2}}k$ and $e^{-\frac{\pi}{4}j} = \frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}j$. Let's check this on j:

$$\begin{aligned}\left(\frac{1}{\sqrt{2}}i + \frac{1}{\sqrt{2}}k\right) j \left(\frac{1}{\sqrt{2}} - \frac{1}{\sqrt{2}}j\right) &= \frac{1}{2}(i+k)(j+1) \\ &= \frac{1}{2}(ij + i + kj + k) = \frac{1}{2}(k + i - i + k) = k.\end{aligned}$$

3.2 Division algebra over $\mathbb{R}, \mathbb{C}$

Proposition 3.2.1. $\mathbb{C}$ is the only finite dimensional division algebra over $\mathbb{C}$.

Proof. Let D be such algebra and $a \in D$. Lemma 2.3.9 says $\mu_a(z) \in \mathbb{C}[z]$ is irreducible, but then $\mu_a(z) = z - \alpha$ where $\alpha \in \mathbb{C}$, so $a \in \mathbb{C}$. □

Proposition 3.2.2. If D is a division algebra over $\mathbb{R}$ and $\dim_{\mathbb{R}} D$ is odd, then $D = \mathbb{R}$.

Proof. Pick $a \in D$, and left multiplication $L_\alpha : D \to D$ admits a real eigenvalue α, so $L_a(x) = \alpha x$ for some $x \in D,\ x \neq 0$, but then $ax = \alpha x \implies (a - \alpha)x = 0 \implies a - \alpha = (a - \alpha)xx^{-1} = 0x^{-1} = 0$, so $a = \alpha \in \mathbb{R}$. □

Definition 3.2.3. For a finite dimensional algebra $(A, \mathbb{F})$, define the *(algebraic) trace* as

$$\mathrm{Tr}_A : A \to \mathbb{F} : a \mapsto \mathrm{Tr}(L_a),$$

the trace of matrix of left multiplication.

Example 3.2.4. $x + yi \in \mathbb{C}$, then $(x + yi)1 = x + yi$ and $(x + yi)i = -y + xi$, so in the basis $1, i,\ L_{x+yi}$ is given by $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$, so $\mathrm{Tr}_{\mathbb{C}}(x + iy) = 2x$.
Similarly $\mathrm{Tr}_{\mathbb{H}}(\alpha + x) = 4\alpha$.

Lemma 3.2.5. If $(A, \mathbb{F})$ is a finite dimensional algebra, then

1. $\mathrm{Tr}_A : A \to \mathbb{F}$ is a linear map
2. $\mathrm{Tr}_A(\alpha 1_A) = \alpha \dim_{\mathbb{F}} A\ \forall \alpha \in \mathbb{F}$

Proof. 1. This is clear after writing $\mathrm{Tr}_A : A \to \mathrm{End}_{\mathbb{F}} A \to \mathbb{F}$ where the two arrow are linear

2. Also trivial since $L_\alpha = \alpha \, \mathrm{id}_A$.

$\square$

Corollary 3.2.6. $A = \mathbb{F} \oplus A_0$ where $A_0 := \ker \mathrm{Tr}_A$.

Lemma 3.2.7. If $a \in A$ then $\mu_a(z)$ is the minimal polynomial of L_a.

Proof. Note that

$$L_{a^n}(x) = a^n x = \underbrace{a \cdots a}_{n} x = (L_a)^n(x),$$

so for any polynomial $f(z)$, $f(L_a) = L_{f(a)}$. Now

$$f(a) = 0 \implies f(L_a) = L_0 = 0$$

and

$$f(L_a) = 0 \implies 0 = f(L_a)(1_A) = L_{f(a)} = f(a)1 = f(a),$$

so L_a and a satisfy the same polynomials. $\square$

Week 6, lecture 1 starts here

Lemma 3.2.8. Let D be a finite division algebra over $\mathbb{R}$ and $a \in D_0 = \ker \mathrm{Tr}_D$. Then $a^2 \in \mathbb{R}$, $a^2 \leq 0$ and $a^2 = 0 \iff a = 0$.

Proof. 1. By 3.1.15 and 2.3.9, the minimal polynomial of a is $\mu_a(x) = x^2 + \alpha x + \beta$ with $\mathcal{D} = \alpha^2 - 4\beta < 0$. Also $\mu_a = \mu_{L_a}$, where $L_a : D \to D$ is a linear map with eigenvalues the roots of $\mu_a(x)$ and $\chi_{L_a}(x) = \mu_a(x)^{\frac{1}{2}\dim D}$. Denote $n = \dim D$ (which is even), then one can write

$$\chi_{L_a}(x) = x^n - \mathrm{Tr}(L_a)x^{n-1} + \cdots = x^n + \frac{n}{2} d x^{n-1} + \cdots ,$$

so $-\mathrm{Tr}(L_a) = \frac{n}{2}\alpha$. But $\mathrm{Tr}(L_a) = \mathrm{Tr}_D(a) = 0$ since $a \in D_0$. It follows $\alpha = 0$, $a^2 + \beta = 0$ and $-4\beta = \mathcal{D} \leq 0$, so $a^2 = -\beta \in \mathbb{R}$ and $a^2 \leq 0$.

2. Obvious since D is a division ring.

$\square$

Definition 3.2.9. Equip D_0 with euclidean form

$$\begin{aligned} q : D_0 &\to \mathbb{R} \\ a &\mapsto -a^2 \geq 0 \end{aligned}$$

and

$$\begin{aligned} \tau : D_0 \times D_0 &\to \mathbb{R} \\ (a,b) &\mapsto \frac{1}{2}\left(q(a+b) - q(a) - q(b)\right) \\ &= \frac{1}{2}\left(-(a+b)^2 + a^2 + b^2\right) = -\frac{1}{2}(ab + ba) \end{aligned}$$

Lemma 3.2.10. (D_0, τ) is a finite dimensional euclidean space.

Proof. Note $\tau(a,b) = -\frac{1}{2}(ab+ba)$ is symmetric bilinear and

$$a \neq 0 \implies \tau(a,a) = q(a) = -a^2 \in \mathbb{R}_{>0}.$$

$\square$

Lemma 3.2.11. If $e_1, \ldots, e_n$ is an orthonormal basis of D_0 then $e_i^2 = -1$ and if $i \neq j$ then $e_ie_j = -e_je_i$.

Proof. First note $e_i^2 = -q(e_i) = -1$. Then

$$0 = \tau(e_i, e_j) = -\frac{1}{2}(e_ie_j + e_je_i),$$

so $e_ie_j = -e_je_i$. $\square$

Corollary 3.2.12. Suppose $i < j < k$, then $e_k = \pm(e_ie_j)^{-1}$.

Proof. Let $u = e_ie_je_k$, then $u^2 = e_ie_j \underbrace{e_ke_i}_{-e_ie_k} \underbrace{e_je_k}_{-e_ke_j} = \underbrace{e_ie_j}_{-e_je_i} e_i \underbrace{e_ke_k}_{-1} e_j = e_je_ie_ie_j = -e_je_j = 1$. Then $u^2 - 1 = (u-1)(u+1) = 0$, and since D is division, $u = \pm 1$, i.e. $e_ie_je_k = \pm 1$, which gives the desired after rearranging. $\square$

Theorem 3.2.13 (Frobenius)**.** A finite dimensional division algebra over $\mathbb{R}$ is isomorphic to $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$.

Proof. Consider values of $n = \dim_{\mathbb{R}} D$.

1. $n = 1$, then $D = \mathbb{R}$.
2. $n = 2$, then e_1 is a basis of D_0 with $e_1^2 = -1$, so $D \cong \mathbb{C}$ via $i \mapsto e_1$.
3. $n = 3$, then $D = \mathbb{R}$ by 3.2.2.
4. $n = 4$, then e_1, e_2, e_3 is a basis of D_0, so $D \cong \mathbb{H}$ via $i \mapsto e_1, j \mapsto e_2, k \mapsto e_1e_2$.
5. $n \geq 5$, then $\exists e_1, e_2, e_3, e_4$, but $e_3 = \pm(e_1e_2)^{-1}$ and $e_4 = \pm(e_1e_2)^{-1}$, so $e_3 = \pm e_4$, contradicting linear independence of a basis.

$\square$

Theorem 3.2.14. A countably generated division algebra over $\mathbb{R}$ is isomorphic to $\mathbb{R}, \mathbb{C}$ or $\mathbb{H}$.

Proof. Consider such D. The Amitsur trick (2.3.10) tells us any $d \in D$ is algebraic over $\mathbb{R}$. But since D is division, $\forall d \in D\backslash\mathbb{R},\ \mu_d(x) = x^2 + \alpha x + \beta$ with $\mathcal{D} < 0$ again by 3.1.15 and 2.3.9. So now suppose $D \neq \mathbb{R}$ and pick $a \in D\backslash\mathbb{R}$, then $a^2 = -\alpha_a a - \beta_a$, so $\mathbb{R}(a) \cong \mathbb{C}$. If $\mathbb{R}(a) = D$ we are done, so suppose $\mathbb{R}(a) \neq D$ and pick $b \in D\backslash\mathbb{R}(a)$. One has

$$\mu_{a+b}(x) = (a+b)^2 + \alpha_{a+b}(a+b) + \beta_{a+b} = a^2 + ab + ba + b^2 + \cdots = 0,$$

so

$$ba = -\left(a^2 + b^2 + ab + \alpha_{a+b}(a+b) + \beta_{a+b}\right).$$

This implies $\mathbb{R}\langle a,b\rangle$, the subalgebra generated by a,b, is spanned by $1,a,b,ab$, so

$$3 \le \dim \mathbb{R}\langle a,b\rangle \le 4,$$

but $\mathbb{R}\langle a,b\rangle$ is a division algebra since $\forall d \in D$,

$$d^{-1} = \beta_d^{-1}(d+\alpha_d),$$

so $\mathbb{R}\langle a,b\rangle = \mathbb{H}$ by Frobenius. If $\mathbb{R}\langle a,b\rangle = D$ we are done, so pick $c \in D\backslash\mathbb{R}\langle a,b\rangle$ and consider $\mathbb{R}\langle a,b,c\rangle$. Similarly, it is division and is spanned by $1,a,b,c,ab,bc,ac$, so

$$5 \le \dim \mathbb{R}\langle a,b,c\rangle \le 7,$$

contradicting Frobenius. □

Week 6, lecture 2 starts here

3.3 Finite division ring

Proposition 3.3.1. If R is a commutative ring and $I \trianglelefteq R$ then I is maximal iff R/I is a field.

Proof. $\Rightarrow$ Pick $0 \neq x+I \in R/I$, then $x \notin I$ and $J := Rx + I \supsetneq I$, so maximality of I tells us $J = R \ni 1$, i.e. $\exists y \in R, z \in I : 1 = xy + z$, but then $1 + I = (x+I)(y+I)$, hence $y + I$ is the inverse of $x + I$.

