Algebra

Sebastian Mücksch, v2, 2018/19

Vector Spaces

Lemma 1.2.4 (Product with Zero Vector).
Let V be an F-vector space, then $\forall\lambda \in F : \lambda\vec{0} = \vec{0}$. Furthermore, $\lambda\vec{v} = \vec{0} \Rightarrow \lambda = 0$ or $\vec{v} = 0$.

Proposition 1.4.5 (Generating a Vector Subspace From a Set).
Let $T \subseteq V$, V begin vector space over F. Then $\langle T\rangle$ is the smallest subspace of V containing T.

Example 1.4.6.
Let $T \subseteq V$, $\vec{v} \in \langle T\rangle$. Then $\langle T \cup \{\vec{v}\}\rangle = \langle T\rangle$.

Exercise 4.
Any intersection of vector subspaces is a vector subspace.

Theorem 1.5.12 (Characterisation of Bases).
Let $E \subseteq V$ of vector space V. The following are equivalent:

(1) E is a basis;
(2) E is a ***minimal generating*** set, i.e. $\forall\vec{v} \in E : E \setminus \{\vec{v}\}$ is not generating;
(3) E is ***maximal linearly independent*** set, $\forall\vec{v} \in V : E \cup \{\vec{v}\}$ is not linearly independent.

Corollary 1.5.13 (The Existence of a Basis).
Let V be a finite vector space over field F. Then V has a basis.

Hint: Take finite generating set, reduce until linearly independent.

Theorem 1.5.14 (Useful Variant on Characterisation of Bases).
Let V be a vector space.

(1) If $L \subset V$ is linearly independent and E is minimal generating set s.t. $L \subseteq E$, then E is a basis.
(2) If $E \subseteq V$ is generating and L is maximal linearly independent set s.t. $L \subseteq E$, then L is a basis.

Theorem 1.5.16 (A Useful Variant on Linear Combinations of Basis Elements).
Let V be a F-vector space, F being a field and $(\vec{v}_i)_{i\in I}$ a family of vectors in V. The following are equivalent:

(1) Family $(\vec{v}_i)_{i\in I}$ is a basis for V;
(2) $\forall\vec{v} \in V$, there exists ***precisely one*** family $(a_i)_{i\in I}$ of elements in F, almost all zero, s.t. $\vec{v} = \sum_{i\in I} a_i\vec{v}_i$.

Theorem 1.6.1 (Fundamental Estimate of Linear Algebra).
Let V be a vector space, $L \subset V$ a linearly independent subset and $E \subseteq V$ a generating set. Then $|L| \leqslant |E|$.

Theorem 1.6.2 (Steinitz Exchange Theorem).
Let V be a vector space, $L \subset V$ a ***finite*** linearly independent subset and $E \subseteq V$ a generating set. Then we can swap elements of E with elements of L and keep it a generating set.

Lemma 1.6.3 (Exchange Lemma).
Let V be a vector space, $M \subseteq V$ a linearly independent, E a generating set s.t. $M \subseteq E$. If $\vec{w} \in V \setminus M$ s.t. $M \cup \{\vec{w}\}$ is linearly independent, then $\exists\vec{e} \in E \setminus M$ s.t. $(E \setminus \{\vec{e}\} \cup \{\vec{w}\})$ is generating.

Hint: $\vec{w} = \sum \alpha_i\vec{e}_i$, $\vec{e}_i \in E$, $M \cup \{\vec{w}\} \Rightarrow \exists\vec{e}_i \notin M$, express that $\vec{e}_i$ with $\vec{w}$.

Corollary 1.6.4 (Cardinality of Bases).
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.

Hint: Theorem 1.6.1 & Contradiction.

Example 1.6.7.
Basis of zero vector space is $\emptyset \Rightarrow$ dimension of zero vector space is 0.

Corollary 1.6.8 (Cardinality Criterion for Bases).
Let V be a finitely generated vector space.

