Rings and Modules

joseph.muscat@um.edu.mt
1 October 2013

1 Semi-Rings

The morphisms on a commutative monoid have two operations: addition and composition, $(\phi+\psi)(x)=\phi(x)+\psi(x)$, $(\phi\circ\psi)(x)=\phi(\psi(x))$. They form the defining template for algebras having two operations:

Definition A **semi-ring** is a set R with two associative operations $+,\cdot$, where $+$ is commutative with identity 0, and $\cdot$ has identity 1, related together by the *distributive laws*

$$a(b+c)=ab+ac, \qquad (a+b)c=ac+bc,$$

and $0a=0=a0$ (0 is a zero for $\cdot$).

A **semi-module** is a semi-ring R acting (left) on a commutative monoid X as endomorphisms, i.e., for all $a,b\in R$, $x,y\in X$,

$$\begin{aligned} a(x+y)&=ax+ay, & a0&=0,\\ (a+b)x&:=ax+bx, & 0x&:=0,\\ (ab)x&:=a(bx), & 1x&:=x \end{aligned}$$

Thus a semi-ring is a semi-module by acting on itself (either left or right).

Repeated addition and multiplication are denoted by $nx=x+\cdots+x$ and $a^n=a\cdots a$. Then $\mathbb{N}$ acts on X, forming a (trivial) semi-module,

$$(m+n)x=mx+nx, \qquad m(nx)=(mn)x,$$
$$n(x+y)=nx+ny, \qquad n0=0, \qquad n(ab)=(na)b=a(nb)$$

(the last follows by induction: $n^+(ab)=n(ab)+(ab)=(na)b+(ab)=(na+a)b=(n^+a)b$.) Thus multiplication is a generalization of repeated addition. (Exponentiation a^b is not usually well-defined e.g. in $\mathbb{Z}_3, 2^1\neq 2^4$.)

$$(a+b)^2=a^2+ab+ba+b^2,$$
$$(a+b)^n=a^n+a^{n-1}b+a^{n-2}ba+\cdots+ba^{n-1}+\cdots+b^n$$

Only for the trivial semi-ring $\{0\}$ is $1=0$. If R doesn't have a 0 or 1, they can be inserted: define $0+a:=a$, $a+0:=a$, $0+0:=0$, $0a:=0$, $a0:=0$, $00:=0$, and extend to $\mathbb{N}\times R$ with (n,a) written as $n+a$ and

$$(n+a)+(m+b):=(n+m)+(a+b),$$
$$(n+a)(m+b):=(nm)+(na+mb+ab).$$

Then the associative, commutative, and distributive laws remain valid, with new zero $(0,0)$ and identity $(1,0)$, and with R embedded as $0 \times R$.

Monoid terminology, such as zero, nilpotent, regular, invertible, etc. are reserved for the multiplication. If they exist, a 'zero' for $+$ is denoted ∞; a $+$-inverse of x is denoted by $-x$ ('negative'), and $(-n)x := n(-x)$.

$+,\cdot$	**Finite**	**Artinian**	**Noetherian**	
Semi-Rings $(x+y)z = xz + yz$			$\mathbb{N}$	$\mathbb{N}^{\mathbb{N}}$
Rings $-x$	$\mathbb{Z}_m[G]$,$M_n(\mathbb{Z}_n)$	$\mathbb{Q}[G]$	$U_n(\mathbb{Z})$	$\mathbb{Z}\langle x, y, \ldots\rangle / \langle x^2, y^3, \ldots\rangle$
Semi-Primitive	/////	/////	$M_n(\mathbb{Z})$	$\mathbb{Q}\langle x, y\rangle$
Semi-Simple	$\mathbb{Z}_p[G]$, $M_n(\mathbb{F}_{p^n})$	$M_n(\mathbb{Q})$, $\mathbb{H}$	/////	/////
Commutative rings $xy = yx$	$\mathbb{Z}_m$, $\mathbb{F}_{p^n} \times \mathbb{F}_{q^m}$	$\mathbb{F}[x]/\langle x^n\rangle$	$\mathbb{Z}_n[x]$	$\mathbb{Z}^{\mathbb{Z}}$, $\mathbb{Z}_n[x, y, \ldots]$
Integral Domains $xy = 0 \Rightarrow x = 0$ OR $y = 0$	/////	/////	$\mathbb{Z}[x]$	$\mathbb{A}_{\mathbb{Z}}$
Principal Ideal Domains	/////	/////	$\mathbb{Z}$, $\mathbb{Q}[x]$	/////
Fields x^{-1}	$\mathbb{F}_{p^n}$	$\mathbb{Q}$	/////	/////

(G finite group)

1.0.1 Examples

- Some small examples of semi-rings (subscripts are ab, with $a0 = 0$, $a1 = a$ suppressed)

$$\begin{array}{c|cc} +_\times & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 1 \end{array} \qquad \begin{array}{c|cc} 0 & 1 & 2 \\ \hline 1 & 2 & 1 \\ 2 & 1 & 0_0 \end{array} \qquad \begin{array}{c|ccc} 0 & 1 & 2 & 3 \\ \hline 1 & 1 & 1 & 1 \\ 2 & 1 & 2_0 & 3_2 \\ 3 & 1 & 3_0 & 3_3 \end{array}$$

- $\mathbb{N}$ with $+, \times$. More generally, sets with disjoint union and direct product.
- Subsets with $\triangle$ and $\cap$.
- $\mathrm{Hom}(X)$ is a semi-ring acting on the commutative monoid X.
- Distributive lattices, e.g. $\mathbb{N}$ with $\max, \min$, $\mathbb{N}$ with $\mathrm{lcm}, \gcd$.
- $\mathbb{N}$ with $\max, +$ (and $-\infty$ as a zero).
- Subsets of a Monoid, with $\cup$ and product $AB := \{\, ab : a \in A, b \in B \,\}$.
- Every commutative monoid is trivially a semi-ring with $xy := 0$ $(x, y \neq 1)$.

- Every semi-ring has a mirror-image *opposite* semi-ring with the same $+$ but $a * b := ba$. R^{op} acts on an R-semi-module X by $x * a := ax$.

Morphisms of semi-modules are *linear* maps $T : X \to Y$,

$$T(x + y) = T(x) + T(y), \quad T(ax) = aT(x).$$

Morphisms of semi-rings are maps $\phi : R \to S$,

$$\begin{array}{cc} \phi(a + b) = \phi(a) + \phi(b), & \phi(ab) = \phi(a)\phi(b), \\ \phi(0) = 0, & \phi(1) = 1 \end{array}$$

The spaces of such morphisms are denoted $\mathrm{Hom}_R(X, Y)$ and $\mathrm{Hom}(R, S)$ respectively.

1. For semi-modules, isomorphisms are invertible morphisms; the trivial module $\{0\}$ is an initial and zero object (i.e., unique $0 \to X \to 0$).
2. $\mathrm{Hom}_R(X, Y)$ is itself an R-semi-module with
$$(S + T)(x) := S(x) + T(x), \quad (aT)(x) := aT(x)$$
3. For semi-rings, $\mathbb{N}$ is an initial object (i.e., unique $\mathbb{N} \to R$). Ring morphisms preserve invertibility, $\phi(a)^{-1} = \phi(a^{-1})$.
4. If a is invertible, then conjugation $\tau_a(x) := a^{-1}xa$ is a semi-ring automorphism. If a is invertible and central ($ax = xa$) then its action on X is a semi-module automorphism.
$a^{-1} + b^{-1} = a^{-1}(b + a)b^{-1}$
5. The module-endomorphisms of a semi-ring are $x \mapsto xa$, hence $\mathrm{Hom}_R(R)$ is isomorphic to R (as a module). Similarly, $\mathrm{Hom}_R(R, X) \cong X$ (via $T \mapsto T(1)$).
6. Every semi-ring is embedded in some $\mathrm{Hom}(X)$ for some commutative monoid X (take $X := R_+$).

Products: The product of R-semi-modules $X \times Y$ and functions X^S are also semi-modules, acted upon by R, with

$$(x_1, y_1) + (x_2, y_2) := (x_1 + x_2, y_1 + y_2), \quad a(x, y) := (ax, ay),$$

$$(f + g)(t) := f(t) + g(t), \quad (af)(t) := af(t).$$

For semi-rings, $(fg)(t) := f(t)g(t)$. A *free* semi-module is given by R acting on R^S. Note the module morphisms $\iota_i : X \to X^n$, $x \mapsto (\ldots, 0, x, 0, \ldots)$ and $\pi_i : X^n \to X$, $(x_1, \ldots, x_n) \mapsto x_i$. $\mathrm{Hom}_R(X \times Y, Z) \cong \mathrm{Hom}_R(X, Z) \times \mathrm{Hom}_R(Y, Z)$ (let $T \mapsto (T_X, T_Y)$ where $T_X(x) := T(x, 0)$).

Matrices: The module morphisms $R^n \to R^m$ can be written as *matrices* of ring elements,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{m1} & \cdots & a_{mn} \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} := \begin{pmatrix} x_1 a_{11} + \cdots + x_n a_{1n} \\ \vdots \\ x_1 a_{m1} + \cdots + x_n a_{mn} \end{pmatrix},$$

forming a semi-module $M_{m\times n}(R)$ with addition and scalar multiplication

$$(a_{ij}) + (b_{ij}) := (a_{ij} + b_{ij}), \qquad r(a_{ij}) := (ra_{ij}).$$

When $n = m$, the matrices form a semi-ring $M_n(R)$ on $+, \circ$. More generally,

$$\mathrm{Hom}_R(X^m, Y^n) = M_{n\times m}(\mathrm{Hom}_R(X, Y))$$

(the matrix of T has coefficients $T_{ij} := \pi_i \circ T \circ \iota_j : X \to X^n \to Y^m \to Y$).

Polynomials: A *polynomial* is a finite sequence $(a_0, \ldots, a_n, 0, \ldots)$, written as a formal sum $a_0 + a_1 x + \cdots + a_n x^n$, $n \in \mathbb{N}$, $a_i \in R$ with addition and multiplication defined by

$$\sum_i a_i x^i + \sum_i b_i x^i := \sum_i (a_i + b_i) x^i, \quad \big(\sum_i a_i x^i\big)\big(\sum_j b_j x^j\big) := \sum_k \big(\sum_{i+j=k} a_i b_j\big) x^k$$

Much more generally, given a semi-ring R and a category $\mathcal{C}$, R can be extended to the semi-ring

$$R[\mathcal{C}] := \{\, a : \mathcal{C} \to R, \mathrm{supp}(a) \text{ is finite} \,\}$$

($\mathrm{supp}(a) := \{\, \phi_i \in \mathcal{C} : a(\phi_i) \neq 0 \,\}$) with 'free' operations of addition and *convolution*

$$(a + b)(\phi_i) := a(\phi_i) + b(\phi_i), \quad (a * b)(\phi_i) := \sum_{\phi_j \phi_k = \phi_i} a(\phi_j) b(\phi_k)$$

(i.e., set $\phi_i \phi_j = 0$ when not compatible) with identity δ given by $\delta(\phi) = 0$ except $\delta(\iota) = 1$ (for any identity morphism ι). (It is the adjoint of the forgetful functor from R-modules to the category.) Elements $a \in R[\mathcal{C}]$ are often denoted as formal (finite) sums $\sum_i a_i \phi_i$ (where $a_i = a(\phi_i)$) with the requirement $(a\phi + b\psi)(c\eta) := (ac)(\phi\eta) + (bc)(\psi\eta)$, etc.; then

$$\big(\sum_i a_i \phi_i\big)\big(\sum_j b_j \phi_j\big) = \sum_k \big(\sum_{\phi_k = \phi_i \phi_j} a_i b_j\big)\phi_k = \sum_k (a * b)_k \phi_k$$

An element $a \in R[\mathcal{C}]$ is invertible $\Leftrightarrow \forall i, a(\phi_i) \neq 0$.

The map $\sum_i a_i \phi_i \to \sum_i a_i$ is a morphism onto R. The *zeta* function is the constant function $\zeta(\phi_i) := 1$; its inverse is called the *Möbius* function μ. If the category is bounded, then the Euler characteristic is $\chi := \mu(0 \to 1)$.

Special cases are the following:

1. *Monoid/Group Algebras* $R[G]$

$$a * b(g) := \sum_h a(h)b(h^{-1}g), \quad \delta(g) = \begin{cases} 1 & g = 1 \\ 0 & \text{o/w} \end{cases}$$

   Every element of finite order gives a zero divisor because $0 = 1 - g^n = (1-g)(1 + g + \cdots + g^{n-1})$ (conjecture: these are the only zero divisors).

   - The *Polynomials* $R[x]$ are the finite sequences that arise when $G = \mathbb{N}$. The sequence $(0, 1, 0, \ldots)$ is often denoted by 'x', so

$$p = a_0 + a_1 x + \cdots + a_n x^n, \quad \exists n \in \mathbb{N}$$

     They are generated by x^n with $x^n x^m = x^{n+m}$, $ax = xa$ for $a \in R$. The *degree* of p is defined by $\max\{\, n \in \mathbb{N} : a_n \neq 0 \,\}$; then

$$\deg(p+q) \leqslant \max(\deg(p), \deg(q)), \quad \deg(pq) \leqslant \deg(p) + \deg(q).$$

   - $R[\mathbb{Z}]$ is the ring of *rational polynomials*,
   - $R[x_1, \ldots, x_n]$ is obtained from $G = \mathbb{N}^n$; e.g. $R[x,y] = R[x][y]$; contains the sub-ring of symmetric polynomials $S[x,y]$ (generated by the elementary symmetric polynomials $1, x+y, xy, \sum_{i<\cdots<j} x_i \cdots x_j$)
   - The "free algebra" $R\langle A\rangle := R[A^*]$ where A^* is the free monoid on A,
   - The power series $R[[x]]$ consists of infinite sequences with the same addition and multiplication as for $R[x]$.

Any combination of variables gives a polynomial in them: $x((y+zx)+y) = 2xy + xzx$

2. The *Incidence Algebras* $R[\leqslant]$, let $a(x,y) := a(x \leqslant y)$;

$$a * b(x,y) := \sum_{x \leqslant z \leqslant y} a(x,z)b(z,b), \quad \delta(x,y) = \begin{cases} 1 & x = y \\ 0 & \text{o/w} \end{cases},$$

$$\mu(x,y) = \begin{cases} -\sum_{x \leqslant z < y} \mu(x,z) & x < y \\ 1 & x = y \end{cases}$$

   - $R[2^X]$, $\mu(A \subseteq B) = (-1)^{|B \setminus A|}$.

Polynomials $\mathbb{N}[x, y, \ldots]$ are sufficiently complex that they can encode many logical statements about the naturals. That is, any computable subset of $\mathbb{N}$ can be encoded as $\{\, x \in \mathbb{N} : \exists y, \ldots,\ p(x, y, \ldots) = 0 \,\}$ for some polynomial p; so polynomials are in general unsolvable (Hilbert's 10th problem).

A **sub-module** is a subset $Y \subseteq X$ that is closed under $+, 0$ and the action of R, i.e., $0 \in Y$, $Y + Y \subseteq Y$, $RY \subseteq Y$,

$$a \in R,\ x, y \in Y \ \Rightarrow\ 0, x+y, ay \in Y.$$

A sub-module induces a congruence relation

$$x_1 = x_2 \pmod{Y} \Leftrightarrow \exists y_1, y_2 \in Y, \quad x_1 + y_1 = x_2 + y_2,$$

with $x + Y \subseteq [x]$ and $[0] = Y^{\text{sub}} := \{\, x \in X : x + y \in Y,\ \exists y \in Y \,\} \supseteq Y$, so can form the **quotient** space X/Y^{sub} of equivalence classes

$$[x_1] + [x_2] := [x_1 + x_2], \qquad a[x] := [ax].$$

A sub-module of a semi-ring R acting on itself is called a **left ideal** $I \leqslant R$, i.e., $I + I, RI \subseteq I$. A is a **sub-semi-ring** of R when it is closed under $+, \cdot, 0, 1$.

1. If M, N are sub-modules, then so are $M + N$ $(= M \vee N)$ and $M \cap N$, thus making sub-modules into a complete modular lattice (for $\subseteq$)

   $$N \subseteq L \;\Rightarrow\; (L \cap M) + N = L \cap (M + N).$$

   A sub-module M is *complemented* by N when $M + N = X$, $M \cap N = 0$, denoted $X = M \oplus N$.

2. *Generated sub-modules*: the smallest sub-module containing $B \subseteq X$ is

   $$[\![B]\!] = R \cdot B := \{\, a_1 x_1 + \cdots + a_n x_n : a_i \in R, x_i \in B, n \in \mathbb{N} \,\}$$

   $[\![x]\!] = Rx$ is called *cyclic* (or principal left ideal for rings). $[\![A \cup B]\!] = [\![A]\!] + [\![B]\!]$, $\sum_i M_i := [\![\bigcup_i M_i]\!]$. A *basis* is a subset B which generates X, and for each x, the coefficients a_i are unique (but a basis need not exist).

3. More generally, if I is a left ideal then

   $$I \cdot B := \{\, a_1 x_1 + \cdots + a_n x_n : a_i \in I, x_i \in B, n \in \mathbb{N} \,\}$$

   is a sub-module (but need not contain B).

4. Module morphisms preserve the sub-module structure: If $M \leqslant N$ then $\phi M \leqslant \phi N$ and $\psi^{-1} M \leqslant \psi^{-1} N$. Ring morphisms also preserve sub-semi-rings.

5. The only left ideal that contains 1 or invertible elements is R (since $x = (xa^{-1})a \in I$).

6. Left ideals of $R \times S$ are of the type $I \times J$, where I, J are left ideals of R, S.

7. A sub-module Y is *subtractive* when $x, x + y \in Y \;\Rightarrow\; y \in Y$. The intersection of subtractive sub-modules is again subtractive, so the smallest subtractive sub-module containing A is A^{sub} a closure operation on sub-modules. If Y is subtractive, so is $\phi^{-1} Y$.

   Example: $k\mathbb{N}$ are the subtractive (left) ideals of $\mathbb{N}$, but $2\mathbb{N} + 3\mathbb{N} = \{\, 0, 2, 3, \ldots \,\}$ is not.

8. The set of elements that have a negative is a subtractive sub-module N, since $-(x+y)=(-x)+(-y)$, $-(ax)=a(-x)$, $x+y\in N \Leftrightarrow x,y\in N$.

9. A left *semi-unit* of a ring is u such that $(Ru)^{\text{sub}}=R$, i.e., $1+au=bu$ for some a,b; e.g. any left invertible element. A subtractive left ideal, except R, cannot contain a semi-unit.

10. The **annihilator** of a subset $B\subseteq X$ is the subtractive left ideal

$$\text{Annih}(B):=\{\,a\in R: aB=0\,\}.$$

For a sub-module, $\text{Annih}(M)$ is an ideal, $\text{Annih}(M+N)=\text{Annih}(M)\cap\text{Annih}(N)$. For semi-rings, $\text{Annih}(B):=\{\,a\in R: aB=0=Ba\,\}$; then $B\subseteq\text{Annih}(\text{Annih}(B))$.

The adjoint of the annihilator is the zero set

$$\text{Zeros}(I):=\{\,x\in X: Ix=0\,\},$$
$$I\leqslant\text{Annih}(Y)\Leftrightarrow Y\leqslant\text{Zeros}(I)$$

More generally, for a sub-module Y,

$$[Y:B]:=\{\,a\in R: aB\subseteq Y\,\},$$
$$[Y:I]^*:=\{\,x\in X: Ix\subseteq Y\,\}$$

$[Y:B]$ is a left ideal (a sub-ring if Y is just a sub-monoid); $[Y:X]$ is an ideal. $[Y:I]^*$ is a sub-module when I is a right ideal; $[Y:R]^*=Y$.

$\text{Annih}(X/Y)=[Y^{\text{sub}}:X]$.

The *torsion radical* is the sub-module $\tau(X):=\{\,x\in X:\exists n\geqslant 1,\ nx=0\,\}$.

11. $R\to\text{Hom}(X)$ is a ring-morphism, with kernel being the congruence relation $ax=bx,\forall x\in X$.

12. $X\to X/Y^{\text{sub}}$, $x\mapsto[x]$ is a module-morphism, and the usual Isomorphism theorems hold (see Universal Algebras), e.g. $R/\ker\phi\cong\phi R$, sub-modules that contain M correspond to sub-modules of $X/\approx_M$.

13. If $\phi:R\to S$ is a ring-morphism, and S acts on X, then R acts on X as a semi-module by $a\cdot x:=\phi(a)x$.

14. A sub-module Y is *maximal* when $Y\neq X$ and there are no other sub-modules $Y\subset Z\subset X$ (i.e., a coatom in the lattice of sub-modules). For example, $3\mathbb{N}$ in the semi-module $\mathbb{N}$.

$Y\subset Z\subseteq X$ is maximal in Z iff $Y=M\cap Z$ for some maximal M in X.

Every (left) ideal of a ring (with $I^{\text{sub}}\neq R$) can be enlarged to a maximal (subtractive left) ideal (by Zorn's lemma).

15. *Generated sub-semi-ring* of $A \subseteq R$ is the smallest sub-semi-ring containing A:
$$[\![A]\!] = \{ \sum a_1 \cdots a_k : a_i \in A \cup \{1\}, k \in \mathbb{N}, \text{finite sums} \}$$
e.g. $[\![x]\!] = \{ k_0 + k_1 x + \cdots + k_n x^n : k_i, n \in \mathbb{N} \}$, $[\![1]\!] = \mathbb{N}$ or $\mathbb{Z}_m$ (in which case R is a ring).

16. Sub-semi-rings can be intersected $A \cap B$, and joined $A \vee B := [\![A \cup B]\!]$, thus forming a complete lattice.

17. The *centralizer* (or commutant) of a subset $A \subseteq R$ is the sub-semi-ring
$$Z(A) := \{ x \in R : \forall a \in A, ax = xa \},$$
in particular the *center* $Z(R)$. $Z(R \times S) = Z(R) \times Z(S)$. $A \subseteq B \Rightarrow Z(B) \subseteq Z(A)$, so if $A \subseteq Z(A)$ then $Z(Z(A))$ is a commutative sub-semi-ring.

18. Given an automorphism σ of R, $\mathrm{Fix}(\sigma) := \{ x : \sigma(x) = x \}$ is a sub-semi-ring. For example, $\mathrm{Fix}(\tau_a) = Z(a)$.

An **ideal** $I \trianglelefteq R$ is a subset that is stable under $+, \cdot$, i.e.,
$$(a + I) + (b + I) \subseteq a + b + I, \quad (a + I)(b + I) \subseteq ab + I,$$
equivalently a left ideal I that is also a right ideal, $IR \subseteq I$. The quotient by the induced congruence R/I^{sub} is a semiring with zero I^{sub} and identity $[1]$.

1. *Generated ideal*: the smallest ideal containing $A \subseteq R$ is
$$\langle A \rangle = R \cdot A \cdot R = \{ x_1 a_1 y_1 + \cdots + x_n a_n y_n : a_i \in A, x_i, y_i \in R, n \in \mathbb{N} \},$$
in particular $\langle a \rangle$ is called a *principal ideal*. In general, Ra is not an ideal; but for "invariant" elements $Ra = aR$, it is.

2. If $I \trianglelefteq J$ then $\phi I \trianglelefteq \phi J$ and $\phi^{-1} I \trianglelefteq \phi^{-1} J$.

3. $I \vee J = \langle I \cup J \rangle = I + J$, $I \wedge J = I \cap J$, so the set of ideals form a modular lattice (wrt $\subseteq$).

4. If I is a left ideal and J a right ideal, then $I \cdot J$ is an ideal, and $J \cdot I \subseteq I \cap J$. This product is distributive over $+$, $(I + J) \cdot K = I \cdot K + J \cdot K$, and is preserved by ring-morphisms, $\phi(I \cdot J) = \phi I \cdot \phi J$. Thus the set of ideals is a semi-ring with $+, \cdot$ and identities 0, R.
$$(I + J) \cdot (I \cap J) \subseteq I \cdot J + J \cdot I \subseteq I \cap J \subseteq I \subseteq I + J$$
Let $I \to J = \{ x \in R : Ix \subseteq J \}$ and $I \leftarrow J = \{ x \in R : xI \subseteq J \}$; then $I \cdot (I \to J) \subseteq J$, so the set of ideals is residuated (see Ordered Sets:2.0.1).

5. The largest ideal inside a left ideal I is its *core* $[I : R]$. It equals $\text{Annih}(R/I)$ since $a(R/I) \subseteq I \Leftrightarrow aR \subseteq I$.

6. The ideals of $R \times S$ are of the form $I \times J$, both ideals.

7. An ideal of a semi-ring $M_n(R)$ consists of matrices (a_{ij}) where $a_{ij} \in I$, an ideal of R. $[M_n(I) : M_n(J)] = M_n[I : J]$.

   Proof: Given an ideal J of matrices, let I be the set of coefficients of the matrices in J; let $E_{rs} := (\delta_{ir}\delta_{sj})$, then $E_{1r}AE_{s1} \in J$ is essentially a_{rs}; so I is an ideal.

2 Rings

Definition A **ring** is a semi-ring in which all elements have negatives. A **module** is the action of a ring on a commutative monoid.

Equivalently, if an element of a semi-ring has a negative and an inverse: $1 + (-a)a^{-1} = (a - a)a^{-1} = 0$, so -1 exists; then $-b = (-1)b$. The Monoid of the module must be a Group since $-x = (-1)x$; it must be commutative since $-x - y = -(x + y) = -y - x$.

When a $+$-cancellative semi-ring R is extended to a group (see Groups), it retains distributivity and becomes a ring: take R^2 and write (a, b) as $a - b$; identify $a - b = c - d$ whenever $a + d = b + c$ (a congruence), and define $(a-b)+(c-d) := (a+c)-(b+d)$, $(a-b)(c-d) := (ac+bd)-(bc+ad)$; R is embedded in this ring via $a \mapsto a-0$ and the negative of a is $0-a$; a cancellative element in R remains so; a congruence $\approx$ on R can be extended to the ring by letting $(a-b) \approx (c-d) := (a+d) \approx (b+c)$.

Examples:

- The integers $\mathbb{Z}$ (extended from $\mathbb{N}$), and $\mathbb{Z}_n$.
- The rational numbers with denominator not containing the prime p. The rational numbers with denominator being a power of p, $\mathbb{Z}[\frac{1}{p}]$.
- The Gaussian integers $\mathbb{Z} + i\mathbb{Z}$ and the quaternions $\mathbb{H} := \mathbb{R}[Q]$.
- The morphisms on an abelian group (called ring representations).
- The elements of a semi-ring having a negative.

Immediate consequences:

1. $0x = 0 = a0$ and $\phi 0 = 0$ now follow from the other axioms.

   Proof: $ax = a(x+0) = ax+a0$, $ax = (0+a)x = 0x+ax$, $\phi(x) = \phi(0+x) = \phi(0) + \phi(x)$.