$\Leftarrow$ It follows 0 and R/I are the only ideals and in particular they are the only R-submodules of R/I. Correspondence theorem gives us a bijection between submodules of R/I and submodules of R containing I. Hence there are only two submodules of R containing I and they can only be R and I, which is equivalent to that I is maximal.

□

Corollary 3.3.2. If R is a PID and $I = (r) \trianglelefteq R$, then the following are equivalent:

1. r is irreducible
2. I is maximal
3. R/I is a field

Proof.
- $2 \iff 3$: This is 3.3.1.
- $2 \implies 1$: We write $r = xy$ and we want to show x or y is a unit. Note (x) contains I, so by maximality either
  1. $(x) = R \ni 1$, hence $\exists z \in R : xz = 1$ so x is a unit; or
  2. $(x) = I \ni r$, hence $\exists z : x = rz$ so $r = xy = rzy$ and since R is a domain $zy = 1$ so y is a unit
- $1 \implies 2$: Pick $J \trianglelefteq R : J \supseteq I$. Then $J = (x) \ni r$, so $\exists y : r = xy$. Since r is irreducible, either
  1. x is a unit, hence $J = R$.

2. y is a unit, hence $x = ry^{-1}$ so $J = (x) = (r) = I$.

$\square$

Recall that if $\mathbb{F}$ is a field then $\mathbb{F}[x]$ is a PID and $R = \mathbb{F}[x]/I$ where $I = (f(x))$ is a field iff f is irreducible.

Lemma 3.3.3. If $\mathbb{F}$ is a field and $\deg f = n$ then for any $z \in \mathbb{F}[x]/(f(x))$,

$$\exists! h(x) \in \mathbb{F}[x]_{\leq n-1} : z = h + I.$$

Proof. Write $z = g(x) + I$, then $g(x) = q(x)f(x) + r(x)$ where $\deg r \leq n-1$, so $z = r + I$. Now suppose $z = r + I = s + I$, then $r - s \in I$ with $\deg(r-s) \leq n-1$, so $r - s = 0 \implies r = s$. $\square$

Example 3.3.4. Consider $A = \mathbb{Q}[x]/I$ where $I = (x^3 - 2x^2 + 1)$. By Eisenstein's criterion $x^3 - 2x^2 + 2$ is irreducible, so A is a field. x^3 is now $2x^2 - 2$ and by previous lemma $1, x, x^2$ is a $\mathbb{Q}$-basis of A. For example,

$$(x+1)^3 = x^3 + 3x^2 + 3x + 1 = 2x^2 - 2 + 3x^2 + 3x + 1 = 5x^2 + 3x - 1,$$

$$x^4 = x(2x^2 - 2) = 2x^3 - 2x = 2(2x^2 - 2) - 2x = 4x^2 - 2x - 4,$$

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

and

$$x^6 = x^3x^3 = (2x^2 - 2)^2 = \cdots$$

In general, one has the multiplication table

	1	x	x^2
1	1	x	x^2
x	x	x^2	$2x^2 - 2$
x^2	x^2	$2x^2 - 2$	$4x^2 - 2x - 4$

and the left multiplication by x and x^2 are

$$L_x = \begin{pmatrix} 0 & 0 & -2 \\ 1 & 0 & 0 \\ 0 & 1 & 2 \end{pmatrix}, \qquad L_{x^2} = \begin{pmatrix} 0 & -2 & -4 \\ 0 & 0 & -2 \\ 1 & 2 & 4 \end{pmatrix}$$

with traces

$$\mathrm{Tr}_A(x) = 2, \qquad \mathrm{Tr}_A(x^2) = 4$$

and $\mathrm{Tr}_A(1) = \dim A = 3$.

Week 6, lecture 3 starts here

Example 3.3.5. $\mathbb{F}_3 = \mathbb{Z}/(3)$ is a field of 3 elements.

Note that $\mathbb{Z}/(9)$ is not a field since $3 \cdot 3 = 0_{\mathbb{Z}/(9)}$. So how do we get a field of 9 elements? It is $\mathbb{F}_9 = \mathbb{F}_3[x]/(f(x))$ where f is monic, quadratic and irreducible, so that $1, x$ is a $\mathbb{F}_3$ basis of $\mathbb{F}_9$. Since $f(x)$ is of the form $x^2 + \cdots$ and one needs $f(0), f(1), f(2) \neq 0$ for f to be irreducible, so f can only be $x^2 + x + 2$, $x^2 + 1$ or $x^2 + 2x + 2$. The 9 elements of $\mathbb{F}_9$ can therefore be explicitly written down as: $0, 1, 2$, two roots of $x^2 + x + 2$, two roots of $x^2 + 1$, and two roots of $x^2 + 2x + 2$.

Lemma 3.3.6. If $\mathbb{F}$ is a field and $G \leq \mathbb{F}^\times$ with $|G| < \infty$, then G is cyclic.

Proof. Suppose $|G| = n$. By the fundamental theorem of finitely generated abelian groups, $G \cong C_{k_1} \times C_{k_2} \times \cdots \times C_{k_m}$ where $k_m \mid k_{m-1} \mid \cdots \mid k_1,\ k_m > 1$, and $n = k_1 \cdots k_m$. Then $\forall g \in G,\ g^{k_m} = 1$, i.e. every $g \in G$ satisfies $f(g) = 0$ where $f(x) = x^{k_m} - 1$, so

$$\prod_{g \in G} (x - g) \mid f(x)$$

since $\mathbb{F}[x]$ is a UFD, so

$$n = \deg \prod_{g \in G} (x - g) \leq k_m$$

hence $m = 1$. □

Proposition 3.3.7. Any finite field is isomorphic (as a ring) to $\mathbb{F}_p[x]/(f)$ where p is prime and $f(x) \in \mathbb{F}_p[x]$ is irreducible.

Proof. Let $\mathbb{F}$ be a finite field. Consider $\varphi : \mathbb{Z} \to \mathbb{F} : n \mapsto n1_{\mathbb{F}}$. Note $\ker \varphi = (p)$ and so $\operatorname{im} \varphi = \mathbb{Z}/\ker \varphi = \mathbb{F}_p \leq \mathbb{F}$ by 1st isomorphism theorem. In particular, $\mathbb{F}$ is an $\mathbb{F}_p$ algebra. By , $\mathbb{F}^\times$ is cyclic, so let $z \in \mathbb{F} : \langle z \rangle = \mathbb{F}^\times$. One has a $\mathbb{F}_p$ algebra homomorphism $\psi : \mathbb{F}_p[x] \to \mathbb{F} : f(x) \mapsto f(z)$. Since powers of z span $\mathbb{F}$, ψ is surjective, so $\mathbb{F} \cong \mathbb{F}_p[x]/\ker \psi$, and since $\mathbb{F}_p[x]$ is a PID one can write $\ker \psi = (h)$. By 3.3.2, since $\mathbb{F}$ is a field, h is irreducible. □

Summary:

1. For any prime power $q = p^n$, $\exists$ a field of size q
2. Such field is unique up to isomorphism
3. This field is $\mathbb{F}_p[x]/(f)$ where $\deg f = n$ but such f is not unique

Proposition 3.3.8 (Chinese remainder theorem for $\mathbb{F}[x]$)**.** Write $f = h_1^{a_1} \cdots h_n^{a_n} \in \mathbb{F}[x]$ where $a_i \in \mathbb{N}$ and h_i distinct irreducibles. Then $\mathbb{F}[x]/(f) \cong \mathbb{F}[x]/(h_1^{a_1}) \times \cdots \times \mathbb{F}[x]/(h_n^{a_n})$.

Lemma 3.3.9. If R is a division ring then

1. $Z(R)$ is a field
2. R is a vector space over $Z(R)$
3. $(R, Z(R))$ is an algebra

Proof.
1. $Z(R)$ is a subring so it suffices to show it's division. Let $x \in Z(R)$, then $\exists x^{-1} \in R$, and for $y \in R$ one has $xy = yx$, so $yx^{-1} = x^{-1}xyx^{-1} = x^{-1}yxx^{-1} = x^{-1}y$, hence $x^{-1} \in Z(R)$.
2. follows from 3.
3. $\mathrm{id} : Z(R) \to Z(R)$ gives the algebra structure.

□

Corollary 3.3.10. If D is a finite division ring then

1. $Z(D) = \mathbb{F}_q$ for prime power q
2. $n = \dim_{\mathbb{F}} D$ is finite
3. $|D| = q^n$

Proof. 1. Note $Z(D)$ is a finite field

2. since D is finite

3.
$$|\mathbb{F}_q^n| = \left| \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} : a_i \in \mathbb{F}_q \right\} \right| = q^n.$$

□

Lemma 3.3.11. If D is a division ring then each centraliser $C(x) = \{a \in D : ax = xa\}$ is a $Z(D)$-subalgebra.

Proof. First note $0, 1 \in C(x)$. Now if $a, b \in C(x)$ then $(a - b)x = ax - bx = xa - xb = x(a - b)$ and $abx = a(xb) = (xa)b$ so $ab, a - b \in C(x)$, hence $C(x)$ is a subring. Also $Z(D) \subseteq C(x)$ so $C(x)$ is closed under scalar multiplication by $\alpha \in Z(D)$. Finally if $a \in C(x)$ then $ax = xa \implies xa^{-1} = a^{-1}axa^{-1} = a^{-1}xaa^{-1} = a^{-1}x$, i.e. $a^{-1} \in C(x)$, hence $C(x)$ is division; so it is a $Z(D)$-subalgebra. □

Week 7, lecture 1 starts here

3.3.1 Finite group action

Recall

Definition 3.3.12. One says a finite group G *acts* on a finite set X if one can specify a map $G \times X \to X : (g, x) \mapsto {}^g x$ such that ${}^1 x = x$ and ${}^{g\,h}x ={}^{gh} x$.
For $x \in X$ one has the orbit of x: $\operatorname{orb}(x) = {}^G x = \{{}^g x : g \in G\}$ and the stabiliser of x: $\operatorname{stab}(x) = G_x = \{g : {}^g x = x\}$.

Proposition 3.3.13 (Orbit–Stabiliser formula)**.**
$$|\operatorname{orb}(x)| = |G : \operatorname{stab}(x)| = \frac{|G|}{|\operatorname{stab}(x)|}.$$

Proof. There exists a bijection $\operatorname{orb}(x) \leftrightarrow G/\operatorname{stab}(x)$. □

Proposition 3.3.14 (Class equation I)**.** Let G act on X and $x_1, \ldots, x_n$ representations of different orbits. Then
$$|X| = \sum_{i=1}^{n} |\operatorname{orb}(x_i)| = \sum_{i=1}^{n} \frac{|G|}{|\operatorname{stab}(x_i)|}.$$

Proof. It follows from that $X = \operatorname{orb}(x_1) \sqcup \cdots \sqcup \operatorname{orb}(x_n)$ and 3.3.13. □

Definition 3.3.15. The *fixed point set* is $X^G := \{x : {}^g x = x \ \forall g\} = \{x : |\operatorname{orb}(x)| = 1\}$.

