1.2 Fields and Vector Spaces

Def 1.2.1 **Field**: set with functions

- $+ : F \times F \to F; (\lambda, \mu) \to \lambda + \mu$
- $\cdot : F \times F \to F; (\lambda, \mu) \to \lambda\mu$

such that $(F, +)$ and $F \setminus \{0\}, \cdot)$ are abelian groups, with

$$\lambda(\mu + \nu) = \lambda\mu + \lambda\nu.$$

Neutral identity elements: $\lambda + 0_F = \lambda$ and $\lambda \cdot 1_F = \lambda$. Additive inverse: $\forall \lambda \in F, \exists -\lambda$ such that $\lambda + (-\lambda) = 0_F$.
Multiplicative inverse: $\forall \lambda \in F, \exists \lambda^{-1}$ such that $\lambda \cdot \lambda^{-1} = 1_F$.

Vector Space: V over a field F is a pair consisting of an abelian group $(V, +)$ and a mapping $V \times F \to V; (\lambda, \vec{v}) \to \lambda\vec{v}$, such that the following identities hold:

- $\lambda(\vec{v} + \vec{w}) = (\lambda\vec{v}) + (\lambda\vec{w})$
- $(\lambda + \mu)\vec{v} = (\lambda\vec{v}) + (\mu\vec{v})$
- $\lambda(\mu\vec{v}) = (\lambda\mu)\vec{v}$
- $1_F\vec{v} = \vec{v}$

1.4 Vector Subspaces

Def 1.4.1: $U \subseteq V$ is a **vector subspace** if U contains the 0 vector, and whenever $\mathbf{u}, \mathbf{v} \in \mathbf{U}$, then $\mathbf{u} + \mathbf{v} \in U$ and $\lambda\mathbf{v} \in U$.

Prop 1.4.5: Let T be a subset of V over F. $\langle T \rangle \subseteq V$, the subset generated by the elements of T, unioned with the 0 vector, is the smallest vector subpsace.

Def 1.4.7 Subset of a vector space is a generating set if its span is the whole vector space.

Def 1.4.9 Power set: of X is the set of all subsets of X.

Prop : Intersection of vector subspaces is itself a vector space.

1.5 Linear Indpendence and Bases

Def 1.5.1 a subset L of a vector space V is called **linearly independent** if for all pairwise different vectors $\vec{v_1}, ...\vec{v_r} \in L$ and arbitrary scalars $\alpha_1, ...\alpha_r \in F$,

$$\alpha_1\vec{v_1} + ...\alpha_r\vec{v_r} = 0 \implies \alpha_1 = ... = \alpha_r.$$

Def 1.5.8 A basis of a vector space V is a linearly independent generating set in V.

Thm 1.5.11 Let $\vec{v_1}, ...\vec{v_r} \in V$ be vectors. The family $(\vec{v_i})_{1 \le i \le r}$ is a basis of V iff the "evaluation" mapping

$$\Phi : F^r \to V; (\alpha_1, ...\alpha_r) \to \alpha_1\vec{v_1} + ... + \alpha_r\vec{v_r}$$

is a bijection ** if every vector can be determined by a **unique** linear combination of elements in the family, then it is a basis.
Proof: fam is a generating set $\iff$ surjection, fam is linearly independent $\iff$ injection.

Thm 1.5.12 **Characterisation of bases** the following are equivalent

- E is a basis
- E is minimal among all generating sets
- E is maximal among all linearly independent sets

Cor 1.5.13 If V is a finitely generated vector space, then V has a basis.

Thm 1.5.14

1. If $L \subset V$ is a linearly independent subset and E is minimal among all generating sets of V with $L \subseteq E$, then E is a basis.
2. If $E \subseteq V$ is a generating set and if L is maximal among all linearly independent sets of V with $L \subseteq E$, then L is a basis.

Def 1.5.15 Let X be a set and F a field. Then the set $\mathrm{Maps}(X, F)$ of all mappings $f : X \to f$ is an F vector space under pointwise addition and scalar multiplication.
free vector space on X : the subset of mappings which send almost all elments of X to zero is a vector subspace:

$$F\langle x \rangle \subseteq \mathrm{Maps}(X, F).$$

Thm 1.5.16 Let $(\vec{v_i})_{i \in I}$ be a family of vectors from V. Then

1. $(\vec{v_i})_{i \in I}$ is a basis of V $\iff$
2. $\forall \vec{v} \in V$, there is exactly one family of elements from $(\alpha_i)_{i \in I}$ from F, almost all of which are zero, and such that

$$\vec{v} = \sum_{i \in I} \alpha_i \vec{v_i}.$$

1.6 Dimension of a Vector Space

Thm 1.6.1 No linearly independent subset of a given vector space has more elements than a generating set. Thus, if V is a vector space, $L \subset V$ a linearly independent subset and $E \subseteq V$ a generating set, then

$$|L| \le |E|.$$

Thm 1.6.2 Let V be a vector space, $L \subset V$ a finite linearly independent subset and $E \subseteq V$ a generating set. Then there is an injection $\phi : L \to E$ such that $(E \setminus \phi(L)) \cup L$ is also a generating set for V.

Thm 1.6.3 Let $M \subset V$ be a linearly independent subset, and $E \subseteq V$ a generating subset, such that $M \subseteq E$. If $\vec{w} \in V \setminus M$ is a vector not belonging to M such that $M \cup \{\vec{w}\}$ is linearly independent, then there exists $\vec{e} \in E \setminus M$ such that $\{E \setminus \vec{e}\} \cup \{\vec{w}\}$ is a generating set for V.

Cor 1.6.4 Let V be a finitely generated vector space.

1. V has a finite basis.
2. V cannot have an infinite basis.
3. Any two bases of V have the same number of elements.

Def 1.6.5 The cardinality of one basis of a finitely generated vector space V is called the dimension of V.

Cor 1.6.8 V finitely gen. vector space.