2. $(-a)x = -(ax) = a(-x)$, $(-a)(-x) = ax$; $\phi(-x) = -\phi(x)$. There is no ∞.

   Proof: $ax+a(-x) = a(x-x) = 0 = (a-a)x = ax+(-a)x$; $0 = \phi(x-x) = \phi(x) + \phi(-x)$. $\infty = \infty + 1$, so $0 = 1$.

3. Every element of a ring is either left cancellative or a left divisor of zero.

   Proof: Either $ax = 0 \Rightarrow x = 0$ or a is a left divisor of zero. In the first case, $ax = ay \Rightarrow a(x - y) = 0 \Rightarrow x = y$.

4. The invertible elements of a ring form a group (but not any group, e.g. not C_5, C_9, C_{11}, etc.).

5. Divisibility $a|b$ (see Groups) induces a (pre-)order on R; there are no known criteria on general rings for when elements have factorizations into irreducibles, or when irreducibles exist.

6. If e is an idempotent, then so is $f := 1 - e$, and $ef = 0 = fe$. So idempotents, except 1, are divisors of zero.

7. There is an associative operation defined by $1 - x * y = (1 - x)(1 - y)$; a is said to be *quasi-regular* when $1 - a$ is invertible, or equivalently there is a b, $a * b = 0 = b * a$.

   (a) If a^n is quasi-regular, then so is a, since
   $$1 - a^n = (1 - a)(1 + a + \cdots + a^{n-1}).$$
   In particular, nilpotents are quasi-regular.

   (b) If ab is quasi-regular, then so is ba,
   $$(1 - ba)^{-1} = 1 + b(1 - ab)^{-1}a.$$

   (c) Idempotents (except 0) cannot be left or right quasi-regular (since $0 = e * b = e + b - eb$, so $e + eb = e(e + b) = eb$).

   (d) A left ideal of left quasi-regulars is also right quasi-regular.
   Proof: $(1 - b)(1 - a) = 1 \;\Rightarrow\; b = ba - a \in I$, so $(1 - c)(1 - b) = 1$; therefore $1 - c = (1 - c)(1 - b)(1 - a) = 1 - a$, and $a = c$ is right quasi-nilpotent.

8. There are various grades of nilpotents:

   (a) '*super nilpotents*', any word containing n a's is 0 (for some n), e.g. central or invariant nilpotents.

   (b) *strong nilpotents*, any sequence $a_{n+1} \in \langle a_n \rangle^2$, $a_0 = a$, is eventually 0 (the last non-zero term is a super nilpotent with $n = 2$).

   (c) *nilpotents*, $a^n = 0$, $\exists n \in \mathbb{N}$.

   (d) *quasi-nilpotents*, $1 - xa$ is invertible for all $x \in R$. A left-ideal of nilpotents is quasi-nilpotent.

9. Sub-modules are subtractive $Y^{\text{sub}} = Y$, and are automatically stable for negatives, $-Y = (-1)Y = Y$. The congruence relation induced by a sub-module Y, $x_1 = x_2 \pmod{Y}$ becomes $x_1 - x_2 \in Y$, so $[x] = x + Y$. For example, $R[x, y] \cong R\langle x, y\rangle/[xy - yx]$.

10. The kernel of a morphism is now the ideal $\ker T = T^{-1}0$; thus a morphism is 1-1 $\Leftrightarrow$ its kernel is trivial. The solutions of the equation $Tx = y$ are $T^{-1}y = x_0 + \ker T$ (particular + homogeneous solutions).

11. $X \to X/Y$, $x \mapsto x+Y$ is a module morphism, and the usual Isomorphism theorems hold (see Universal Algebras), e.g. sub-modules that contain M correspond to sub-modules of X/M, $(M+N)/N \cong M/(M\cap N)$, $R/\ker\phi \cong \phi R$.

12. The module morphism $R \to X$, $a \mapsto ax$, has kernel $\mathrm{Annih}(x)$, so
$$R/\mathrm{Annih}(x) \cong [\![x]\!].$$
Let $T_a(x) := ax$, then $\mathrm{Hom}_R(X) = Z(\{\, T_a : a \in R \,\})$ since
$$S(ax) = aS(x) \;\Leftrightarrow\; ST_a = T_aS,\ \forall a \in R$$
If the ring action is faithful, then R is embedded in $\mathrm{Hom}(X)$.

13. Generated subrings are now
$$[\![A]\!] = \{\, \sum \pm a_1 \cdots a_k : a_i \in A \cup \{\,1\,\}, k \in \mathbb{N}, \text{finite sums}\,\}.$$

14. (Jacobson) If R acts faithfully on a module X, then it is a 'dense' subring of its double centralizer in $\mathrm{Hom}_{\mathbb{Z}}(R)$, i.e., for any $x_1, \ldots, x_n$ and any s in the double centralizer, then there is an $r \in R$, $rx_i = sx_i$. In a sense, R is indistinguishable from S for finite sets.

15. The ideals of $R[x]$ are of the type $I_0 + I_1x + \cdots$ where $I_0 \subseteq I_1 \subseteq \cdots$; then $R[x]/I[x] \cong (R/I)[x]$ (via the morphism $R[x] \to (R/I)[x]$, $x^k \mapsto (1+I)x^k$); $I[x]$ is prime iff I is prime.

Since there is now a correspondence between sub-modules/ideals and congruence relations, the analysis of modules and rings becomes simpler. The quotient space X/Y simplifies:
$$(x+Y) + (y+Y) = (x+y) + Y, \qquad a(x+Y) = ax + Y.$$

3 Module Structure

To analyze a module, one typically splits X into a sub-module Y and an image X/Y; one can continue this process until perhaps all such modules are *simple* (or *irreducible*) when they have no non-trivial sub-modules.

For **simple modules**,

1. $X = Rx \cong R/\mathrm{Annih}(x)$ for any $x \neq 0$. So each $\mathrm{Annih}(x)$ is a maximal left ideal in R. The structure of a simple module thus mirrors that of the ring R itself, or rather of the left-simple ring $R/\mathrm{Annih}(x)$; such a ring whose only left ideals are trivial is called a *division ring*.

2. The image of any module morphism to a simple module X, and the kernel of any morphism from X, can only be the whole module or 0. So any linear map between simple modules is either 0 or an isomorphism. In particular, the ring $\mathrm{Hom}_R(X)$ consists of 0 and invertible maps (automorphisms), thus a division ring.

3. The simple $\mathbb{Z}$-modules are the simple abelian groups, i.e., $\mathbb{Z}_p$.

Decomposition of a module as $X \cong Y \times Z$ is a special case of finding quotients.

1. $X = M + N \cong M \times N \Leftrightarrow M \cap N = [\![0]\!]$, since the map $(x, y) \mapsto x + y$ is an onto module morphism with kernel $\{ (x, -x) : x \in M \}$, so 1-1 when $M \cap N = 0$. M and N are complements in the lattice of sub-modules.

   To any decomposition there correspond projections $e : x+y \mapsto x$, $X \to M$, and $f : X \to N$, which are idempotents in $\mathrm{Hom}_R(X)$ such that $e + f = 1$, $ef = 0 = fe$, $\ker e = N = \operatorname{im} f$, $X = eX \oplus fX$.

   In general, $X \cong \bigoplus_i M_i$ iff $X = \sum_i M_i$, $M_i \cap \sum_{j \neq i} M_j = 0$.

2. Every module can be decomposed into sub-modules $X = Y \oplus Z$ until indecomposable sub-modules are reached. A module is indecomposable iff $\mathrm{Hom}_R(X)$ has only trivial idempotents iff R has trivial idempotents.

   Indecomposable need not be simple because a sub-module need not necessarily be complemented (e.g. $\mathbb{Z}_4$ is indecomposable but contains the ideal $\langle 2 \rangle$).

3. X is a *free* module $\bigoplus_{e \in E} R$ iff it has a (Hamel) **basis** E, i.e., $[\![E]\!] = X$ and E independent ($e \in E \Rightarrow e \notin [\![E \smallsetminus e]\!]$, equivalently $\sum_i a_i e_i = 0 \Rightarrow a_i = 0$). Thus every module element is a unique (finite) linear combination of e_i's,

$$x = \sum_i a_i e_i, \quad \exists! a_i \in R$$

   Proof: Each $e \in E$ corresponds to $u_e \in R^E$, $t \mapsto \begin{cases} 1 & t = e \\ 0 & t \neq e \end{cases}$. So $1 = \sum_{e \in E} u_e$, $x(t) = \sum_e x(e) u_e(t)$; if $\sum_e a_e u_e = 0$ then $0 = a_e u_e(e) = a_e$. Conversely, the map $(a_i) \mapsto \sum_i a_i e_i$ is an isomorphism.

   Every module is the quotient of some free module (with the generators of X). Every ring has the basis $\{ 1 \}$.

   The number of basis elements need not be well-defined (when it is, it is called the *rank* of X). For example, the ring of 2×2 matrices has the basis $\{ I \}$ as well as the basis $E_1 := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $E_2 := \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ (any AE_1 has a zero second column; $I = E_1^\top E_1 + E_2^\top E_2$.)

   (Note that a linearly independent set need not be part of a basis, e.g. $\{ 2 \}$ in $\mathbb{Z}$.)

4. Matrices $M_{m\times n}(R)$ form a free module with basis $E_{rs} = [\delta_{ir}\delta_{js}]$. Polynomials $R[x]$ form a free module with basis $1, x, x^2, \ldots$.

5. The map $x \mapsto (x + Y_1, \ldots, x + Y_n)$ is a morphism $X \to \prod_i (X/Y_i)$ with kernel $Y_1 \cap \cdots \cap Y_n$.

   Proposition 1

   If Y_i are sub-modules such that $X = Y_i + \bigcap_{j\neq i} Y_j$, then

   $$\frac{X}{Y_1 \cap \cdots \cap Y_n} \cong \frac{X}{Y_1} \times \cdots \times \frac{X}{Y_n}.$$

   That is, $x = x_i \pmod{Y_i}$ can be solved modulo $\bigcap_i Y_i$.

   Proof: To show surjectivity: Given x_i, by induction $\exists y = x_i \pmod{Y_i}$ for all $i = 1, \ldots, n-1$. But $x_n - y = a + b \in Y_n + \bigcap_{j\neq n} Y_j$; let $x := x_n - a = y + b$. Then $x - y = b \in \bigcap_{j<n} Y_j$, $x - x_n = -a \in Y_n$, so $x = y = x_i \pmod{Y_i}$ and $x = x_n \pmod{Y_n}$.

   For rings, it is enough to have mutually co-prime ideals $I_i + I_j = R$, $i \neq j$ (since by induction $R = I_1 + \bigcap_{i=2}^{n-1} I_i$, so $1 = a + b$ and $I_n \subseteq I_n \cdot I_1 + \bigcap_{i=2}^{n} I_i$, hence $R = I_1 + I_n \subseteq I_1 + \bigcap_{i=2}^{n} I_i$). This gives a method for solving $x = x_i \pmod{I_i}$; $1 = a_{ij} + a_{ji}$ with $a_{ij} \in I_i$, so $1 = a_{i1} + a_{1i}(a_{i2} + a_{2i}) = \cdots = a_i + b_i$ ($b_i = \prod_{j\neq i} a_{ji} \in \bigcap_{j\neq i} I_j$); so $x = \sum_i b_i x_i$.

6. If Y_i are sub-modules of X_i, then using the map $(x_1, \ldots, x_n) \mapsto (x_1 + Y_1, \ldots, x_n + Y_n)$,

   $$\frac{X_1 \times \cdots \times X_n}{Y_1 \times \cdots \times Y_n} \cong \frac{X_1}{Y_1} \times \cdots \times \frac{X_n}{Y_n}$$

7. X^n is not isomorphic to X^m unless $n = m$ (by Jordan-Hölder).

3.0.2 Composition Series

The most refined version of decomposition is a *composition* series

$$0 \leqslant \cdots < Y_i < Y_{i^+} < \cdots \leqslant X$$

with Y_{i^+}/Y_i (unique) simple modules. The (maximum) number of terms is called the *length* of X. For example, $\cdots < 2^3\mathbb{Z} < 2^2\mathbb{Z} < 2\mathbb{Z} < \mathbb{Z}$. There are two standard ways of starting this out:

- Top approach: Maximal sub-modules (if there are any), so X/M is simple. If $M_1, M_2, \ldots$ are maximal sub-modules, then

$$\cdots < M_2 \cap M_1 < M_1 < X$$

is part of a composition series since $M_1/(M_2 \cap M_1) \cong (M_1 + M_2)/M_2$ simple. Their intersection is the (Jacobson) *radical*

$$\operatorname{Jac}(X) := \bigcap \{ M : \text{maximal sub-module} \}$$

More generally, the *radical* of a sub-module Y is the intersection of all maximal sub-modules containing Y,

$$\operatorname{rad}(Y) := \bigcap \{ Y \leqslant M : M \text{ maximal sub-module} \}.$$

If Y is a sub-module then $\operatorname{Jac}(Y) = Y \cap \operatorname{Jac}(X)$. If $T : X \to Y$ is a module-morphism then $T\operatorname{Jac}(X) \subseteq \operatorname{Jac}(Y)$. For $Y \leqslant \operatorname{Jac}(X)$, $\operatorname{Jac}(X/Y) = \operatorname{Jac}(X)/Y$, so $X/\operatorname{Jac}(X)$ has no radical.

Note: if $Rx + Y = X$, but $x \notin Y$, there is a maximal sub-module Z with the property $x \notin Z$; so $x \notin \operatorname{Jac}(X) \subseteq Z$.

- Bottom approach: Minimal sub-modules (if there are any) are simple. If $Y_1, Y_2, \ldots$ are minimal sub-modules, then

$$0 < Y_1 < Y_1 \oplus Y_2 < \cdots$$

is part of a composition series since $Y_1 \cap Y_2 = 0$ as a sub-module of Y_1; thus $(Y_1 \oplus Y_2)/Y_1 \cong Y_2$. Their sum is the *socle*

$$\operatorname{Soc}(X) := \sum \{ Y : \text{minimal sub-module} \}$$

Such considerations can also be used for a linear map T on X, as it induces an ascending and descending chain of sub-modules:

$$0 \leqslant \ker T \leqslant \ker T^2 \leqslant \ker T^3 \leqslant \cdots \leqslant \bigcup_n \ker T^n$$

$$\bigcap_n \operatorname{im} T^n \leqslant \cdots \leqslant \operatorname{im} T^3 \leqslant \operatorname{im} T^2 \leqslant \operatorname{im} T \leqslant X$$

3.1 Semi-primitive Modules

are modules whose radical is zero. So, by $x \mapsto (x + M_i)$, the module is embedded in a product of simple modules,

$$X \subsetneq \prod_{M_i \text{ maximal}} \frac{X}{M_i}$$

For every module, $X/\operatorname{Jac}(X)$ has zero Jacobson radical, i.e., is semi-primitive.

3.2 Semi-simple Modules

A module is **semi-simple** when it can be decomposed into simple sub-modules $X = \sum_i Y_i = \mathrm{Soc}(X)$. (The sum, without repetitions, can be taken to be direct since $Y_i \cap \sum_j Y_j$ is a sub-module of Y_i.)

1. Every sub-module is complemented.

   Proof: Given $X = \sum_i Y_i$ and a sub-module Y, let $M := \sum_{i \leqslant r} Y_i$ for some maximal r with $Y \cap M = 0$; then for any $j > r$, $0 \neq x \in Y \cap (M + Y_j)$ for some $x = a + b \in M + Y_j$, $0 \neq b = x - a \in (Y + M) \cap Y_j$; but Y_j is simple, so $Y_j \subseteq M + Y$ and $M + Y = X$. Conversely, for $x \neq 0$, let Z be that maximal submodule st $x \notin Z$; then $X = Z \oplus A$ with $x \in A$ simple.

2. Sub-modules, images X/Y, and products are again semi-simple (since $X \times Y = (X \times 0) \oplus (0 \times Y)$).

3. Semi-simple modules are semi-primitive.

   Proof: Each Y_i has a complement Y_i' and $Y_i \cong X/Y_i'$, so Y_i' is maximal; hence $\mathrm{Jac}(X) \subseteq \bigcap_i Y_i' = 0$.)

4. *Proposition* 2

   (Wedderburn)

   For X, Y non-isomorphic simple R-modules,

   $$\mathrm{Hom}_R(X \times Y) = \mathrm{Hom}_R(X) \times \mathrm{Hom}_R(Y),$$
   $$\mathrm{Hom}_R(X^n) = M_n(F), \ \textbf{where } F = \mathrm{Hom}_R(X) \ (\textbf{division ring})$$
   $$\mathrm{Hom}_R(X^n \times \cdots \times Y^m) = M_n(F_X) \times \cdots \times M_m(F_Y)$$

   Proof: A linear map on $X \times Y$ induces a map $X \to X \times Y \to Y$, which is 0 unless $X \cong Y$. Similarly, a linear map $T : X^n \to Y^m$ induces a map $X \to X^n \to Y^m \to Y$, so $T = 0$ unless $X \cong Y$. So $\mathrm{Hom}_R(X^n \times Y^m) = \mathrm{Hom}_R(X^n) \times \mathrm{Hom}_R(Y^m) \cong M_n(F_X) \times M_m(F_Y)$.

5. Every element of $\mathrm{Hom}(X)$ is regular (von Neumann ring).

   Proof: $X = \ker T \oplus Y$, and $X = TY \oplus Z$; $T|_Y$ is an isomorphism $Y \to TY$; let S be the inverse $TY \to Y$, so that $TST = T$.

3.3 Finitely Generated Modules

$X = [\![x_1, \ldots, x_n]\!] = [\![x_1]\!] + \cdots + [\![x_n]\!]$.

1. Images remain finitely generated, but sub-modules need not be, e.g. every ring is finitely generated by 1, but not necessarily its left ideals (e.g. $\mathbb{Z}\times\mathbb{Q}$ with $1 := (1,0)$, $(0,1)^2 := (0,0)$).
2. If both X/Y and Y are finitely generated, then so is X.
3. If $X = \sum_i Y_i$ then a finite number of Y_i suffice to generate X (since $x_i \in \sum_{i=1}^n Y_i$); thus finitely generated semi-simple modules have finite length.
4. (Nakayama) If X is finitely generated, and $J := \mathrm{Jac}(R)$, then $J \cdot X < X$ (except for $X = 0$) and $J \cdot X$ is superfluous.

   Proof: Suppose $J \cdot X = X = [\![x_1, \ldots, x_n]\!]$, a minimal generating set. Then $x_n = \sum_{i=1}^n a_i x_i$ with $a_i \in J$, so $x_n = \sum_{i=1}^{n-1}(1-a_n)^{-1}a_i x_i$ (since $1-a$ is invertible, see below), a contradiction. If $J \cdot X + Y = X$ then $(1-J)\cdot X = Y$, so $X = Y$.

3.3.1 Noetherian Modules

are modules in which every non-empty subset of sub-modules has a maximal element; equivalently, every ascending chain of sub-modules is finite.

Noetherian modules are finitely generated since the chain

$$0 \leqslant [\![x_1]\!] \leqslant [\![x_1, x_2]\!] \leqslant \cdots \leqslant X$$

with $x_{n+1} \notin [\![x_1, \ldots, x_n]\!]$ stops at some n. Every sum of sub-modules equals a finite sum, e.g. $\mathrm{Soc}(X)$ is a finite sum of minimal sub-modules.

Sub-modules, quotients, and finite products are obviously Noetherian, and each proper sub-module is contained in a maximal sub-module. If X/Y and Y are Noetherian, then so is X.

Artinian modules have the dual property: every non-empty subset of sub-modules has a minimal element and every descending chain of modules is finite. Thus every sub-module contains a minimal (simple) sub-module. Every intersection of sub-modules equals some finite intersection; e.g. $\mathrm{Jac}(X)$ is the finite intersection of maximal sub-modules.

There are examples of Artinian modules that are not Noetherian and vice versa.

3.3.2 Modules of finite length

Modules of finite length have a finite composition series, i.e., are both Artinian and Noetherian. $\ell(X) = \ell(X/Y) + \ell(Y)$.

1. X is the sum of a finite number of indecomposable sub-modules (Krull-Schmidt: unique).

2. Important examples are the finite products of simple modules (finite-length semi-simple):

$$\begin{aligned} X \cong Y_1 \times \cdots \times Y_n \quad (Y_i \text{ simple}) &\Leftrightarrow X \text{ is Noetherian semi-simple} \\ &\Leftrightarrow X \text{ is Artinian semi-primitive} \end{aligned}$$

   Proof: That $Y_1 \times Y_2$ is semi-simple of finite length is trivial. If $X = \bigoplus_i Y_i$ is Noetherian semi-simple then

$$0 \leqslant Y_1 \leqslant Y_1 \oplus Y_2 \leqslant \cdots \leqslant \mathrm{Soc}(X) = X$$

   shows X is a finite sum. If X is Artinian semi-primitive then

$$X \geqslant M_1 \geqslant M_1 \cap M_2 \geqslant \cdots \geqslant \mathrm{Jac}(X) = 0$$

   and so X is embedded in a finite product of simple modules, hence semi-simple.

3. (Fitting) Every linear map T on X of finite length induces a decomposition $X = \ker T^n \oplus \operatorname{im} T^n$ for some n.

   Proof: The ascending and descending chains of T stop, so $\operatorname{im} T^{n+1} = \operatorname{im} T^n$, $\ker T^{n+1} = \ker T^n$. For every $x \in X$, $T^n x = T^{2n} y$, so $x - T^n y \in \ker T^n$, and $X = \operatorname{im} T^n + \ker T^n$. If $x \in \operatorname{im} T^n \cap \ker T^n$, i.e., $T^n x = 0$, $x = T^n y$, then $T^{2n} y = 0$, so $y \in \ker T^n = \ker T^n$, and $x = T^n y = 0$.

   Thus if X is indecomposable, then T is either invertible or nilpotent; hence $\mathrm{Hom}_R(X)$ is a local ring since it cannot have idempotents.

4 Ring Structure

1. A ring is decomposable when it contains an idempotent $e \in R$. Then $\mathrm{Annih}(e) = R(1-e)$, so

$$\begin{gathered} R = Re \oplus R(1-e) \cong Re \times R(1-e), \\ R = eRe \oplus eR(1-e) \oplus (1-e)Re \oplus R(1-e) \cap (1-e)R \\ x = exe + ex(1-e) + (1-e)xe + (1-e)x(1-e). \end{gathered}$$

   If $R = I \oplus J$ (ideals) then $I = Re$ for some central idempotent (since $1 = e + f$ so $0 = ef = e - e^2$; for every $x \in I$, $x = xe + xf = ex + fx$, uniquely, so $xe = ex$).

   Then any R-module splits as $X = R \cdot X = (Re) \cdot X + (Rf) \cdot X$.

2. The central idempotents ($e^2 = e$, $ae = ea$) form a Boolean algebra with $e \wedge f := ef$ and $e \vee f := e + f + ef$. If an idempotent commutes with all other idempotents, then it is central.

   For example, in a reduced ring (no nilpotents except 0), all idempotents are central. (Proof: $e(x - xe)e(x - xe) = 0$ and $(x - ex)e(x - ex)e = 0$, so $e(x - xe) = 0$, i.e., $ex = exe = xe$).

3. A **nilpotent** ideal is one for which $I^n = 0$, e.g. $6\mathbb{Z}$ in $\mathbb{Z}_{12}$. Its elements are super-nilpotent. For a nilpotent ideal, $I \cdot X \subset X$ (else $X = I^n X = 0$). If I is a nilpotent left ideal, then $I \cdot R$ is nilpotent.

   The sum of nilpotent ideals $I + J$ is again nilpotent ($(I+J)^{m+n} = 0$). The sum of all nilpotent ideals (not necessarily itself nilpotent) is denoted

   $$\mathrm{Nilp}(R) := \sum\{\, I : \text{nilpotent} \,\} = \{\, a \in R : \text{supernilpotent} \,\}.$$

   Proof: $a_1(x_1+x_2)a_2(x_1+x_2)\cdots = b_1x_1b_2x_1\cdots \in I_1^k = 0$ if enough factors are taken.

   (Note: The notation I^n is ambiguous: in a module, it usually means $I \times \cdots \times I$, but in a ring it means $I \cdots I$.)

4. $I \cdot J \subseteq I \cap J$ but the two may be distinct. S is a **semi-prime** ideal iff

   $$\begin{aligned} I \cdot J \subseteq S \;&\Rightarrow\; I \cap J \subseteq S, \\ \exists n \in \mathbb{N},\ I^n \subseteq S \;&\Rightarrow\; I \subseteq S, \\ xRx \subseteq S \;&\Rightarrow\; x \in S. \end{aligned}$$

   Proof: $I \cdot I \subseteq S \;\Rightarrow\; I = I \cap I \subseteq S$, so $I^{2n} \subseteq S \;\Rightarrow\; I^n \subseteq S \;\Rightarrow\; I \subseteq S$ by induction. $xRx \subseteq S \Leftrightarrow \langle x \rangle^2 \subseteq S$. If $I \cdot J \subseteq S$ and $x \in I \cap J$, then $xRx \subseteq I \cdot J \subseteq S$, so $x \in S$.

   Every nilpotent ideal is contained in every semi-prime one: $I^n = 0 \subseteq S \Rightarrow I \subseteq S$; and $I \cdot J$ is semi-prime only when $I \cdot J = I \cap J$.

5. An **irreducible** ideal is lattice-irreducible, i.e., for any ideals I and J,

   $$P = I \cap J \;\Rightarrow\; P = I \text{ or } P = J,$$

   e.g. $4\mathbb{Z}$ in $\mathbb{Z}$. The lattice-prime ideals are those that satisfy

   $$I \cap J \subseteq P \;\Rightarrow\; I \subseteq P \text{ or } J \subseteq P$$

   hence irreducible. But for rings, it is more relevant to define the **prime** ideals P by the stronger condition

   $$\begin{aligned} & I \cdot J \subseteq P \;\Rightarrow\; I \subseteq P \text{ or } J \subseteq P, \\ \text{equivalently,}\quad & xRy \subseteq P \;\Rightarrow\; x \in P \text{ or } y \in P, \end{aligned}$$

   e.g. $2\mathbb{Z}$. Morphisms $\phi : R \to S$ pull prime ideals in S to prime ideals in R.

   Since $I \cdot J \subseteq I \cap J$, the intersection of two ideals cannot be prime, unless $I \subseteq J$ or vice-versa.

6. The intersection of prime ideals is a semi-prime ideal (and conversely).

   Proof: If $I \cdot J \subseteq \bigcap_i P_i \subseteq P$ then $I \subseteq P$ or $J \subseteq P$, so $I \cap J \subseteq P$ for any P. Conversely, R/S has no non-trivial nilpotent ideals, so for every $a \notin S$, let $a_1 := a$, $a_{n+1} := a_n r_n a_n \notin S$, let P be maximal wrt $a_n \notin P$, so P is prime with $a \notin P$.