Corollary 3.3.16 (Class equation II)**.** Let $y_1, \ldots, y_k$ be representatives of orbits of size ≥ 2, then

$$|X| = |X^G| + \sum_{i=1}^{n} \frac{|G|}{|\text{stab}(y_i)|}.$$

We already know if D is a finite division ring then $Z = Z(D)$ is a field of size $q = p^n$ where p is prime and $|D| = q^m$ where $m = \dim_Z D$.

Now consider $G = D^\times$ (so $|G| = q^m - 1$) and let G act on D (called an *inner automorphism*) by conjugation: ${}^g d = gdg^{-1}$. This is indeed an action: ${}^1 d = 1d1^{-1} = d$ and ${}^g {}^h d = {}^g(hdh^{-1}) = ghdh^{-1}g^{-1} = (gh)d(gh)^{-1} = {}^{(gh)}d$,

The stabiliser of x is

$$\text{stab}(x) = \{g \in D^\times : gxg^{-1} = x\} = C(x)^\times$$

and note that the fixed point set is $D^G = Z(D) = Z$.

Proposition 3.3.17. In the notation above, $\exists d_1, \ldots, d_k \in \mathbb{Z}^+ : d_i \mid m, d_i < m \ \forall i$ and

$$q^m = q + \sum_{i=1}^{k} \frac{q^m - 1}{q^{d_i} - 1}.$$

Proof. If $m = 1$ then $D = Z$ and we take $k = 0$ (empty set of d_i's). The desired is then a tautology: $q = q$.

Now suppose $m > 1$ and let $y_1, \ldots, y_k$ be representatives of G-orbits of size ≥ 2. By 3.3.16,

$$|D| = |D^G| + \sum_{i=1}^{k} \frac{|G|}{|\text{stab}(y_i)|}$$

and by previous observation, this implies

$$q^m = q + \sum_{i=1}^{k} \frac{q^m - 1}{|C(y_i)^\times|},$$

where $C(y_i)$ is a division algebra over Z by 3.3.11, hence $|C(y_i)| = q^{d_i}$ where $d_i \geq 1$. Also $|\text{orb}(y_i)| \geq 2 \implies C(y_i) \subsetneq D \implies d_i < m$. Finally, since D is a vector space over $C(y_i)$, define $C(y_i) \times D \to D : (a, b) \mapsto ab$ and let $a_i = \dim_{C(y_i)} D$, then

$$|D| = |C(y_i)|^{a_i} \implies q^m = (q^{d_i})^{a_i} \implies d_i a_i = m,$$

and in particular $d_i \mid m$. $\square$

Lemma 3.3.18. If $d \mid n$ then $(x^d - 1) \mid (x^n - 1)$ in $\mathbb{Z}[x]$.

Proof. Write $z = x^d$, then

$$\frac{x^n - 1}{x^d - 1} = \frac{z^{n/d} - 1}{z - 1} = z^{n/d-1} + z^{n/d-2} + \cdots + 1.$$

$\square$

In $\mathbb{C}[x]$, let $\alpha_k = e^{\frac{2\pi k}{n} i}$ so that $\alpha_0, \ldots, \alpha_{n-1}$ are all nth roots of 1 and one can write

$$x^n - 1 = (x - \alpha_0) \cdots (x - \alpha_{n-1}).$$

Lemma 3.3.19. Let $d_k = \gcd(n, k)$. Then

1. $|\alpha_k| = \frac{n}{d_k}$,
2. α_k is $\frac{n}{d_k}$th primitive root of unity
3. If $d_k = 1$ then α_k is nth primitive root of unity

Proof. 1 implies 2 which trivially implies 3, so let's prove 1.

$$(\alpha_k)^{n/d_k} = \alpha_1^{\frac{kn}{d_k}} = (\alpha_1^n)^{\frac{k}{d_k}} = 1,$$

so $|\alpha_k| \mid \frac{n}{d_k}$. Now suppose $|\alpha_k| = m < \frac{n}{d_k}$, then

$$\alpha_k^m = 1 \implies \alpha_1^{km} = 1 \implies n \mid km \implies \frac{n}{d_k} \mid \frac{k}{d_k} m \implies \frac{n}{d_k} \mid m.$$

So $|\alpha_k| = \frac{n}{d_k}$. □

Week 7, lecture 2 starts here

3.3.2 Cyclotomic polynomial

Definition 3.3.20 (Cyclotomic polynomial)**.**

$$\phi_n(x) = \prod_{k=1, \gcd(k,n)=1}^{n} \left(x - \alpha^k\right)$$

where $\alpha = e^{\frac{2\pi}{n} i}$.

Proposition 3.3.21.

$$x^n - 1 = \prod_{d \mid n} \phi_d(x) \qquad \in \mathbb{C}[x].$$

Proof. $(x - \alpha^k)$ appears once in both sides since $x^n - 1 = \prod_{k=1}^n \left(x - \alpha^k\right)$ and $(x - \alpha^k)$ appears in $\phi_d(x)$ where $d = |\alpha^k|$ in $\mathbb{C}^\times$. □

Example 3.3.22. If p is prime then

$$\phi_p(x) = \frac{x^p - 1}{\phi_1(x)} = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1.$$

Proposition 3.3.23. $\phi_n(x) \in \mathbb{Z}[x]$ and is monic.

Proof. One proves by induction on n using 3.3.21. If $n = 1$ then $\phi_1(x) = x - 1$ so done. Now suppose the statement is true for all values $< n$. Then

$$x^n - 1 = \phi_n(x) \cdot \underbrace{\prod_{d \mid n, d < n} \phi_d(x)}_{:= f(x)}$$

where $f(x) \in \mathbb{Z}[x]$ and is monic by inductive hypothesis. Now from the above one can write

$$(x^n + \cdots) = (\alpha x^a + \cdots)(x^b + \cdots)$$

so $x^n = \alpha x^{a+b}$ hence $\alpha = 1$, i.e. monic. Now the division

$$\phi_n(x) = \frac{x^n - 1}{f(x)}$$

can be thought of as the rewriting rule $x^b \rightsquigarrow x^b - f(x) \in \mathbb{Z}[x]_{\leq b-1}$ applied repeatedly to $x^n - 1$. The fact that the result is $\in \mathbb{Z}[x]$ simply follows from that $x^b - f(x)$ is integer-valued. $\square$

3.3.3 Unabomber theorem

Theorem 3.3.24. A finite division ring is a field.

Proof. Suppose such D is not a field. $Z(D)$ is a field, $|Z(D)| = q$ and $|D| = q^m$ where $m \geq 2$. Rewrite 3.3.17 as

$$q - 1 = q^m - 1 + \sum_{i=1}^{k} \frac{q^m - 1}{q^{d_i} - 1} \qquad (*)$$

and consider $\phi_m(q) \in \mathbb{Z}$. Since $\phi_m(z) \mid z^m - 1$ by 3.3.21 one has $\phi_m(q) \mid q^m - 1$. Also $\phi_m(z) \nmid z^{d_i} - 1$ so $\phi_m(z) \mid \frac{z^m-1}{z^{d_i}-1}$, hence $\phi_m(q) \mid \frac{q^m-1}{q^{d_i}-1}$, i.e. $\phi_m(q)$ divides the RHS of $*$, so $\phi_m(q) \mid q - 1$. Now

$$\phi_m(q) = \prod_{k|m, \gcd(k,m)=1} \left(q - e^{\frac{2\pi k}{m} i}\right)$$

but note that

$$\left|q - e^{\frac{2\pi k}{m} i}\right| > |q - 1| \ \forall k$$

since $m \geq 2$, an absurdity. $\square$

3.4 Laurent series

Definition 3.4.1. Given a ring R one has new rings $R[x] \leq R[[x]] \leq R((x))$ where the last one is defined as

$$R((x)) := \left\{ \sum_{k=N}^{\infty} a_k x^k \right\}$$

where N is allowed to be negative, called the *Laurent series.* (The series infinite in both directions $R[[x, x^{-1}]]$ do not form a ring.)
Addition is defined by

$$\sum_{k=N}^{\infty} a_k x^k + \sum_{k=M}^{\infty} b_k x^k = \sum_{k=\min(N,M)}^{\infty} (a_k + b_k) x^k$$

and multiplication is defined by

$$a x^k \cdot b x^m = ab x^{k+m}$$

extended by "infinite transitivity":

$$\sum_{k=N}^{\infty} a_k x^k \cdot \sum_{k=M}^{\infty} b_k x^k = \sum_{k=N+M}^{\infty} c_k x^k$$

where

$$c_k = \sum_{i+j=k} a_i b_j.$$

Note that although $R[x][y] = R[y][x]$ naively, it's not true that $R((x))((y)) = R((y))((x))$:

$$\underbrace{\sum_{k=-\infty}^{0} (x^{-k})(y^k)}_{\notin R((x))((y))} = \sum_{n=0}^{\infty} x^n y^{-n} = \underbrace{\sum_{n=0}^{\infty} (y^{-n}) x^n}_{\in R((y))((x))}$$

since you are not allowed to sum from $-\infty$.

Week 7, lecture 3 starts here

Lemma 3.4.2. *$t = a_n x^n + \cdots \in R((x))$ where $a_n \neq 0$ is invertible in $R((x))$ iff a_n is invertible in R.*

Proof. $\Leftarrow$: Write $t^{-1} = z_{-n} x^{-n} + z_{-n+1} x^{-n+1} + \cdots$ and solve $t \cdot t^{-1} = 1$:

$$\begin{cases} a_n z_{-n} = 1 \\ a_n z_{-n+1} + a_{n+1} z_{-n} = 0 \\ a_n z_{-n+2} + a_{n+1} z_{-n+1} + a_{n+2} z_{-n} = 0 \\ \vdots \end{cases}$$

which can be solved recursively if a_n^{-1} exists:

$$\begin{aligned} z_{-n} &= a_n^{-1} \\ z_{-n+1} &= -a_n^{-1} a_{n+1} z_{-n} = -a_n^{-1} a_{n+1} a_n^{-1} \\ z_{-n+2} &= -a_n^{-1} a_{n+1} z_{-n+1} - a_n^{-1} a_{n+2} z_{-n} \\ &= a_n^{-1} a_{n+1} a_n^{-1} a_{n+1} a_n^{-1} - a_n^{-1} a_{n+2} a_n^{-1} \\ &\vdots \end{aligned}$$

□

Corollary 3.4.3. If R is division then $R((x))$ is division.

This gives us division algebras $\mathbb{H}((x))$, $\mathbb{H}((x))((y))$ and so on.

Consider $\mathbb{C}((z,\sigma))$ which is equal to $\mathbb{C}((z))$ as abelian groups but with extra rule $z\alpha = \overline{\alpha} z$ where $\alpha \in \mathbb{C}$, i.e.

$$\alpha z^n \cdot \beta z^m = \begin{cases} \alpha\beta z^{n+m} & n \text{ is even} \\ \alpha\overline{\beta} z^{n+m} & n \text{ is odd} \end{cases}$$

extended by infinite transitivity. It's also a division ring. Note that

$$Z(\mathbb{H}((x))) = \mathbb{R}((x)), \qquad Z(\mathbb{C}((z,\sigma))) = \mathbb{R}((z^2))$$

which are isomorphic via $x \mapsto z^2$, but $\mathbb{H}((x)) \not\cong \mathbb{C}((z,\sigma))$ as rings.