1. Each lin. indep subset $L \subset V$ has at most $\dim V$ elements, and if $|L| = \dim V$ then L is a basis.
2. each gen. set $E \subseteq V$ has at least $\dim V$ elements, and if $E = \dim V$ then E is a basis.

Cor 1.6.9 A proper vector subspace of a finite dim. vector space has a strictly smaller dimension.
Thm 1.6.11 V vector space, $U, W \subseteq V$ vector subspaces. Then

$$\dim(U) + \dim(W) = \dim(U + W) + dim(U \cap W)$$

1.7 Linear Mappings

Def 1.7.1 V and W vector spaces over F. A map $f : V \to W$ is a linear map or homomorphism if $\forall \vec{v_1}, \vec{v_2} \in V$ and $\lambda \in F$

$$f(\vec{v_1} + \vec{v_2}) = f(\vec{v_1}) + f(\vec{v_2}), \quad f(\lambda\vec{v_1}) = \lambda f(\vec{v_1})$$

Bijective homomorphism= **isomorphism**, homomorphism $V \to V$ = **endomorphism**. Isomorphism $V \to V$ = **automorphism**.

Def 1.7.5 Fixed point: sent to itself by a mapping. Set of fixed points of a map $f : X \to X$: $X^f = \{x \in X \ : \ f(x) = x\}$.

Def 1.7.6 Two vector subspaces U, W of a vector space V are complementary if addition defines a bijection $U \times W \to V$. V is the direct sum of U and W.

Thm 1.7.7 Let n be a natural number. Then any vector space over F is isomorphic to F^n iff it has dimension n.

Lem 1.7.8 V, W vector spaces over F and $B \subset V$ a basis. The restriction of a mapping gives a bijection

$$Hom_f(V, W) \to Maps(B, W), \quad f \to f|_B$$

A linear map determines and is determined by the values it takes on a basis.

Prop 1.7.9

1. Every injective linear map $f : V \to W$ has a left inverse (g such that $g \circ f = id_v$).
2. Every surjective linear map $f : V \to W$ has a right inverse (g such that $f \circ g = id_w$)

1.8 Rank-Nullity Theorem

Def 1.8.1 $im(f)$ is a vec. subspace of W. $ker(f) = f^{-1}(0) = \{v \in V \ : \ f(v) = 0\}$ is a vec. subspace of V.
Lem 1.8.2 linear mapping is injective iff kernel is 0.

Thm 1.8.4 Rank-Nullity Theorem:

$$\dim(V) = \dim(ker f) + \dim(im f)$$

2.1 Linear Mappings $F^m \to F^n$ and Matrices

Thm 2.1.1 Let $m, n \in \mathbb{N}$. $\exists$ bijection between the space of linear mappings $F^m \to F^n$ and $\mathrm{Mat}(n \times m; F)$:

$$M : \mathrm{Hom}_F(F^n, F^m) \tilde{\to} \mathrm{Mat}(n \times m; F), f \mapsto [f]$$

Note: the columns of the representing matrix are the images of f under the standard basis elements of F^m:

$$[f] = (f(\vec{e_1})...f(\vec{e_m}))$$

Prop M is an isomorphism of vector spaces.
Def 2.1.6 Lrt $n, m, l \in \mathbb{N}$, F a field, and let $A \in Mat(n \times m; F), B \in Mat(m \times l; F)$. The product $A \circ B \in Mat(n \times l; F)$ is defined by

$$(AB)_{ik} = \sum_{j=1}^{m} A_{ij}B_{jk}$$

Thm 2.1.8 Let $g : F^l \to F^m$ and $f : F^m to F^n$ be linear mappings. Then $[f \circ g] = [f] \circ [g]$.
Prop 2.1.9 properties of matrices (trivial).
Exercise 26: $(AB)^T = B^T A^T$

2.2 Basic Properties of Matrices

Def 2.2.1 Matrix A is invertible if $\exists$ B and C such that $BA = I$ and $AC = I$
Following are equivalent for a square A:

1. $\exists$ square matrix B such that $BA = I$
2. $\exists$ square matrix C such that $AC = I$
3. A is invertible.

inverse of A is unique, denoted by A^-1.

Def General Linear Group: group of invertible $n \times n$ matrices, denoted $GL(n; F) := Mat(n; F)^{\times}$.

Def 2.2.2 elementary matrix: differs from the identity matrix in at most on entry.

Thm 2.2.3 every square matrix with entries in a field can be written as the product of elementary matrices.

Def 2.2.4 Any matrix whose only nonzero entries lie on the diagonal, and which has first 1's along the diagonal and then 0's is in Smith Normal Form.

Thm 2.2.5 For each matrix $A \in Mat(n \times m; F)$, there exist invertible matrices P and Q such that PAQ is in Smith Normal Form.

Def 2.2.6 Column/row rank is the dimension of the subspace generated by the columns/rows of A.

Thm 2.2.7 The column rank and row rank of any matrix are equal.

Def 2.2.8 full rank: maximal rank.

2.3 Abstract Linear Mappings and Matrices

Thm 2.3.1 F a field, V and W vector spaces over F with ordered bases $A = (\vec{v_1}, ..., \vec{v_2})$ and $B = (\vec{w_1}, ..., \vec{w_2})$. To each map $f : V \to W$ we associate a rep. matrix ${}_B[f]_A$ with

$$f(\vec{v_j}) = a_{1j}\vec{w_1} + ... + a_{nj}\vec{w_n} \in W$$

note: ${}_B[f]_A = B^{-1}[f]A$, where $[f]$ is in standard basis.

Thm 2.3.2 Let F be a field and U, V, W finite dimensional vector spaces over F with ordered basis A, B, C. If $f : U \to V$ and $g : V \to W$, then

$${}_C[g \circ f]_A ={}_C [g]_B \circ_B [f]_A$$

3.1 Rings

Def 3.1.1 a ring is a set with two operations $(R, +, \cdot)$, that satisfy:

1. $(R, +)$ is an abelian group.
2. $(R, \cdot)$ is a monoid - $\cdot$ is associative and has an identity element such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$
3. $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ and $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

If multiplication is commutative, then R is a commutative ring.