7. The set of prime ideals is called the *spectrum* of the ring; the spectrum of an ideal is
$$\mathrm{Spec}(I) := \{\, P \geqslant I : \text{prime} \,\}$$
   (a) $I \leqslant J \;\Rightarrow\; \mathrm{Spec}(I) \supseteq \mathrm{Spec}(J)$,
   (b) $\mathrm{Spec}(I \cdot J) = \mathrm{Spec}(I) \cup \mathrm{Spec}(J)$,
   (c) $\mathrm{Spec}(I + J) = \mathrm{Spec}(I) \cap \mathrm{Spec}(J)$

   Two ideals are *co-prime* when $I + J = R$, i.e., $a + b = 1$ for some $a \in I$, $b \in J$. Then $I \cap J = I \cdot J + J \cdot I$.

8. The *prime radical* of R is the smallest semi-prime ideal
$$\mathrm{Prime}(R) := \bigcap \{\, P : \text{prime} \,\}$$
   More generally, the smallest semi-prime ideal containing an ideal I is its *prime radical* $\mathrm{prad}(I) := \bigcap\{\, P \geqslant I : \text{ prime} \,\} = \bigcap \mathrm{Spec}(I)$.

9. $\mathrm{Prime}(R)$ is the set of strong nilpotents. Thus $\mathrm{Prime}(R/\mathrm{Prime}(R)) = 0$.

   Proof: If x is not a strong nilpotent, choose a sequence a_n such that $a_0 = x \neq 0$, $0 \neq a_{n+1} \in \langle a_n \rangle^2$; let P be an ideal which is maximal wrt $\forall n,\ a_n \notin P$. Then $I, J \not\subseteq P$ implies there are $n \geqslant m$, say, with $a_n \in I + P$, $a_m \in J + P$. Thus $a_{n+1} \in (I + P)(J + P) = IJ + P$, so $IJ \not\subseteq P$. Thus P is prime and $x \notin \mathrm{Prime}(R)$. Conversely, the last term of the sequence a_n of a strong nilpotent a is of the type $aRa = 0 \subseteq \mathrm{Prime}$, so $a \in \mathrm{Prime}$. Since $R/\mathrm{Prime}(R)$ has no super nilpotents, its prime radical is 0.

10. Recall *radical* sets $r(A) := \{\, x \in R : x^n \in A, \exists n \in \mathbb{N} \,\}$ (see Groups). Radical ideals are clearly semiprime. $x \in r(I) \Leftrightarrow (x + I)$ is nilpotent in R/I. The union and intersection of radical ideals is radical,
$$r(I \cup J) = r(I) \cup r(J), \quad r(I \cdot J) = r(I \cap J) = r(I) \cap r(J)$$

11. $\mathrm{Prime}(R \times S) = \mathrm{Prime}(R) \times \mathrm{Prime}(S)$; $\mathrm{Prime}(M_n(R)) = M_n(\mathrm{Prime}(R))$ (since an ideal of $M_n(R)$ is prime when it is of the type $M_n(P)$, P prime in R).

12. A *nil* ideal is one that consists of nilpotents. The sum of nil ideals is again nil (since $(a + b)^{mn} = (a^m + c)^n = c^n = 0$), so the largest nil ideal exists and is called the *nilradical* $\mathrm{Nil}(R)$.

    The nilradical of $R/\mathrm{Nil}(R)$ is 0 (proof: Let I/Nil be a nil ideal in R/Nil; then for every $a \in I$, $a^n \in (I + \mathrm{Nil})^n = \mathrm{Nil}$, so $a^{nm} = 0$, and $I \subseteq \mathrm{Nil}$).

    (Köthe's conjecture: $\mathrm{Nil}(M_n(R)) = M_n(\mathrm{Nil}(R))$, or all nil left ideals are in Nil.)

13. The core of a maximal left ideal is called a *primitive* ideal; equivalently it is the annihilator of a simple module X.

    Proof: M is a maximal left ideal of $R \Leftrightarrow X \cong R/M$ is a simple module, $\Leftrightarrow \operatorname{Annih}(X) = [M : R]$.

14. Maximal $\Rightarrow$ Primitive $\Rightarrow$ Prime.

    Proof: A maximal ideal $\tilde{M}$ is contained in a maximal left-ideal M, so $[M : R] = \tilde{M}$. If $I \not\subseteq [M : R]$, then $I \not\subseteq M$, so $I + M = R$; thus if $I, J \not\subseteq [M : R]$, then $IJ + M = (I + M)(J + M) = R$, so $IJ \not\subseteq M$.

15. A left ideal I is in all the maximal left ideals $\Leftrightarrow$ it is superfluous $\Leftrightarrow$ it consists of quasi-nilpotents.

    The *Jacobson radical* of a ring is

    $$\begin{aligned}\operatorname{Jac}(R) = \operatorname{rad}(0) &= \bigcap\{\, M \leqslant X : \text{ maximal/primitive left ideal}\,\}\\ &= \sum\{\, I \leqslant X : \text{superfluous}\,\} \quad \text{(see Ordered Sets)}\\ &= \{\, a \in R : \text{quasi-nilpotent}\,\}\end{aligned}$$

    Proof: There is a maximal left ideal M such that $I \leqslant M < R$, so $I + J \leqslant I + M = M < R$. $a \in I \Rightarrow xa \in I \Rightarrow Rxa$ is superfluous, but $R = Rxa + R(1 - xa)$, so $R = R(1 - xa)$ and a is quasi-nilpotent. $I + M = R \Rightarrow 1 = a + b \Rightarrow b = 1 - a$ is invertible, so $M = R$, a contradiction; thus $I + M = M$.

    (a) $\operatorname{Jac}(R)$ is an ideal (since $a \in J \Leftrightarrow Ra \subseteq J \Leftrightarrow a \in [J : R]$ an ideal).

    (b) $\operatorname{Jac}(R)$ is the largest left ideal such that $1 + J \subseteq \mathcal{G}(R)$ (the group of invertibles).

    (c) $\operatorname{Jac}(R)$ contains no idempotents, except for 0 ($1 - e$ is invertible).

    (d) $\operatorname{Jac}(R)X \subseteq \operatorname{Jac}(X)$ (using $T : a \mapsto ax$); in particular $\operatorname{Jac}(R)$ annihilates every (semi-)simple R-module.

    (e) $\operatorname{Jac}(R \times S) = \operatorname{Jac}(R) \times \operatorname{Jac}(S)$ (since $(1, 1) - (x, y)(a, b)$ is invertible for all x, y iff $a \in \operatorname{Jac}(R)$, $b \in \operatorname{Jac}(S)$).

    (f) $\operatorname{Jac}(M_n(R)) = M_n(\operatorname{Jac}(R))$ (since $TJ \subseteq J(TR)$).

    The dual notions are, if they exist, *minimal* ideals, their upperbounds the *essential* ideals, and their sum the *socle*.

16. Nilp $\subseteq$ Prime $\subseteq$ Nil $\subseteq$ Jac $\subseteq$ Br

    Proof: For any nilpotent ideal, $I^n = 0 \subseteq P(\text{prime}) \Rightarrow I \subseteq P$. Elements of Prime are nilpotent. Nil ideals are superfluous since $N + I = R$ implies $1^n = (a + b)^n = a^n + c = c \in I$. If $a \in \text{Nil}$, then for any x, xa is nilpotent, hence a is quasi-nilpotent. $\operatorname{Br}(R)$ is defined as the intersection of all maximal ideals, so includes $\operatorname{Jac}(R)$.

    Nil is the intersection of those prime ideals that are not contained in a nil ideal.

17. The sum of those minimal left ideals that are isomorphic to I form an ideal B_I. For I, J non-isomorphic minimal left-ideals, $B_I B_J = 0$.

    Proof: For $J \cong I$, and any $a \in R$, Ja is a left ideal and there is a module morphism $J \to Ja$, so $Ja = 0$ or $Ja \cong J \cong I$, so $Ja \subseteq B_I$.

18. A minimal left ideal is either nilpotent, $I^2 = 0$, or generated by an idempotent $I = Re$; in either case, it consists entirely of zero divisors.

    Proof: If $I^2 \neq 0$, then there is an $a \in I$ such that $I = Ia \neq 0$; so there is an $e \in I$ such that $ea = a$; also $\text{Annih}(a) \cap I$ is a left ideal, so must be 0; but $e^2 - e$ belongs to this intersection, so $e^2 = e$; $Re \subseteq I$, so $Re = I$.

4.1 Division rings

are rings in which every non-zero is invertible; equivalently left-simple rings F, i.e., the only left ideals are 0 and F (for any $a \neq 0$, $Fa = F$, so a has a left-inverse b, and b has a left-inverse c, so $a = c = b^{-1}$). Note: left-simple is stronger than simple. The composition series is just $0 < F$.

The smallest sub-ring is $\mathbb{Z}$ or $\mathbb{Z}_p$, called the *characteristic* of F.

1. The centralizers $Z(A)$ of a division ring are themselves division rings (since $xy = yx \ \Rightarrow\ yx^{-1} = x^{-1}y$); in particular the center $Z(F)$ (a field).

2. A division ring is generated by its center and its commutators.

   Proof: Any $a \notin Z(F)$ must have a b such that $[a, b] \neq 0$; hence $a[a, b] = [a, ab]$, so $a = [a, ab][a, b]^{-1}$.

3. If $2 \neq 0$, then any sub-division ring E which is closed under commutators of F must be a field (similarly if it is closed under conjugates $x^{-1}Ex$).

   Proof: For $x \in E \leqslant F$, $y \notin E$, $2y[y, x] = [y^2, x] + [y, [y, x]] \in E$, so $[y, x] = 0$. For $z \in E$, $xz = xy^{-1}yz = y^{-1}xyz = y^{-1}yzx = zx$.

4. Finite domains are fields (Wedderburn).

   'Proof': For $a \neq 0$, $x \mapsto ax$ is 1-1, hence onto, so both $ax = 1$ has a solution; similarly for $x \mapsto xa$. So R is an algebra over its center F, which is a finite field of size p^n, hence R has size p^{nm}. As groups, the conjugacy class equation is $p^{nm} = p^n + \sum_i [R : C_i]$; a counting argument then shows $m = 1$.

4.1.1 Vector Spaces

are modules over a division ring. For example, division rings themselves are vector spaces over their center.

1. $ax = 0 \ \Rightarrow\ a = 0$ OR $x = 0$.

2. Any vector space is free, $\bigoplus_E F$; i.e., there is always a basis.

   Proof: Given a (well-ordered) generating set W and a linearly independent set U, if $w \in W$, $w \notin [\![U]\!]$, then $U \cup \{ w \}$ is linearly independent. A chain of independent set U_i can be formed by adding elements of W. Moreover, any linear combination in $\bigcup_i U_i$ is a finite sum so must belong to some U_j, and cannot be 0. By Zorn's lemma there is a maximal linearly independent set E which generates X (and includes U).

3. All bases have the same number of elements, called the *dimension* $\dim X$.

   Proof: If $w \in W$, $w \in [\![U]\!]$, then there is a $u \in U$, $[\![U \smallsetminus u]\!] + [\![w]\!] = [\![U]\!]$; so a finite generating set cannot have less elements than an independent set. For an infinite W, each $w = \sum_i a_{ij} u_j$ are finite sums, so the total number of u_j involved in such sums does not exceed $|W|$; any missed u would be a linear combination of some w's, hence some u_i's, a contradiction.

4. Subspaces are complemented: $X = V \oplus W$, thus have a smaller dimension than X.

   Proof: Start with a basis e_i for V, then extend to a basis w_k for X. The basis vectors not in V are a basis f_j for X/V (since $x = \sum_k a_k w_k = \sum_j a_j f_j \pmod V$, $0 = \sum_j a_j f_j \pmod V \;\Rightarrow\; \sum_j a_j f_j \in V \;\Rightarrow\; a_j = 0$).

   So $\dim X = \dim(X/Y) + \dim Y$. For example, for any linear map T, $\dim X = \dim\ker T + \dim\operatorname{im} T$.

$$\begin{aligned}
\operatorname{rank}(S+T) &\leqslant \operatorname{rank}(S) + \operatorname{rank}(T)\\
\operatorname{rank}(ST) &\leqslant \operatorname{rank}(S) \wedge \operatorname{rank}(T)\\
\operatorname{null}(ST) &\leqslant \operatorname{null}(S) + \operatorname{null}(T)
\end{aligned}$$

5. Products: $\dim(X \times Y) = \dim X + \dim Y$, since the vectors $(e_i, 0)$ with $(0, e'_j)$ form a basis for $X \times Y$.

6. The ring $\operatorname{Hom}_F(X)$ is semi-simple and contains the unique minimal ideal K of finite-rank linear maps (i.e., $\operatorname{im} T$ is finitely generated), which is prime and idempotent; the other ideals are contained in each other, each being the linear maps whose rank has a certain cardinality. $\operatorname{Hom}_F(X)$ acts on the unique simple faithful module $Kx = X$.

   $B := \operatorname{Hom}_F(X)$ acts faithfully on the simple module eB (since there is a projection $e : X \to Fx \subseteq X$, and the map $J : B \to X$, $T \mapsto Tx$ is linear, onto, $(\ker J)e = 0$, $\ker J = B(1-e)$, so $X \cong Be$ as modules over B).

7. $\dim\operatorname{Hom}(X, Y) = \dim X \dim Y$ (using the basis E_{rs}).

8. $\operatorname{Hom}(X, Y)$ is a simple ring (suppose I is an ideal containing $A \neq 0$, then $E_{mn} = a_{ji}^{-1} E_{mi} A E_{jn} \in I$, so $I = \operatorname{Hom}(X, Y)$).

$M_n(F) = \mathrm{Hom}_F(F^n)$ is a simple ring since its ideals are of the type $M_n(I)$, where I is an ideal of F, so $I = 0, F$. $M_{m\times n}(F) \cong F^{nm} = Y_1 \oplus \cdots \oplus Y_n$ as modules, where $Y_i = M_n(F)E_{ii}$ is the simple sub-module of matrices having zero columns except for the ith column.

9. Center $Z(M_n(F)) = Z(F)$ (by considering $E_{rs}T = TE_{rs}$, to get $a_{rr} = a_{ss}$).

10. $\mathrm{Hom}_{F_1}(X_1) \cong \mathrm{Hom}_{F_2}(X_2) \Leftrightarrow F_1 \cong F_2$ and X_1,X_2 have the same dimension.

    Proof: $R := \mathrm{Hom}_F(X)$ acts faithfully simply on X; so given $\tau : R_1 \to R_2$ isomorphism, then R_1 also acts on X_2 faithfully simply, so there is an isomorphism $T : X_1 \to X_2$ of R_1-modules. For every $S \in R$, $TSx = STx$ gives $TST^{-1} = \tau(S)$, a morphism on X_2; in particular the maps $S_a : x \mapsto ax$, hence $TS_aT^{-1} = S_{f(a)}$; in fact $f : F_1 \to F_2$ is a 1-1 ring morphism; conversely, $T^{-1}S_aT = S_b$, so f is invertible. So $T(\lambda v) = S_{f(\lambda)}Tv = f(\lambda)Tv$. Thus every k linearly independent vectors in X_1 correspond to k linearly independent vectors in X_2, so must have the same dimension.

    Thus F can be thought of as linear maps of simple modules ($F \cong \mathrm{Hom}_F(F)$).

11. $R \leqslant \mathrm{Hom}_F(X)$ is 1-transitive $\Rightarrow$ R is primitive.

4.1.2 Projective Spaces

are the spaces PX of subspaces $[\![x]\!]$ of a vector space X.

PY is a projective subspace, when Y is a subspace of X; the dimension of PY is defined as one less than the dimension of Y. Projective subspaces of dimension 0 are called *points*, of dimension 1 are called *lines*, 2 *planes*, etc.

$[\![x]\!], \ldots, [\![y]\!]$ are said to be linearly independent when $x, \ldots, y$ are linearly independent in X.

There is exactly one n-plane passing through $n + 2$ generic points (i.e., any $n + 1$ points being linearly independent), in particular there is exactly one line passing through any two independent points in PX (namely $[\![x, y]\!]$); there is exactly one point meeting two lines in a plane.

Linear maps induce maps on PX by $T[\![x]\!] = [\![Tx]\!]$; eg $\lambda[\![x]\!] = [\![x]\!]$; the set of such maps $PGL(X) = GL(X)/[\![\lambda]\!]$ (ie $S = T$ in $PGL \Leftrightarrow S = \lambda T$ in GL);

The *cross-ratio* of 4 collinear points is $(x, y; u, v) := \alpha/\beta$ where $x\wedge u = \alpha x\wedge v$, $y \wedge u = \beta y \wedge v$; it is invariant under $PGL(X)$.

A **finite geometry** is a set of points and lines such that every line has $n+1$ points and every point has $n + 1$ lines; there must be $n^2 + n + 1$ points (and lines); for example, projective planes of finite division rings $\mathbb{F}_n$. e.g. $n = 1$ is the triangle, $n = 2$ is the Fano plane.

- A finite geometry has the Desargues property (Aa, Bb, Cc are concurrent $\Leftrightarrow$ $AB \cap ab$, $BC \cap bc$, $CA \cap ca$ are collinear) $\Leftrightarrow$ it is embedded in some projective plane PF^3.

- A finite geometry has the Pappus property (two lines ABC, abc give another line $Ab \cap aB$, $Bc \cap bC$, $Ca \cap cA$) $\Leftrightarrow$ it is embedded in a projective plane PF^3 with F a field.

4.2 Local Rings

A *local ring* is one such that the non-invertibles form an ideal J.

1. Equivalently,

   (a) The sum of any two non-invertibles is non-invertible

   (b) Either x or $1-x$ is invertible

   (c) There is a single maximal left ideal.

   Proof: (b) $\Rightarrow$ (c) Let M be a maximal left ideal and $x \notin M$, then $M+Rx = R$ so $1 = a + bx$ gives $bx = 1 - a$ is invertible, making $cx = 1$ for some c; both x and c are invertible else $(c-1)x = 1 - x$ gives a contradiction; so every proper left ideal is contained in M. (c) $\Rightarrow$ (lr) If M is the unique maximal left ideal, then it is the radical (ideal) and R/M is a division ring, hence for each $x \in R \smallsetminus M$, there is a y, $1 - xy \in M$, quasinilpotent, which implies xy $(= yx)$, and thus x, are invertible.

2. Every left (or right) invertible is invertible (since $1 \in Ru \;\Rightarrow\; u \notin J$).

3. The radical is J, which is the maximal ideal.

4. R/I is again a local ring. R/J has no left ideals (a division ring).

5. Local rings have only trivial idempotents, so are indecomposable and have no proper co-prime ideals (since e or $1-e$ must be 1).

6. In any ring, if $\mathrm{prad}(I)$ is maximal, so is the only prime ideal that contains I, then R/I is a local ring.

Examples: $F[[x]]$ ($J = xF[[x]]$, for F a division ring); $\mathbb{Z}_{p^n}$ ($J = p\mathbb{Z}_{p^n}$); $\mathbb{F}_p[G]$ with G a p-group ($J = \{ (a_n) : \sum_n a_n = 0 \}$); $\mathbb{Q}_{(p)}$ fractions that omit a prime p from the denominator ($J = p\mathbb{Z}_{(p)}$).

4.3 Semi-Prime Rings

are rings in which $\mathrm{Prime}(R) = \bigcap_i P_i = \{ 0 \}$ (P_i prime ideals), i.e., $I^n = 0 \;\Rightarrow\; I = 0$, or $I \cdot J = 0 \;\Rightarrow\; I \cap J = 0$.

Thus R is embedded in $\prod_i R_i$ where $R_i = R/P_i$ are **prime rings**, i.e., have the property $I \cdot J = 0 \;\Rightarrow\; I = 0$ OR $J = 0$.

The matrix ring of a semi-prime (or prime) ring is again semi-prime (or prime). So is $R[x]$.

For any ring, $R/\mathrm{Prime}(R)$ is a semi-prime ring. *Reduced rings* are rings whose only nilpotent is 0; so $\mathrm{Prime}(R) \subseteq \mathrm{Nil}(R) = 0$.

4.4 Semi-primitive Rings

are rings in which $\mathrm{Jac}(R) = \bigcap_i P_i = \{0\}$ (P_i primitive ideals), i.e., there are no quasi-nilpotents (hence semi-prime).

Examples: $\mathbb{Z}$; any finite product of simple rings; for any ring, $R/\mathrm{Jac}(R)$ is a semi-primitive ring; any ring where the sum of invertibles is again invertible or 0 (since $1+a$ invertible implies $a=0$), such as $F\langle x,y\rangle$.

R is embedded in $\prod_i R_i$ where $R_i = R/P_i$ are **primitive rings**, i.e., $\{0\}$ is a primitive ideal, or equivalently $[M:R]=0$ for some maximal left-ideal M. Thus a primitive ring acts faithfully on the simple module $X := R/M$ (since $\mathrm{Annih}(X) = [M:R] = 0$). (Conversely, if X is a simple module, $R/\mathrm{Annih}(X)$ is a primitive ring.)

Of course, primitive rings are prime rings and semi-primitive ($\mathrm{Jac}(R) = \bigcap_{M \text{ max}}[M:R] = 0$). A prime ring R acting faithfully on a module of finite length must be primitive; let $I_n := \mathrm{Annih}(M_i/M_{i-1})$. $M_n(R)$ is again primitive ($[M_n(I) : M_n(R)] = M_n[I:R] = 0$).

The action of a semi-primitive ring gives a semi-primitive module. R acts faithfully on a semi-simple module (e.g. on $\sum_i X_i$ where X_i are non-isomorphic simple modules, so $\mathrm{Annih}(X) = \bigcap_i \mathrm{Annih}(X_i) = \mathrm{Jac}(R) = 0$).

4.4.1 von Neumann ring

is a ring in which every element is regular $a = aba$, $\exists b$.

Equivalently, every $\langle x_1, \ldots, x_n\rangle = Re$ for some idempotent e. Proof: If $Ra = Re$, then $a = be$ and $e = ca$; so $aca = ae = be = a$. Conversely, Given $x = xax$, then $e := ax$ is an idempotent and $x = xe$, so $Re \leqslant Rx \leqslant Re$. Given $Re_1 + Re_2$, then $Re_2(1-e_1) = Rf$; clearly, $R(e_1+f) \subseteq Re_1 + Re_2(1-e_1) \subseteq Re_1 + Re_2$;

$$\begin{aligned} a_1e_1 + a_2e_2 &= a_1e_1 + a_2e_2e_1 + a_2e_2(1-e_1) \\ &= r_1e_1 + rf \\ &= r_1(e_1+f) + (r-r_1)f(e_1+f) \end{aligned}$$

shows $Re_1 + Re_2 = R(e_1+f)$.

They are semi-primitive (since $a \in J \;\Rightarrow\; Ra = Re$, so $e \in J$, $1-e$ is invertible, and thus $e = (1-e)^{-1}0 = 0$).

Examples: division rings; $M_n(F)$ (use Gaussian elimination to write any matrix $A = UJV$, then $A(UV)^{-1}A = A$); Boolean lattices.

$\mathrm{Hom}_F(X)$ is von Neumann, primitive, but not simple.

4.4.2 Simple Rings

have trivial ideals.

1. Simple rings are primitive (since the core of any maximal left ideal must be 0).

2. The center $Z(R)$ is a field (proof: if $a \in Z \smallsetminus 0$, then the ideal $Ra = R$, so $1 = ba$ invertible; for any $c \in R$, $(ca^{-1} - a^{-1}c)a = 0$, so $ca^{-1} = a^{-1}c$).

3. Ring-morphisms to/from a simple ring are 0 or 1-1/onto.

4. $M_n(R)$ is again simple.

5. Similarly to semi-primitive rings, a ring with a trivial $\mathrm{Br}(R)$ ideal is embedded in a product of simple rings.

(Note: simple rings need not be Artinian or Noetherian or semi-simple, e.g. the Weyl algebra.)

4.5 Noetherian Rings

when R is Noetherian as a (left) module.

1. (Levitzky) Nilp = Prime = Nil

   Proof: The number of nilpotent ideals in the sum $N := \mathrm{Nilp}(R)$ must be finite, hence N is a nilpotent ideal. Let I be a nil ideal which is not in N; pick $a \in I \smallsetminus N$ which makes $[N : a]$ maximal. If $[N : a] = R$ then $a \in N$; otherwise for any $x \in R$, if $ax \in I \smallsetminus N$, then there is an n such that $(ax)^n \in N$ but $(ax)^{n-1} \notin N$ since ax is nilpotent; so $ax \in [N : (ax)^{n-1}] = [N : a]$; in any case, $axa \in N$, so $\langle a \rangle^2 \subseteq N$ making $\langle a \rangle$ nilpotent and $a \in N$. Thus $I \subseteq N$.

   Hence $\mathrm{prad}(I)^n = I, \exists n$ (working in R/I).

2. R/I and I are again Noetherian, but subrings need not be.

3. Every finitely generated R-module is Noetherian.

4. A Noetherian ring is isomorphic to $R\langle x_1, \ldots, x_n \rangle / I$ for some finitely generated left ideal I (so has a presentation).

5. (Hilbert basis theorem) $R[x_1, \ldots, x_n]$ is again Noetherian (also $R[[x]]$).

   Proof: Let I be a left ideal of $R[x]$; choose polynomials $p_{n+1} \in I$, each of minimal degree in $J_n := \langle p_1, \ldots, p_n \rangle$. Then the left ideal of their leading coefficients $\langle a1, a2, \ldots \rangle \subseteq R$ is finitely generated, say by the first n terms. Then $a_{n+1} = \sum_{i=1}^n b_i a_i$; let $q(x) := \sum_{i=1}^n b_i x^{r(i)} p_i(x) \in J_n$, where $r(i) = \deg(p_{n+1}) - \deg(p_i)$. Yet $q - p_{n+1} \in J_n$ has degree less than p_{n+1}. Thus $I = J_n$ is finitely generated.

6. $M_n(R)$ is again Noetherian.

7. (Jacobson's conjecture: $\bigcap_n \mathrm{Jac}^n = 0$.)

8. $\mathbb{Z}$ is Noetherian semi-primitive but not Artinian. $\begin{pmatrix} \mathbb{Z} & \mathbb{Q} \\ 0 & \mathbb{Q} \end{pmatrix}$ is right, but not left, Noetherian.

4.5.1 Artinian/Finite-Length Rings

when R is Artinian as a module.

1. Every element is either invertible or a two-sided zero divisor.

   Proof: $R \geqslant Ra \geqslant Ra^2 \geqslant \cdots \geqslant Ra^n = Ra^{n+1}$. So for some $b \in R$, $(1-ba)a^n = 0$; either $1 = ba$ or a is a right zero divisor. (Similarly for b, but b cannot be a right zero divisor, so $1 = cb$, and a is invertible.) Similarly, a is either right invertible or a left zero divisor.

2. Nilp = Prime = Nil = Jac = Br, so nil ideals are nilpotent, prime ideals are maximal, and quasi-nilpotents are nilpotents.