4 Semisimplicity

4.1 Direct sum

Definition 4.1.1. For R-modules $M_i,\ i \in I$, their *direct product* is

$$\prod M_i = \{(m_i) : m_i \in M_i\} = \left\{f : I \to \bigcap M_i : f(i) \in M_i\right\}$$

and their *direct sum* is

$$\bigoplus M_i = \left\{(m_i) \in \prod M_i : \text{for all but finitely many } i,\ m_i = 0\right\} = \left\{f : I \to \bigcup M_i : |\mathrm{supp}(f)| < \infty\right\}$$

where

$$\mathrm{supp}(f) = \{i : f(i) \neq 0\}.$$

It follows that if $|I| < \infty$, $\bigoplus\limits_{i \in I} M_i = \prod\limits_{i \in I} M_i$.

Example 4.1.2. Let $M_i = \mathbb{R}$ be a $\mathbb{Q}$-module and $I = \mathbb{N}$. Then

$$\prod M_i = \{(a_0, a_1, \ldots)\} \qquad \text{all sequences}$$

and

$$\bigoplus M_i = \{(a_0, a_1, \ldots)\} \qquad \text{eventually 0 sequences, i.e. } \exists N : \forall n > N,\ a_n = 0.$$

These are characterised as "external": producing new modules from existing ones. On the other hand, if M is a R-module with $M_i < M,\ i \in I$, the question of when we can say M is a direct sum of its submodules is characterised as an "internal" one. In this situation we have a homomorphism of R-modules:

$$\varphi : \bigoplus_{i \in I} M_i \to M$$
$$(m_i) \mapsto \sum_{i \in I} m_i$$

which is well defined since the sum $\sum_{i \in I} m_i$ is finite.

Definition 4.1.3. Define the *sum* $\sum_{i \in I} M_i := \operatorname{im} \varphi$ in the above notation.

In particular, if φ is surjective then $M = \sum_{i \in I} M_i$. If φ is injective then $\bigoplus_{i \in I} M_i \cong \operatorname{im} \varphi$. In this case we identify $\sum M_i$ with $\bigoplus M_i$ and call $\sum M_i$ the *internal direct sum*.

If φ is bijective then $\bigoplus M_i \cong M$. In this case M is a direct sum of its submodules M_i.

4.1.1 Peirce decomposition

In this section we consider how to decompose M into $M_1 \oplus \cdots \oplus M_n$.

Example 4.1.4. Let $M = V$ be a 2-dimensional vector space over $\mathbb{F}$. How do we get $V = U \oplus W$? If we have we have 2 projection operators $p : V \to U \to V : u + w \mapsto u \mapsto u$ and $q : V \to W \to V : u + w \mapsto w \mapsto w$. Both $p, q \in \mathrm{End}_{\mathbb{F}} V$. Note that $p + q = \mathrm{id}_V = 1_{\mathrm{End}_{\mathbb{F}} V}$, $p^2 = p,\ q^2 = q$ and $pq = qp = 0$. This is a system of orthogonal idempotents.

Claim: idempotents $e \in \mathrm{End}_{\mathbb{F}} V$ are projection operators.

Indeed, $e^2 - e = 0 \implies \mu_e(x) \mid x(x-1) \implies e$ is diagonalisable with $1, 0$ on the diagonal $\implies$ one can let V be the 1-eigenspace of e (i.e. $\operatorname{im} e$) and W be the 0-eigenspace (i.e. $\ker e$).

Therefore, in the previous example, $U = \operatorname{im} p = \ker q$ and $W = \ker p = \operatorname{im} q$.

Let's define properly.

Definition 4.1.5. $R \ni e$ is *idempotent* if $e^2 = e$.

Idempotent e, f are *orthogonal* if $ef = fe = 0$.

$e_1, \ldots, e_n$ is a *full system of orthogonal idempotents* if $\begin{cases} \forall i,\ e_i^2 = e_i \\ \forall i \neq j,\ e_i e_j = e_j e_i = 0 \\ e_1 + \cdots + e_n = 1 \end{cases}$.

Example 4.1.6.

1. For $R = R_1 \times \cdots \times R_n, e_i := (0, \ldots, \underbrace{1}_{i\text{th position}}, \ldots, 0)$ form such system.
2. If $e \in R$ is idempotent than $f = 1-e$ is as well since $f^2 = (1-e)^2 = 1-2e+e^2 = 1-e = f$, and $ef = e(1-e) = 0$ and $fe = 0$, so e, f form such system.

Proposition 4.1.7. If M is a R-module then there is a bijection between

$$\{\text{decompositions of } R\text{-modules } M = M_1 \oplus M_2 \oplus \cdots \oplus M_n \text{ with all } M_i \neq 0\}$$

and

$$\{\text{full systems of orthogonal idempotents in } \mathrm{End}_R M\}.$$

These are called Peirce decompositions.

Proof. 1→2 Define $e_i : M \twoheadrightarrow M_i \hookrightarrow M$, i.e. $m = \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} \mapsto \begin{pmatrix} 0 \\ \vdots \\ m_i \\ \vdots \\ 0 \end{pmatrix}$. Then it's trivial that

i. $e_i \in \mathrm{End}_R M$
ii. $e_i^2 = e_i$
iii. $e_i e_j = 0$ for $i \neq j$
iv. $e_1 + \cdots + e_n = 1_{\mathrm{End}_R M}$

2→1 Define $M_i = \operatorname{im} e_i = M e_i$. Since e_i is a homomorphism of R-modules, $\operatorname{im} e_i$ is a submodule. It remains to check $\psi : \bigoplus_{i=1}^n M_i \to M$ is bijective:

i. ψ is surjective: let $m \in M$ so that $me_i \in M_i$, and

$$\begin{pmatrix} me_1 \\ \vdots \\ me_n \end{pmatrix} \overset{\psi}{\longmapsto} me_1 + \cdots + me_n = m(e_1 + \cdots + e_n) = m1 = m$$

ii. ψ is injective: let $x = \begin{pmatrix} m_1 e_1 \\ \vdots \\ m_n e_n \end{pmatrix} \in \ker \psi$, then $0 = \psi(x) = m_1 e_1 + \cdots + m_n e_n$. Multiplying this by e_i gives

$$0 = m_1 e_1 e_i + \cdots + m_n e_n e_i = m_i e_i$$

by orthogonality, hence $x = 0$.

Finally, they are inverse bijections by construction. □

4.1.2 Primary decomposition (example of Peirce decomposition)

Let A be an abelian group under $+$ such that $\exists N : \forall x \in A,\ |x| < N$, i.e. order of an element is bounded. Let $n = \operatorname{lcm}\{|x| : x \in A\}$. Note that A is a $\mathbb{Z}$-module with

$$E = \operatorname{End}_{\mathbb{Z}} A \geq \mathbb{Z}/(n) = \{x \mapsto kx\}$$

where k is the natural image of quotient map $\mathbb{Z} \to \mathbb{Z}/(n)$. Now if one decomposes n into $p_1^{a_1} \cdots p_k^{a_k}$ where p_i are distinct primes, then Chinese remainder theorem gives

$$\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{a_1}) \times \cdots \times \mathbb{Z}/(p_k^{a_k}) \leq E$$

which gives a full system of orthogonal idempotents

$$e_i = (0, \ldots, 1 + (p_i^{a_i}), \ldots, 0) \in E$$

and the Peirce decomposition of the group

$$A = Ae_1 \oplus \cdots \oplus Ae_k,$$

called the *primary decomposition.*

Claim 4.1.8. $Ae_i = \{x \in A : |x| = p_i^{b_i} \text{ where } b_i \leq a_i\}$.

Proof. $\subseteq$: Write $x = ye_i$ and note that $p_i^{a_i} x = p_i^{a_i} y e_i = y(p_i^{a_i} e_i) = y0_E = 0$, so $|x| \mid p_i^{a_i}$.

$\supseteq$: Write $x = x1_E = xe_1 + \cdots + xe_k$ and note that

$$0 = p_i^{b_i} x = p_i^{b_i} xe_1 + \cdots + p_i^{b_i} xe_k, \tag{$*$}$$

since $|xe_j| = p_j^{b_j}$, one has for $j \neq i,\ xe_j \neq 0 \implies p_i^{b_i} xe_j \neq 0$, i.e.

$$\text{for } j \neq i,\ p_i^{b_i} xe_j = 0 \implies xe_j = 0.$$

But $*$ is a direct sum decomposition, so all $p_i^{b_i} e_j = 0$, hence $xe_j = 0\ \forall j \neq i$, therefore $x = xe_i \in Ae_i$.

□

Week 8, lecture 2 starts here

4.1.3 Primary decomposition on a vector space

Let V be a finite dimensional vector space over $\mathbb{F}$ and $T : V \to V$ a linear operator. Suppose $\chi_T(z) = \pm(z - \alpha_1) \cdots (z - \alpha_n)$ with $\alpha_i \in \mathbb{F}$. Consider the minimal polynomial $\mu_T(z) = (z - \beta_1)^{a_1} \cdots (z - \beta_k)^{a_k}$ with $i \neq j \implies \beta_i \neq \beta_j$ and $a_i \geq 1$. Let $R = \mathbb{F}[x]$ so that V is a left R-module via $x \cdot v = T(v)$. We then have a homomorphism $\varphi : \mathbb{F}[x] \to \operatorname{End}_R V : x \mapsto (v \mapsto T(v))$ with $\ker \varphi = (\mu_T(z))$. Therefore by 1st isomorphism and Chinese remainder theorems

$$\operatorname{im} \varphi \cong \mathbb{F}[z]/(\mu_T(z)) \cong \mathbb{F}[z]/((z - \beta_1)^{a_1}) \times \cdots \times \mathbb{F}[z]/((z - \beta_k)^{a_k})$$

and one gets a full system of orthogonal idempotents $e_1, \ldots, e_k \in \operatorname{End}_R V$ where

$$e_i = (0, \ldots, 1 + ((z - \beta_i)^{a_i}), \ldots, 0)$$

with a corresponding Peirce decomposition

$$V = Ve_1 \oplus \cdots \oplus Ve_k,$$

called the *primary decomposition* of V with respect to T. See Dmitriy's notes for a proof of

$$Ve_i = \{v \in V : \exists a \geq 1 : (T - \beta_i)^a(v) = 0\},$$

where the right hand side is called the *generalised eigenspace* with eigenvalue β_i. This implies generalised eigenvectors for distinct eigenvalues are linearly independent.