Prop 3.1.7 A natural number is divisible by 3, precisely when the sum of its digits is divisible by 3.

Def 3.1.8 a field is a nonzero commutative ring F in which every nonzero element has an inverse $a^{-1} \in F$ such that $a \cdot a^{-1} = 1 = a^{-1}a$.

Prop 3.1.11 Let m be a positive integer. The commutative ring $\mathbb{Z} \setminus m\mathbb{Z}$ is a field iff m is prime.

3.2 Properties of Rings

Lem 3.2.1 Let R be a ring and $a, b \in \mathbb{R}$. Then

- $0a = 0 = a0$
- $(-a)b = -(ab) = a(-b)$
- $(-a)(-b) = ab$

Def 3.2.3 Let $m \in \mathbb{Z}$. The m-th multiple ma of an element a in an abelian group R is

$$ma = a + a + a + ... + a \ \ if m > 0$$

with $0a = 0$¡ and negative multiples defined by $(-m)a = -(ma)$.

Lem 3.2.4

- $m(a + b) = ma + mb$
- $(m + n)a = ma + na$
- $m(na) = (mn)a$
- $m(ab) = (ma)b = a(mb)$
- $(ma)(nb) = (mn)(ab)$

Def 3.2.6 An element $a \in R$ is called a unit if it has a multiplicative inverse in R. That is, $\exists a^{-1} \in R$ such that $aa^{-1} = 1 = a^{-1}a$.

Prop 3.2.10 The set $R^{\times}$ of units in a ring R forms a group under multiplication.

Def 3.2.12 In a ring R a nonzero element a is called a divisor of zero if $\exists$ a nonzero element b such that $ab = 0$ or $ba = 0$.

Def 3.2.13 an integral domain is a nonzero commutative ring that has no zero-divisors, and therefore

1. $ab = 0 \implies a = 0$ or $b = 0$, and
2. $a \neq 0$ & $b \neq 0 \implies ab \neq 0$

Prop 3.2.16 R an integral domain. If $ab = ac$ and $a \neq 0$, then $b = c$.

Prop 3.2.17 $m \in \mathbb{N}$. Then $\mathbb{Z} \setminus m\mathbb{Z}$ is an integral domain iff m is prime.

Thm 3.2.18 Every finite integral domain is a field.

3.3 Polynomials

Def 3.3.1 Let R be a ring. A polynomial over R is an expression of the form

$$P = a_0 + a_1X + a_2X^2 + ... + a_mX^m$$

for some nonnegative integer m and elements $a_i \in R$ for $0 \leq i \leq m$. The set of all polynomials over R is denoted $R[X]$. In case a_m is nonzero, the polynomial P has degree m, written deg(P), and a_m is its leading coefficient. When $a_m = 1$, then P is monic.

Def 3.3.2 $R[X]$ is a ring of polynomials ith coefficients in R. The zero and identity of R is the same identity as $R[X]$.

Lem 3.3.3

1. If R is a ring with no zero divisors, then $R[X]$ has no zero divisors and $deg(PQ) = deg(P) + deg(Q)$ for nonzero $P, Q \in R[X]$.
2. If R is an integral domain then so is $R[X]$.

Prop if R is an integral domain then $R[X]^{\times} = R^{\times}$.

Thm 3.3.4 Let R be an integral domain and let $P, Q \in R[X]$ with Q monic. THen $\exists$ unique $A, B \in R[X]$ such that $P = AQ + B$ and $deg(B) < deg(Q)$ or $B = 0$.

Def 3.3.6 Let R be a commutative ring and $P \in R[X]$ a polynomial. THen the polynomial P can be evaluated at the element $\lambda \in R$ to produce $P(\lambda)$ by replacing the powers of X in the polynomial P by the corresponding powers of λ. In this way we have a mapping $R[X] \to Maps(R, R)$. An element $\lambda \in R$ is a root of P if $P(\lambda) = 0$.

Prop 3.3.9 Let R be a commutative ring, $\lambda \in R$ and $P(X) \in R[X]$. Then λ is a root of $P(X)$ iff $(X - \lambda)$ divides $P(X)$.

Thm 3.3.10 Let R be a field, or generally an integral domain. Then a nonzero polynomial $P \in R[X] \setminus \{0\}$ has at most $deg(P)$ roots in R.

Def 3.3.11 A field F is algebraically closed if each nonconstant polynomial $P \in F[X] \setminus F$ with coefficients in F has a root in F

Thm 3.3.13 The field of complex numbers, $\mathbb{C}$ is algebraically closed.

Thm 3.3.14 If F is an algebraically closed field, then every nonzero polynomial $P \in F[X] \setminus \{0\}$ decomposes into linear factors

$$P = c(X - \lambda_1)(X - \lambda_2)(X - \lambda_3)$$

This decomposition is unique up to ordering.

3.4 Homomorphisms, Ideals and Subrings

Def 3.4.1 Let R and S be rings. A mapping $f : R \to S$ is a ring homomorphism if the following hold for all $x, y \in R$:

- f(x+y)=f(x)+f(y)
- f(xy)=f(x)f(y)

Note: identity is not necessarily preserved! The identiy is idempotent, i.e. $f(1^2) = f(1) \implies f(1)(f(1) - 1) = 0$, so either $f(1) = 1$ or $f(1) = 0$, in which case $f = 0$ is the zero ring homomorphism.
Note: composition of ring homomorphisms is a ring homomorphism and inverse of a ring isomorphism is a ring isomorphism.