   Proof: For $J := \mathrm{Jac}(R)$, $J \geqslant J^2 \geqslant \cdots \geqslant J^n = J^{n+1}$. Suppose $J^n \neq 0$, then let I be minimal among those ideals with $J \cdot I = I \neq 0$. So there is an $a \in I$, $Ja \neq 0$; $J \cdot J^n a = J^n a$ implies $I = J^n a$, so $a = ba$ with $b \in J^n \subseteq J$. Thus $(1-b)a = 0$, hence $a = 0$ since b is quasi-nilpotent. This contradiction gives $J^n = 0$. Now R/J is semi-primitive so $\mathrm{Br}(R/J) = 0$, i.e., there are no maximal ideals that contain J properly, and $\mathrm{Br}(R) = J$.

3. Every Artinian R-module is Noetherian (and so of finite length). In particular, Artinian rings are Noetherian.

   Proof: For $J := \mathrm{Jac}(R)$, $X \geqslant JX \geqslant J^2X \geqslant \cdots J^nX = 0$. If $Y = J^iX$ is Artinian and $JY = J^{i+1}X$ is Noetherian, then the semi-primitive ring R/J acts on Y/JY as an Artinian semi-primitive module, so is Noetherian. Thus Y is Noetherian, and by induction, X is too.

4. Every finitely generated R-module is of finite length.

5. Semi-prime Artinian rings are semi-simple; and prime rings are simple (since semi-simple).

6. For R Artinian, $M_n(R)$ and $R[G]$ for G finite (Connel), are again Artinian, e.g. $F[x]/\langle x^n \rangle$.

4.5.2 Semi-simple rings

when R is a sum of minimal left ideals.

R is of finite length (since $1 \in \sum_{i=1}^n I_i$). Every left ideal is Re for some (central) idempotent (hence von Neumann).

1. Equivalently, a semi-prime Artinian ring, or a von Neumann Noetherian ring.

   Proof: If R is semi-simple then $R \cong \mathrm{Hom}_R(R)$ is von Neumann and semi-primitive. Conversely, every left ideal I of a Noetherian ring is finitely generated, hence of the type Re where e is an idempotent (von Neumann); so I is complemented by $R(1-e)$. Otherwise,semi-prime Artinian rings are semi-primitive Artinian, thus semi-simple.

2. An R-module is again semi-simple ($X = \sum_{x\in X} Rx$ with $Rx \cong R/\mathrm{Annih}(x)$ semi-simple, so X is a sum of simple modules.)

3. $M_n(R)$ is again semi-simple.

   Proof: $M_n(R) = I_1 \oplus \cdots \oplus I_n$ where I_i consists of matrices that are zero except for ith column. $I_i \cong R^n$ which is semi-simple.

4. Every primitive Artinian ring is of the type $M_n(F)$, where F is a division ring, thus simple.

   Proof: A primitive Artinian ring is prime, hence simple, of finite length $R \cong I^n$ for some minimal left ideal $I = Re$; so $R \cong \mathrm{Hom}_R(I^n) = M_n(F)$ where $F = \mathrm{Hom}_R(I) = eRe$ is a division ring with e as identity.

5. *Proposition* 3

   (Wedderburn)

   A semi-simple ring is the finite product of matrix rings over division rings

   $$R \cong \mathrm{Hom}_R(R) \cong M_{n_1}(F_1) \times \cdots \times M_{n_k}(F_k)$$

   Each matrix ring is different unless the ring is simple Artinian. That is, $R \cong B_1 \times \cdots \times B_r$ where $B_i = I_i^{n_i} = I_i \oplus \cdots \oplus I_i \cong M_{n_i}(F_i)$, $F_i = \mathrm{Hom}_R(I_i)$, each I_i is a vector space over F_i. All the simple left ideals of R are isomorphic to one of I_i (since $I = Ra \cong R/\mathrm{Annih}(a)$, so $R = I \oplus \mathrm{Annih}(a)$, so I appears in the sum of R).

6. If R has no nil ideals, then $R[x]$ is semi-simple.

7. (Maschke) $R[G]$ (G group) is semi-simple iff G is finite and $|G|$ is invertible in R. Thus, $\mathbb{Z}[G]$ is not semi-simple, $\mathbb{C}[G] \cong M_n(\mathbb{C}) \times \cdots \times M_m(\mathbb{C})$ (irreducible representations of G, one for each conjugacy class).

4.5.3 Finite rings

The simple finite rings are $M_n(\mathbb{Z}_p)$. A finite ring R of size $n = p_1^{r_1} \cdots p_k^{r_k}$ is the product of rings of size $p_i^{r_i}$ (each $R_i \cong \{\, a \in R : p_i^m a = 0, \exists m \,\}$). So the classification of finite rings depends on finding those of size p^n.

1. p – only one ring (field) $\mathbb{Z}_p$.
2. p^2 – $\mathbb{Z}_{p^2}$, $\mathbb{Z}_p \times \mathbb{Z}_p$, $[\![a : p1 = 0, a^2 = 0]\!]$, $\mathbb{F}_{p^2}$.
3. p^3 – 12 rings for $p > 2$, 11 for $p = 2$.

(There are many more ‘rings’ without an identity.)

5 Commutative Rings

$$xy = yx$$

Products and subrings are obviously commutative. For example, $\mathbb{Z}_n$.

1. Binomial theorem:

   $$(x+y)^n = x^n + nx^{n-1}y + \cdots + \binom{n}{k} x^k y^{n-k} + \cdots + nxy^{n-1} + y^n$$

   For example, if the prime sub-ring is $\mathbb{Z}_p$ (p prime), then $x \mapsto x^p$ is a morphism.

2. There is no distinction between ideals and left/right ideals; so $I \cdot J = J \cdot I$, $\mathrm{Br}(R) = \mathrm{Jac}(R)$.

3. $\langle a \rangle = Ra$; $\langle a \rangle \langle b \rangle = \langle ab \rangle$; $\langle a \rangle = R \Leftrightarrow a$ is invertible $\Leftrightarrow \forall x, a|x$.

4. P is a prime ideal when $xy \in P \;\Rightarrow\; x \in P$ OR $y \in P$ (i.e., X/P has no zero-divisors).

   p is called *prime* when $\langle p \rangle$ is prime, i.e., $p|xy \;\Rightarrow\; p|x$ OR $p|y$.

5. If $I \leqslant P_1 \cup \cdots \cup P_n$ then $I \leqslant P_i$ for some i.

   Proof: Take n to be minimal, i.e., $\exists a_i \in I \cap P_i$, $a_i \notin P_j$ $(j \neq i)$. Then $a_2 \cdots a_n \in I \cap P_2 \cap \cdots \cap P_n$ but not in P_1, so $a_1 + a_2 \cdots a_n \in I$ but not in $P_1 \cup \cdots \cup P_n$; hence $n = 1$.

6. S is a semi-prime ideal when $x^n \in S \;\Rightarrow\; x \in S$, that is when S is a radical ideal.

7. $\langle a \rangle$ is nilpotent iff a is nilpotent.

8. The sum of two nilpotents is again nilpotent (by the binomial theorem), so the set of all nilpotents is an ideal, in fact $\mathrm{Nil}(R) = \mathrm{Prime}(R)$ (since $a^n = 0 \in P \;\Rightarrow\; a \in P$).

   More generally, $r(I)$ is an ideal, so $\mathrm{prad}(I) = r(I)$.

9. If I_i are mutually co-prime, then $I_1 \cdots I_n = I_1 \cap \cdots \cap I_n$ (by induction on $I \cap J = I \cdot J + J \cdot I = I \cdot J$). In particular, for p, q co-prime, i.e., $\langle p \rangle + \langle q \rangle = R$, $pq|x \Leftrightarrow p|x$ AND $q|x$.

   For modules, $IX \cap JX = (I \cdot J)X$ (since $x \in IX \cap JX \;\Rightarrow\; x = ax + bx \in IJX + JIX = IJX$), so $X/(IJX) \cong X/IX \times X/JX$.

   If $I + J = R$ and $I \cdot J = K^n$ then $I = L^n$ (with $L = I + K$).

10. For a regular element, $a = a^2 u$ with u invertible. The regular elements are closed under multiplication; there are no regular nilpotent elements except 0.

    Proof: If $a = a^2 b$, take $u := 1 - ab + ab^2$, with $u^{-1} = 1 - ab + a.ac = a^2bc^2d = (ac)^2(bd)$. $a^{n-1} = a^{2(n-1)}b^{n-1} = 0$.

11. a is said to be *irreducible* when $a = xy \Rightarrow a \approx x$ OR $a \approx y$ (i.e., equality up to invertible elements); equivalently, $\langle a\rangle$ is maximal with respect to principal ideals, $\langle a\rangle \subset \langle x\rangle \Rightarrow \langle x\rangle = R$. Otherwise a is called *composite* when $\langle a\rangle \subset \langle b\rangle$.

12. $r\langle p_1^{m_1} \cdots p_n^{m_n}\rangle = \langle p_1 \cdots p_n\rangle$ for p_i co-prime primes.

    Proof: $pq \in r\langle p^s q^t\rangle$ since $(pq)^{\max(s,t)} \in \langle p^s q^t\rangle$; conversely, if $x^m \in \langle p^s q^t\rangle \subseteq \langle p\rangle \cap \langle q\rangle$, then $x \in \langle p\rangle \cap \langle q\rangle = \langle pq\rangle$.

13. A **primary** ideal is defined as one such that

$$ab \in Q \;\Rightarrow\; a \in Q \text{ OR } b \in Q \text{ OR } a, b \in r(Q)$$
$$ab \in Q \;\Rightarrow\; a \in Q \text{ OR } b \in r(Q)$$

    i.e., R/Q has invertibles or nilpotents only (so is a local ring).

    Examples include prime ideals and $\langle p^n\rangle$ for any prime element.

    (a) Q primary $\Rightarrow$ $r(Q)$ prime.

    Proof: $ab \in r(Q) \Rightarrow a^n b^n \in Q$, so if $a \notin r(Q)$ then $a^n \notin Q$, so $b^n \in r(Q)$, i.e., $b \in r(Q)$.

    (b) But various primary ideals Q may induce the same prime $r(Q)$. If $a \notin Q$ then $[Q : a]$ is also primary and $r[Q : a] = r(Q)$.

    Proof: If $bc \in [Q : a]$ but $c \notin [Q : a]$ then $abc \in Q$, $ac \notin Q$, so $b^n \in Q \subseteq [Q : a]$. If $b \in [Q : a]$ ($ab \in Q$) then $b \in r(Q)$, so $Q \subseteq [Q : a] \subseteq r(Q)$, and $r(Q) = r[Q : a]$.

    (c) $r(I)$ maximal $\Rightarrow$ I primary.

    Proof: If $ab \in I$ but $b \notin r(I)$ then $r(I)+\langle b\rangle = R$, so $1 = cb+d$, $d^n \in I$, and $a(1-d) \in I$. Let $r := 1 + d + \cdots + d^{n-1}$, so $r(1-d) = 1-d^n$; then $a = ra(1-d) + ad^n \in I$.

    (d) Thus powers of maximal ideals are primary: $r(M^n) = r(M) = M$.

14. Primitive ideals are maximal (since a maximal 'left' ideal is its own core), and primitive rings are simple.

15. A simple commutative ring is called a **field**. A commutative

    (a) semi-primitive ring is embedded in a product of fields,

    (b) semi-simple ring is a finite product of fields,

    (c) von Neumann ring is reduced, and localizes at any maximal ideal to a field.

16. $R[x]$ is again commutative but $M_n(R)$ is only commutative for $n = 1$ or $R = 0$ since $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

5.0.4 Modules over Commutative Rings

1. In a free module X, if A is linearly independent and B spans, then $|A| \leqslant |B|$. Hence any two bases of X have the same cardinality, called its *dimension* $\dim X$.

   Proof: Let I be a maximal ideal of R, then $V := X/(I \cdot X)$ is a vector space over the field R/I; also $x_i + I \cdot X$ ($x_i \in B$) generates V and $y_i + I \cdot X$ ($y_i \in A$) remain linearly independent, hence $|A| \leqslant |B|$.

2. A *torsion* element x of a module is one such that there is a cancellative $a \in R$, $ax = 0$. The set of torsion elements is a sub-module X_{tor}. X/X_{tor} is torsion-free.

   Proof: $ax = 0 \pmod{X_t}$ implies $ax = y \in X_t$, so $bax = by = 0$; but ba is cancellative, so $x = 0 \pmod{X_t}$.

3. A sub-module Y is *primary* when $ax \in Y \;\Rightarrow\; x \in Y$ OR $a^n X \subseteq Y$. Then $\text{Annih}(X/Y)$ is a primary ideal.

4. The *dual space* $X^\top := \text{Hom}_R(X, R)$ is an R-module. There are dual concepts for subsets $A \subseteq X$, $\Phi \subseteq X^\top$, and linear maps $T \in \text{Hom}_R(X, Y)$:

$$\begin{aligned} &A^\circ := \{\, \phi \in X^\top : \phi A = 0 \,\}, \quad \text{sub-module of } X^\top, \\ &\Phi^\circ := \{\, x \in X : \Phi x = 0 \,\}, \quad \text{sub-module of } X, \\ &T^\top : Y^\top \to X^\top, \quad \phi \mapsto \phi \circ T, \quad \text{linear map.} \end{aligned}$$

   (a) $\Phi \leqslant A^\circ \;\Leftrightarrow\; A \leqslant \Phi^\circ$, so the dual maps are adjoints; hence $A \subseteq B \;\Rightarrow\; B^\circ \subseteq A^\circ$; $[\![A]\!] \subseteq A^{\circ\circ}$, $[\![A]\!]^\circ = A^\circ$; $(A \cup B)^\circ = A^\circ \cap B^\circ$; $(A \cap B)^\circ \supseteq A^\circ + B^\circ$;

   (b) $(A \times B)^\circ = A^\circ \times B^\circ$; $X^\top / A^\circ \cong [\![A]\!]^\top, (X/Y)^\top \cong Y^\circ$;

   (c) $T \mapsto T^\top$ is a linear map; $(ST)^\top = T^\top S^\top$; $(T^{-1})^\top = (T^\top)^{-1}$; $\ker T^\top = (\operatorname{Im} T)^\circ$;

   (d) the map $X \to X^{\top\top}$, $x^{\top\top}(\phi) := \phi(x)$ is linear, and then it also maps $A \to A^{\circ\circ}$, and $T \mapsto T^{\top\top}$;

5. Given $T : X \to X$ linear, we can consider the action of $R[T]$ on X (a submodule); Y is a submodule of X in this action $\Leftrightarrow$ $TY \subseteq Y$; then T can be defined on X/Y via $T(x + Y) = Tx + Y$.

5.0.5 Polynomials

1. Polynomials become functions: they can be *evaluated* at any element a using the morphism $R[x] \to R$, $p \mapsto p(a)$.

2. Division algorithm: Every polynomial p can be divided by a monic polynomial s to leave unique *quotient* and *remainder*

$$p = qs + r, \quad \deg r < \deg s.$$

In particular, $p(x)=q(x)(x-a)+p(a)$, and $p(a)=0 \Leftrightarrow p\in\langle x-a\rangle$.

Proof: Let $s(x):=x^m+b_{m-1}x^{m-1}+\cdots+b_0$, then

$$\begin{aligned}p(x)&=a_nx^n+\cdots+a_0\\&=a_nx^{n-m}(x^m+\cdots+b_0)+(c_{n-1}x^{n-1}+\cdots+c_0),\\&=a_nx^{n-m}s(x)+r_{n-1}(x)\end{aligned}$$

where $r_{n-1}=q's+r$ by induction, so $p=(a_nx^{n-m}+q')s+r$.

3. Translation $\tau_a : x\mapsto x+a$ is an automorphisms on $R[x]$:

$$p(x+a)=p(a)+b_1(a)x+b_2(a)x^2+\cdots+b_n(a)x^n,$$
$$\text{where } b_r(a)=\sum_{k=r}^{n}\binom{k}{r}a_ka^{k-r}$$

4. When $(x-\alpha_1)\cdots(x-\alpha_n)$ is expanded out, its $(n-i)$th coefficient is a symmetric polynomial in α_i, $(-1)^i\sum_{j_1<\cdots<j_i}\alpha_{j_1}\cdots\alpha_{j_i}$.

5. A polynomial is nilpotent iff the ideal generated by its coefficients is nilpotent. A monic polynomial is invertible only when it has degree 0.

6. a is called a *root* or *zero* of $p\neq 0$ when $p(a)=0$. It is said to be a *multiple* root of p when $p\in\langle(x-a)^r\rangle$, i.e., $b_i(a)=0$ for $i=0,\ldots,r-1$.

   Polynomials may have any number of roots, e.g. in $\mathbb{Z}_6[x]$, x^2+1 has no roots, x^n has one root, $x^2+x=x(x+1)=(x-2)(x-3)$ has 4, x^3-x has 6 roots; in $\mathbb{H}[x]$, x^2+1 has an infinite number of roots $ai+bj+ck$ with $a^2+b^2+c^2=1$).

7. (a) If p is of degree $\geqslant 2$ and has a root then it is reducible.
   (b) If it is monic of degree $\leqslant 3$ and has no roots, then it is irreducible (otherwise a factor must have degree 1);
   (c) Monic polynomials of degree $\geqslant 4$ may be reducible yet have no roots, e.g. $x^4+4=(x^2+2x+2)(x^2-2x+2)$, $x^4+x^2+1=(x^2+x+1)(x^2-x+1)$ in $\mathbb{Z}[x]$.

8. If a satisfies a monic polynomial with coefficients b_i, then a is said to be *integral* over the sub-ring $[\![b_0,\ldots,b_n]\!]$. For example, an *algebraic integer* is an element that satisfies some $p\in\mathbb{Z}[x]$.

5.0.6 Ring of Fractions

Given any subset $S\subseteq R$ that is cancellative (contains no zero divisors), the ring is embedded in a larger ring in which elements of S become invertible: extend S to contain all its products and 1 (it will not contain 0) and take the *localization* ring $S^{-1}R$ to be $R\times S$, with element pairs (x,a) denoted by x/a or $\frac{x}{a}$, in which

$$\frac{x}{a}=\frac{y}{b}\Leftrightarrow bx=ay$$

$$\frac{x}{a} + \frac{y}{b} := \frac{xb + ya}{ab}, \qquad \frac{x}{a}\frac{y}{b} := \frac{xy}{ab}$$

so $(a/1)^{-1} = 1/a$, and the map $x \mapsto x/1$ is an embedding of R. The same construction applies to localization of a module $S^{-1}X$, with X replacing R and $S \subseteq R$ not annihilating any element of X ($\forall a \in S, ax = 0 \Rightarrow x = 0$). Typical localizations are:

- The *ring of fractions* $\text{Frac}(R)$ is the localization of the (multiplicative) set of all cancellative elements (thus all non zero divisors become invertible). For example, the ring of fractions of $\mathbb{Z}$ is $\mathbb{Q}$; that of $\mathbb{Z}[\sqrt{d}]$ is $\mathbb{Q}[\sqrt{d}]$, of $\mathbb{F}[x]$ consists of the 'rational' functions $p(x)/q(x)$.
- The localization R_P at a prime ideal P, with $S := R \smallsetminus P$ (multiplicative); $S^{-1}R$ is a local ring with radical $S^{-1}P$. The sub-ideals of P remain intact in $S^{-1}R$ but all sup-ideals vanish. For example, $S_p^{-1}\mathbb{Z}$ with $S_p = \| \smallsetminus \langle p \rangle$ gives $\mathbb{Q}_{(p)}$.
- The localization at a single cancellative element x is $R[x^{-1}]$ (using $S := \{1, x, x^2, \ldots\}$); e.g. $\mathbb{Z}$ at $n \neq 0$ gives $\mathbb{Z}[1/n]$.

1. $S^{-1}(X+Y) = S^{-1}X + S^{-1}Y$, $S^{-1}(X \cap Y) = S^{-1}X \cap S^{-1}Y$, $S^{-1}(X/Y) \cong S^{-1}X/S^{-1}Y$.
2. $\text{Spec}(S^{-1}R) \subseteq \text{Spec}(R)$.
3. $\bigcap_{M \text{ maximal}} R_M = R$.
4. The ring of fractions of a local ring with radical P can be given a natural uniform topology from the base P^m, making it a topological ring, called the P-adic ring; when the ring is Noetherian, the topology is T_2.
5. Elements of a commutative ring R can be thought of as continuous functions $C(\text{Spec}(R))$, with $f_a(P) := a + P \in \text{Frac}(R/P)$.

5.1 Noetherian commutative rings

1. Irreducible ideals are primary.

   Proof: Let I be irreducible and $ab \in I$; then

   $$[I : b] \leqslant [I : b^2] \leqslant \cdots \leqslant [I : b^n] = [I : b^{n+1}]$$

   so $I = (\langle a \rangle + I) \cap (\langle b^n \rangle + I)$ since $c = ra = sb^n \pmod I$ implies $cb = 0 = sb^{n+1} = sb^n = c \pmod I$, so $c \in I$; thus either $I = \langle a \rangle + I$ or $I = \langle b^n \rangle + I$.
2. Every primary ideal Q satisfies $r(Q^n) \subseteq Q$ for some n (since nil ideals are nilpotent).
3. $S^{-1}R$ is Noetherian/Artinian when R is.

4. For any R-module X, the maximal elements in the set of annihilators $\text{Annih}(x)$, $x \neq 0$, are prime ideals $\text{Annih}(x_0)$, called the *associated prime ideals* of X.

   Proof: If $ab \in P := \text{Annih}(x_0)$ but $b \notin P$, then $bx_0 \neq 0$ yet $abx_0 = 0$, but $\text{Annih}(bx_0) \geqslant \text{Annih}(x_0) = P$, so $a \in \text{Annih}(bx_0) = P$.

Proposition 4

(Lasker-Noether)

Every proper ideal has a decomposition into primary ideals, $I = Q_1 \cap \cdots \cap Q_n$, with distinct and unique $r(Q_i)$, and no Q_i contains the intersection of the other primary ideals.

Proof: Every such ideal can be decomposed into a finite number of irreducible ideals, since R is Noetherian; if $r(Q_1) = r(Q_2) = P$ then $Q_1 \cap Q_2$ is still primary and $r(Q_1 \cap Q_2) = P \cap P = P$, so one can assume each Q has a different $r(Q)$; if $Q_i \supseteq \bigcap_{j \neq i} Q_j$ then remove it.

More generally, given a finitely generated R-module, every sub-module is the finite intersection of primary sub-modules: decompose $Y = M_1 \cap M_2$ and continue until the remaining sub-modules cannot be written as an intersection; for such "irreducible" sub-modules X/M_i is primary.

5.1.1 Finite Length (Artinian) commutative rings

1. Prime ideals = Maximal (since R/P is Artinian but has no zero divisors, so is simple, i.e., P is maximal).

2. Their spectrum is finite.

3. They are a finite product of local Artinian rings (since Jac is the finite intersection of maximal ideals; so $0 = \prod_i M_i^k = \bigcap_i M_i^k$, so R is isomorphic to a finite product of R/M_i^k which are local, by CRT).

4. $R/\text{Jac}(R)$ is isomorphic to a finite product of fields (since primitive commutative rings are fields).

5.2 Integral Domains

are cancellative commutative rings, so without proper zero divisors,

$$xy = 0 \;\Rightarrow\; x = 0 \text{ or } y = 0$$

Equivalently, $[\![0]\!]$ is prime, i.e., a commutative prime ring.

(More generally, semi-prime commutative rings have $\text{Nil} = 0$; equivalently reduced commutative rings.)

Subrings are again integral domains. The smallest sub-ring is either $\mathbb{Z}$ or $\mathbb{Z}_p$, called the *characteristic* of R ($\mathbb{Z}_{pq}$ has zero divisors).

Examples include $\mathbb{Z}$, and the center of any prime ring.

1. There are no non-trivial idempotents, so indecomposable. There are no proper nilpotents, so $\mathrm{Nil} = 0$.

2. All ideals are isomorphic as modules, using $Ra \to Rb$, $xa \mapsto xb$.

3. Divisibility becomes an order (mod the invertible elements) i.e., $x|y$ AND $y|x \Rightarrow x \approx y$; an inf of two elements is called their *greatest common divisor*, a sup is called their *lowest common multiple*.

4. Prime elements are irreducible ($p = ab \Rightarrow p|a$ (say) $\Rightarrow pr = a \Rightarrow prb = ab = p \Rightarrow rb = 1$).

5. The ring of fractions $\mathrm{Frac}(R)$ is a field; so integral domains are subrings of fields.

6. $R[x]$ is again an integral domain; its field of fractions is $R(x)$; that of $R[[x]]$ is $R((x))$ (Laurent series). The invertibles of $R[x]$ are the invertibles of R.

7. Any polynomial of degree n has at most n roots.

   Proof: By the division algorithm, $p(x) = q(x)(x - a_1)^{r_1}$, so $q(a_2) = 0$; repeating this process must end after at most n steps since the degree of q decreases each time.

8. Every polynomial in $R[x_1, \ldots, x_n]$ can be rewritten with highest degree y_n^m, under the change of variables $y_i := x_i + x_n^{r^i}$, $y_n := x_n$ for large enough r.

9. For X finitely generated, X is torsion-free iff it is embedded in some finitely generated free module.

   Proof: $X = [\![x_1, \ldots, x_n]\!]$, split them into $x_1, \ldots, x_s$ linearly independent and the rest depend on them; so $Y := [\![x_1, \ldots, x_s]\!] \cong R^s$ is free; $a_{s+i}x_{s+i} \in Y$, so $T_{a_s \cdots a_r}X \subseteq Y$ with T 1-1; so X is embedded in Y.

10. Finite Integral Domains are fields (see later).

5.2.1 GCD Domains

are integral domains in which divisibility is a semi-lattice relation (up to invertible elements): any two elements have a gcd $x \wedge y$ and an lcm $x \vee y$.

1. (a) $(ax) \wedge (ay) = a(x \wedge y)$, (since $a|ax, ay$ so $ab = (ax \wedge ay)$, so $ab|ax, ay$ and $b|x, y$, hence $ab|a(x \wedge y)$), so they are lattice monoids,

   (b) $x \wedge y = 1$ AND $x|yz \Rightarrow x|z$ (since $x|(xz \wedge yz) = z$),

   (c) $(xy) \wedge z = 1 \Leftrightarrow (x \wedge z) = 1 = (y \wedge z)$ (since $a|xy, z \Rightarrow a|(xz \wedge xy) = x(z \wedge y) = x$, so $a|(x \wedge z) = 1$),

(d) $x \wedge (y + xz) = x \wedge y$.

2. Irreducibles = Primes (If p is irreducible then either $p|x$ or $p \wedge x = 1$ for any x, so $p|ab$ AND $p \not| a \Rightarrow p|b$.)