4.1.4 Peirce decomposition and matrix

Let R be any ring. One has $\mathrm{End}_R R \cong R$ (1.3.10) and submodules of ${}_R R$ are left ideals. One therefore has

Proposition 4.1.9 (4.1.7 where $M = R$)**.** There is a bijection between

$$\{\text{full systems of orthogonal idempotents in } R\}$$

and

$$\{\text{decompositions } R = L_1 \oplus \cdots \oplus L_n\}$$

where L_i are left ideals.

Now for a full system $e_1, \ldots, e_r \in R$ and ${}_R M$ a left R-module, one can write

$$M = \bigoplus_{i=1}^{n} e_i M = \begin{pmatrix} e_1 M \\ e_2 M \\ \vdots \\ e_n M \end{pmatrix}$$

and with R itself one has

$$R = \bigoplus_{i,j=1}^{n} e_i R e_j = \begin{pmatrix} e_1 R e_1 & \cdots & e_1 R e_n \\ \vdots & e_i R e_j & \vdots \\ e_n R e_1 & \cdots & e_n R e_n \end{pmatrix}$$

where $e_i R e_j$ are distinct abelian groups. This is called the *double Peirce decomposition.*

Theorem 4.1.10.

1. If R is a $\mathbb{F}$-algebra, all $e_i R e_j$ and $e_i M$ are vector spaces over $\mathbb{F}$.
2. Each $e_i R e_i$ is a nonzero ring.
3. $e_i M$ is a $e_i R e_i$-module.
4. Multiplication in R and R-action on M satisfy standard "matrix rules":

$$\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix} \begin{pmatrix} s_{11} & \cdots & s_{1n} \\ \vdots & & \vdots \\ s_{n1} & \cdots & s_{nn} \end{pmatrix} = \left(\sum_R r_{iR} s_{Rj} \right)$$

where $r_{ij}, s_{ij} \in e_i R e_j$, and

$$\begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix} \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = \left(\sum_{i=1}^{n} r_{ik} m_k \right).$$

Proof. 1. Let $\alpha \in \mathbb{F},\ x \in e_iRe_j$. Then one can write $x = e_iye_j$ with $y \in R$, and

$$\alpha x = \alpha e_i y e_j = e_i(\alpha y)e_j \in e_iRe_j,$$

so e_iRe_j is a $\mathbb{F}$-vector subspace. Similar for e_iM.

2. Note $(e_ixe_i)(e_iye_i) = e_i(xe_iy)e_i \in e_iRe_i$, so it's closed under product. Also $1_{e_iRe_i} = e_i \neq 0$, so nonzero ring (but not a subring or R).

3. One has

$$(e_ire_i)e_im = e_i(re_im) \in e_iM, \quad \text{and} \quad 1_{e_iRe_i}e_im = e_i^2m = e_im$$

4. By definition,

$$(r_{ij})(s_{ij}) = \left(\sum r_{ij}\right)\left(\sum s_{ij}\right) = \sum_{i,j,k,m} r_{ij}s_{km}$$

where

$$r_{ij}s_{km} = e_ire_je_kse_m = \begin{cases} 0 & \text{if } j \neq k \\ e_ire_jse_m & \text{if } j = k \end{cases},$$

so

$$\sum_{i,j,k,m} r_{ij}s_{km} = \sum_{i,j,m} r_{ij}s_{jm} = \sum_{i,m}\left(\sum_j r_{ij}s_{jm}\right).$$

Similar for $R \times M \to M$.

□

Week 8, lecture 3 starts here

Lemma 4.1.11. Let $e, f, g \in R$ be 3 idempotents.

1. $eRf \cong \mathrm{Hom}_R(Re, Rf)$ as abelian groups.
2. This $\cong$ commutes with compositors, i.e.

$$\begin{array}{ccc} \alpha, \beta & \longmapsto & \alpha\beta \\ \mathrm{Hom}_R(Re, Rf) \times \mathrm{Hom}_R(Rf, Rg) & \longrightarrow & \mathrm{Hom}_R(Re, Rg) \\ \cong & & \cong \\ eRf \times fRg & \longrightarrow & eRg \\ a, b & \longmapsto & ab \end{array}$$

is commutative.

This is a generalisation of the ring isomorphism $\mathrm{End}_R R \cong R$ (which is the special case $e = f = 1$).

Proof. 1. Consider homomorphism of abelian groups

$$\begin{aligned} \psi : eRf &\to \operatorname{Hom}(Re, Rf) \\ exf &\mapsto (se \mapsto sexf). \end{aligned}$$

This is

injective: let $exf \in \ker \psi$, then $e\psi(exf) = e^2xf = exf = 0$.

surjective: consider $\varphi : Re \to Rf$. Then

$$\varphi(re) = \varphi(re^2) = \varphi((re)e) = re\varphi(e)$$

and

$$\varphi(e) = \varphi(e^2) = e\varphi(e)$$

so $\varphi(e) = eRf$ and $\psi(\varphi(e)) = \varphi$.

2. Let $(a, b) \in eRf \times fRg$ and write $a = exf$. Then $a = e^2xf^2 = e(exf)f = eaf$ and similarly $b = fbg$. So one can see

$$\begin{tikzcd}
(\alpha : x \mapsto xeaf, \beta : y \mapsto yfbg) \arrow[r, mapsto] & \alpha\beta : x \mapsto xeafbg \\
(eaf, fbg) \arrow[u, mapsto, "\cong"] \arrow[r, mapsto] & eafbg. \arrow[u, mapsto, "\cong"']
\end{tikzcd}$$

□

4.2 Semisimple module

Definition 4.2.1. M is *semisimple* if M is a direct sum of simple (sub-)modules.

Remark. 1. The sum is not necessarily finite.

2. The sum can be empty. This gives a zero module, which is semisimple.

3. If $R = \mathbb{F}$ is a field then ${}_{\mathbb{F}}\mathbb{F}$ is the only simple left R-module, and since every vector space has a basis, every R-module is semisimple.

4. If $R = \mathbb{F}[x]$, then a simple R-module is R/L where L is a maximal left ideal by 2.2.3, and we know L is of the form $(f(x))$ where f is irreducible. In particular, if $\mathbb{F}$ is algebraically closed, then all simple modules have the form $R/(x - \alpha)$, i.e. 1-dimensional.

5. In the case of the considered object in section 4.1.3, V as a R-module is semisimple iff T is diagonalisable.

Definition 4.2.2. For ${}_RM$, the *socle* of M is

$$\operatorname{soc} M := \sum_{S \leq M,\ S \text{ is simple}} S.$$

Example 4.2.3. Consider an abelian group A as a $\mathbb{Z}$-module. The simple $\mathbb{Z}$-modules are $\mathbb{Z}/(p)$ where p is prime, and the simple submodules of A are $\{\mathbb{Z}x : x \in A,\ |x| = p,\ p \text{ prime}\}$, so

$$\operatorname{soc} A = \sum_{|x| \text{ is prime}} \mathbb{Z}x = \{x \in A : |x| \text{ is square free}\}.$$

Example 4.2.4. Let $\mathbb{F}$ be an algebraically closed field and V a $\mathbb{F}[x]$-module. Simple submodules are then $\{\mathbb{F}v : v \text{ is an eigenvector of } T\}$ and $\operatorname{soc} V = \operatorname{span}\{\text{eigenvectors}\}$.

Lemma 4.2.5.

1. M is semisimple iff $M = \operatorname{soc} M$.
2. More precisely, if $M = \sum_{i\in I} S_i$ where S_i are all simple, then $\exists J \subseteq I : M = \bigoplus_{i\in J} S_i$.

Proof.

1. $\Rightarrow$: trivial since
$$M = \bigoplus_{i\in X,\ L_i \text{ simple}} L_i \implies \operatorname{soc} M \supseteq \sum L_i = M.$$
$\Leftarrow$: follows from 2.

2. Consider the poset $\mathcal{P} := \{J \subseteq I : \sum_{i\in J} S_i = \bigoplus_{i\in J} S_i\}$ under $\subseteq$. Since $\varnothing \in \mathcal{P}$, one has $\mathcal{P} \neq \varnothing$ and so can apply Zorn's lemma. Consider the chain $\mathcal{C} : J_1 \subseteq J_2 \subseteq \cdots \subseteq J_\infty \subseteq \cdots$ in $\mathcal{P}$ and define $Y = \bigcup_{J\in\mathcal{C}} J$. It's clear that once $Y \in \mathcal{P}$, it is an upper bound of $\mathcal{C}$ and thus by Zorn's $\mathcal{P}$ has a maximal element J. Examine the map
$$\begin{aligned}\varphi_Y : \bigoplus_{i\in Y} S_i &\to \sum_{i\in Y} S_i\\ (s_i) &\mapsto \sum s_i\end{aligned}$$
which is clearly surjective, and it's injective iff $\sum_{i\in Y} S_i$ is direct iff $Y \in \mathcal{P}$. Let $x \in \ker\varphi$, and write $x = (x_1, x_2, \ldots, x_n, 0, \ldots, 0)$. Then $1, 2, \ldots, n \in Y$, and since there are only finitely many positions, $\exists J \in \mathcal{C} : 1, \ldots, n \in J$. But φ_J is an isomorphism by construction, so $x_1 = \cdots = x_n = 0$, hence $x = 0$.

   Week 9, lecture 1 starts here

   Remark. If V is a $\mathbb{F}$-vector space, then there exists a basis $\{e_i : i \in I\}$ which gives a decomposition into 1-dimensional subspaces ${}_{\mathbb{F}}V = \bigoplus_{i\in I} \mathbb{F}e_i$. Now note that $\mathbb{F}e_i \cong {}_{\mathbb{F}}\mathbb{F}$: this leads to the idea of a free module. Also, $\mathbb{F}e_i$ is simple, so this also leads to the idea of semisimple module. The proof of 4.2.5 now proceeds.

   Now let $N = \sum_{i\in J} S_i = \bigoplus_{i\in J} S_i$ where J is the maximal element the argument above yields. If $N = M$ then we are done. If not, $\exists 0 \in I : S_0 \not\subseteq N$ (so $0 \notin J$) and since S_0 is simple one has $S_0 \cap N = \{0\}$. Let $\widehat{J} := J \cup \{0\}$. Consider $\psi : \bigoplus_{i\in\widehat{J}} S_i \to \sum_{i\in\widehat{J}} S_i = S_0 + N$ and let $x \in \ker\psi$. Write $x = (x_0, x_1, \ldots, x_n, 0, \ldots, 0)$ where $x_0 \in S_0$. Then $0 = \psi(x) = x_0 + \cdots + x_n$ so $x_0 = -(x_1 + x_2 + \cdots + x_n) \in S_0 \cap N = \{0\}$, hence $x_0 = x_1 + \cdots + x_n = 0$. But $\sum_{i\in J} S_i = \bigoplus_{i\in J} S_i$, so $x_1 = \cdots = x_n = 0$. Therefore ψ is injective and hence an isomorphism, and thus $\widehat{J} \in \mathcal{P}$, which contradicts maximality of J.

□

Corollary 4.2.6. A quotient module of a semisimple module is semisimple.