Lem 3.4.5 Let R and S be rings and $f : R \to S$ a ring homomorphism. Then $\forall x, y \in R$ and $m \in \mathbb{Z}$:

- $f(0_R) = 0_s$
- $f(-x) = -f(x)$
- $f(x - y) = f(x) - f(y)$
- $f(mx) = mf(x)$
- $f(x)^n = (f(x))^n$

Def 3.4.7 A subset I of a ring R is an ideal, written $I \trianglelefteq R$ if the following hold:

1. $I \neq \emptyset$
2. I is closed under subtraction
3. $\forall i \in I$ and $r \in R$ we have that $ri, ir \in I$

Def 3.4.11 Let $T \subset R$ and R a commutative ring. Then the ideal of R generated by T is the set

$${}_R\langle T \rangle = \{r_1t_1 + ... + r_mt_m \ : \ t_1, ..., t_m \in T, r_1, ..., r_m \in R\}$$

Prop 3.4.14 Let R be a commutative ring and let $T \subseteq R$. THen ${}_R\langle T \rangle$ is the smallest ideal of R that containss T.

Def 3.4.15 Let$R$ be a commutative ring. An ideal I of R is called a principal ideal if $I = \langle T \rangle$ for some $t \in R$.

Def 3.4.17 Let R and S be rings with zero elements 0_R and 0_S respectively and let $f : R \to S$ be a ring homomorphism. Since f is in particular a group homomorphism from $(R, +)$ to $(S, +)$, the kernel of f already has a meaning

$$\ker(f) = \{r \in R \ : \ f(r) = 0_S\}$$

Prop 3.4.18 $\ker(f)$ is an ideal of R.

Lem 3.4.20 f is injective iff $\ker(f) = \{0\}$

Lem 3.4.21 The intersection of a collection of ideals of R is an ideal of R.

Lem 3.4.22 Let I and J be ideals of R. THen $I + J = \{a + b \ : \ a \in I, b \in J\}$ is an ideal of R.

Def 3.4.23 A subset R' of R is asubring of R if R' itself is a ring under the operation of addition and multiplication defined in R.
Prop 3.4.26 textbfTest for Subring:

1. R' has a multiplicative identity,
2. R' is closed under subtraction,
3. R' is closed under multiplication.

Prop 3.4.29 Let $f : R \to S$ be a ring homomorphism.

1. if R' is a subring of R, then $f(R')$ is a subring of S. In particular, $im(f)$ is a subring of S.
2. Assume $f(1_R) = 1_S$. If x is a unit in R, $f(x)$ is a unit in S and $(f(x))^{-1} = f(x^{-1})$.

3.5 Equivalence Relations

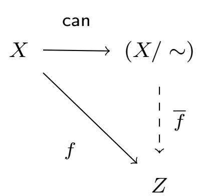
Def 3.5.1 A **relation** R on a set X is a subset $R \subseteq X \times X$. In this context, and only in this context, instead of writing $(x, y) \in R$, I will write xRy. Then R is an **equivalence relation on** X when for all elements $x, y, z \in X$ the following hold:

1. **Reflexivity**: xRx;
2. **Symmetry**: $xRy \Leftrightarrow yRx$;
3. **Transitivity**: (xRy and yRz) $\to xRz$.

Def 3.5.3 An element of an equivalence class is called a representative of the class.
Def 3.5.5 Given an equivalence relation $\sim$ on the set X**set of equivalence classes**, which is a subset of the power set $\mathcal{P}(X)$, is given by

$$(X/\!\sim) := \{E(x) : x \in X\}$$

There is a canonical mapping can : $X \to (X/\!\sim), x \mapsto E(x)$. It is a surjection.
Remark: Universal property of the set of equivalence classes:



Def 3.5.7 $g : (X/\ ) \to Z$ is well defined if I can find a mapping $f : X \to Z$ such that $x\ y \to f(x) = f(y)$ and $g = \bar{f}$.

3.6 Factor Rings and the First Isomorphism Theorem

Def 3.6.1 Let $I \trianglelefteq R$ be an ideal in a ring R. The set

$$x + I := \{x + i : i \in I\} \subseteq R$$

is a **coset of** I **in** R or the **coset of** x **with respect to** I **in** R.

Def 3.6.3 Let R be a ring, $I \trianglelefteq R$ an ideal, and $\sim$ the equivalence relation defined by $x \sim y \Leftrightarrow x - y \in I$. Then R/I, **the factor ring of** R **by** I or **the quotient of** R **by** I, is the set $(R/\sim)$ of cosets of I in R.

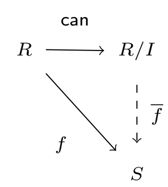
Thm 3.6.4 Let R be a ring and $I \trianglelefteq R$ an ideal. Then R/I is a ring, where addition and multiplication are defined by

$$(x + I) \dot{+} (y + I) = (x + y) + I \qquad \text{for all } x, y \in R$$

$$(x + I) \cdot (y + I) = xy + I \qquad \text{for all } x, y \in R.$$

Thm 3.6.7 (Universal Prop. of Factor Rings) R a ring and I an ideal of R.

1. The mapping can : $R \to R/I$ sending r to $r + I$ for all $r \in R$ is a surjective ring homomorphism with kernel I.
2. If $f : R \to S$ is a ring homomorphism with $f(I) = \{0_S\}$, so that $I \subseteq \ker f$, then there is a unique ring homomorphism $\overline{f} : R/I \to S$ such that $f = \overline{f} \circ$ can.



Thm 3.6.9 (First Isomorphism Theorem for Rings) Let R and S be rings. Then every ring homomorphism $f : R \longrightarrow S$ induces a ring isomorphism

$$\overline{f} : R/\ker f \xrightarrow{\sim} imf.$$

3.7 Modules

Def 3.7.1 A **(left) module** M **over a ring** R is a pair consisting of an abelian group $M = (M, \dot{+})$ and a mapping

$$\begin{array}{rcl} R \times M & \to & M \\ (r, a) & \mapsto & ra \end{array}$$

such that for all $r, s \in R$ and $a, b \in M$ the following identities hold:

$$\begin{array}{rcl} r(a \dot{+} b) & = & (ra) \dot{+} (rb) \\ (r + s)a & = & (ra) \dot{+} (sa) \\ r(sa) & = & (rs)a \\ 1_R a & = & a \end{array}$$

Def 3.7.8 Let R be a ring and M an R-module.