3. The 'content' of a polynomial is $\mathrm{con}(p) := \gcd(a_0, \ldots, a_n)$. Every polynomial can be written as $p = \mathrm{con}(p)\tilde{p}$ where $\mathrm{con}(\tilde{p}) = 1$; such a $\tilde{p}$ is called a *primitive* polynomial.

$$\mathrm{con}(ap) = \gcd(aa_0, \cdots, aa_n) = a\,\mathrm{con}(p)$$

4. The product of primitive polynomials is primitive,

$$\mathrm{con}(pq) \approx \mathrm{con}(p)\mathrm{con}(q)$$

Proof: Let $p(x) = a_0 + \cdots + a_n x^n$ and $q(x) = b_0 + \cdots + b_m x^m$ be primitive polynomials; let $c := \mathrm{con}(pq)$, $d := c \wedge a_n$, then $d|c|pq$ and $d|a_n$, so $d|(p - a_n x^n)q$ which has a lower degree; so by induction, $d|\mathrm{con}(p - a_n x^n)\mathrm{con}(q)$; hence $d|(p - a_n x^n)$ and so $d|\mathrm{con}(p) \approx 1$. Thus $c \wedge a_n \approx 1 \approx c \wedge b_m$; but $c|a_n b_m$, so $c \approx 1$. More generally, for any p, q not necessarily primitive,$\mathrm{con}(pq) \approx \mathrm{con}(\mathrm{con}(p)\mathrm{con}(q)\tilde{p}\tilde{q}) \approx \mathrm{con}(p)\mathrm{con}(q)$.

5. A polynomial $p(x) \in R[x]$ is irreducible iff it is primitive and it is irreducible over its field of fractions, $F[x]$.

Proof: If p is reducible in $R[x]$ then either it is so in $F[x]$ or $p = \mathrm{con}(p)\tilde{p}$. Suppose $p(x) = r(x)s(x)$ with $r, s \in F[x]$; then $p(x) = \frac{a}{b}\tilde{r}(x)\frac{c}{d}\tilde{s}(x)$ where $\tilde{r}, \tilde{s} \in R[x]$ are primitive. But then $bd|\mathrm{con}(ac\tilde{r}\tilde{s}) = ac$, so $\frac{ac}{bd} \in R$ and r, s can be taken to be in $R[x]$.

Thus, a primitive polynomial $p(x) \in R[x]$ has no roots that are in the field of fractions F that are not in R.

6. (Eisenstein) A convenient test that checks whether a primitive polynomial $p(x) = a_0 + \cdots + a_n x^n$ is irreducible is: Find a prime ideal P such that $a_0, \ldots, a_{n-1} \in P$, $a_n \notin P$, $a_0 \notin P^2$.

Proof: If $p = gh$, then $gh = a_n x^n \pmod{P}$, so $b_0, c_0 = 0 \pmod{P}$ and $a_0 = b_0 c_0 \in P^2$.

Examples include $x^n - p$ (p prime), $1 + x + \cdots + x^{p^n - 1}$ (first translate by 1 to get $p + \binom{p}{2}x + \cdots + x^{p-1}$).

7. $R[x]$ is again a GCD.

Proof: Let $d := p \wedge q$ in $F[x]$; then $d|p$, $d|q$ in $F[x]$, hence in $R[x]$; and $c|p$, $c|q$ in $R[x]$ implies $c|d$ in $F[x]$, hence in $R[x]$.

5.2.2 Unique Factorization Domains

In general, one can try to decompose an element into factors $x = yz$, and repeat until perhaps one reaches irreducible elements. An integral domain has a factorization of every element into irreducibles iff its principal ideals satisfy ACC (e.g. commutative Noetherian); such factorizations are unique iff irreducibles are prime.

$$\forall x,\ \exists! p_1, \ldots, p_m \text{ prime}, \quad x \approx p_1 \ldots p_m$$

Proof: $\langle x_1 \rangle < \langle x_2 \rangle < \cdots$ is equivalent to $x_1 = a_1 x_2 = a_1 a_2 x_3 = \cdots$ with a_i not invertible. Such an x_1 can only have a finite factorization iff the principal ideals eventually stop. See Factorial Monoids for uniqueness.

Equivalently a UFD is an integral domain in which every prime ideal contains a prime.

1. UFDs are GCD domains: the gcd is the product of the common primes $(p^{\min(r_a, r_b)} \cdots)$, the lcm is the product of all the primes without repetition $(p^{\max(r_a, r_b)} \cdots)$.
2. $R[x]$ is a UFD.

   Proof: $F[x]$ is a UFD (since it is an ER), so $p \in R[x]$ has a factorization in irreducible polynomials $q_i \in F[x]$, which are in $R[x]$. This factorization is unique since irreducibles of $R[x]$ are primes.

5.2.3 Principal Ideal Domains

are integral domains in which every ideal is principal $\langle x \rangle$.

1. $\langle x \rangle + \langle y \rangle = \langle \gcd(x, y) \rangle$, $\langle x \rangle \cap \langle y \rangle = \langle \operatorname{lcm}(x, y) \rangle$. So the gcd can be written as $a \wedge b = sa + tb$ for some $s, t \in R$. For example, $\langle x \rangle$, $\langle y \rangle$ are co-prime when $\gcd(x, y) = 1$.
2. $ax + by = c$ has a solution in $R \Leftrightarrow \gcd(a, b) | c$.
3. If $R \subseteq S$ are PIDs, then $\gcd(a, b)$ is the same in both R and S (since $(a \wedge b)_S | sa + tb = (a \wedge b)_R$).
4. PIDs are Noetherian, hence UFDs.

   Proof: For any increasing sequence of ideals

   $$\langle x_1 \rangle \leqslant \langle x_2 \rangle \leqslant \cdots \leqslant \bigcup_i \langle x_i \rangle = \langle y \rangle,$$

   so $y \in \langle x_n \rangle$, implying $\langle x_n \rangle = \langle x_{n+1} \rangle = \cdots = \langle y \rangle$.
5. p is irreducible/prime $\Leftrightarrow$ $\langle p \rangle$ is maximal; i.e., prime ideals = maximal.

   Proof: If $\langle p \rangle \leqslant \langle a \rangle$, then $p = ab$ so either a or b is invertible, i.e., $\langle a \rangle = R$ or $\langle a \rangle = \langle p \rangle$.

6. But $\langle a\rangle$ is irreducible iff primary iff $\langle p^n\rangle$ for some prime p.

   Proof: If $\langle a\rangle$ is primary, then $r\langle a\rangle = \langle p\rangle$ prime; if $a = p^n q^m \cdots$ is its prime decomposition, then $q \in r\langle a\rangle = \langle p\rangle$, so $a = p^n$.

   The decomposition of ideals into primary ideals becomes $\langle a\rangle = \langle p^r\rangle \cdots \langle q^s\rangle$.

7. In general, $R[x]$ need not be a PID (unless R is a field), e.g. $\langle 1, x\rangle$ is not principal in $\mathbb{Z}[x]$.

8. Smith Normal form: Every matrix in $M_n(R)$ has a unique form for a suitable generating set of elements, $\begin{pmatrix} \lambda_1 & 0 & \\ 0 & \lambda_2 & \\ & & \ddots \end{pmatrix}$. Hence can solve linear equations in PIDs efficiently.

   Proof: Use Gaussian elimination of row/column subtractions and swaps to reduce to gcd.

9. The ideal $\mathrm{Annih}(X)$ of a module is principal $\langle r\rangle$, with r called the *order* of X.

Important examples of PIDs are **Euclidean Domains**, defined as integral domains with a 'norm' $|\cdot| : R\smallsetminus 0 \to \mathbb{N}$ and a division:

$$\forall x, y \neq 0, \exists a, r, \quad x = ay + r, \text{ where } 0 \leqslant |r| < |y| \text{ OR } r = 0$$

Proof: Let I be a non-trivial ideal; pick $y \in I$ with smallest norm; then $\forall x \in I, x = ay + r$ AND $r \neq 0 \;\Rightarrow\; r = x - ay \in I$ impossible, so $r = 0$ and $x = ay$, i.e., $I = \langle y\rangle$.

Examples include $\mathbb{Z}$ with $|n| := \begin{cases} n & n > 0 \\ -n & n < 0 \end{cases}$, and $F[x]$ with $|p| := \deg(p)$.

5.2.4 Finitely-Generated PID Modules

1. Submodules of finitely-generated free modules are also free.

   Proof: Let $Y_1 := \{\, x = (a_1, 0, \ldots) \in R^A : x \in Y \,\}$ and $Y_2 = \{\, x = (0, a_2, \ldots) \in R^A : x \in Y \,\}$, both submodules of R^A; in fact $Y_1 = [\![e_1]\!] \cong R$ (or $Y_1 = 0$); by induction $Y_2 = R^C$, so that $Y \cong R \times R^C = R^{1+C}$.

2. X is torsion-free $\Leftrightarrow$ free.

   Proof: Let $e_1, \ldots, e_n$ be generators with the first k being linearly independent; suppose $k \neq n$, then for $i > k$, $a_i e_i = \sum_j \lambda_j e_j$, let $a := a_{k+1} \cdots a_n \neq 0$, so $[\![a]\!]$ is a submodule of the free module $[\![e_1, \ldots, e_k]\!]$, so itself must be free; but $x \mapsto ax$ is an isomorphism, so $X = [\![a]\!]$ is free.

3. A finitely generated module over a PID is isomorphic to

$$X \cong R^n \times \frac{R}{\langle p^m\rangle} \times \ldots \times \frac{R}{\langle q^k\rangle}$$

where $p, \ldots, q$ are unique primes.

Proof: Let X be indecomposable. The order of X is p^n since $r = ab$ coprime gives $sa + tb = 1$, so $x = (sa + tb)x \in M_b + M_a$ where $M_a = \{ x \in X : ax = 0 \}$; if $x \in M_a \cap M_b$ then $ax = 0 = bx$, so $x = (sa + tb)x = 0$. Suppose $x \neq 0$, then $X = [\![x]\!] \cong R/\mathrm{Annih}(x) = R/\langle p^n \rangle$.

5.3 Fields

are commutative rings in which every $x \neq 0$ has an inverse $xx^{-1} = 1$. Equivalently, they are

- simple commutative rings (since the only possible ideals are 0 and F);
- finite-length integral domains (since elements of Artinian rings are either invertible or zero divisors; this can be seen directly for finite integral domains as $0x, 1x, r_3x, \ldots, r_nx$ are all distinct, so must contain 1).
- von Neumann integral domains (since regular cancellatives are invertible).

The smallest subfield in F, called its *prime subfield*, is isomorphic to $\mathbb{F}_p := \mathbb{Z}_p$ or $\mathbb{Q}$ (depending on whether the prime sub-ring is $\mathbb{Z}_p$ or $\mathbb{Z}$); it is fixed by any 1-1 morphism. Thus every field is a vector space (algebra) over its prime subfield.

Examples include fields of fractions of an integral domain, such as $\mathbb{Q}$, the center of any division ring, and R/I with R commutative and I maximal, such as $F[x]/\langle p \rangle$ with p irreducible.

1. Every finite (multiplicative) sub-group of $F \smallsetminus 0$ is cyclic.

   Proof: Being a finite abelian group, $G \cong \mathbb{Z}_{p^n} \times \mathbb{Z}_{q^r} \times \cdots$; so all elements satisfy $x^m = 1$ where $m = \mathrm{lcm}(p^n, q^r, \ldots)$. But the number of roots of $x^m = 1$ is at most m. Hence $p, q, \ldots$ are distinct primes, so G is cyclic.

2. The polynomials $F[x]$ form a Euclidean domain with $|p(x)| := \deg(p)$.

3. $\frac{F[x]}{\langle p(x) \rangle} \cong \frac{F[x]}{\langle p_1^{r_1} \rangle} \times \cdots \times \frac{F[x]}{\langle p_n^{r_n} \rangle}$ with $p_i(x)$ irreducible (Lasker).

4. If the prime subfield is $\mathbb{F}_p$, then $x \mapsto x^p$ is a 1-1 morphism which preserves $\mathbb{F}_p$ (since $a \in \mathbb{F}_p \;\Rightarrow\; a^p = a$, $x^p = 0 \;\Rightarrow\; x = 0$).

5. The finite fields are of the type $\mathbb{F}_{p^n} := \mathbb{F}_p[x]/\langle q(x) \rangle$, where q is an irreducible polynomial in $\mathbb{F}_p[x]$ of degree n. Its dimension over $\mathbb{F}_p$ is n, so it has p^n elements.

   Existence: take the splitting field for $x^{p^n} = x$ (see later); its p^n roots form a field since $(a + b)^{p^n} = a^{p^n} + b^{p^n} = a + b$, and similarly $(-a)^{p^n} = -a$ (even if $p = 2$), $(ab)^{p^n} = ab$, $(a^{-1})^{p^n} = a^{-1}$. Uniqueness: every non-zero element satisfies $x^{p^n - 1} = 1$, so every element satisfies $x^{p^n} = x$ and there are no multiple roots (derivative is -1); F is thus the splitting field for a polynomial.

6. For $M_n(F)$, the Smith normal form is $\begin{pmatrix} I & 0 \\ 0 & 0 \end{pmatrix}$ for suitable bases.

Formally real fields: those such that $\sum_i a_i^2 = 0 \Rightarrow a_i = 0$.

Perfect fields: has prime subfield either $\mathbb{Q}$ or $\mathbb{F}_p$ with $x \mapsto x^p$ an automorphism.

5.3.1 Algebraically Closed Fields

when every non-constant polynomial in $F[x]$ has a root in F (hence has deg(p) roots, i.e., 'splits'); equivalently, when its irreducible polynomials are of degree 1, i.e., $x + a$.

Every field has an algebraically closed extension, unique up to isomorphisms (e.g. list all irreducible polynomials, if possible, and keep extending by roots).

6 Algebras

Definition An **algebra** is a ring R with a sub-field F in its center,

$$\lambda(xy) = (\lambda x)y = x(\lambda y)$$

They are vector spaces with an associative bilinear product. Examples include

- Integral domains or division rings, at least over their prime sub-field $\mathbb{Q}$ or $\mathbb{Z}_p$;
- $\mathrm{Hom}_F(X)$ when F is a field acting on a vector space X;
- Group algebras $F[G]$ (for example, $\mathbb{H} := \mathbb{R}[Q]$ where Q is the quaternion group $i^2 = j^2 = k^2 = -1$; $F[C_n] \cong F[x]/\langle x^n - 1\rangle$).

Morphisms preserve $+, \cdot, F$:

$$\phi(x+y) = \phi(x) + \phi(y), \quad \phi(xy) = \phi(x)\phi(y), \quad \phi(\lambda x) = \lambda\phi(x), \quad \phi(1) = 1.$$

Note that as $\phi(\lambda) = \lambda$, morphisms fix F.

Subalgebras are sub-rings that contain F; e.g. the center. The subalgebra generated by A is the smallest subalgebra that contains F and A, denoted $F[A]$.

Every algebra is a subalgebra of $\mathrm{Hom}_F(X)$ for some vector space (take $X = R$ and the isomorphism $x \mapsto T_x$ where $T_x(y) = xy$).

1. A free algebra with a basis e_i is characterized by its structure constants $\gamma_{ij}^k \in F$, defined by $e_i e_j = \gamma_{ij}^k e_k$.

2. Every element is either **algebraic**, i.e., satisfies a non-zero polynomial in $F[x]$, or **transcendental** wrt F (otherwise). If a is algebraic, the polynomials it satisfies form an ideal $\langle p_a \rangle$, where p_a is called its *minimal* polynomial. The roots of p_a are called the 'eigenvalues' of a. Idempotents $x^2 = x$ and nilpotents $x^n = 0$ are algebraic.

3. Morphisms between algebras over F map $\phi(p(a)) = p(\phi(a))$, so they preserve algebraic and transcendental numbers.

4. If a is algebraic, then $F[x] \to F[a]$, $q(x) \mapsto q(a)$, is an algebra morphism with kernel $\langle p_a \rangle$. So $F[a]$ has dimension $\deg(p_a)$.

5. The set of algebraic elements form an algebra R^{alg}. The minimal polynomials of $a + \alpha$, αa, a^{-1}, a^n, $b^{-1}ab$ are related to that of a (but not so for $a + b$ and ab).

   Proof: If a is algebraic, then so is the ring $F[a] \subseteq R$ since it is finite dimensional. Hence for a, b algebraic, $a + b, ab \in F[a][b]$ are algebraic.

6. The algebraic elements of $\text{Jac}(R)$ are the nilpotents (since for $r \in J$, $1+ar$ is invertible, so the minimal polynomial must be $0 = a_k r^k + \cdots + a_n r^n = a_k r^k (1 + ar)$ hence $r^k = 0$).

7. Every set of group morphisms $G \to R \smallsetminus 0$ is F-linearly independent.

   Proof: If $a_1\sigma_1 + \cdots + a_n\sigma_n = 0$, then also for all $g \in G$,

   $$a_1\sigma_1(g)\sigma_1(x) + \cdots + a_n\sigma_n(g)\sigma_n(x) = 0,$$
   $$\therefore a_1(\sigma_1(g) - \sigma_n(g))\sigma_1 + \cdots + a_n(\sigma_{n-1}(g) - \sigma_n(g))\sigma_{n-1} = 0,$$

   so by induction, $a_i(\sigma_i(g) - \sigma_n(g)) = 0$; but for each i there is a g such that $\sigma_i(g) \neq \sigma_n(g)$, so $a_i = 0$. Hence also $a_n = 0$.

Let $G := \text{Aut}_F(R)$ be the group of algebra automorphisms of R. To each subalgebra $F \leqslant S \leqslant R$ there is a group

$$\text{Gal}(S) := \{\, \sigma \in G : \forall x \in S, \sigma(x) = x \,\}$$

and for a subgroup $H \leqslant G$, there is a subalgebra of R,

$$\text{Fix}(H) := \{\, x \in R : \forall \sigma \in H, \sigma(x) = x \,\}$$

They are adjoints,

$$H \leqslant \text{Gal}(S) \;\Leftrightarrow\; \text{Fix}(H) \geqslant S$$

1. Writing $S' := \text{Gal}(S)$, $H' := \text{Fix}(H)$, it follows, as for all adjoints, that $S_1 \leqslant S_2 \;\Rightarrow\; S_2' \leqslant S_1'$, $H_1 \leqslant H_2 \;\Rightarrow\; H_2' \leqslant H_1'$; $S \leqslant S''$, $H \leqslant H''$; $S''' = S'$, $H''' = H'$.

2. $\text{Fix}(\sigma H \sigma^{-1}) = \sigma\text{Fix}(H)$ (since $\sigma H \sigma^{-1}(x) = x \;\Leftrightarrow\; \sigma^{-1}(x) \in \text{Fix}(H)$).

3. $\sigma\text{Gal}(S)\sigma^{-1} = \text{Gal}(\sigma S)$ (since $\sigma\tau\sigma^{-1} = \omega \;\Leftrightarrow\; \sigma^{-1}\omega\sigma(x) = x, \forall x \in S$, so $\omega\sigma(x) = \sigma(x)$).

6.1 Algebraic Algebras

are algebras in which every element is algebraic, i.e., satisfies some polynomial in $F[x]$. For example, R^{alg}.

1. If R is algebraic on E which is algebraic on F, then R is algebraic on F

   Proof: Every $r \in R$ satisfies a poly $p = \sum_i a_i x^i \in E[x]$; so $F \leqslant F[a_0, \ldots, a_n] \leqslant F[a_0, \ldots, a_n, r]$, each extension being finite dimensional; hence the last algebra is algebraic.

2. $\text{Jac}(R) = \text{Nil}(R)$ (since all algebraic numbers in J are nilpotent).

3. Non-commutative algebraic algebras over $\mathbb{F}_{p^n}$ have non-trivial nilpotents, e.g. algebraic division algebras over $\mathbb{F}_{p^n}$ are fields.

4. The algebraic division algebras over $\mathbb{R}$ are $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.

   Proof: For any $a \notin \mathbb{R}$, $\mathbb{R}[a] \cong \mathbb{C}$; so R is a vector space over $\mathbb{C}$; now R splits into two subspaces: those that anti/commute with i, $x = (ix + xi)/2i + (ix - xi)/2i$. If all commute then $R \cong \mathbb{C}$; otherwise choose a that anti-commutes, the map $x \mapsto a^{-1}x$ converts anti-commuting to commuting; hence $R \cong \mathbb{C} + a\mathbb{C}$; note that a^2 commutes, so $a^2 \in \mathbb{C}$, yet is also algebraic over $\mathbb{R}$, hence $0 > a^2 \in \mathbb{R}$; let $j := a/|a|$, so $R \cong \mathbb{C} + j\mathbb{C} = \mathbb{H}$.

6.2 Finite-dimensional Algebras

1. An algebra is finite-dimensional iff it is algebraic (of bounded degree) and finitely generated.

   Proof: For any $a \in R$, then $1, a, a^2, \ldots$ are linearly dependent, so a is algebraic. $F[a_1] < F[a_1, a_2] < \cdots$ where $a_n \notin F[a_1, \ldots, a_{n-1}]$; for finite dimensions, $R = F[a_1, \ldots, a_n]$. Conversely, $F[a]$ is finite dimensional over F, since a is algebraic, hence by induction $F[a_1, \ldots, a_n]$ is finite dimensional over F.

2. Every finite-dimensional algebra can be represented by matrices in $M_n(F)$; each element has corresponding 'trace' and 'determinant'. For example, for $\mathbb{Q}(i)$, the trace of z is $\text{Re}(z)$, the determinant is $|z|^2$.

   If $x_i x_j = \gamma_{ij}^k x_k$, then x_i corresponds to the matrix $x_j \mapsto x_i x_j$, i.e., $[\gamma_{ij}^k]$ (fixed i).

3. Every simple finite-dimensional algebra is isomorphic to $M_n(H)$, where H is a division ring (Wedderburn).

4. (Noether normalization lemma) Every finite-dimensional commutative algebra over F is a finitely generated module over $F[x_1, \ldots, x_n]$, where x_i are not algebraic in the rest of the variables.

   Proof: If $p(x_1, \ldots, x_n) = \sum_{\boldsymbol{k}} a_{\boldsymbol{k}} x^{\boldsymbol{k}} = 0$ (not algebraically independent) then define new variables $y_i := x_i - x_n^r$, $y_n := x_n$ to get a new polynomial

$x_n^m + q_{m-1}(x_1,\ldots,x_{n-1})x_n^{m-1} + \cdots = 0$, satisfied by x_n. The result follows by induction on n.

5. (Zariski lemma) If R is a field which is a finitely generated algebra over F, then it is a finite dimensional field extension of F. (since R is a finitely generated module over $F[x_1,\ldots,x_n]$, yet R is a field (simple), so $n = 0$).

6. Recall the adjoint maps connecting subsets of F^N and ideals in $F[x_1,\ldots,x_N]$,

$$I \leqslant \text{Annih}(A) \Leftrightarrow A \leqslant \text{Zeros}(I)$$

If F is algebraically closed, then every maximal ideal in $F[x_1,\ldots,x_n]$ is the kernel of an evaluation F-morphism $p(x_1,\ldots,x_n) \mapsto p(a_1,\ldots,a_n)$, i.e., the ideal generated by $(x-a_1)\cdots(x-a_n)$. Thus each maximal ideal M corresponds to a point in F^n, $M = \text{Annih}(\boldsymbol{a})$.

Proof: Let $R := F[x_1,\ldots,x_n]$; $F \to R \to R/M$ is an isomorphism, since R/M is finitely generated algebra over F and is a field, so it is a finite-dimensional (algebraic) extension of F; but F is algebraically closed, so $R/M \cong F$ and M is the kernel of the morphism $\phi : R \to R/M \to F$; $a_i = \phi(x_i)$.

7. (Weak Nullstellensatz) If F is algebraically closed, and I is a proper ideal of $F[x_1,\ldots,x_n]$, then I has a zero, i.e., $\text{Zeros}(I) \neq \varnothing$. (since $I \leqslant M$ maximal ideal, which corresponds to $(a_1,\ldots,a_n)$. Thus $\text{Zeros}(I) \supseteq \text{Zeros}(M) = \{\, \boldsymbol{a} \,\}$.)

8. (Strong Nullstellensatz) For an algebraically closed field, $\text{Annih}\circ\text{Zeros}(I) = r(I)$.

Proof: If $p(x)^n \in I$ and $a \in \text{Zeros}(I)$, then $p(a)^n = 0$, so $p(a) = 0$, i.e., $p \in \text{Annih}\circ\text{Zeros}(I)$. Conversely, let $q(x_1,\ldots,x_{n+1}) := 1 - p(x_1,\ldots,x_n)x_{n+1}$; then $I + \langle q\rangle$ has no zeros in F^{n+1}, so $I + \langle q\rangle = F[x_1,\ldots,x_{n+1}]$. Thus $1 = r_1q_1 + \cdots + r_nq_n + r_{n+1}q$; the map $F[x_1,\ldots,x_{n+1}] \to F[x_1,\ldots,x_n][p^{-1}]$ that takes $x_{n+1} \mapsto p^{-1}$ but fixes x_i, gives $1 = (r_1/p^{k_1})q_1 + \cdots + (r_n/p^{k_n})q_n + r_{n+1}(1-p/p)$, hence $p^N = \sum_{k=1}^n s_kq_k \in I$.

6.3 Field Extensions

A field E with a subfield F form an algebra, called a *field extension*. (Note: $F[x]$ is a subalgebra of $E[x]$.)

The field generated by a subset A is the smallest field in E containing F and A, denoted $F(A)$; it equals the field of fractions of $F[A]$, thus 'independent' of E. $F(a)$ is called a *simple* extension, and a a *primitive* element. Note that $F(A \cup B) = F(A)(B)$.

1. If $a \in E$ are algebraic numbers which are roots of an irreducible (minimal) polynomial $p(x) \in F[x]$, then

$$F(a) \cong \frac{F[x]}{\langle p\rangle} \cong F[a]$$

which has dimension $\deg(p)$.

Proof: The morphism $q \mapsto q(a)$ has kernel $\langle p\rangle$ and its image contains F and a. Every polynomial $q = sp + r = r \pmod p$ with $\deg(r) < \deg(p) = n$, and $1, a, \ldots, a^{n-1}$ are linearly independent. Thus a corresponds to the polynomial x; $p(x + \langle p\rangle) = p(x) + \langle p\rangle = \langle p\rangle$.

For example, 'quadratic algebras' are algebras of dimension 2 obtained from irreducible quadratic polynomials.

$F(a)$ need not include the other roots of $p(x)$ and may include other linearly independent non-roots such as perhaps a^2.

Note that the generators of a field extension need not, in general, be a basis: e.g. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ has dimension 4 with basis $\{ 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \}$; $\mathbb{Q}(i, \sqrt{n}) = \mathbb{Q}(i + \sqrt{n})$.

2. If a is transcendental, $F(a) \cong \{ p(x)/q(x) : p, q \in F[x], q \neq 0 \}$ is an infinite-dimensional extension.

3. If a is algebraic over F, then

   (a) the coefficients of its minimal polynomial generate F,

   Proof: Suppose they generate $K \subseteq F$. Since $p(x)$ remains minimal in $K[x] \subseteq F[x]$, its degree equals $\dim_K F(a) = \dim_F F(a)$, so $K = F$.