Proof. Suppose M is semisimple and write $M = \bigoplus_{i\in I} S_i$. For a submodule $N \leq M$, consider M/N and the quotient map $\varphi : M \to M/N$. Then $M/N = \sum_{i\in I} \varphi(S_i)$, and since S_i is simple, $\varphi(S_i) = S_i$ or 0, so
$$M/N = \sum_{i\in I,\ \varphi(S_i)=S_i} \varphi(S_i)$$
and by 4.2.5 one has M/N is semisimple. □

Comparing with quotient modules, submodules are harder: e.g. $\mathbb{R}^2 = \mathbb{R}e_1 \oplus \mathbb{R}e_2 = \bigoplus_{i\in I} S_i$, but $\mathbb{R}\begin{pmatrix}1\\1\end{pmatrix} \neq \bigoplus_{i\in J} S_i$ for any $J \subseteq I$. We need something more.

Definition 4.2.7. ${}_RM$ is *completely reducible* if $\forall N \leq M,\ \exists K \leq M : {}_RM = {}_RN \oplus {}_RK$. Such K is the *direct complement* to N.

Lemma 4.2.8. If $N \leq M$, then any direct complement K is isomorphic to M/N as modules.

Proof. Consider quotient map $\varphi : M \to M/N$ and restrict to K: $\varphi|_K : K \to M/N$, which is injective since if $x \in \ker \varphi|_K \subseteq \ker \varphi = N$ then $x \in N \cap K = \{0\}$ and surjective since if $m + N \in M/N$ then $m = n + k$ where $n \in N, k \in K$, so $\varphi|_K(k) = \varphi|_K(m - n) = m - n + N = m + N$. $\square$

Lemma 4.2.9. A submodule of a completely reducible module is completely reducible.

Proof. Let $N \leq M$ with M being completely reducible and let $K \leq N$. We need to find a direct complement for K. By assumption $M = K \oplus P$ for some P. Consider $\pi : M \to K$, projection along P. This induces a restriction $\widehat{\pi} := \pi|_N : N \to K$ with $\operatorname{im}\widehat{\pi} \subseteq \operatorname{im}\pi = K$, but $\pi(k) = k\ \forall k \in K$ so $K \subseteq \operatorname{im}\widehat{\pi}$, hence $\operatorname{im}\widehat{\pi} = K$ and by the 1st isomorphism theorem one can write $N = \operatorname{im}\widehat{\pi} \oplus \ker\widehat{\pi} = K \oplus \ker\widehat{\pi}$ where $\ker\widehat{\pi}$ is the direct complement we are looking for. $\square$

Week 9, lecture 2 starts here

Lemma 4.2.10. A nonzero completely reducible module contains a simple submodule.

Proof. Let M be such a R-module and $x \in M$ with $x \neq 0$. Consider homomorphism

$$\begin{aligned} \varphi_x : {}_RR &\to M \\ r &\mapsto rx \end{aligned}$$

and note that $Rx \cong R/\operatorname{Ann}(x) \leq M$ by remark before 2.2.4, so Rx is completely reducible by 4.2.9. Now $\operatorname{Ann}(x) \subseteq L$, the maximal left ideal, so one can consider the surjection

$$\begin{aligned} \psi : Rx &\twoheadrightarrow R/L \\ r + \operatorname{Ann}(x) &\mapsto r + L \end{aligned}$$

where R/L is simple by 2.2.3. Let P be the direct complement of $\ker\psi \leq Rx$, i.e. $Rx = \ker\psi \oplus P$. But $Rx = \ker\psi \oplus \operatorname{im}\psi$ where $\operatorname{im}\psi = R/L$, so P is simple. $\square$

Theorem 4.2.11. M is semisimple iff M is completely reducible.

Proof. $\Leftarrow$: By 4.2.10 one has $\operatorname{soc} M \neq 0$. If $M = \operatorname{soc} M$ we are done, so suppose $M \neq \operatorname{soc} M$, then $\exists P \leq M : M = \operatorname{soc} M \oplus P$ with $P \neq 0$. But P is completely reducible, so again by 4.2.10 there is a simple $S \leq P$, but this means $S \not\subseteq \operatorname{soc} M$, an absurdity.

$\Rightarrow$: Write $M = \bigoplus_{i\in I} S_i \geq N$ and we need a direct complement for N. Consider quotient map $\varphi : M \to M/N$. Since S_i is simple,

$$\varphi(S_i) \cong S_i/(S_i \cap N) = \begin{cases} 0 \\ \cong S_i \end{cases},$$

so

$$M/N = \sum_{i\in I,\ \varphi(S_i)\neq 0} \varphi(S_i),$$

and by 4.2.5 one has $\exists J \subseteq I : M/N = \bigoplus_{i\in J} \varphi(S_i)$ and $\varphi(S_i) \cong S_i$ for $i \in J$. Then

$$M = N \oplus \left(\sum_{i\in J} S_i \right).$$

Indeed, consider

$$\psi : N \oplus \left(\sum_{i\in J} S_i \right) \to M.$$

ψ is surjective: let $m \in M$ then $M/N \ni m + N = \varphi(m) = \varphi(x_1) + \cdots + \varphi(x_n)$ where $x_i \in S_i, i \in J$, so

$$m - x_1 - \ldots - x_n \in N$$

and hence

$$m = y + x_1 + \cdots + x_n \in \operatorname{im} \psi$$

for some $y \in N$.

ψ is injective: let $(m, x_1 + \cdots + x_n) \in \ker \psi$ where $m \in N, x_i \in S_i, i \in J$, then

$$m + x_1 + \cdots + x_n = 0$$

and so

$$\varphi(x_1) + \cdots + \varphi(x_n) = 0$$

since $\varphi(m) = 0$, which follows from that $\sum_{i\in J} \varphi(s_i)$ is direct, so $x_1 = \cdots = x_n = 0$ and hence $m = 0$ and therefore $(m, x_1 + \cdots + x_n) = 0$.

□

Corollary 4.2.12. A submodule of a semisimple module is semisimple.

4.2.1 Radical

Definition 4.2.13. A submodule P of M is *cosimple* if M/P is simple.

The *radical* of M is

$$\operatorname{rad} M := \bigcap_{P\leq M,\ P \text{ is cosimple}} P.$$

Recall for M/N one has the bijective correspondence

$$\{P \leq M : P \supseteq N\} \leftrightarrow \{Q \leq M/N\},$$

and for M/N to be simple it means both sets only have two elements, N, M and $0, M/N$, so N is maximal.

Example 4.2.14. ${}_{\mathbb{Z}}\mathbb{Z}$ has no simple submodules, and the simple $\mathbb{Z}$-modules are $\mathbb{Z}/(p)$ where p is prime, so

$$\operatorname{soc} \mathbb{Z} = \sum_{\varnothing} = 0$$

and

$$\operatorname{rad} \mathbb{Z} = \bigcap_p \mathbb{Z}/(p) = \{n : p \mid n\ \forall p\} = 0.$$

Example 4.2.15. Consider $M = \mathbb{Z}/(n)$ and $R = \mathbb{Z}$. For $n \in \mathbb{N}$, recall we also had a definition for radical of n: $\operatorname{rad} n = p_1 \cdots p_k$ with $n = p_1^{a_1} \cdots p_k^{a_k}$ where $a_i \geq 1$ and p_i are primes, e.g.

$$\operatorname{rad} 12000 = \operatorname{rad} 3 \times 2^5 \times 5^3 = 3 \times 2 \times 5 = 30.$$

A submodule Rx of M is simple when $|x| = p_i$, so $x = \frac{n}{p_i}$ and

$$\operatorname{soc} M = \mathbb{Z}\frac{n}{p_1} + \cdots + \mathbb{Z}\frac{n}{p_k} = \mathbb{Z}\frac{n}{p_1 \cdots p_k} = \mathbb{Z}\frac{n}{\operatorname{rad} n},$$

which also gives

$$\operatorname{soc} M \cong \mathbb{Z}/(p_1) \oplus \cdots \oplus \mathbb{Z}/(p_k) \cong \mathbb{Z}/(\operatorname{rad} n),$$

and by 4.2.5 M is semisimple iff $n = \operatorname{rad} n$, i.e. n is squarefree.

Similarly, a submodule Rx is cosimple if $M/Rx \cong \mathbb{Z}/(p_i)$, where an obvious choice for x is p_i, and

$$\operatorname{rad} M = \bigcap_{p_i} \mathbb{Z}(p_i + (n)) = \{x \in M : \forall i,\ p_i \mid x\} = \mathbb{Z}p_1 \cdots p_k = \mathbb{Z}\operatorname{rad} n,$$

so $M/\operatorname{rad} M \cong \mathbb{Z}/(\operatorname{rad} n) \cong \operatorname{soc} M$, which is semisimple. This implies if $\operatorname{rad} M = 0$ then M is semisimple. Let's see this in more generality.

Lemma 4.2.16. If M is semisimple then $\operatorname{rad} M = 0$.

Proof. Write $M = \bigoplus_{i \in I} S_i$. For i, let

$$P_i := \bigoplus_{k \in I \setminus \{i\}} S_k,$$

so that $M/P_i \cong S_i$ is simple, i.e. P_i is cosimple. But then $\operatorname{rad} M \subseteq \bigcap_i P_i = 0$. □

Definition 4.2.17. ${}_RM$ is *artinian* if any descending chain of submodules terminates, i.e. for any chain $P_1 \geq P_2 \geq \cdots \geq P_k \geq \cdots, \exists N : P_N = P_{N+1} = \cdots$.

A ring is *left artinian* if ${}_RR$ is artinian.

Theorem 4.2.18. If ${}_RM$ is artinian then M is semisimple iff $\operatorname{rad} M = 0$.

Week 9, lecture 3 starts here

Proof. By 4.2.16, it remains to prove the $\Rightarrow$ direction. Since $\operatorname{rad} M = 0$, $\exists$ cosimple submodules

$$P_1, \ldots, P_n, \ldots : P_1 \cap \cdots \cap P_n \cap \cdots = \operatorname{rad} M = 0.$$

This induces a descending chain

$$P_1 \supseteq P_1 \cap P_2 \supseteq P_1 \cap P_2 \cap P_3 \supseteq \cdots$$

which, by assumption, must terminate at some $P_1 \cap \cdots \cap P_n = 0$. Consider

$$\psi : M \to \underbrace{M/P_1 \oplus \cdots \oplus M/P_n}_{\text{semisimple}}$$

$$m \mapsto (m + P_1, \ldots, m + P_n),$$

whose kernel is precisely $P_1 \cap \cdots \cap P_n = 0$, hence ψ is injective and M is a submodule of $M/P_1 \oplus \cdots \oplus M/P_n$, therefore M is semisimple by 4.2.12. □

We are finally strong enough.

4.3 Semisimple ring

4.3.1 Artin–Wedderburn theorem

Theorem 4.3.1 (Artin–Wedderburn)**.** The following are equivalent for a ring R.