1. $0_R a = 0_M$ for all $a \in M$.
2. $r 0_M = 0_M$ for all $r \in R$.
3. $(-r)a = r(-a) = -(ra)$ for all $r \in R, a \in M$. Here the first negative is a negative in R, the last two are negatives in M.

Def 3.7.11 Let R be a ring and let M, N be R–modules. A mapping $f : M \to N$ is an R**–homomorphism** or **homomorphism** if the following hold for all $a, b \in M$ and $r \in R$

$$\begin{array}{rcl} f(a + b) & = & f(a) + f(b) \\ f(ra) & = & rf(a) \end{array}$$

The **kernel** of f is $\ker f = \{a \in M : f(a) = 0_N\} \subseteq M$ and the **image** of f is $imf = \{f(a) : a \in M\} \subseteq N$. If f is a bijection then it is an R**-module isomorphism** or **isomorphism**, I write $M \cong N$ and say M and N are **isomorphic**.

Def 3.7.15 A non–empty subset M' of an R–module M is a **submodule** if M' is an R–module with respect to the operations of the R–module M **restricted** to M'.

Prop 3.7.20 (Test for a submodule) Let R be a ring and let M be an R–module. A subset M' of M is a *submodule* if and only if

1. $0_M \in M'$
2. $a, b \in M' \Rightarrow a - b \in M'$
3. $r \in R, a \in M' \Rightarrow ra \in M'$. Note if f is an R-module homomorphism, then $\ker f$ and imf are submodules of M and N respectively.

Lem 3.7.22 Let R be a ring, let M and N be R-modules and let $f : M \to N$ be an R-homomorphism. Then f is injective if and only if $\ker f = \{0_M\}$.
Def 3.7.23 Let R be a ring, M an R-module and let $T \subseteq M$. Then the **submodule of** M **generated by** T is the set

$$_R\langle T \rangle = \{r_1 t_1 + \cdots + r_m t_m : t_1, \ldots, t_m \in T, r_1, \ldots, r_m \in R\},$$

together with the zero element in the case $T = \emptyset$. Cyclic means generated by a singleton: $M = {}_R\langle t \rangle$.
Lem 3.7.28 Let $T \subseteq M$. Then $_R\langle T \rangle$ is the smallest submodule of M that contains T.
Lem 3.7.29 The intersection of any collection of submodules of M is a submodule of M.
Lem 3.7.30 Let M_1 and M_2 be submodules of a M. Then

$$M_1 + M_2 = \{a + b : a \in M_1, b \in M_2\}$$

is a submodule of M.

Thm 3.7.31 Let R be a ring, M an R-module and N a submodule of M. For each $a \in M$ the **coset of** a **with respect to** N **in** M is

$$a + N = \{a + b : b \in N\}$$

It is a coset of N in the abelian group M and so is an equivalence class for the equivalence relation $a \sim b \Leftrightarrow a - b \in N$. I define M/N, **the factor of** M **by** N or **the quotient of** M **by** N, to be the set $(M/\sim)$ of all cosets of N in M, with

$$\begin{array}{rcl} (a + N) \dot{+} (b + N) & = & (a + b) + N \\ r(a + N) & = & ra + N \end{array}$$

The zero of M/N is the coset $0_{M/N} = 0_M + N$. The negative of $a + N \in M/N$ is the coset $-(a + N) = (-a) + N$.

Thm 3.7.33 (First Isomorphism Theorem for Modules) Let R be a ring and let M and N be R-modules. Then every R-homomorphism $f : M \longrightarrow N$ induces an R-isomorphism

$$\overline{f} : M/\ker f \xrightarrow{\sim} imf.$$

4.1 Sign of Permutation

Def 4.1.1 The group of all permutations of the set $\{1, 2, \ldots, n\}$, also known as bijections from $\{1, 2, \ldots, n\}$ to itself, is denoted by $\mathfrak{S}_n$ and called the n-**th symmetric group**. It is a group under composition and it has $n!$ elements.
A **transposition** is a permutation that swaps two elements of the set and leaves all the others unchanged.
Def 4.1.2 An **inversion** of a permutation $\sigma \in \mathfrak{S}_n$ is a pair (i, j) such that $1 \leqslant i < j \leqslant n$ and $\sigma(i) > \sigma(j)$. The number of inversions of the permutation σ is called the **length of** σ and written $\ell(\sigma)$. In formulas:

$$\ell(\sigma) = |\{(i, j) : i < j \text{ but } \sigma(i) > \sigma(j)\}|$$

The **sign of** σ is defined to be the parity of the number of inversions of σ. In formulas:

$$\text{sgn}(\sigma) = (-1)^{\ell(\sigma)}$$

even permutation has $\text{sign}(\sigma) = +1$, odd has $\text{sign}(\sigma) = -1$.
Note: the transposition that swaps i and j, leaving everything else unchanged, has length $2|i - j| - 1$
Lem 4.1.5 For each $n \in \mathbb{N}$ the sign of a permutation produces a group homomorphism $\text{sgn} : \mathfrak{S}_n \to \{+1, -1\}$ from the symmetric group to the two-element group of signs. In formulas:

$$\text{sgn}(\sigma\tau) = \text{sgn}(\sigma)\text{sgn}(\tau) \quad \text{for all } \sigma, \tau \in \mathfrak{S}_n$$

.
Def 4.1.7 (Alternating Group, A_n) For $n \in \mathbb{N}$, the set of even permutations in $\mathfrak{S}_n$ forms a subgroup of $\mathfrak{S}_n$ because it is the kernel of the group homomorphism $\text{sgn} : \mathfrak{S}_n \to \{+1, -1\}$.
Note: every permutation in $\mathfrak{S}_n$ can be described as a product of transpositions of neighbouring numbers, that is of the permutations $(i\ i{+}1)$ swapping i and $i + 1$ for some $1 \leqslant i \leqslant n - 1$.