   (b) there are only a finite number of subfields $F \leqslant E \leqslant F(a)$ (since the minimal polynomial $q(x)$ of a in $E[x]$ is a factor of that in $F[x]$, of which there are a finite number; and E is generated by the coefficients of q).

4. (a) An algebra morphism $\phi : E_1 \to E_2$ sends roots of $p(x)$ in E_1 to roots in E_2, since
$$p(\phi(a)) = \phi(p(a)) = 0$$
   If $\phi : E \to E$ is 1-1, it permutes these roots.

   (b) A 1-1 algebra morphism on E is an automorphism on E^{alg} (since for $a \in E^{\mathrm{alg}}$ with $p(a) = 0$, ϕ permutes its roots in E, in particular $\phi(b) = a$ and $\phi(a) \in E^{\mathrm{alg}}$).

   (c) If a, b have the same minimal polynomial $p(x)$, then $F(a) \cong F(b)$, $a \mapsto b$ (since $a \leftrightarrow x \leftrightarrow b$). Thus there are $\deg(p)$ 1-1 algebra morphisms $F(a) \to E$, each mapping a to a different root of $p(x)$.

5. Two co-prime polynomials in $F[x]$ cannot have a common root in $E[x]$ (since their gcd is 1 in both). Roots of the same irreducible polynomial are called *conjugates*; they partition E^{alg}. Conjugates must satisfy the same algebraic properties because of the morphisms between them.

6. There is a field $E \geqslant F$ in which a given polynomial p has all $\deg(p)$ roots (possibly repeated), called a *splitting* field of p: when extending to $F(a)$, p decomposes but may still contain irreducible factors; keep extending

to contain all the roots, so the polynomial splits into linear factors. For example

$$\begin{array}{rll} & \mathbb{Q} & x^3-2 \\ & \mathbb{Q}(\alpha) & (x-\alpha)(x^2+\alpha x+\alpha^2) \\ \text{splitting field} & \mathbb{Q}(\alpha,\beta) & (x-\alpha)(x-\beta)(x+\alpha+\beta) \end{array}$$

Of course, every irreducible quadratic polynomial splits with the addition of one root, e.g. x^2+1 splits in $\mathbb{Q}(i)$.

Note that a field may split several polynomials, for example, $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$ splits $x^2-2=(x-\sqrt{2})(x+\sqrt{2})$, $x^2-3=(x-\sqrt{3})(x+\sqrt{3})$, and $x^4-10x^2+1=\prod(x\pm\sqrt{2}\pm\sqrt{3})$; $\mathbb{Q}(i)$ splits both x^2+1 and x^2+2x+2; $\mathbb{Q}(\sqrt{3})$ splits $x^2+2nx+(n^2-3)$ $(n\in\mathbb{Z})$.

A field extension which is closed for conjugates is called *normal*. The normal closure of E is the smallest normal extension containing E, namely the splitting field for its generators (e.g. the normal closure of $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Q}(\sqrt[3]{2},\omega)$).

7. It is quite possible for an irreducible polynomial to have a multiple root in an extension: all roots are then equally multiple; so the number of roots divides the degree of p. But for this to happen, $p(a)=0=p'(a)$, so $p'=0$ since p is irreducible, hence $na_n=0$ for each n, so $n=0 \pmod p$ prime and
$$p(x)=a_0+a_1x^p+\cdots+a_n(x^p)^n,$$
For 'perfect' fields, such as those with $\mathbb{Q}$ as prime subfield, or finite fields ($x^p=x$), or algebraically closed fields, this is not possible, i.e., every irreducible polynomial has simple roots, called *separable*.

8. If $p(x)$ splits into simple roots $a,\ldots$, then the splitting field is a simple extension. More generally, every separable finite-dimensional field extension is a simple extension.

   Proof: Let p,q be minimal polynomials for a,b, and let K be their splitting field, so p has roots $a,a_2,\ldots,a_n$, and q has roots $b,b_2,\ldots,b_m$. Pick a $c\in F$ such that $\alpha:=a+cb\neq a_i+cb_j$ for any i,j. Then $F(a,b)=F(\alpha)$ since the only common root of $q(x)$ and $p(\alpha-cx)$ is b: $q(x)=0=p(\alpha-cx) \Rightarrow \alpha-cb_i=a_j \Rightarrow x=b$; thus b and $a=\alpha-cb\in F(\alpha)$. By induction $F(a_1,\ldots,a_n)=F(\beta)$.

9. If $p(x)\in F''[x]$ splits in E then it has simple roots.

   Proof: If $p(x)\in F''[x]$ is an irreducible factor with roots $a_1,\ldots,a_n\in E$, let $q(x):=(x-a_1)\cdots(x-a_n)$. Any $\sigma\in G=F'$ fixes F'' hence permutes the roots of p, hence fixes q; the coefficients of q must be in F''. But $q|p$, so $p=q$ is separable.

10. Translations and scalings of polynomials $p(ax+b)$ $(a\neq 0)$ are automorphisms, and have corresponding effects on their roots. Indeed, $\operatorname{Aut}F[x]$ consists precisely of these *affine* automorphisms.

11. The automorphism group of $F(x)$ is $PGL_2(F)$, i.e., $p(x) \mapsto p(\frac{ax+b}{cx+d})$ $(ad-bc \neq 0)$ with kernel consisting of $a=d$, $b=c=0$.

6.3.1 Algebraic Extensions

are extensions all of whose elements are algebraic over F.

1. Every subring $F \leqslant R \leqslant E$ is a subfield (since any $a \in R$ is algebraic, so the field $F(a) = F[a] \leqslant R$, so a is invertible in R).

2. Every 1-1 algebra morphism $E \to E$ is onto.

3. The algebraic closure of a field, $\bar{F}$, contains all the roots of all the polynomials in $\bar{F}[x]$. The algebraic closure of E is the same as that of F.

   Proof: Let $p \in \bar{F}[x]$ be irreducible; then there is a field $B \geqslant \bar{F}$ which has a root b of $p(x) = \sum_{i=1}^{n} a_i x^i$; so $F < F[a_0, \ldots, a_n, b] \leqslant B$ are finite-dimensional, hence algebraic, over F, so $b \in \bar{F}$ is algebraic, and p is of degree 1.

4. If $F \leqslant K \leqslant E$, every 1-1 algebra morphism $\phi : K \to \bar{F}$ extends to $E \to \bar{F}$.

   Proof: By Zorn's lemma any chain of extensions is capped by $\bigcup_i K_i =: L$; if $a \in E \smallsetminus L$, its minimal polynomial maps to an irreducible polynomial in $\bar{F}$, so has a root $b \in \bar{F}$ and $\tilde{\phi}(a) = b$; in particular, $L(a) \to \bar{F}$ is an extension; hence $L = E$.

6.3.2 Finite Dimensional Extensions

1. $F(A) = F[A]$ (since $F[a_1]\cdots[a_n] = F(a_1)\cdots(a_n) = F(a_1, \ldots, a_n)$).

2. E is a normal extension of $F \Leftrightarrow E$ is the splitting field of some polynomial in $F[x] \Leftrightarrow$ every F-automorphism $\bar{F} \to \bar{F}$ restricts to an F-automorphism of E.

   Proof: $E = F(a_1, \ldots, a_n)$, each a_i has a minimal polynomial $p_i(x)$ whose conjugates belong to E (since normal), so $p_i(x)$ splits in E. Thus the polynomial $p(x) := p_1(x)\cdots p_n(x)$ splits in E, and has roots a_i. Any $\sigma : \bar{F} \to \bar{F}$ maps roots of $p(x)$ to roots, so $\sigma E = F(\sigma(a_1), \ldots, \sigma(a_n)) = F(a_1, \ldots, a_n) = E$. Finally, let $a \in E$ with minimal polynomial $p(x)$; any conjugate root is obtained from a via $a_i = \sigma_i(a)$, $\sigma_i \in \operatorname{Aut} \bar{F}$; if $\sigma E = E$, then $a_i \in E$ and E is normal.

   Hence conjugate roots are connected via automorphisms in G.

3. For E separable finite dimensional, the number of 1-1 algebra morphisms $E \to \bar{F}$ is $\dim E$.

   Proof: For any subfield, $|\operatorname{Aut}_F K| = |G|/|K'|$. For a simple extension K, the number of 1-1 algebra morphisms $K \to \bar{F}$ equals $\dim K$, one for each distinct root; hence the number of such morphisms on $E = F(a_1, \ldots, a_n)$ equals $\dim F(a_1) \dim_{F(a_1)} F(a_1, a_2) \cdots = \dim E$.

6.3.3 Galois extensions

A field E is called a *Galois* extension of F when it is finite dimensional and is closed under the adjoint maps Fix and Gal,

$$F = G' = F'' = \text{Fix} \circ \text{Gal}(F)$$

Every finite dimensional extension is Galois over F''.

1. For any subfield, $K'' = K$ (since $a \notin K$ has a minimal polynomial $p(x)$ with some conjugate root $\sigma(a) = b \neq a$, where $\sigma \in K'$; so $a \notin K''$).

2. A subfield K is Galois $\Leftrightarrow$ $K' \trianglelefteq G$. Then $\text{Aut}_F K \cong G/K'$.

   Proof: If K is Galois, $\sigma \in G$, $a \in K$,$\tau \in K'$, then $\tau\sigma(a) = \sigma(a) \in K'' = K$, so $\sigma^{-1}\tau\sigma \in K'$. If $K' \trianglelefteq G$, $\sigma \in G$ then $\sigma K = \sigma K'' = K'' = K$, so K is a normal extension wrt E. The map $\sigma \mapsto \sigma|_K$ (valid since K is normal) is a morphism with kernel $\sigma|_K = I \Leftrightarrow \sigma \in \text{Aut}_K E = K'$.

3. E is a Galois extension iff E is the splitting field for some separable polynomial in $F[x]$, iff E is a normal separable extension of F.

   Proof: $G = \text{Aut}_F(E)$ is finite since E is finite dimensional. Let $a \in E$ and take the orbit $a_i := \sigma_i(a)$ for $\sigma_i \in G$. Then G fixes the polynomial $p(x) := (x - a_1) \cdots (x - a_n) \in F''[x]$. It is the minimal polynomial for a since $q(a) = 0 \;\Rightarrow\; q(a_i) = \sigma_i q(a) = 0$, so $p|q$. Thus every minimal polynomial splits into simple factors, so E is normal and separable.

   If E is normal separable, then $G'' = G$ (see below) so $\dim_{F''} E = |\text{Aut}_{G'}(E)| = |G''| = |G| = |\text{Aut}_F(E)| = \dim_F E$, hence $F = F''$.

   The Galois group of a separable polynomial $p(x)$ is denoted $\text{Gal}(p) := \text{Gal}(E)$ where E is the splitting field of p. Note that p has exactly $\deg(p)$ roots in E, which form a basis for E.

4. For a Galois extension E, $|G| = \dim E$; $|K'| = \dim E/K$.

   Proof: For E normal, every algebra automorphism $\bar{F} \to \bar{F}$ restricts to an automorphism in G. When E is also separable, there are exactly $\dim E$ of them; hence $|G| = \dim E$. For any subfield K, E remains a Galois extension of K, so $|\text{Aut}_K E| = \dim_K E$.

5. Any separable polynomial $p(x)$ with roots a_i, satisfies $a_i = \phi_i(a)$ for ϕ_i all the 1-1 algebra morphisms $F(a) \to \bar{F}$, so $p(x) = (x - a) \cdots (x - \phi_n(a))$.

6. $H'' = H$, in particular $G'' = G$.

   Proof: $E = H'(a)$ (simple extension since E is separable), let $p(x) := (x - \sigma_1(a)) \cdots (x - \sigma_n(a))$ for $\sigma_i \in H$, then $p(x) \in H'[x]$ since any $\sigma \in H$ permutes the roots and fixes p's coefficients. Therefore, $\dim E/H' = \dim_{H'} H'(a) \leqslant \deg(p) = |H| \leqslant |H''| = \dim_{H'} E$. So $H'' = H$.

Proposition 5

Galois

> **The subfields of a Galois extension correspond to the subgroups of its Galois group, via the maps $K \mapsto \mathrm{Gal}(K)$, $H \mapsto \mathrm{Fix}(H)$. The Galois subfields correspond to the normal subgroups.**

Proof: The map $K \mapsto K'$ is onto since $H'' = H$ and 1-1 since $K_1' = K_2' \Rightarrow K_1 = K_1'' = K_2'' = K_2$.

So given a subgroup H of G, its largest normal subgroup corresponds to the smallest normal extension of F that contains H'.

7. If p has only simple roots, then each irreducible factor corresponds to an orbit of the roots (under $\mathrm{Gal}(p)$); the degree of the factor equals the size of the orbit.

   Proof: Each irreducible factor corresponds to a selection of roots, $(x - a_i)\cdots(x - a_j)$. For any two roots a, b, there is an isomorphism $a \leftrightarrow b$; thus an isomorphism $F(a) \to F(a_1, \ldots, a_n)$, which can be extended to an automorphism of $F(a_1, \ldots, a_n)$.

   The stabilizer subgroup which fixes a root α has $|G|/\deg(p)$ elements; this is non-trivial precisely when $E = F(\alpha)$.

8. Example: the $\mathbb{Q}$-automorphisms of $x^4 - 10x^2 + 1$ form the group $C_2 \times C_2$ generated by $\sqrt{2} \leftrightarrow -\sqrt{2}$, $\sqrt{3} \leftrightarrow -\sqrt{3}$; each automorphism fixes one of $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$, $\mathbb{Q}(\sqrt{2} + \sqrt{3})$, $\mathbb{Q}(\sqrt{6})$.

9. The *discriminant* of a polynomial $p(x)$ with roots α_i is $\Delta(p) := \prod_{i<j}(\alpha_i - \alpha_j)$ (defined up to a sign), which can be written in terms of the coefficients of p. It determines when there are repeated roots, $\Delta(p) = 0$. Since each transposition of roots introduces a minus sign (unless the characteristic is 2, when $-1 = +1$), then $\sigma\Delta = \mathrm{sign}(\sigma)\Delta$; thus $\Delta(p)$ is invariant under $\mathrm{Gal}(p) \Leftrightarrow \mathrm{Gal}(p) \leqslant A_n$.

10. Example: The irreducible polynomial $x^4 - 2$ has roots $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$, so its splitting field is $\mathbb{Q}(\sqrt[4]{2}, i)$, which is Galois. It has dimension 8, with a Galois group D_4, generated by $i \mapsto -i$ and $\sqrt[4]{2} \mapsto i\sqrt[4]{2}$. The subgroups of D_4, namely two $C_2 \times C_2$, C_4, and five C_2, correspond to the fields (respectively) $\mathbb{Q}(\sqrt{2})$ (normal) and $\mathbb{Q}(i\sqrt{2})$ (normal), $\mathbb{Q}(i)$ (normal), and $\mathbb{Q}(i\sqrt[4]{2})$, $\mathbb{Q}(\sqrt[4]{2})$, $\mathbb{Q}(i, \sqrt{2})$, $\mathbb{Q}((1+i)\sqrt[4]{2})$, $\mathbb{Q}((1-i)\sqrt[4]{2})$.

Radical Extensions

Let F be a perfect field, so irreducible polynomials do not have multiple roots. A polynomial is solvable by radicals when its roots are given by formulas of elements of F that use $+, \times, \sqrt[n]{}$; this means that there is a *radical* extension field $F(a_1, \ldots, a_n)$ and $r_1, \ldots, r_n \in \mathbb{N}$ such that

$$\begin{aligned}
&a_n^{r_n} \in F(a_1, \ldots, a_{n-1}) \\
&\quad \ldots \\
&a_2^{r_2} \in F(a_1) \\
&a_1^{r_1} \in F
\end{aligned}$$

1. The roots of $x^n - a \in F[x]$ are of the form $\alpha\beta$ where α is a single root of $x^n - a$, and β are the roots of $x^n - 1$. If $x^n - a$ is irreducible, so $\alpha \notin F$, then also $\alpha^k \notin F$ for $\gcd(k, n) = 1$ (else $a = a^{sk+tn} = \alpha^{skn}a^{tn} = (\alpha^{ks}a^t)^n$).

2. The polynomial $x^n - 1$ contains the factor $x^m - 1$ iff $m|n$; so it decomposes into "cyclotomic" polynomials ϕ_m. For example,

   $$\begin{aligned}
   x^3 - 1 &= \phi_1\phi_3 = (x-1)(x^2+x+1), \\
   x^4 - 1 &= \phi_1\phi_2\phi_4 = (x-1)(x+1)(x^2+1), \\
   x^6 - 1 &= \phi_1\phi_2\phi_3\phi_6 = (x-1)(x+1)(x^2+x+1)(x^2-x+1).
   \end{aligned}$$

   Of course, whether ϕ_n is irreducible or not depends on the field; they are in $\mathbb{Q}$, but $x^2 + 1 = (x+1)^2$ in $\mathbb{F}_2$.

3. The splitting field of $x^n - 1 = (x-1)(x-\zeta)\cdots(x-\zeta^{n-1})$ is $F(\zeta)$, where ζ is a root of ϕ_n. If the characteristic of F is p and $p|n$, then $x^n - 1 = (x-1)^p(x-\zeta)^p\cdots(x-\zeta^{n/p-1})^p$; otherwise all ζ^i are distinct. The automorphisms are $\zeta \mapsto \zeta^k$ with $\gcd(k, n) = 1$, i.e., the Galois group is a subgroup of $\Phi_n := \mathbb{Z}_n^*$; it equals Φ_n if ϕ_n is irreducible and F does not have characteristic $p|n$ because then ϕ_n is the minimal polynomial of ζ.

4. The splitting field of $x^n - a$ is $F(\zeta, \alpha)$ where α is a single root of $x^n - a$. The automorphisms that fix $F(\zeta)$ are $\sigma(\alpha) = \alpha\zeta^i$ (the other roots), so the Galois group over $F(\zeta)$ is C_n since $\sigma \mapsto \zeta^i$ is an isomorphism (its image is a subgroup of C_n, i.e., C_m, $m|n$, so $\zeta^{im} = 1$ for all i, hence $\sigma(\alpha^m) = \alpha^m$ for all σ, so $\alpha^m \in F$, a contradiction unless $m = n$).

5. The Galois group of a radical Galois extension is solvable.

   Proof: The Galois group of each extension $F(\sqrt[r]{a}) = F(\zeta, \alpha)$ is cyclic over $F(\zeta)$, whose group is abelian over F. Hence $\text{Aut}_F(\zeta, \alpha)$ is abelian; by induction, the Galois group of E gives normal subgroups $1 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_k$ each with abelian factors.

6. Example: For $x^7 - 1$, the splitting field is $\mathbb{Q}(\zeta)$; its subfields correspond to the subgroups of C_6, namely $C_3 : \zeta \mapsto \zeta^2$ associated with $\mathbb{Q}(\zeta + \zeta^2 + \zeta^4)$, and $C_2 : \zeta \mapsto \zeta^{-1}$ associated with $\mathbb{Q}(\zeta + \zeta^{-1})$.

   The splitting field for $x^5 - 2$ is $\mathbb{Q}(\zeta, \sqrt[5]{2})$; its roots are $\zeta^i\sqrt[5]{2}$. The Galois group is generated by $\sigma : \zeta \mapsto \zeta, \sqrt[5]{2} \mapsto \zeta\sqrt[5]{2}$, and $\tau : \zeta \mapsto \zeta^2, \sqrt[5]{2} \mapsto \sqrt[5]{2}$, i.e., $\sigma = (12345)$ and $\tau = (2345)$; their corresponding fixed subfields are $\mathbb{Q}(\zeta)$ and $\mathbb{Q}(\sqrt[5]{2})$.

7. If K is a radical extension, then so is K''.

   Proof: $K = F(a_1, \ldots, a_n)$ with each a_i having $p_i(x)$ as minimal polynomial; thus K'' splits $\prod_i p_i(x)$; but $a_i^{n_i} \in F(a_1, \ldots, a_j)$ so the other roots of $p_i(x)$ also belong to it by applying $\sigma : a_i \mapsto b$; hence every root of $\prod_i p_i(x)$ is radical, so K'' is radical.

8. If $\mathbb{Q} \subsetneq F$ then a polynomial is solvable by radicals iff it has a solvable Galois group.

9. Knowing the abstract Galois group allows us to solve for the roots (if possible). For example, if there are 4 roots with group $C_2 \times C_2$, then $C_2 \times C_1$ fixes roots γ, δ but switches α, β; so it fixes $\alpha + \beta$ and $\alpha\beta$, so $\alpha+\beta, \alpha\beta \in \mathbb{Q}(\gamma, \delta)$ and α, β can be found by solving $x^2-(\alpha+\beta)x+\alpha\beta = 0$; similarly $\gamma + \delta, \gamma\delta \in \mathbb{Q}$ (because they are fixed by $C_1 \times C_2$).

10. By translating, every monic polynomial can be written in reduced form

$$x^n + a_{n-2}x^{n-2} + \cdots + a_0$$

   The discriminant and Galois group for the low degree reduced polynomials in $\mathbb{Q}[x]$ are:

   (a) Quadratics $x^2 + a$; $\Delta^2 = -4a$, $S_2 = C_2 \triangleright 1$ depending on whether $\Delta \in \mathbb{Q}$, e.g. $x^2 - 2$, $x^2 - 1$;

   (b) Cubics $x^3 + bx + a$; $\Delta^2 = -4b^3 - 27a^2$, $S_3 \triangleright A_3$, e.g. $x^3 - x + 1$, $x^3 - 3x + 1$, depending on $\Delta \in \mathbb{Q}$ if irreducible;

   (c) Quartics $x^4 + cx^2 + bx + a$; $27\Delta^2 = 4I^3 - J^2$ where $I = 12a + c^2$, $J = 72ac - 27b^2 - 2c^3$, $S_4 \triangleright A_4 \triangleright C_2 \times C_2$.

   (d) If $p(x) \in \mathbb{Q}[x]$ is irreducible with degree p prime with $p-2$ real roots and 2 complex roots, then its Galois group is S_p, e.g. $x^5 - 6x + 3$ (proof: $i \leftrightarrow -i$ is an automorphism; but there must be a p-cycle by Cauchy's theorem, so the whole group is S_p). So, in general, quintic polynomials or higher are not solvable since $A_n \triangleleft S_n$ are not solvable groups for $n \geqslant 5$.

   For example, the roots of $x^7 = 1$ cannot be written in radicals (but those of $x^n = 1$, $n < 7$ can).

11. Let F^n represent the space of polynomials of degree n (in reduced form). In general factoring out the permutations of the roots, $F^n \to F^n/S_n$, maps the roots to the coefficients; the 'discriminant' subset of F^n is a number of hyperplanes, maps to a variety, whose complement has fundamental group equal to the braid group with n strands.

12. Examples: x^2+x+1 over $\mathbb{Z}_2$: it is irreducible, and has a simple extension $\mathbb{Z}_2(\zeta)$ where $\zeta^2 = \zeta + 1$, in which $x^2 + x + 1 = (x + \zeta)(x + 1 + \zeta)$.

    $x^2 - (1+i)$ over $\mathbb{Z}_2(1+i)$: extension $\mathbb{Z}_2(1+i, \alpha)$, so $(x-\alpha)^2 = x^2 - \alpha^2 = x^2 - (1+i)$, so there are no other roots; so $x^2 - (1 + i)$ is irreducible in $\mathbb{Z}_2(1 + i)$ since there are no other roots and it is non-separable.

13. A number α is *constructible* by ruler and compasses iff $\mathbb{Q}(\alpha)$ is a radical extension of dimension $\dim_{\mathbb{Q}} \mathbb{Q}(\alpha) = 2^n$ (since intersections of lines and circles are points x such that $x^2 \in \mathbb{Q}(\beta, \ldots, \gamma)$ and $\dim_{\mathbb{Q}(\beta,\ldots,\gamma)} \mathbb{Q}(x) = 2$).
    (a) $\sqrt[3]{2}$ is not constructible since $\dim \mathbb{Q}(\sqrt[3]{2}) = 3$; so no doubling of the cube.
    (b) $e^{2\pi i/n}$ is not constructible unless $n = 2^r p_1 \cdots p_s$ where p_i are distinct Fermat primes $p = 2^k + 1$ (since $\dim \mathbb{Q}(e^{2\pi i/n}) = \phi(n) = \prod_{p^r|n} \phi(p^r)$ and $2^k = \phi(p^r) = (p-1)p^{r-1} \Leftrightarrow p = 2$ OR $p = 2^k + 1$). A Fermat prime must be of the form $2^{2^r}+1$ (since $x^{mn}+1 = (x^m+1)(x^{m(n-1)} - x^{m(n-2)} + \cdots + 1)$ for n odd); the five known Fermat primes have $r = 0, \ldots, 4$. So the regular heptagon and nonagon are not constructible, and in general angles cannot be trisected.
    (c) $\sqrt{\pi}$ is not constructible since it is transcendental; so no squaring of the circle.

7 Lie Rings

The product xy of a ring in which $2 \neq 0$ splits into two invariant bilinear non-associative products:

$$xy = \frac{1}{2}(xy + yx) + \frac{1}{2}(xy - yx) =: x \circ y + [x, y]$$

The first symmetric part of the product gives a *Jordan* 'ring', the second anti-symmetric part of the product gives a *Lie* 'ring'.

Jordan rings: $y \circ x = x \circ y$, $(x \circ x) \circ (y \circ x) = ((x \circ x) \circ y) \circ x$;

Lie rings: $[y, x] = -[x, y]$, $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$;

Although these are not associative rings, much of the theory of rings can be applied to them. Every Lie ring, but not every Jordan ring, is induced from a ring.

Morphisms preserve the respective products, e.g. $\phi([x, y]) = [\phi(x), \phi(y)]$, an ideal satisfies $[x, I] \subseteq I$. Products are again Jordan/Lie rings.

1. A **derivation** on a ring is a map d on R such that

$$d(x + y) = d(x) + d(y), \quad d(xy) = d(x)y + x\,d(y),$$

so

$$\begin{aligned} &d(1) = 0, \quad d(nx) = nd(x), \\ &d(xyz) = d(x)yz + x\,d(y)z + xy\,d(z), \\ &d(x^n) = d(x)x^{n-1} + x\,d(x)x^{n-2} + \cdots + x^{n-1}d(x), \\ &d(x) = 1 \ \Rightarrow\ d(x^n) = nx^{n-1}, \\ &d^n(xy) = \sum_k \binom{n}{k} d^k(x) d^{n-k}(y) \quad \text{(Leibniz)} \end{aligned}$$

The derivations form a Lie ring $\mathrm{Der}(R)$ with $[d_1, d_2] = d_1 d_2 - d_2 d_1$.

2. The *inner derivation* associated with a is $\pounds_a(x) := [a, x]$. The rest are called *outer* derivations. An outer derivation becomes an inner derivation in some larger ring.