1. Every left R-module is semisimple.
2. ${}_RR$ is semisimple.
3. $\exists$ division rings $D_1, \dots, D_k : R \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$.

Proof. 1⇒2: trivial.

2⇒1: Let ${}_RM$ be a left R-module and $X \subseteq M$ a generating set. Consider

$$\begin{aligned}\varphi : \overbrace{\bigoplus_X {}_RR}^{\text{semisimple}} &\to M \\ (a_i)_{i\in X} &\mapsto \sum_{i\in X} a_i i,\end{aligned}$$

so M is a quotient of a semisimple module, hence by 4.2.6 M is semisimple.

3⇒2: Note that $D_i^{n_i}$ is a simple R-module, since $M_{n_i}(D_i)$ acts on it by matrix multiplication, so that every nonzero vector can be mapped to another. Now

$$M_{n_i}(D_i) = \underbrace{\begin{pmatrix} * & 0 & \cdots & 0 \\ * & 0 & \cdots & 0 \\ \vdots & \vdots & \cdots & \vdots \\ * & 0 & \cdots & 0 \end{pmatrix}}_{\cong D_i^{n_i}} \oplus \underbrace{\begin{pmatrix} 0 & * & \cdots & 0 \\ 0 & * & \cdots & 0 \\ \vdots & \vdots & \cdots & 0 \\ 0 & * & \cdots & 0 \end{pmatrix}}_{\cong D_i^{n_i}} \oplus \cdots \cong (D_i^{n_i})^{n_i}$$

so ${}_RM_{n_i}(D_i)$ is semisimple, hence ${}_RR$ is semisimple as well.

2⇒3: Write ${}_RR = \bigoplus_{i\in I} S_i$ where S_i is simple. Then

$$1_R = x_1 + \cdots + x_n \qquad x_i \in S_i, \text{all } x_i \neq 0$$

(note that n is finite) and any $r \in R$ can be written as

$$r = r1 = rx_1 + \cdots + rx_n,$$

so effectively ${}_RR = S_1 \oplus \cdots \oplus S_n$. Therefore $\exists$ idempotents $e_1, \dots, e_n \in \mathrm{End}_R R \cong R$ yielding this decomposition, i.e. $S_i = Re_i$. We now change the order:

$$\begin{aligned}{}_RR = &S_1 \oplus \cdots \oplus S_{a_1} \oplus \\ &S_{a_1+1} \oplus \cdots \oplus S_{a_1+a_2} \oplus \\ &\quad\vdots \\ &S_{a_1+\cdots+a_{k-1}+1} \oplus \cdots \oplus S_{a_1+\cdots+a_k}\end{aligned}$$

so that every module in a line are isomorphic and modules in different lines are not. Now apply double Peirce decomposition

$$R = \bigoplus_{i,j=1}^{n} e_i R e_j$$

and let $D_i := \mathrm{End} S_i$, which is a division ring by 2.2.8, and by 4.1.11

$$e_i R e_j \cong \mathrm{Hom}(Re_i, Re_j) = \begin{cases} 0 & \text{if } i,j \text{ are in different lines} \\ D_i \psi_{i,j} & \text{if } i,j \text{ are in the same line} \end{cases}$$

for some fixed isomorphism $\psi_{i,j}$ by construction, and hence

$$R = \left(\begin{array}{c|c|c|c|c} D_1 & 0 & 0 & \cdots & 0 \\ \hline 0 & D_2 & 0 & \cdots & 0 \\ \hline 0 & 0 & \ddots & & \end{array}\right) \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k).$$

□

Note that the 3rd statement does not mention any sides but 1st and 2nd are left. The corollary is then

Corollary 4.3.2. ${}_R R$ is semisimple iff R_R is semisimple. In this case one says the ring R is *semisimple.*

4.3.2 Semisimple algebra

If $(R, \mathbb{F})$ is an algebra and a semisimple ring, then $R = M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$ where all D_i are $\mathbb{F}$-algebras. Our knowledge so far (recall 3.2.1, 3.2.14, 3.3.10) allows us to write the following.

Proposition 4.3.3. 1. A countable dimensional semisimple $\mathbb{C}$-algebra is isomorphic to

$$\prod_{i=1}^{k} M_{n_i}(\mathbb{C}).$$

2. A countable dimensional semisimple $\mathbb{R}$-algebra is isomorphic to

$$\prod_{i=1}^{k} M_{n_i}(D_i) \qquad \text{where } D_i \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}.$$

3. A finite dimensional semisimple $\mathbb{F}_q$-algebra is isomorphic to

$$\prod_{i=1}^{k} M_{n_i}\left(\mathbb{F}_{q^{a_i}}\right).$$

4.3.3 Maschke's theorem

Let G be a group and $\mathbb{F}$ a field of characteristic p. Define the group algebra

$$\mathbb{F}G := \left\{ \sum_{g\in G} \alpha_g g : \alpha_g \in \mathbb{F} \right\} \qquad \text{with multiplication } \alpha g \beta h := \alpha\beta gh$$

Theorem 4.3.4. The following are equivalent for a group G and a field $\mathbb{F}$ of characteristic p.

1. $\mathbb{F}G$ is semisimple.
2. G is finite and $p \nmid |G|$.

Remark. 2⇒1 is called Maschke's theorem.

Proof. 1⇒2: Let $R = \mathbb{F}G$. Consider $\mathbb{F}$ as a trivial R-module with $\forall \alpha \in \mathbb{F},\ g\alpha = \alpha\ \forall g \in G$. So $\exists$ surjective homomorphism

$$\psi : {}_R R \to \mathbb{F}$$
$$g \mapsto 1$$

Since R is semisimple and $\ker\psi \le {}_R R$, one has ${}_R R = \ker\psi \oplus P$ for some P and hence ${}_R P \cong {}_R \mathbb{F}$. So $\exists x \in P : P = \mathbb{F}x$. Write $x = \sum_{g\in G} \alpha_g g$. Since $P \cong \mathbb{F},\ hx = x\ \forall h \in G$, i.e.

$$\sum_{g\in G} \alpha_g hg = \sum_{g\in G} \alpha_g g \qquad \forall h \in G,$$

it follows that all α_g are equal and $\neq 0$. Therefore G has to be finite because if it's not then $x = \sum_{g\in G} \alpha g$ which is not well defined. Now suppose $|G| = n$ and $p \mid n$, then $x \in \mathbb{F}G$ and $\psi(x) = n\alpha = 0$, i.e. $x \in \ker\psi$, a contradiction to the direct sum.

Week 10, lecture 1 starts here

2⇒1: We will show every $\mathbb{F}G$-module is completely reducible and then apply 4.2.11, 4.3.1 and 4.3.2. Let ${}_{\mathbb{F}G}M > {}_{\mathbb{F}G}N$ and the goal is to find a direct complement for N. One can write $M = N \oplus K$ as $\mathbb{F}$-vector spaces. Consider the corresponding projection $p : M \twoheadrightarrow N \hookrightarrow M$ which is idempotent. Let $\alpha \in \mathbb{F}$ satisfy $|G|\alpha = 1_{\mathbb{F}}$ (one can think of α as $\frac{1}{|G|}$). Define $\widehat{p} \in \mathrm{End}_{\mathbb{F}}M$ by $x \mapsto \alpha \sum_{g\in G} g(p(g^{-1}x))$. Since N is a submodule, $\mathrm{im}\,\widehat{p} \subseteq N$. Now for any $x \in N,\ g^{-1}x \in N$ and so

$$\widehat{p}(x) = \alpha \sum_{g\in G} g(p(g^{-1}x)) = \alpha \sum_{g\in G} g(g^{-1}x) = \alpha|G|x = x,$$

so $\mathrm{im}\,\widehat{p} = N$ and $\widehat{p}^2 = \widehat{p}$, i.e. $\widehat{p}$ is idempotent. Moreover, for $g \in G$ and $y \in M$,

$$\begin{aligned}\widehat{p}(gy) &= \alpha \sum_{h\in G} h(p(h^{-1}gy)) = \alpha \sum_{k_1,k_2\in G: k_1k_2 = g} k_1(p(k_2 y)) \\ &= \alpha \sum_{h\in G} gh(p(h^{-1}y)) = g\widehat{p}(y),\end{aligned}$$

so $\widehat{p} \in \mathrm{End}_R M$, hence one can write $M = \mathrm{im}\,\widehat{p} \oplus \ker\widehat{p} = N \oplus \ker\widehat{p}$, where $\ker\widehat{p}$ is the direct complement we are looking for.

□

Example 4.3.5. Consider $\mathbb{F}C_n$ where $C_n = \langle x \mid x^n = 1\rangle$, which can be written as $\mathbb{F}[y]/(y^n - 1)$. If one writes $y^n - 1 = f_1^{a_1} \cdots f_1^{a_1}$ where $f_i \in \mathbb{F}[y]$ are irreducible and $a_i \geq 1$, then using Chinese remainder theorem one has

$$\mathbb{F}C_n \cong \mathbb{F}[y]/(f_1^{a_1}) \times \cdots \times \mathbb{F}[y]/(f_n^{a_n}),$$

which is semisimple iff

$$\begin{aligned} & a_1 = \cdots = a_n = 1 \\ \iff & z^n - 1 \text{ has no multiple factors} \\ \iff & \gcd((z^n-1),(z^n-1)'') = 1 \\ \iff & p \nmid n, \end{aligned}$$

which is what Maschke's theorem tells us as well.

If $\mathbb{F} = \mathbb{C}$ then

$$z^n - 1 = \prod_{k=0}^{n-1} \left(z - e^{\frac{2\pi k}{n} i}\right)$$

so

$$\mathbb{C}C_n \cong \prod_{k=0}^{n-1} \mathbb{C}[z]/\left(z - e^{\frac{2\pi k}{n} i}\right) \cong \mathbb{C}^n.$$

If $\mathbb{F} = \mathbb{Q}$ then $z^n - 1 = \prod_{d \mid n} \phi_d(z)$ where ϕ_d is the cyclotomic polynomial. So

$$\mathbb{Q}C_n \cong \prod_{d \mid n} \mathbb{Q}[z]/(\phi_d) \cong \prod_{d \mid n} \mathbb{Q}\left(\sqrt[d]{1}\right).$$

Example 4.3.6. Consider $\mathbb{R}Q_8$ where $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\} \leq \mathbb{H}^\times$. 4.3.3.2 applies. Now note that for each Artin–Wedderburn factor $M_n(\mathbb{F})$ there is a different surjective $\mathbb{R}$-algebra homomorphism $\mathbb{R}Q_8 \to M_n(\mathbb{F})$ given by projection

$$\begin{aligned} \eta : \mathbb{R}Q_8 &\twoheadrightarrow \mathbb{H} \\ \pm i &\mapsto \pm i \\ \pm j &\mapsto \pm j \end{aligned}$$

or

$$\begin{aligned} \theta_{\epsilon,\delta} : \mathbb{R}Q_8 &\twoheadrightarrow \mathbb{R} \\ i &\mapsto \epsilon \\ j &\mapsto \delta \end{aligned}$$

where $\epsilon, \delta \in \{\pm 1\}$. Since there can be $2 \times 2 = 4$ different $\theta_{\epsilon,\delta}$ and just one η, we conclude

$$\mathbb{R}Q_8 \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}.$$

Proposition 4.3.7. If

$$_R M = \bigoplus_{i=1}^n S_i = \bigoplus_{j=1}^m N_j$$

where S_i, N_j are simple, then $n = m$ and $\exists \sigma \in \mathrm{Sym}_n : S_i \cong N_{\sigma(j)}$.