4.2 Determinants

Def 4.2.1 Let R be a commutative ring and $n \in \mathbb{N}$. Then $\det : \text{Mat}(n; R) \to R$ is given by:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix} \mapsto \det(A) = \sum_{\sigma \in \mathfrak{S}_n} \text{sgn}(\sigma) a_{1\sigma(1)} \cdots a_{n\sigma(n)}$$

4.3 Characterising the Determinant

Def 4.3.1 Let U, V and W be F-vector spaces. A **bilinear form on** $U \times V$ **with values in** W is a mapping $H : U \times V \to W$ which is a linear mapping in both of its entries. It satisfies

$$\begin{aligned} H(u_1 + u_2, v_1) &= H(u_1, v_1) + H(u_2, v_1) \\ H(\lambda u_1, v_1) &= \lambda H(u_1, v_1) \\ H(u_1, v_1 + v_2) &= H(u_1, v_1) + H(u_1, v_2) \\ H(u_1, \lambda v_1) &= \lambda H(u_1, v_1) \end{aligned}$$

Symmetric: if $U = V$ and $H(u, v) = H(v, u)$ for all $u, v \in U$
Alternating: if $U = V$ and $H(u, u) = 0$ for all $u \in U$

Def 4.3.4 Let V and W be F-vector spaces. A multilinear form $H : V \times \cdots \times V \to W$ is **alternating** if it vanishes on every n-tuple of elements of V that has at least two entries equal, in other words if:

$$(\exists\, i \neq j \text{ with } v_i = v_j) \to H(v_1, \ldots, v_i, \ldots, v_j, \ldots, v_n) = 0$$

Thm 4.3.6 Let F be a field. The mapping $\det : \text{Mat}(n; F) \to F$ is the unique alternating multilinear form on n-tuples of column vectors with values in F that takes the value 1_F on the identity matrix.

4.4 Calculating Determinants

Thm 4.4.1 Let R be a commutative ring and let $A, B \in \text{Mat}(n; R)$. Then

$$\det(AB) = \det(A)\det(B).$$

Thm 4.4.2 The determinant of a square matrix with entries in a field F is non-zero if and only if the matrix is invertible.

Rem if A is invertible then $\det(A^{-1}) = \det(A)^{-1}$.
Rem $\det(A) = \det(B^{-1}AB)$

Lem 4.4.4 For all $A \in \text{Mat}(n; R)$ with R a commutative ring

$$\det(A^{\mathsf{T}}) = \det(A)$$

Def 4.4.6 Let $A \in \text{Mat}(n; R)$ for some commutative ring R and natural number n. Let i and j be integers between 1 and n. Then the (i, j) **cofactor of** A is $C_{ij} = (-1)^{i+j}\det(A\langle i, j\rangle)$ where $A\langle i, j\rangle$ is the matrix I obtain from A be deleting the i-th row and the j-th column.

Thm 4.4.7 Let $A = (a_{ij})$ be an $(n \times n)$-matrix with entries from a commutative ring R. For a fixed i the i-**th row expansion of the determinant** is

$$\det(A) = \sum_{j=1}^{n} a_{ij} C_{ij}$$

and for a fixed j the j-**th column expansion of the determinant** is

$$\det(A) = \sum_{i=1}^{n} a_{ij} C_{ij}$$

Def 4.4.8 Let A be an $(n \times n)$-matrix with entries in a commutative ring R. The **adjugate matrix** $\text{adj}(A)$ is the $(n \times n)$-matrix whose entries are $\text{adj}(A)_{ij} = C_{ji}$ where C_{ji} the (j, i)-cofactor.

Thm 4.4.9 Let A be an $(n \times n)$-matrix with entries in a commutative ring R. Then

$$A \cdot \text{adj}(A) = (\det A) I_n$$

.
Cor 4.4.11 $A \in \text{Mat}(n; R)$ is invertible if and only if $\det(A) \in R^{\times}$.

4.5 Eigenvalues and Eigenvectors

Def 4.5.1 Let $f : V \to V$ be an endomorphism of an F-vector space V.
A scalar $\lambda \in F$ is an **eigenvalue of** f iff there exists a non-zero vector $\vec{v} \in V$ such that $f(\vec{v}) = \lambda\vec{v}$.
Each such vector is called an **eigenvector of** f **with eigenvalue** λ.
For any $\lambda \in F$, the **eigenspace of** f **with eigenvalue** λ is

$$E(\lambda, f) = \{\vec{v} \in V : f(\vec{v}) = \lambda\vec{v}\}$$

Thm 4.5.4 Each endomorphism of a non-zero finite dimensional vector space over an algebraically closed field has an eigenvalue.

Def 4.5.6 Let R be a commutative ring and let $A \in \text{Mat}(n; R)$ be a square matrix with entries in R. The polynomial $\det(A - xI_n) \in R[x]$ is called the **characteristic polynomial of the matrix** A. It is denoted by

$$\chi_A(x) := \det(A - xI_n)$$

Thm 4.5.8 Let F be a field and $A \in \text{Mat}(n; F)$ a square matrix with entries in F. The eigenvalues of the linear mapping $A : F^n \to F^n$ are exactly the roots of the characteristic polynomial χ_A.

4.6 Triangular, Diagonal, Cayley-Hamilton

Prop 4.6.1 Triangularisable iff $\chi_A(x)$ decomposes into linear factors in $F[x]$.

Rem 4.6.2 endomorphism A is triangularisable iff it is conjugate to an upper triangular matrix.