(1) $L \subset V$ linearly independent, then $|L| \leqslant \dim V$ and $|L| = \dim V \Rightarrow L$ is a basis.
(2) $E \subseteq V$ generating, then $\dim V \leqslant |E|$ and $|E| = \dim V \Rightarrow E$ is a basis.

Hint: Theorem 1.6.1 & 1.5.12.

Corollary 1.6.9 (Dimension Estimate of Vector Subspaces).
Let $U \subset V$ be a proper subspace of ***finite*** vector space V. Then $\dim U < \dim V$.

Remark 1.6.10.
If $U \subseteq V$ subspace of arbitrary vector space, then $\dim U \leqslant \dim V$ and $\dim U = \dim V < \infty \Rightarrow U = V$.

Theorem 1.6.11 (The Dimension Theorem).
Let $U, W \subseteq V$ be subspaces. Then

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

Hint: $f : U \oplus W \to V$; $(\vec{u}, \vec{w}) \mapsto \vec{u} + \vec{w}$ $\Rightarrow \operatorname{im} f = U + W$, $\ker f = U \cap W$. Rank-Nullity.

Exercise 6.
Let $V_1, \ldots, V_n$ be F-vector spaces, then $\dim(V_1 \oplus \ldots \oplus V_n) = \dim(V_1) + \ldots + \dim(V_n)$.

Exercise 10.
The image/preimage of a vector subspace under a linear mapping is a vector subspace.

Exercise 12.
Let $V_1, \ldots, V_n, W$ be vector spaces, $f_i : V_i \to W$ linear mappings. Then $f : V_1 \oplus \ldots \oplus V_n \to W$ with $f(\vec{v}_1, \ldots, \vec{v}_n) = f_1(\vec{v}_1) + \ldots + f_i(\vec{v}_n)$ is a new linear mapping. This gives a bijection:

$$\operatorname{Hom}(V_1, W) \times \ldots \times \operatorname{Hom}(V_n, W) \xrightarrow{\sim} \operatorname{Hom}(V_1 \oplus \ldots \oplus V_n, W)$$

with inverse $f \mapsto (f \circ \mathrm{in}_i)_i$.

Theorem 1.7.7 (Classification of Vector Space by Dimension).
Let V be vector space over F, $n \in \mathbb{N}$. Then $F^n \cong V \Leftrightarrow \dim V = n$.

Exercise 17.
Let $U \subseteq V$ be subspace of vector space V and $f : U \to W$. Then f can be extended to a ***linear*** mapping $\tilde{f} : V \to W$.

Theorem 1.8.4 (Rank-Nullity Theorem).
Let $f : V \to W$ be a linear mapping. Then

$$\dim V = \dim(\operatorname{im} f) + \dim(\ker f)$$

Hint: V finite $\Rightarrow \operatorname{im} f, \ker f$ finite, contrapositive shows Theorem holds for V infinite case. Assume V finite, then Cor. 1.5.13 & Ex. 18.

Exercise 18.
Let $f : V \to W$ be a linear map. If $\vec{v}_1, \ldots, \vec{v}_s$ is a basis for $\ker f$ and extended by $\vec{v}_{s+1}, \ldots, \vec{v}$ it is basis of V, then $f(\vec{v}_{s+1}), \ldots, f(\vec{v}_n)$ is basis of $\operatorname{im} f$.

Exercise 19.
Let $U, W \subseteq V$ be subspaces of V. U, W are complementary $\Leftrightarrow V = U + W$ and $U \cap W = \{0\}$.

Exercise 20.
Let $U, W \subseteq V$ be subspaces of V. U, W are complementary $\Leftrightarrow V = U + W$ and $\dim U + \dim W \leqslant \dim V$.

Linear Mappings and Matrices

Theorem 2.2.3.
Every square matrix with entries in a field can be written as a product of elementary matrices.

Theorem 2.2.5.
For every $A \in \operatorname{Mat}(n \times m; F)$ there exist ***invertible*** matrices P, Q s.t. PAQ is in Smith Normal Form.