Proof. We prove by induction on n. If $n = 0$ then $M = 0$ so $m = 0 = n$. If $n = 1$ then $M = S_1$ is simple so $m = 1$ and $S_1 = N_1$. Now suppose the statement is true for values $\leq n-1$ and consider projection $\pi : M \twoheadrightarrow S_n$ along $\bigoplus_{i=1}^{n-1} S_i$. Then

$$S_n = \pi(M) = \sum_{j=1}^{m} \pi(N_j) \qquad \text{where } \pi(N_j) \text{ is either } 0 \text{ or } N_j$$

but S_n is simple, so it has to be that $S_n \cong N_{j_0}$ for some $j_0 \in \{1, \dots, m\}$. One then has that $\bigoplus_{j \neq j_0} N_j$ is a direct complement of S_n, so

$$\bigoplus_{j \neq j_0} N_j \cong \bigoplus_{i=1}^{n-1} S_i$$

and by inductive hypothesis, $n-1 = m-1$, so $n = m$; and $\exists \widehat{\delta} \in \mathrm{Sym}_{n-1} : S_i \cong N_{\widehat{\delta}(i)}$. Together with $S_n \cong N_{j_0}$ this completes the proof. $\square$

Corollary 4.3.8. For a semisimple ring $R \cong \prod M_{a_i}(D_i)$, the division rings D_i and a_i are unique up to permutation.

4.4 Jacobson radical

Definition 4.4.1. $x \in R$ is *nilpotent* of $\exists n : x^n = 0$, *quasiregular* if $1 + x$ is invertible.

Example 4.4.2. Let $\mathbb{F}$ is a field and $x \in M_n(\mathbb{F})$, then x is nilpotent iff 0 is the only eigenvalue, and quasiregular iff -1 is not an eigenvalue of x. In particular, nilpotent implies quasiregular in this case.

Week 10, lecture 2 starts here

Notation. $J(R) = \mathrm{rad}_R R$.

Definition 4.4.3. An ideal I is *nilpotent* if $\exists n : I^n = 0$, *nil* if every $x \in I$ is nilpotent and *quasiregular* if every $x \in I$ is quasiregular.

Lemma 4.4.4. Nilpotent ideals $\subsetneq$ nil ideals $\subsetneq$ quasiregular ideals.

Proof. That nilpotent ideals $\subseteq$ nil ideals is obvious ($\exists n : I^n = 0$ means $\exists n$: any product of n elements of I is 0).
It remains to show that a nilpotent element is quasiregular, but

$$x^n = 0 \implies (1 + x)(1 - x + x^2 - \cdots + (-1)^{n-1} x^{n-1}) = 1.$$

$\square$

Example 4.4.5. $R = \mathbb{C}[[x]] \leq \mathbb{C}((x))$. Set $J := (x) = \{\alpha_1 x + \cdots + \alpha_n x^n + \cdots\}$. Then J is quasiregular: write

$$J \ni z = \alpha_n x^n + \cdots \qquad \text{where } a_n \neq 0,\ n \geq 1$$

then

$$(1 + z)^{-1} = \sum_{k=0}^{\infty} (-1)^k z^k.$$

J is also maximal since $R/J \cong \mathbb{C}$, a field. We will later see that this implies $J = J(R)$.
Note that J is not nil; in fact R is a domain.

Example 4.4.6. $S = \mathbb{C}[x_1, x_2, \ldots],\ I = (x_1^2, x_2^2, \ldots),\ R = S/I,\ \overline{x_i} = x_i + I,\ J = (\overline{x_1}, \overline{x_2}, \ldots)$. Then J is trivially nil, so quasiregular. Again $R/J \cong \mathbb{C}$ so J is maximal, hence $J = J(R)$.

Note that J is not nilpotent since $\overline{x_1}\,\overline{x_2} \cdots \overline{x_n} \neq 0$.

Proposition 4.4.7. If $I, J \trianglelefteq R$ and $I^n = J^m = 0$, then $(I+J)^{n+m} = 0$. In particular, the sum of two nilpotent ideals is nilpotent.

Proof. $(I+J)^a$ is the $\mathbb{R}$-span of elements of the form

$$\prod_{i=1}^{a}(x_i + y_i) = \prod_{i=1}^{a} x_i + \text{terms with } y_i$$

where $x_i \in I,\ y_i \in J$, hence $(I+J)^a \subseteq I^a + J$, and so

$$(I+J)^{n+m} = ((I+J)^n)^m \subseteq (I^n + J)^m \subseteq J^m = 0.$$

$\square$

Conjecture (Köthe)**.** If $I, J \trianglelefteq^l R$ and I, J are nil, then $I + J$ is nil.

Theorem 4.4.8. For a ring R, $J_1 = \cdots = J_7$ where

- $J_1 = \operatorname{rad}{}_R R$
- $J_2 = \operatorname{rad} R_R$
- $J_3 = \displaystyle\bigcap_{L \trianglelefteq^l_{\max} R} L$
- $J_4 = \displaystyle\bigcap_{I \trianglelefteq^r_{\max} R} I$
- $J_5 = \{x \in R : \forall \text{ simple } {}_R M,\ xM = 0\}$
- $J_6 = \{x \in R : \forall \text{ simple } M_R,\ xM = 0\}$
- J_7 is the largest 2-sided quasiregular ideal

Week 10, lecture 3 starts here

Proof.
1. $J_1 \subseteq J_5$: let $x \in J_1$ and ${}_R M$ a simple left R-module. $\forall m \in M$, $\operatorname{Ann}_R(m)$ is maximal, so $x \in \operatorname{Ann}_R(m)$, hence $xm = 0 \implies xM = 0 \implies x \in J_5$.
2. $J_5 \subseteq J_3$: let $x \in J_5$ and $L \trianglelefteq^l_{\max} R$. Then R/L is a simple R-module, so $xR/L = 0$ and in particular $x(1+L) = 0 + L$, so $x \in L$ and hence $x \in J_3$.
3. J_3 is quasiregular: let $x \in J_3$. Note that $R(1+x) = R$, since if $R(1+x) \neq R$, then $\exists L \trianglelefteq^l_{\max} R$ which contains $R(1+x)$ and in particular $1 + x \in L$ and since $x \in \displaystyle\bigcap_{L \trianglelefteq^l_{\max} R} L$ one has $x \in L$ as well, therefore $1 \in L$ and so $L = R$, a contradiction. Hence $1 + x$ has a left inverse $1 + z$, and
$$\begin{aligned}(1+z)(1+x) &= 1\\ z + x + zx &= 0\\ z = -(1+z)x &\in J_3\end{aligned}$$

so z also has a left inverse. Denote it t, then

$$t = t1 = t(1+z)(1+x) = 1+x$$

so

$$1 = t(1+z) = (1+x)(1+z),$$

hence $1+z$ is also the right inverse of $1+x$.

4. J_1 contains every left quasiregular ideal: suppose $\exists I \trianglelefteq^l_{\text{quasiregular}} R : I \not\subseteq J_1$, so $\exists L \trianglelefteq^l_{\max} R$ and $x \in I : x \notin L$. This implies $L + Rx = R$ and in particular $a + bx = 1$ for some $a \in L, b \in R$. Since $-bx \in I$ which is quasiregular, $a = 1 - bx$ has a left inverse t, but then $1 = ta \in L$ so $L = R$, a contradiction.

5. J_5 is a 2-sided ideal: we already know J_5 is a left ideal. Now pick $x \in J_5,\ r \in R$ and let ${}_RM$ be a simple left R-module. Then $(xr)M \subseteq x(rM) \subseteq xM = 0$, so $xr \in J_5$ and hence J_5 is also a right ideal.

The 5 steps prove $J_1 = J_3 = J_5 = J_7$. The proof for $J_2 = J_4 = J_6 = J_7$ is analogous. □

Remark.

1. Radical property: $J(R/J(R)) = 0$. The philosophy is: radical is the bad stuff we can get rid off.

2. A ring R with $J(R) = 0$ are also called semisimple in literature. This watershed between classical semisimplicity and Jacobson semisimplicity is presented in the following proposition.

Proposition 4.4.9. The following are equivalent.

1. R is semisimple.

2. R is left artinian and $J(R) = 0$.

Theorem 4.4.10. If R is left artinian then $J(R)$ is nilpotent.

Proof. Denote $J = J(R)$. Consider descending chain

$$J \supseteq J^2 \supseteq \cdots \supseteq J^n \supseteq \cdots$$

since R is artinian, $\exists n : J^n = J^{n+1} = \cdots$. We claim $J^n = 0$. Let

$$I = \operatorname{Ann}_R(J^n_R) = \{x \in R : J^n x = 0\}.$$

Note that I is a 2-sided ideal: let $x \in I, y \in R$, then $J^n xy \subseteq 0y \subseteq 0$ and $J^n yx \subseteq J^n x = 0$, so $xy, yx \in I$. If $I \supseteq J^n$ then we are done since $J^n = J^{2n} = J^n J^n \subseteq J^n I = 0$ by construction, so suppose $I \not\supseteq J^n$ and consider quotient homomorphism $\psi : R \to R/I =: S$. Then $\psi(J^n) \neq 0$. Since $J^n \subseteq J = J(R)$, (see HW4 P4) $\psi(J^n) \subseteq \psi(J) \subseteq J(S)$. Since R is artinian, so is S, hence $\exists L \trianglelefteq^l_{\min} S : L \subseteq \psi(J^n)$. Then L is a simple S-module, so $\psi(J^n)L \subseteq J(S)L = 0$ by 4.4.8. Apply ψ^{-1} and one has $J^n\psi^{-1}(L) \subseteq I$, and

$$J^n\psi^{-1}(L) = J^{2n}\psi^{-1}(L) = J^n(J^n\psi^{-1}(L)) \subseteq J^n I = 0,$$

so $\psi^{-1}L \subseteq I$ and hence $L = 0$, a contradiction. □

Corollary 4.4.11. For a left artinian ring R, $J(R)$ is the largest nilpotent 2-sided/left/right ideal of R.

Proof. R being nilpotent follows from 4.4.10. Let $I \lhd R$ be nilpotent. Then it's quasiregular so $I \subseteq J(R)$ by 4.4.8.

Now let $L \lhd^l R$ with $L^n = 0$, then $LR \trianglelefteq R$ and $(LR)^n = L(RL)^{n-1}R \subseteq L^n R = 0$, so by above $L \subseteq LR \subseteq J(R)$. Similar for right. $\square$