3. A *Lie ideal* of a Lie ring is a subset that is an ideal wrt $[,]$, i.e., is closed under $+, \pounds_a$. Examples include any ring ideal, and the center. The inner derivations form a Lie ideal in the Lie ring of derivations, i.e., $[d, \pounds_x] = \pounds_{d(x)}$; in particular, $[\pounds_x, \pounds_y] = \pounds_{[x,y]}$. Quotients by a Lie ideal form a Lie ring.

4. The map $R \to \mathrm{Der}(R)$, $x \mapsto \pounds_x$ is a morphism from a ring to its Lie ring of derivations, whose kernel is the center.

5. The ring of differentiation operators of an R-algebra is defined as that generated by left multiplication and derivations. For example, the Weyl algebra is the algebra of differentiation operators on polynomials $R[x]$, where $xa = ax + \mathrm{d}(a)$.

6. The derivations of an algebra must satisfy in addition $d(\lambda x) = \lambda\, d(x)$; Lie ideals must be invariant under scalar multiplication. The statements above remain valid for Lie algebras.

7. The *derived algebra* of a Lie algebra is the ideal $\mathcal{A}' := [\mathcal{A}, \mathcal{A}]$; $\mathcal{A}/\mathcal{A}'$ is the largest abelian image of $\mathcal{A}$; $[\mathcal{A}, \mathcal{A}']/[\mathcal{A}, \mathcal{A}''] \trianglelefteq Z(\mathcal{A}/[\mathcal{A}, \mathcal{A}''])$.

   For example, $gl(n)' = sl(n)$ (traceless matrices, $sl(n) = \ker \mathrm{tr}$).

For any Lie algebra, the following 'derived series' can be formed:

$$\cdots \leqslant \mathcal{A}''' \trianglelefteq \mathcal{A}'' \trianglelefteq \mathcal{A}' \trianglelefteq \mathcal{A}$$

Solvable Lie algebras have a finite derived series ending in 0. The last ideal $0 \triangleleft \mathcal{A}^{(n)}$ is abelian. Subalgebras and images are solvable. The sum of solvable ideals is again solvable (since both J and $(I + J)/J \cong I/(I \cap J)$ are solvable). Hence the sum of all solvable ideals is the largest solvable ideal in $\mathcal{A}$, called the *radical*.

Nilpotent Lie algebras have a finite central series of ideals

$$0 \trianglelefteq \ldots \trianglelefteq [\mathcal{A}, \mathcal{A}'] \trianglelefteq [\mathcal{A}, \mathcal{A}] \trianglelefteq \mathcal{A}$$

$$\Leftrightarrow \forall x_i, [x_1, [x_2, \ldots [x_{n-1}, x_n] \ldots]] = 0$$

Note that $\mathcal{A}'' = [\mathcal{A}', \mathcal{A}'] \subseteq [\mathcal{A}, \mathcal{A}']$, so nilpotent Lie algebras are solvable; subalgebras and images are nilpotent; the series can be built up using the centers (as in groups); $\mathcal{A}$ is nilpotent iff $x \mapsto [x, \cdot]$ is nilpotent (Engel).

Abelian Lie algebras: $[x, y] = 0$.

Semi-simple Lie algebras have no solvable ideals (except 0), thus no abelian ideals, no radical, no center. Every derivation is inner. They are isomorphic to a product of non-abelian simple Lie algebras.

Simple Lie algebras are either abelian or semi-simple (since the radical is either 0 or $\mathcal{A}$ with $\mathcal{A}' = 0$). The only simple abelian Lie algebras are 0 and F.

7.0.4 Finite-Dimensional Lie algebras over an Algebraically Closed Field that contains $\mathbb{Q}$

1. Every finite-dimensional Lie algebra can be represented by matrices with $[S,T] = ST - TS$, via $x \mapsto L_x := [x, \cdot]$. Every such representation has a *dual* representation $x \mapsto -L_x^\top$.

2. The *trace* map $\operatorname{tr} : \mathcal{A} \to F$ is a Lie morphism since $\operatorname{tr}[S,T] = 0$.

3. Let γ be the structure constants[1]: $[e_i, e_j] = \gamma_{ij}^k e_k$. There is a Killing form (Cartan metric) $\langle x, y\rangle := \operatorname{tr}(L_x L_y) = \gamma_{is}^t \gamma_{jt}^s$; so

$$\gamma_{ijk} = g_{ks}\gamma_{ij}{}^s = \operatorname{tr}[X_i, X_j]X_k = \gamma_{ij}{}^s \gamma_{kt}{}^r \gamma_{sr}{}^t$$

   is completely anti-symmetric.

   (a) $\langle [x, y], z\rangle = \langle x, [y, z]\rangle$

   (b) If $\mathcal{I}$ is an ideal, then so is $\mathcal{I}^\perp := \{\, x : \forall a \in I,\ \langle x, a\rangle = 0 \,\}$ (since for $b \in \mathcal{I}^\perp$, $a \in \mathcal{I}$, $\langle [x, b], a\rangle = \langle [x, a], b\rangle = 0$).

   (c) If $I \cap J = 0$ then $I \perp J$.

   (d) A Lie algebra is semi-simple when its Killing form is non-degenerate, $\mathcal{A}^\perp = 0$; it is solvable when $\mathcal{A} \perp \mathcal{A}'$.

   Proof: If $\mathcal{A}$ has an abelian Lie ideal $I \neq 0$ then for $a \in I$, $x \in \mathcal{A}$, $[a, x] \in I$, so $[x, [a, x]] \in I$, so $(L_a L_x)^2 = [a, [x, [a, x]]] = 0$, so $\langle a, x\rangle = 0$.

4. For a semi-simple Lie algebra, the *Casimir* (or Laplacian) element $\sum_i e_i e^i$ (for any basis) is in the center.

5. Every finite-dimensional solvable Lie algebra can be represented by upper triangular matrices.

   Proof: $\mathcal{A}' < \mathcal{A}$, so there is a maximal ideal $I \supseteq \mathcal{A}'$, $\mathcal{A} = I \oplus FT$. By induction, $Sv = \lambda_S v$ for all $S \in I$. Then $STv = TSv + [S,T]v = \lambda_S Tv$ ($\lambda_{[S,T]} = 0$ since by induction, S is upper triangular with respect to the vectors $v, Tv, T^2v, \ldots$, so $n\lambda = \operatorname{tr}[S,T] = 0$). In fact, any w generated by these vectors is a common eigenvector of I; choosing it to be an eigenvector of T shows there is a common eigenvector for all of $\mathcal{A}$; hence, by induction, every matrix is triangulizable.

6. Every finite-dimensional nilpotent Lie algebra is represented by nilpotent matrices (i.e., strictly upper triangular) since $L_x^n y = [x, \ldots, [x, y]] = 0$.

7. The *Cartan subalgebra* of $\mathcal{A}$ is the maximal subalgebra $\mathcal{H}$ which is abelian and consists of diagonalizable elements. It has the property $[x, \mathcal{H}] = 0 \Rightarrow x \in \mathcal{H}$.

[1] The Einstein convention suppresses the summation sign $\sum$ over repeated indices, so the given formula means $\sum_k \gamma_{ij}^k e_k \gamma_{ij}^k e_k$

The rest of $\mathcal{A}$ is generated by "step operators" e_α, such that $[h_i, e_\alpha] = \lambda_{i,\alpha} e_\alpha$ (this is essentially a diagonalization of $\gamma^\gamma_{i\beta}$ to give the 'Cartan-Weyl' basis).

8. (Cartan) Each eigenvalue $\lambda_{i,\alpha}$ corresponds to a unique eigenvector e_α, so λ_i can be written instead of $\lambda_{i,\alpha}$, i.e., $[h_i, e_\alpha] = \lambda_i e_\alpha$ (since from the Lie sum, $[h_i, [h_j, e_\alpha]] = \lambda_i [h_j, e_\alpha]$). Each e_α has an associated *root* vector $\alpha = (\lambda_i)$:

   (a) $[h_i, e_\alpha] = \alpha e_\alpha$,
   $[h_i, e_{-\alpha}] = [h_i, e^*_\alpha] = -\lambda_i e_{-\alpha}$,
   $[e_\alpha, e_{-\alpha}] = \alpha \cdot h =: |\alpha|^2 h_\alpha$,
   $[e_\alpha, e_\beta] = \begin{cases} (\alpha+\beta) e_{\alpha+\beta} & \alpha+\beta \text{ is a root,} \\ 0 & \alpha+\beta \text{ is not a root} \end{cases}$
   $[h_\alpha, h_\beta] = 0, \qquad [h_\alpha, e_\beta] = n_{\alpha\beta} e_\beta, \qquad (n_{\alpha\alpha} = 1)$
   (since by the Lie sum again, $[h_i, [e_\alpha, e_\beta]] = (\alpha_i + \beta_i)[e_\alpha, e_\beta]$; and $\langle h_i, [e_\alpha, e_{-\alpha}] \rangle = \langle e_{-\alpha}, [h_i, e_\alpha] \rangle = \alpha_i$).

   (b) For this basis,
   $$\langle h_i, h_j \rangle = 0, \quad \langle h_i, e_\alpha \rangle = 0, \quad \langle e_\alpha, e_\beta \rangle = 0,$$
   but $\langle e_\alpha, e_{-\alpha} \rangle \neq 0$ (since $\alpha_j \langle h_i, e_\alpha \rangle = \langle h_i, [h_j, e_\alpha] \rangle = \operatorname{tr} h_i [h_j, e_\alpha] = \operatorname{tr}[h_i, h_j] e_\alpha = 0$, and $\lambda \langle e_\alpha, e_\beta \rangle = \langle e_\alpha, [e_{\alpha-\beta}, e_\beta] \rangle = \operatorname{tr} e_\alpha [e_{\alpha-\beta}, e_\beta] = \operatorname{tr}[e_\alpha, e_{\alpha-\beta}] e_\beta = 0$);

   (c) For each α, h_α and e_α form an $su(2)$ algebra, with $e_\alpha/|\alpha|$ raising the eigenvalues of h_α by $1/2$; so the eigenvalues of h_α are half-integers, $[h_\alpha, e_\beta] = n_\alpha e_\beta$, where $n_\alpha := \alpha \cdot \beta / |\alpha|^2 \in \frac{1}{2}\mathbb{Z}$.

   (d) Any two roots have an angle of $\pi/2$ or $\pi/3$ or $\pi/4$ or $\pi/6$ or 0.
   Proof: $\alpha \cdot \beta \leqslant |\alpha||\beta|$ implies that $n_\alpha n_\beta \leqslant 4$ where $n_\alpha = 2\alpha \cdot \beta / |\alpha|^2$; so n_α, n_β can take the values $0, 0$, or $1, 1$, or $2, 1$, or $3, 1$, or $2, 2$); if j is the eigenvalue of h_β, there are roots between $\alpha - (j + n_\alpha/2)\beta, \ldots, \alpha + (j - n_\alpha/2)\beta$.

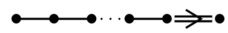
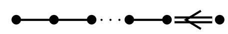
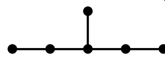
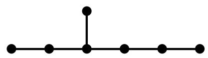
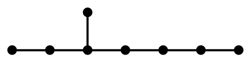
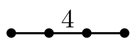
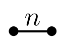
9. Finite-dimensional Lie algebras are products of simple and abelian algebras (take the maximal ideal at each stage).

   The semi-simple ones are the direct product of non-abelian simple Lie algebras; $\mathcal{A}' = \mathcal{A}$ (to avoid being solvable).

   Proof: If $\mathcal{A}$ is semi-simple, then $I \cap I^\perp = 0$ else it would be solvable; thus $\mathcal{A} = I \oplus I^\perp$, with each again semi-simple.

10. Every Lie algebra modulo its radical is semi-simple.

11. The non-abelian simple finite-dimensional Lie algebras over an algebraically closed field are classified:

Lie algebra	Dynkin diagram	Representation
A_n,		$sl(n+1)$, $su(n+1)$,
B_n $(n \geqslant 2)$,		$so(2n+1)$,
C_n $(n \geqslant 3)$,		$sp(2n)$
D_n $(n \geqslant 4)$,		$so(2n)$
E_6,		
E_7,		
E_8,		
F_4,		
G_2,		

Proof: A root system can be drawn as a Dynkin diagram: circles are simple roots (ie extremal roots), pairs are joined by n_α lines. Disconnected diagrams correspond to a decomposition $\mathcal{A} = I \oplus I^\perp$, so simple Lie algebras have connected Dynkin diagrams.

8 Examples

Size	Rings (with 1)	Commutative Rings	Fields
1			$\mathbb{F}_1$
2			$\mathbb{F}_2$
3			$\mathbb{F}_3$
4		$\mathbb{Z}_4$	$\mathbb{F}_4$
		$\mathbb{Z}_2 \times \mathbb{Z}_2$	
		$\mathbb{Z}_2[a]/\langle a^2 \rangle$	
5			$\mathbb{F}_5$
6		$\mathbb{Z}_6$	
7			$\mathbb{F}_7$
8	$U_2(\mathbb{F}_2) = \begin{pmatrix} \mathbb{F}_2 & \mathbb{F}_2 \\ 0 & \mathbb{F}_2 \end{pmatrix}$	$\mathbb{Z}_8$	$\mathbb{F}_8$
		$\mathbb{Z}_2 \times \mathbb{Z}_4$	
		$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$	
		$\mathbb{Z}_2 \times \mathbb{F}_4$	
		$\mathbb{Z}_2[a]/\langle a^3 \rangle$	
		$\mathbb{Z}_2[a, b : a^2 = ab = b^2 = 0]$	
		$\mathbb{Z}_2[a, b : a^2 = ab = 0, b^2 = b]$	
		$\mathbb{Z}_2[a : 2a = 0 = a^2]$	
		$\mathbb{Z}_2[a : 2a = 0, a^2 = 2]$	

Size	Rings (with 1)	Commutative Rings	Fields
9		$\mathbb{Z}_9$	$\mathbb{F}_9$
		$\mathbb{Z}_3 \times \mathbb{Z}_3$	
		$\mathbb{Z}_3[a]/\langle a^3 \rangle$	
10		$\mathbb{Z}_{10}$	
11			$\mathbb{F}_{11}$
12		$\mathbb{Z}_{12}$	
		$\mathbb{Z}_3 \times \mathbb{Z}_4$	
		$\mathbb{Z}_3 \times \mathbb{F}_4$	
		$\mathbb{Z}_3 \times (\mathbb{Z}_2[a]/\langle a^2 \rangle)$	
13			$\mathbb{F}_{13}$
14		$\mathbb{Z}_{14}$	
15		$\mathbb{Z}_{15}$	
16	13	23	1

1. $\mathbb{N}$ is a commutative semi-ring without invertibles (except 1). The prime ideals of $\mathbb{N}$ are $2\mathbb{N} + 3\mathbb{N}$ and $p\mathbb{N}$ (p prime or 1).

   Proof: Let p be the smallest non-zero element of P; then p is prime or 1; if $P \smallsetminus p\mathbb{N}$ has a smallest element q, then $p\mathbb{N} + q\mathbb{N} \subseteq P$ contains all numbers at least from $(pq)^2$ onwards; so must contain all primes, so $p = 2$, $q = 3$.

   There are no proper automorphisms of $\mathbb{N}$: $f(1) = f(0+1) = f(0) + f(1)$ and $f(1) = f(1 \cdot 1) = f(1)^2$, so $f(0) = 0$, $f(1) = 1$, and $f(n) = f(1 + \cdots + 1) = n$.

2. $\mathbb{Z}$ is a Euclidean Domain.

   (a) The primes are infinite in number (otherwise $p_1 \cdots p_n + 1$ is not divisible by any p_i).

   (b) If m, n are co-prime then $m + n\mathbb{Z}$ has infinitely many primes.

   (c) $\mathrm{Jac}(\mathbb{Z}) = 0 = \mathrm{Soc}(\mathbb{Z})$.

3. $\mathbb{Z}_m$, $m = p^r q^s \cdots$, is a commutative ring:

   (a) The invertibles are the coprimes $\gcd(n, m) = 1$; the zero divisors are multiples of $p, \ldots$; the nilpotents are multiples of $pq \cdots$.

   (b) The maximal/prime ideals are $\langle p \rangle, \ldots$; the irreducible ideals are $\langle p^i \rangle, \ldots$; so $\mathrm{Jac} = \langle pq \cdots \rangle = \mathrm{Nilp}$.

   (c) The minimal ideals are $\langle n/p \rangle, \ldots$; so $\mathrm{Soc} = \langle n/pq \cdots \rangle$.

   (d) $\mathbb{Z}_m \cong \mathbb{Z}_{p^r} \oplus \cdots \oplus \mathbb{Z}_{q^s}$.

   (e) Special cases include $\mathbb{Z}_{pq\cdots}$ (i.e., m square-free) which is semi-simple, $\mathbb{Z}_{p^n}$ which is a local ring, and $\mathbb{Z}_p$ which is a field.

   (f) $x = a_i \pmod{m_i}$ has a solution when m_i are co-prime (Chinese remainder theorem).

(g) The $\mathbb{Z}$-module-morphisms $\mathbb{Z}_m \to \mathbb{Z}_n$ are multiplications $x \mapsto rx$ where r is a multiple of $n/\gcd(m,n)$ (since $m\phi(1) = \phi(m) = 0$; there are no ring morphisms except 0 and 1 if $m = n$).

(h) $n^{\phi(m)} = 1$ for n invertible; so, for n invertible, $x = y \pmod{\phi(m)} \Rightarrow n^x = n^y \pmod m$;

4. $\mathbb{F}_{p^n}$ are the finite fields; they have size p^n with p prime: its prime subfield is $\mathbb{Z}_p$ and $\mathbb{F}_{p^n}$ is an n-dimensional vector space (Galois extension) over it.

   (a) The generator ω of the cyclic group $\mathbb{F}_{p^n} \smallsetminus 0$ is called a 'primitive root of unity'. All extensions are simple since $E \smallsetminus 0$ is a cyclic group generated by, say, a, so $E = F(a) = F[a]$.

   (b) $\mathbb{F}_{p^n} \cong \mathbb{F}_p[x]/\langle q \rangle$ where $q(x)$ is an irreducible polynomial of degree n having ω as a root.

   (c) The automorphism group $GL(\mathbb{F}_p^n)$, i.e., the Galois group of $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$, is $C_{p^{n-1}}$ generated by $x \mapsto x^p$ (since $\sigma(x) = x \Leftrightarrow x^p = x \Leftrightarrow x \in \mathbb{F}_p$).

   (d) The subfields of $\mathbb{F}_{p^n}$ are $\mathbb{F}_{p^k} = \{\, x : x^k = x \,\}$ for each $k|n$; the corresponding subgroups are $C_{p^{n-k}}$.
   Proof: $\mathbb{F}_{p^n}$ is a vector space over $\mathbb{F}_{p^k}$ i.e., $\dim_{\mathbb{F}_{p^k}} \mathbb{F}_{p^n} = n - k$; conversely, for all $x \in \mathbb{F}_{p^k}$, $x^{p^k} = x$, so $x^{p^n} = x$.).

   (e) The algebraic closure is the field $\bigcup_{n\in\mathbb{N}} \mathbb{F}_{p^n}$.

5. $\mathbb{F}_p$

   (a) The product of all the invertible pairs is $(p-2)! = 1 \pmod p$.

   (b) The squares x^2 are called 'quadratic residues'; when $p \neq 2$ exactly half of the non-zero numbers are squares.

   (c)

$\times$	sq.	non-sq.
sq.	sq.	non-sq.
non-sq.	non-sq.	sq.

   (d) Quadratic reciprocity:

      i. $x^2 = -1$ has a solution $\Leftrightarrow p = 1 \pmod 4$;
      ii. $x^2 = 2$ has a solution $\Leftrightarrow p = \pm 1 \pmod 8$;
      iii. $x^2 = -3$ has a solution $\Leftrightarrow p = 1 \pmod 3$;
      iv. $x^2 = 5 \Leftrightarrow p = \pm 1 \pmod 5$;
      v. For p, q odd primes, q is a square in $\mathbb{Z}_p \Leftrightarrow p$ is a square in $\mathbb{Z}_q$ and -1 is a square in $\mathbb{Z}_p$ or $\mathbb{Z}_q$, or p is a non-square in $\mathbb{Z}_q$ and -1 is a non-square in $\mathbb{Z}_p$ and $\mathbb{Z}_q$.
      vi. $x^2 = 2 \Rightarrow x^4 = 2$ when $p = 3 \pmod 4$;
      vii. $x^4 = 2 \Leftrightarrow p = a^2 + 64b^2$ when $p = 1 \pmod 4$.

6. $\mathbb{Q}$ is a field: $\mathrm{Hom}(\mathbb{Q}) \cong \mathbb{Q}$. It has no proper automorphisms (since for $n \in \mathbb{N}$, $f(n) = n$, so $1 = f(\frac{1}{n} + \cdots + \frac{1}{n}) = nf(\frac{1}{n})$ and $f(\frac{m}{n}) = f(\frac{1}{n} + \cdots + \frac{1}{n}) = \frac{m}{n}$.

7. $\mathbb{Z}[\sqrt{d}]$: invertibles of $\mathbb{Z}[i\sqrt{d}]$ are ± 1; of $\mathbb{Z}[i]$ are $\pm 1, \pm i$; of $\mathbb{Z}[\sqrt{d}]$ are infinitely many (Pell's equation). For $d \geqslant 3$, $\mathbb{Z}[\sqrt{-d}]$ is not a GCD (2 is irreducible but not prime).

8. $\mathcal{O}_F$ Ring of Algebraic Integers: these are those algebraic numbers over F whose minimal polynomials are monic in $\mathbb{Z}[x]$.

$$\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{when } d = 0, 2, 3 \pmod 4, \\ \{\, \frac{1}{2}(m + n\sqrt{d}) : m, n \text{ both odd or both even} \,\} & \text{when } d = 1 \pmod 4 \end{cases}$$

For d square-free, $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ is a UFD/PID only for (the italic are not EDs)

$$\begin{aligned} d = &\mathit{-163}, \mathit{-67}, \mathit{-43}, \mathit{-19}, -11, -7, -3, -2, -1, \\ &2, 3, 5, 6, 7, 11, 13, \mathit{14}, 17, 19, 21, 29, 33, 37, 41, 57, 73, \ldots \end{aligned}$$

and (conjecture) for infinitely many $d > 0$.

For example, Fermat's theorem: A prime can be expressed as a sum of two squares iff $p = 1 \pmod 4$ or $p = 2$ (since $p = a^2 + b^2 = (a + ib)(a - ib)$ in $\mathbb{Z}[\sqrt{-1}]$).

Every algebraic number over $\mathbb{Q}$ is a fraction times an algebraic integer: if x satisfies $\sum_i \frac{m_i}{n_i} x^i = 0$ then multiplying by $n := \mathrm{lcm}(n_i)$ gives $\sum_i m_i r_i (nx)^i = 0$. The only rational algebraic integers over $\mathbb{Q}$ are the integers (since if m/n satisfies a polynomial, then multiply by n^k to get $m^k + q(m)n + a_0 n^k = 0$, so $p|n \;\Rightarrow\; p|m$.) For example, $\sqrt{n}$ (n not a square) is irrational.

9. $\mathbb{Q}_{(2)}$ (rationals without 2 in denominator) is a local ring and a PID. The invertibles have odd numerator/denominator; the only irreducible/prime element is 2; $\mathrm{Jac} = \langle 2 \rangle$ and $\mathrm{Nil} = 0$.

10. $\mathbb{Z}$ acting on $\mathbb{Q}$: $\mathrm{Jac} = \mathbb{Q}$, $\mathrm{Soc} = 0$; no maximal or minimal sub-modules; not finitely generated; torsion-free; not free; $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}) \cong \mathbb{Q}$.

11. $\mathbb{Q}[x]$ is a Euclidean domain.

    (a) If a polynomial p is reducible in $\mathbb{Q}[x]$ then it is reducible in $\mathbb{F}_p[x]$ for all p; but there are irreducible polynomials in $\mathbb{Q}[x]$ that are reducible in all $\mathbb{F}_p[x]$.

    (b) If a monic polynomial splits in $\mathbb{Z}_p[x]$ into irreducible factors (having simple roots) of degrees n_i, then the Galois group of $p(x)$ has a permutation with cycle structure n_i, e.g. $x^5 - x - 1$ is irreducible in $\mathbb{Z}_3[x]$ so there is a cycle (12345), but in $\mathbb{Z}_2[x]$, it equals $(x^2 + x + 1)(x^3 + x^2 + 1)$ so there is a cycle $(ab)(cde)$, hence the Galois group is S_5.

(c) The cyclotomic polynomials are irreducible.
Proof: If $\phi_n(x) = p(x)q(x)$ with p irreducible, then ζ is a root of $p(x)$ but ζ^p is not a root, for some $p \not| n$, wolog prime; so ζ is a root of both $p(x)$ and $q(x^p)$, so there is a common factor of $p(x)$ and $q(x^p) = q(x)^p$ in $\mathbb{F}_p[x]$, hence $p(x)$, $q(x)$ have a common factor in $\mathbb{F}_p[x]$, so $x^n - 1$ has multiple factors, a contradiction.
Hence the root ζ_n of $x^n = 1$ is an algebraic integer of degree $\phi(n)$ (=degree of ϕ_n).

12. $F[x, y]$: $\langle x, y\rangle$ is maximal; $\langle x\rangle$, $\langle x, y\rangle, \ldots$ are prime; $\langle x^r, y^s\rangle$ are irreducible. $\langle x, y\rangle^2 \subset \langle x^2, y\rangle \subset \langle x, y\rangle$, so $\langle x^2, y\rangle$ does not have a factorization into prime ideals.

8.1 Matrix Algebras $M_n(V)$

1. Idempotents are the *projections* $P|_{\ker P} = 0$ AND $P|_{\operatorname{im} P} = I$, so $X = \operatorname{im} P \oplus \ker P$.
   Proof: $x = Py \;\Rightarrow\; Px = P^2y = Py = x$, $P^2x = P(Px) = Px$; $x = (x - Px) + Px \in \ker P + \operatorname{im} P$, $x \in \ker P \cap \operatorname{im} P \;\Rightarrow\; x = Px = 0$.

2. The following definitions for a square matrix T are independent of a basis,

Trace	$\operatorname{tr} T := T^i_i$,	$\operatorname{tr}(S+T) = \operatorname{tr} S + \operatorname{tr} T$, $\operatorname{tr}(ST) = \operatorname{tr}(TS), \operatorname{tr} T^\top = \operatorname{tr} T$
Determinant	$\det T := \sum_{\sigma \in S_n} \operatorname{sign}\sigma$	$\prod_{i=1}^n T_i^{\sigma(n)} = \epsilon^{ij\cdots k} T_{1i}T_{2j}\cdots T_{nk}$, $(\epsilon^{ij\cdots k} = \operatorname{sign}(ij\cdots k)$ $\det(ST) = \det S \det T$, $\det T^\top = \det T, \det\lambda = \lambda^n$

   (expansion by co-factors; use Gaussian elimination).
   Cauchy-Binet identity: for $A : U \to V$, $B : V \to W$,
   $$\det_{I,J}(BA) = \sum_{|K|=n} (\det_{J,K} B)(\det_{K,I} A),$$
   where $\det_{K,I} A$ is the determinant of the square matrix with rows I and columns K, and $|I| = |J| = |K|$.