Def 4.6.5 An endomorphism $f : V \to V$ of an F-vector space V is **diagonalisable** if and only if there exists a basis of V consisting of eigenvectors of f.

Thm 4.6.9 If $\chi_A(x)$ is the characteristic polynomial of endomorphism A, then $\chi_A(A) = 0$.

5.1 Inner Product Spaces: Definitions

Def 5.1.1 Let V be a vector space over $\mathbb{R}$. An **inner product** on V is a mapping

$$(-, -) : V \times V \to \mathbb{R}$$

that satisfies the following for all $\vec{x}, \vec{y}, \vec{z} \in V$ and $\lambda, \mu \in \mathbb{R}$:

1. $(\lambda\vec{x} + \mu\vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$
2. $(\vec{x}, \vec{y}) = (\vec{y}, \vec{x})$
3. $(\vec{x}, \vec{x}) \geqslant 0$, with equality if and only if $\vec{x} = \vec{0}$

Def 5.1.3 Let V be a v.s. over $\mathbb{C}$. An **inner product** on V is a map $(-, -) : V \times V \to \mathbb{C}$ that satisfies the followingb $\forall \vec{x}, \vec{y}, \vec{z} \in V, \lambda, \mu \in \mathbb{C}$:

1. $(\lambda\vec{x} + \mu\vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$
2. $(\vec{x}, \vec{y}) = \overline{(\vec{y}, \vec{x})}$
3. $(\vec{x}, \vec{x}) \geqslant 0$, with equality if and only if $\vec{x} = \vec{0}$

ex 5.1.2 Standard inner product is given by

$$\begin{aligned} (\vec{v}, \vec{w}) &= v_1 w_1 + v_2 w_2 + \cdots + v_n w_n \quad (\mathbb{R}) \\ (\vec{v}, \vec{w}) &= v_1 \overline{w_1} + v_2 \overline{w_2} + \cdots + v_n \overline{w_n} \quad (\mathbb{C}) \end{aligned}$$

Def 5.1.5 **norm** $\|\vec{v}\| \in \mathbb{R}$ of a vector $\vec{v}$ is defined as the non-negative square root

$$\|\vec{v}\| = \sqrt{(\vec{v}, \vec{v})}$$

Vectors whose length is 1 are called **units**. Two vectors $\vec{v}, \vec{w}$ are **orthogonal** and I write $\vec{v} \perp \vec{w}$ if and only if $(\vec{v}, \vec{w}) = 0$.
ex 72 In an inner product space V show that: $\|\lambda\vec{v}\| = |\lambda|\|\vec{v}\|$ for all $\vec{v} \in V$ and all $\lambda \in \mathbb{R}$ or $\mathbb{C}$.
ex 5.1.6 If two vectors $\vec{v}$ and $\vec{w}$ in an inner product space are at right-angles then Pythagoras' Theorem holds

$$\|\vec{v} + \vec{w}\|^2 = \|\vec{v}\|^2 + \|\vec{w}\|^2$$

Def 5.1.7 A family $(\vec{v}_i)_{i \in I}$ for vectors from an inner product space is an **orthonormal family** if all the vectors $\vec{v}_i$ have length 1 and if they are pairwise orthogonal to each other, meaning

$$(\vec{v}_i, \vec{v}_j) = \delta_{ij}$$

An orthonormal family that is a basis is an **orthonormal basis**.
Rem 5.1.9 Suppose that V is an inner product space and that $(\vec{v}_i)_{i \in I}$ is an orthonormal basis. Then I can write any $\vec{w} \in V$ in the form

$$\vec{w} = \sum_{i \in I} (\vec{w}, \vec{v}_i)\vec{v}_i$$

5.1.10 Every finite dim. inner product space has an orthonormal basis.

5.2 Orthogonal Complements and Projections

Def 5.2.1 Let V be an inner product space and let $T \subseteq V$ be an arbitrary subset. Define

$$T^{\perp} = \{\vec{v} \in V : \vec{v} \perp \vec{t} \text{ for all } \vec{t} \in T\},$$

calling this set the **orthogonal** to T.

ex 73 In an inner product space, V, $T^{\perp}$ is a subspace for *any* $T \subseteq V$. In particular,

$$T^{\perp} = \langle T \rangle^{\perp}.$$

Prop 5.2.2 Let V be an inner product space and let U be a finite dimensional subspace of V. Then U and $U^{\perp}$ are complementary in the sense of Def 1.7.6. That is,

$$V = U \oplus U^{\perp}$$

Def 5.2.3 Let U be a finite dimensional subspace of an inner product space V. The space $U^{\perp}$ is the **orthogonal complement to** U. The **orthogonal projection from** V **onto** U is the mapping

$$\pi_U : V \to V$$

that sends $\vec{v} = \vec{p} + \vec{r}$ to $\vec{p}$.

Prop 5.2.4 Let U be a finite dimensional subspace of an inner product space V and let π_U be the orthogonal projection from V onto U.

1. π_U is a linear mapping with $\operatorname{im}(\pi_U) = U$ and kernel $\ker(\pi_U) = U^{\perp}$.
2. If $\{\vec{v}_1, \ldots, \vec{v}_n\}$ is an orthonormal basis of U, then π_U is given by the following formula for all $\vec{v} \in V$

$$\pi_U(\vec{v}) = \sum_{i=1}^{n} (\vec{v}, \vec{v}_i)\vec{v}_i$$

3. $\pi_U^2 = \pi_U$, that is π_U is an idempotent.

Thm 5.2.5 (Cauchy Schwarz Inequality) Let $\vec{v}, \vec{w}$ be vectors in an inner product space. Then

$$|(\vec{v}, \vec{w})| \leqslant \|\vec{v}\|\|\vec{w}\|$$

with equality if and only $\vec{v}$ and $\vec{w}$ are linearly dependent.