3. A matrix T is invertible $\Leftrightarrow$ T is 1-1 $\Leftrightarrow$ T is onto $\Leftrightarrow$ $\det T \neq 0 \Leftrightarrow$ T is not a divisor of 0 (since $\dim \operatorname{im} T = \dim V \;\Leftrightarrow\; \operatorname{im} T = V$), $T^{-1} = \frac{1}{\det T}\operatorname{Adj}(T)$;

4. For finite dimensions, $M_n(V)$ has no proper ideals, so Jac $= 0$.

5. Each eigenvalue λ of T has a corresponding eigenspace $\bigcup_i \ker(T - \lambda)^i$ that is T-invariant.
   (a) For each eigenvalue, $Tx = \lambda x$, $T^{-1}x = \lambda^{-1}x$, $p(T)x = p(\lambda)x$.
   Proof: $m(x) = (x - \lambda)p(x) \;\Rightarrow\; 0 = m(T) = (T - \lambda)p(T) \;\Rightarrow\; \exists v \neq 0, (T - \lambda)v = 0$. Conversely, $\forall v,\; 0 = m(T)v = m(\lambda)v \;\Rightarrow\; m(\lambda) = 0$,

(b) Distinct eigenvectors are linearly independent.
Proof: If $\sum_i a_i v_i = 0$ then $\sum_i a_i \lambda_i v_i = 0$; if $a_j \neq 0$, then $\sum_i a_i(\lambda_i - \lambda_j)v_i = 0$ so by induction $a_i = 0, i < j$, so $a_j v_j = 0$.

6. (a) T is said to be diagonalizable when there is a basis of eigenvectors; equivalently the minimum polynomial has distinct roots, or each eigenspace is $\ker(T - \lambda)$.
   (b) Every matrix has a triangular form.
   Proof: c_T splits in the algebraic closure of F, so for any root λ and eigenvector v, $[\![v]\!]$ is T-invariant, and so T can be defined on $X/[\![v]\!]$; hence by induction).
   (c) If S, T are invertible diagonalizable symmetric matrices, and $S + \alpha T$ is non-invertible for n values of α, then S, T are simultaneously diagonalizable.
   Proof: $S^{-1}T - \lambda_i$ is non-invertible i.e., $\exists v_i, S^{-1}Tv_i = \lambda_i v_i$ for n values of λ_i; so $\lambda_i v_i^\top S v_j = (S^{-1}Tv_i)^\top S v_j = v_i^\top T^{-1} v_j = \lambda_j v_i^\top S v_j$, hence $\lambda_i \neq \lambda_j \;\Rightarrow\; v_i^\top S v_j = 0 = v_i^\top T v_j$.

7. Nilpotent matrices have the form $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ & & \vdots \end{pmatrix}$ (with respect to the following basis: consider the T-invariant subspaces $0 \leqslant T^{-1}0 \leqslant T^{-2}0 \leqslant \ldots \leqslant T^{-n}0 = X$, so $X = T^{-1}0 \times \frac{T^{-2}0}{T^{-1}0} \times \cdots \times \frac{T^{-n}0}{T^{-n+1}0}$; then if $u_i + T^{-k}0$ are linearly independent, then so are $Tu_i + T^{-k+1}0$; thus start with a basis for $T^{-n}0/T^{-n+1}0$, and extend for each subspace until $T^{-1}0$);

8. The (upper) triangular matrices form a subalgebra $U_n(F^n)$, which contains the sub-algebra Diag of the diagonal matrices. The Jacobson radical of U_n consists of the strictly triangular matrices $\mathcal{N}(F^n)$ (since the map $U_n \to Diag$, $A \mapsto D$ is a morphism with kernel being the (super-)nilpotents, i.e., Jac), U_n/Jac is semi-simple with n simple sub-modules.

9. Jordan Canonical Form: If F is agebraically closed, the minimum polynomial splits into factors $(x-\lambda)^k$, consider the decomposition $T = \lambda + (T - \lambda)$, with $(T - \lambda)^k = 0$, so that T is the sum of a diagonal and a nilpotent matrix. So $\det T = \prod_i \lambda_i$, $\operatorname{tr} T = \sum_i \lambda_i$;

10. Every matrix T decomposes into a 'product' of irreducible matrices $\begin{pmatrix} T_1 & & \\ & T_2 & \\ & & \ddots \end{pmatrix}$ (via the decomposition of $F[T]$ into T-invariant submodules M_p, where $[\![x]\!] = F[T]x = [\![x, Tx, \ldots, T^{m-1}x]\!]$). The minimum polynomial of such a product is the lcm of the minimum polynomials of T_i; conversely, when $m_T(x) = p_1(x) \ldots p_r(x)$ is its irreducible decomposition, then $T_i = \begin{pmatrix} \lambda & 1 & \\ & \lambda & \\ & & \ddots \end{pmatrix}$.

The characteristic polynomial of this 'product' is the product of the characteristic polynomials.

11. Linear Representations (in the group of automorphisms $GL(n)$): the number of inequivalent irreducible representations = number of conjugacy classes; $\sum_i n_i^2 = |G|$, where n_i are the dimensions of the irreducible representations; if the representation is irreducible then $\boldsymbol{\chi} \cdot \boldsymbol{\chi} = |G|$; for two irreducible representations, $\boldsymbol{\chi}_T \cdot \boldsymbol{\chi}_S = 0$.

8.1.1 Tensor Algebras

A multi-linear map is a map on $X^r \times (X^*)^s$ which is linear in each variable. They form the *tensor algebra* $\mathcal{T}_s^r(X)$, with product

$$T \otimes S(x, \dots, y, \dots) := T(x, \dots)S(y, \dots),$$

or in coordinates, $T^{i\cdots}{}_{j\cdots}S^{k\cdots}{}_{l\cdots}$. It is associative and graded, i.e., if $S \in \mathcal{T}_s^r(X)$ and $T \in \mathcal{T}_{s'}^{r'}(X)$ then $S \otimes T \in \mathcal{T}_{s+s'}^{r+r'}(X)$.

Tensor algebras have dual tensor algebras, $\mathcal{T}(X)^* \cong T(X^*)$ ($S^* \otimes T^{**}(x, y^*) = S^*(x)T^{**}(y^*)$ is an isomorphism).

Contraction: For each $x \in X$, the map $A_{i\dots} \mapsto A_{i\dots}x^j$ is a morphism $\mathcal{T}_s^r(X) \to \mathcal{T}_s^{r+1}(X)$; its dual map is *contraction* by x, $A_{i\dots}x^j \mapsto A_{i\dots}x^i$, $\mathcal{T}_s^r(X) \to \mathcal{T}_{s-1}^r(X)$, here generically denoted by $A \cdot x$.

1. Every bilinear form splits into a symmetric and an anti-symmetric part (if $2 \neq 0$) since $T(x, y) = \frac{1}{2}(T(x, y) + T(y, x)) + \frac{1}{2}(T(x, y) - T(y, x))$; the symmetric part is determined by the *quadratic* form $T(x, x)$ since the polarization identity holds:

$$\frac{1}{2}(T(x, y) + T(y, x)) = \frac{1}{2}(T(x + y, x + y) - T(x, x) - T(y, y))$$

2. An *inner product* $\langle \cdot, \cdot \rangle$ is a symmetric bilinear form g_{ij}.

   (a) When invertible, there is a correspondence between vectors and covectors (raising and lowering of indices), via $A_i = g_{ij}A^j$, so $V^* \cong V$.

   (b) It extends to act on tensors, $\langle A, B \rangle = A_{ij\dots}B^{ij\cdots}$ if of the same grade, otherwise 0.

   (c) Any 2-tensor can be decomposed into $\alpha g_{ij} + A_{ij} + B_{ij}$ where A is anti-symmetric, B is traceless symmetric (spin-0+spin-1+spin-2).

3. A *symplectic* form is an anti-symmetric bilinear form. Example: $X \times X^*$ has a symplectic form $\omega(\begin{pmatrix} x \\ \phi \end{pmatrix}, \begin{pmatrix} y \\ \psi \end{pmatrix}) := \psi(x) - \phi(y)$; the canonical one-form is $\theta \begin{pmatrix} x \\ \phi \end{pmatrix} = \phi(x)$.

8.1.2 Clifford Algebras and Exterior Algebras

Given a vector space X over F with an inner product $\langle , \rangle$, then the *Clifford algebra* $\mathcal{C}\ell(X)$ is an algebra over F that contains X such that for $x \in X$,

$$x^2 = \langle x, x \rangle.$$

It is realized as the quotient of the tensor algebra $\mathcal{T}(X)/\langle x^2 - \langle x, x\rangle \rangle$ (more generally, for any ring, $R\langle x_1, ..., x_n\rangle/\langle x_i x_j + x_j x_i = 0, x_i^2 = \langle x_i, x_i\rangle\rangle$). Thus

$$\langle x, y\rangle = \frac{1}{2}(xy + yx), \quad x \wedge y := \frac{1}{2}(xy - yx) = -y \wedge x,$$

$$\text{so} \qquad xy = \langle x, y\rangle + x \wedge y$$

(assuming throughout $2 \neq 0$; $x, y, \dots$ denote vectors, $a, b, \dots$ tensors).

Three special cases are:

1. The *exterior* algebra $\Lambda(X)$ with $\langle , \rangle = 0$. It consists of the totally anti-symmetric tensors, $A_{\sigma(i\dots)} = \text{sign}(\sigma) A_{i\dots}$ (in indices it is written as $A_{[i\dots]}$).
2. *Euclidean* algebra with $g = 1$, i.e., $\langle e_i, e_j\rangle = \delta_{ij}$,
3. *Spinor* algebra with $g = -1$, i.e., $e_i^2 = -1$.

$\wedge$ is extended to tensors by taking it to be associative, and distributive over $+$.

1. For example, for $g_{ij} = \begin{pmatrix} 1 & & \\ & 1 & \\ & & -1 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ -1 \\ 1 \end{pmatrix} \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix} = 3\boldsymbol{i} - 3\boldsymbol{j} + \boldsymbol{k} - 4\boldsymbol{ijk}$.
2. Orthogonal vectors satisfy $\langle x, y\rangle = 0$, so $xy = x \wedge y = -yx$; more generally, $x \cdots y = x \wedge \dots \wedge y$.
3. For an orthonormal basis,
$$x_1 \wedge \dots \wedge x_n = \frac{1}{n!} \varepsilon^{i_1 \cdots i_n} x_{i_1} \cdots x_{i_n} = \det[x_1, \dots, x_n] e_1 \dots e_n,$$
where the matrix columns are the x_i's in terms of the basis.
4. (a) Vectors are invertible with $x^{-1} = x/\langle x, x\rangle$, unless $\langle x, x\rangle = 0$, when x is called *null*.
   (b) $xyx = 2\langle x, y\rangle x - x^2 y$ (since $xy = \langle x, y\rangle + \frac{xy - yx}{2}$).
5. The algebra is *graded*: as a vector space it is isomorphic to $\sum_k \Lambda_k(X)$
   (a) $\Lambda_0(X) = F$, scalars,
   (b) $\Lambda_1(X) = X$, vectors,

(c) $\Lambda_2(X)$ consists of 2-forms A^{ij}; for x, y linearly independent, $x \wedge y$ corresponds to the plane $[\![x, y]\!]$ (with an orientation),

(d) $\Lambda_k(X)$ is generated by $e_{i_1} \cdots e_{i_k}$ $(i_1 < \cdots < i_k)$, so has dimension $\binom{n}{k}$ where $n = \dim X$. Each $x_1 \wedge \ldots \wedge x_k$ defines a sub-space $[\![x_1, \ldots, x_k]\!]$, which satisfies the equation $x \wedge (x_1 \wedge \ldots \wedge x_k) = 0$.

(e) When finite-dimensional, the 'highest' space is a one-dimensional space of *pseudo-scalars*, $\Lambda_n(X) = [\![\omega]\!]$, generated by $\omega := e_1 \cdots e_n$, with indices $\varepsilon_{i\ldots j}$.

The dimension of the algebra is thus 2^n.

6. $\mathcal{C}\ell(X)$ splits into the even and odd elements $\Lambda_{even} \oplus \Lambda_{odd}$; products of an even/odd number of vectors is of even/odd grade:

	even	odd
even	even	odd
odd	odd	even

thus the even-graded elements form a sub-algebra, isomorphic to the Clifford algebra on $e^\perp$ with symmetric form $-\langle e, e\rangle g$ for any non-degenerate e.

7. (a) $a \wedge b = \pm b \wedge a$ with $+$ when a, b are both odd or both even; even and odd elements are 'invariant', $a \wedge b = c \wedge a$.

   (b) $x \wedge y + \cdots + x' \wedge y' = 0 \Rightarrow x, x' \in [\![y, \ldots, y']\!]$,

   (c) $x \wedge \ldots \wedge y = 0 \Leftrightarrow x, \ldots, y$ are linearly dependent;

   (d) $a \wedge a = 0 \Leftrightarrow a = x \wedge y$ (the set of such a is called the Klein quadric)

8. Contraction by $x \in V$ maps $\Lambda_k \to \Lambda_{k-1}$, and is the dual map of $x\wedge$.

   (a) $x \cdot (y \cdot a) = -y \cdot (x \cdot a)$, so double contraction by x gives 0.

   (b) $x \cdot (a \wedge b) = (x \cdot a) \wedge b \pm a \wedge (x \cdot b)$, with $+$ when a is even.

9. The radical of ΛX is the ideal generated by the generators x_i; the center is generated by the even elements and the nth element. ΛX and its center are local rings.

10. In finite dimensions, the *Clifford group* is the group of invertible elements a for which $ax(Pa)^{-1}$ is a vector for all $x \in X$; it acts on X by $x \mapsto ax(Pa)^{-1}$. The subgroup of elements of norm 1 is called $\mathrm{Pin}(X)$, and its subgroup of $\det = 1$ is called $\mathrm{Spin}(X)$.

11. In finite dimensions,

    (a) $\varepsilon^{ab\cdots}\varepsilon_{cd\ldots} = \sum_\sigma \mathrm{sign}(\sigma)\delta^a_{\sigma(c)}\delta^b_{\sigma(d)}$, in particular $\varepsilon^{abc}\varepsilon_{ade} = \delta^b_d\delta^c_e - \delta^b_e\delta^c_d$, $\varepsilon^{ab\cdots}\varepsilon_{ab\ldots} = n!$;

    (b) Hodge-dual map $* : \Lambda_k(X) \to \Lambda^{n-k}(X)$, $a_{i\cdots k} \mapsto \varepsilon^{i\cdots k\cdots n}a_{i\cdots k} = \omega a?$; $** = \pm\pm 1$ with first $-$ when n is even and k odd, and second $+$ when the number of -1s of the inner product g is even; $*(\alpha \wedge *.) = (-1)^{nk}(\alpha\wedge)^*$ (contraction with α).

(c) $\Lambda_k \cong \Lambda_{n-k}$ via the Hodge map, $*a \cdot b\varepsilon = a \wedge b$;

12. Linear transformations $T : X \to Y$ extend to $T : \mathcal{C}\ell(X) \to \mathcal{C}\ell(Y)$ (linear) by $T(a \wedge b) := Ta \wedge Tb$. Then $T\omega = (\det T)\omega$, so $\det(ST) = \det S \det T$ (since $\det(ST)\omega = (ST)(\omega) = S(\det T\omega) = \det T \det S\omega$). $T^*\omega(x_1, \ldots, x_n) = \omega(Tx_1, \ldots, Tx_n) = (\det T)\omega(x_1, \ldots, x_n)$.
    $T^{-1} = \frac{1}{\det T}\omega T^\top \omega^{-1}$.

13. Morphisms $T(xy) = (Tx)(Ty)$ are the linear transformations that preserve the inner product, $\langle Tx, Ty\rangle = \langle x, y\rangle$.

14. Reflections P have the property $P^2 = I$, $Px = -x$; they fix the even subalgebra but not the odd. For example, in Euclidean algebra, $x \mapsto -uxu$ is a reflection along the normal u (since $u \mapsto -u$, $u^\perp \mapsto u^\perp u^2 = u^\perp$).

15. There is a transpose, $(x \cdots y)^\top := y \cdots x$, e.g. $1^\top = 1$, $x^\top = x$, $a^\top = \pm a$ for a even/odd; $\omega^\top = \pm\omega$ (+ when $n = 0, 1 \pmod 4$).
$$(ab)^\top = b^\top a^\top, \qquad a^{\top\top} = a.$$
    Conjugation is then $a \mapsto a^* := Pa^\top$, so $x^* = -x$, $(xy)^* = -yx$.

16. A *rotor* in the plane $a := xy$, where $x^2y^2 = \pm 1$, is the map $R : x \mapsto a^\top xa$.
$$\langle Ru, Rv\rangle = \frac{1}{2}(RuRv + RvRu) = \frac{1}{2}yx(uv + vu)xy = \langle u, v\rangle.$$
    Over $\mathbb{R}$, $a = xy = \cos\frac{\theta}{2} + \sin\frac{\theta}{2}\, b = e^{\frac{1}{2}\theta b}$ ($b^2 = -1$); A *spinor* is of the type $a = \alpha + \beta\omega$; then $R : v \mapsto a^\top va$ gives $Rv = (\alpha^2 + \beta^2)v$ (for $\dim X = 0, 3 \pmod 4$).

17. The inner product extends to a bilinear product on $\mathcal{C}\ell(X)$ by $\langle a, b\rangle := (a^\top b)_0$ (the scalar term of $a^\top b$).
    (a) For a, b of grades r, s, $ab =: a * b + \cdots + a \wedge b$, where $a * b$ has grade $|r - s|$; in particular, $xa = x * a + x \wedge a$, $a * x = \pm x * a$; for a of grade 2, $ab = a * b + [a, b] + a \wedge b$.
    (b) $\langle a, b\rangle = \sum_{k=0}^n (a)_k(b)_k$
    (c) $\langle x, y \cdots z\rangle = \frac{1}{2}(xy \cdots z \pm y \cdots zx)$
    (d) $\langle x \cdots y, z\rangle = \langle x, z\rangle \cdots \langle y, z\rangle$.
    (e) $\langle x, y \wedge z\rangle = -\langle y \wedge z, x\rangle$
    (f) $\langle x_1 \wedge \ldots \wedge x_k, y_1 \wedge \ldots \wedge y_l\rangle := \det[\langle x_i, y_j\rangle]$ for $k = l$, and 0 otherwise.
    (g) $\langle x^\top y, z\rangle = \langle y, xz\rangle$, $\langle yx^\top, z\rangle = \langle y, zx\rangle$
    (h) $a * (b\omega) = (a \wedge b)\omega$ for a, b of low enough grade (since $(ab\omega)_k = (ab)_{n-k}\omega$).

18. The Clifford algebras over $\mathbb{R}$ and $\mathbb{C}$ are classified:

    Over $\mathbb{R}$, every non-degenerate symmetric form is equivalent to one with 'signature' p, q, i.e., $e_i^2 = \pm 1$. The even sub-algebra of $\mathcal{C}\ell_{p,q}(\mathbb{R})$ is $\mathcal{C}\ell_{p,q-1}(\mathbb{R})$ if $q > 0$, and $\mathcal{C}\ell_{q,p-1}(\mathbb{R})$ if $p > 0$; so $\mathcal{C}\ell_{p,q}(\mathbb{R})$ equals

$\mathcal{C}\ell_{p,q}(\mathbb{R})$	$s = p - q \pmod 8$							
$n = p + q$	-3	-2	-1	0	1	2	3	4
0				$\mathbb{R}$				
1			$\mathbb{C}$		$\mathbb{R}^2$			
2		$\mathbb{H}$		$M_2(\mathbb{R})$		$M_2(\mathbb{R})$		
3	$\mathbb{H}^2$		$M_2(\mathbb{C})$		$M_2(\mathbb{R})^2$		$M_2(\mathbb{C})$	
4		$M_2(\mathbb{H})$		$M_4(\mathbb{R})$		$M_4(\mathbb{R})$		$M_2(\mathbb{H})$
				$\dots$				
$2m$		$M_{2^{m-1}}(\mathbb{H})$		$M_{2^m}(\mathbb{R})$		$M_{2^m}(\mathbb{R})$		$M_{2^{m-1}}(\mathbb{H})$
$2m+1$	$M_{2^{m-1}}(\mathbb{H})^2$		$M_{2^m}(\mathbb{C})$		$M_{2^m}(\mathbb{R})^2$		$M_{2^m}(\mathbb{C})$	
.								

    (For example,$\mathcal{C}\ell_{0,2}(\mathbb{R})$ has basis $1, \boldsymbol{i}, \boldsymbol{j}, \omega$; the even sub-algebra is $\mathbb{C}$. $\mathcal{C}\ell_{0,3}(\mathbb{R})$ has basis $1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}, i := \boldsymbol{ij}, j, k, \omega$; the even sub-algebra is $\mathbb{H}$.).

    Over $\mathbb{C}$, every non-degenerate symmetric form is equivalent to I, so $\mathcal{C}\ell_n(\mathbb{C})$ equals

n	0	1	2	$\cdots$	$2m$	$2m+1$
$\mathcal{C}\ell_n(\mathbb{C})$	$\mathbb{C}$	$\mathbb{C}^2$	$M_2(\mathbb{C})$		$M_{2^m}(\mathbb{C})$	$M_{2^m}(\mathbb{C})^2$.

8.1.3 Weyl algebra

The Weyl algebra over $F \supseteq \mathbb{Q}$ is the algebra of differential operators on $F[x]$; it is that algebra generated by x, y such that $[y, x] = 1$; it is realized as $F\langle x, y\rangle/[yx - xy - 1]$, and is the smallest algebra that contains $F[x]$ in which $\partial_x = \mathcal{L}_y$.

For more variables it is similar: $[x_i, x_j] = 0 = [y_i, y_j]$, $y_i x_j = 0$, $[y_i, x_i] = 1$; it acts on $F[x_1, ..., x_n]$ via multiplication and differentiation.

1. A Weyl algebra is simple: every non-zero Lie ideal contains 1.

   Proof: Elements of the form $x^a y^b$ generate the algebra since $yx = xy + 1$. $\mathcal{L}_x = \partial_x$, $\mathcal{L}_y = \partial_y$. But differentiation reduces the degree of a polynomial, so if $a \in I$, $a \neq 0$, then $\mathcal{L}_x(a) \neq 0$, so a sequence of derivatives $\mathcal{L}_x \mathcal{L}_y ...(a) \neq 0$.

2. The same proof shows that the center of a Weyl algebra is F.

8.1.4 Incidence algebra $\mathbb{N}[\leqslant]$

consists of functions $f(m, n)$, where $m|n$, with

$$(f + g)(m, n) := f(m, n) + g(m, n), \quad f * g(m, n) := \sum_{m|i|n} f(m, i)g(i, n)$$

The identity is the Kronecker delta function $\delta(m,n)$.

The inverse of the constant function 1 is $\mu'(m,n) := \mu(n/m)$ where μ is the Möbius function $\mu(n) = \begin{cases} (-1)^k & n = p_1 \cdots p_k, \text{ square free} \\ 0 & n \text{ not square-free} \end{cases}$; $\mu(mn) = \mu(m)\mu(n)$.

The incidence algebra on a (finite) ordered space $\mathbb{Q}[\leqslant]$ is isomorphic to the algebra of upper triangular matrices in which $A_{ij} = 0$ for $i \not\leqslant j$ (in the ordered space).

8.1.5 Lie algebras

1. $so(n)$ the skew-symmetric matrices $\langle Ax, y\rangle = -\langle x, Ay\rangle$, i.e., $A^\top g = -gA$; has basis of $F_{ij} := -i(E_{ij} - E_{ji})$ and $H_i := F_{2i-1,2i}$; dimension $\binom{n}{2}$; $[H_i, F_{2i-1,j}] = iF_{2i,j}$, $[H_i, F_{2i,j}] = -iF_{2i-1,j}$. $so(3)$ $(g = 1)$ is generated by $l_1 := \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $l_2 := \begin{pmatrix} 0 & 0 & -1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$, $l_3 := \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$ with $[l_i, l_j] = \epsilon_{ijk} l_k$; or $L_i := il_i$ with $[L_i, L_j] = i\epsilon_{ijk} L_k$. $L^2 := L_1^2 + L_2^2 + L_3^2$ commutes with each L_i, so the eigenstates of L^2 (with eigenvalues $n(n+1)$) are common to all L_i. But $e^{2\pi i l} = -1$ not $+1$, so e^{itl} really act on spinors, not vectors. $so(4)$ and $so(5)$ have rank 2.

2. $sl(n)$ the traceless matrices; basis of $H_i := E_{ii} - E_{i+1,i+1}$ and E_{ij} $(i \neq j)$; dimension n^2-1; $[H_i, E_{ij}] = E_{ij}$, $[H_i, E_{i+1,j}] = -E_{i+1,j}$, $[H_i, E^\top] = -E^\top$, $[H_i, E_{i,i+1}] = 2E_{i,i+1}$, $[E_{ij}, E_{ji}] = E_{ii} - E_{jj}$.

3. $u(n)$ the skew-adjoint matrices $A^*g = -gA$. Contains $su(n)$, the traceless skew-adjoint matrices. The simplest, of rank 1, is $su(2) \cong so(3)$ $(g = 1)$, generated by the 'Pauli' matrices $\sigma_1 = i\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $\sigma_3 = i\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, with $[\sigma_i, \sigma_j] = \epsilon_{ijk}\sigma_k$; or by $\sigma_+ = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, $\sigma_- = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, σ_3, with $[\sigma_+, \sigma_-] = \sigma_3$, $[\sigma_3, \sigma_\pm] = 2\sigma_\pm$.

   $su(3)$ has rank 2, having Cartan subalgebra $\begin{pmatrix} 1 & & \\ & -1 & \\ & & 0 \end{pmatrix}$, $\frac{1}{\sqrt{3}}\begin{pmatrix} 1 & & \\ & 1 & \\ & & -2 \end{pmatrix}$.

4. $sp(2n)$ matrices $A^\top\Omega = -\Omega A$ where $\Omega = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$; basis of $H_i := E_{ii} - E_{i+n,i+n}$, $A_{ij} := E_{ij} - E_{i+n,j+n}$, $B_{ij} := E_{i+n,j+n} + E_{j+n,i+n}$, $C_{ij} = 2E_{i+n,j+n}$; dimension $\binom{2n}{2}$.

5. Upper triangular matrices of dimension $\binom{n+1}{2}$; contains the sub-algebra of Nilpotent matrices of dimension $\binom{n}{2}$, e.g. $n = 3$ is called the Heisenberg algebra.