Cor 5.2.6 The norm $\|\cdot\|$ on an inner product space V satisfies, for any $\vec{v}, \vec{w} \in V$ and scalar λ:

1. $\|\vec{v}\| \geqslant 0$ with equality if and only if $\vec{v} = \vec{0}$.
2. $\|\lambda \vec{v}\| = |\lambda| \|\vec{v}\|$
3. $\|\vec{v} + \vec{w}\| \leqslant \|\vec{v}\| + \|\vec{w}\|$, the **triangle inequality**

Thm 5.2.7 Let $\vec{v}_1, \ldots, \vec{v}_k$ be a linearly independent vectors in an inner product space V. Then there exists an orthonormal family $\vec{w}_1, \ldots, \vec{w}_k$ with the property that for all $1 \leqslant i \leqslant k$

$$\vec{w}_i \in \mathbb{R}_{>0}\vec{v}_i + \langle \vec{v}_{i-1}, \ldots, \vec{v}_1 \rangle$$

ex 74 There is a unique orthonormal family whose elements satisfy the property displayed in the statement of Thm 5.2.7.

5.3 Adjoints and Self-Adjoints

Def 5.3.1 Let V be an inner product space. Two endomorphism $T, S : V \to V$ are **adjoint** to one another if for all $\vec{v}, \vec{w} \in V$,

$$(T\vec{v}, \vec{w}) = (\vec{v}, S\vec{w})$$

In this case I will write $S = T^*$ and call S the **adjoint** of T.

Rem 5.3.2 Any endomorphism has at most one adjoint. This is because if both S and S' are adjoint to T then $(\vec{v}, S\vec{w} - S'\vec{w}) = 0$ for all $\vec{v}, \vec{w} \in V$, so the positivity axiom for an inner product space immediately implies that $S\vec{w} = S'\vec{w}$ for all $\vec{w}$.

ex 75 If T^* is the adjoint of T, then T^* has an adjoint and it is $(T^*)^* = T$.

ex 5.3.3 The adjoint of multiplication by A in $\mathbb{R}^n$ is multiplication by A^{T}. The adjoint of multiplication by A in $\mathbb{C}^n$ is multiplication by $\overline{A}^{\mathsf{T}}$.

Thm 5.3.4 Let V be a finite dimensional inner product space. Let $T : V \to V$ be an endomorphism. Then T^* exists. That is, there exists a unique linear mapping $T^* : V \to V$ such that for all $\vec{v}, \vec{w} \in V$

$$(T\vec{v}, \vec{w}) = (\vec{v}, T^*\vec{w})$$

Def 5.3.5 An endomorphism of an inner product space $T : V \to V$ is **self-adjoint** if it equals its own adjoint, that is if $T^* = T$.

ex 5.3.6 A real $(n \times n)$-matrix A describes a self-adjoint mapping on the standard inner product space $\mathbb{R}^n$ precisely when A is symmetric, that is when $A^{\mathsf{T}} = A$. A complex $(n \times n)$-matrix A describes a self-adjoint mapping on the standard inner product space $\mathbb{C}^n$ precisely when $A = \overline{A}^{\mathsf{T}}$ holds. Such matrices are called **hermitian**.

Thm 5.3.7 Let $T : V \to V$ be a self-adjoint linear mapping on an inner product space V.

1. Every eigenvalue of T is real.
2. If λ and μ are distinct eigenvalues of T with corresponding eigenvectors $\vec{v}$ and $\vec{w}$, then $(\vec{v}, \vec{w}) = 0$.
3. T has an eigenvalue.

Thm 5.3.9 (The Spectral Theorem for Self-Adjoint Endomorphisms) Let V be a finite dimensional inner product space and let $T : V \to V$ be a self-adjoint linear mapping. Then V has an orthonormal basis consisting of eigenvectors of T.

Def 5.3.11 an **orthogonal matrix** is an $(n \times n)$-matrix P with real entries such that $P^{\mathsf{T}}P = I_n$. In other words, an orthogonal matrix is a square matrix P with real entries such that $P^{-1} = P^{\mathsf{T}}$.

ex 76 The condition that $P^{\mathsf{T}}P = I_n$ is equivalent to the columns of P forming an orthonormal basis for $\mathbb{R}^n$ with its standard inner product.

ex 77 The set $\{P \in \mathrm{Mat}(n; \mathbb{R}) : P^{\mathsf{T}}P = I_n\}$ is a group. It is called the **orthogonal group**, $O(n)$.

Cor 5.3.12 (The Spectral Theorem for Real Symmetric Matrices) Let A be a real $(n \times n)$-symmetric matrix. Then there is an $(n \times n)$-orthogonal matrix P such that

$$P^{\mathsf{T}}AP = P^{-1}AP = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$$

where $\lambda_1, \ldots, \lambda_n$ are the (necessarily real) eigenvalues of A, repeated according to their multiplicity as roots of the characteristic polynomial of A.

Def 5.3.14 An **unitary matrix** is an $(n \times n)$-matrix P with complex entries such that $\overline{P}^{\mathsf{T}}P = I_n$. In other words, a unitary matrix is a square matrix P with complex entries such that $P^{-1} = \overline{P}^{\mathsf{T}}$.

ex 78 The condition that $\overline{P}^{\mathsf{T}}P = I_n$ is equivalent to the columns of P forming an orthonormal basis for $\mathbb{C}^n$ with its standard inner product.

ex 79 The set $\{P \in \mathrm{Mat}(n; \mathbb{C}) : \overline{P}^{\mathsf{T}}P = I_n\}$ is a group. It is called the **unitary group**, $U(n)$.

Cor 5.3.15 [The Spectral Theorem for Hermitian Matrices] Let A be a $(n \times n)$-hermitian matrix. Then there is an $(n \times n)$-unitary matrix P such that

$$\overline{P}^{\mathsf{T}}AP = P^{-1}AP = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$$

where $\lambda_1, \ldots, \lambda_n$ are the (necessarily real) eigenvalues of A, repeated according to their multiplicity as roots of the characteristic polynomial of A.