Hint: First row operations to echelon form, then column operations.

Theorem 2.2.7.
For any matrix, column and row rank are equal.

Hint: Column & Row rank of matrix and its Smith Normal Form are equal as P, Q in Theorem 2.2.5 are invertible.

Theorem 2.4.3 (Change of Basis).
Let $f : V \to W$, $\mathcal{A}, \mathcal{A}'$ ordered bases of V, $\mathcal{B}, \mathcal{B}'$ ordered bases of W. Then

$${}_{\mathcal{B}'}[f]_{\mathcal{A}'} = {}_{\mathcal{B}'}[\mathrm{id}_W]_{\mathcal{B}} \circ {}_{\mathcal{B}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'}$$

Corollary (unlisted).
Let $f : \mathbb{R}^n \to \mathbb{R}^m$, $\mathcal{A} = \{\vec{a}_i\}$ ordered basis of R^n, $\mathcal{B} = \{\vec{b}_i\}$ ordered basis of $\mathbb{R}^m$. Then

$${}_{\mathcal{B}}[f]_{\mathcal{A}} = ({}_{\mathcal{S}(m)}[\mathrm{id}_{\mathbb{R}^m}]_{\mathcal{B}})^{-1} \circ {}_{\mathcal{S}(m)}[f]_{\mathcal{A}} = (\vec{b}_1|\vec{b}_2|\ldots|\vec{b}_m)^{-1}(f(\vec{a}_1)|f(\vec{a}_2)|\ldots|f(\vec{a}_n))$$

Theorem 2.4.4.
Let $f : V \to V$, $\mathcal{A}, \mathcal{A}'$ ordered bases of V. Then

$${}_{\mathcal{A}'}[f]_{\mathcal{A}'} = ({}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'})^{-1} \circ {}_{\mathcal{A}}[f]_{\mathcal{A}} \circ {}_{\mathcal{A}}[\mathrm{id}_V]_{\mathcal{A}'}$$

Exercise 32.
Let $f : V \to V$. Then f nilpotent $\Rightarrow$ there exists an order basis of V s.t. representing matrix of f is upper triangular with only 0's along diagonal. Additionally, $M \in \operatorname{Mat}(n; F)$ upper triangular with only 0's along diagonal $\Rightarrow M^n = 0$.

Exercise 33.
Let A, B be matrices of appropriate sizes, then $\operatorname{tr}(AB) = \operatorname{tr}(BA)$.

Corollary 33.
Conjugate matrices have equal trace.

Hint: Ex. 33 with $A = T^{-1}M, B = T$.

Exercise 35.
Let $f : V \to V$ be idempotent, i.e. $f^2 = f$, then $\operatorname{tr}(f) = \dim(\operatorname{im} f)$.

Rings and Modules

Proposition 3.1.11.
Let $m \in \mathbb{N}$, then $\mathbb{Z}/m\mathbb{Z}$ is a field if and only if m is prime.
Hint: ($\Rightarrow$) $\overline{a} \in \mathbb{Z}/m\mathbb{Z} \Rightarrow \exists \overline{b} \in \mathbb{Z}/m\mathbb{Z}$ s.t. $\overline{ab} = 1 \Leftrightarrow ab = km + 1$. a does not divide 1, so cannot divide m. ($\Longleftarrow$) $\overline{a} \in \mathbb{Z}/m\mathbb{Z}$, $\text{hcf}(a, m) = 1 \Leftrightarrow ab + mk = 1 \Leftrightarrow \overline{ab} = 1$.

Proposition 3.2.10. The set $R^\times$ of units in R forms a ***group under multiplication***.

Remark (unknown). If R is an integral domain, then for $a, b \in R$:

(1) $ab = 0 \Rightarrow a = 0$ or $b = 0$, and
(2) $a \neq 0$ and $b \neq 0 \Rightarrow ab \neq 0$.

Proposition 3.2.16 (Cancellation Law of Integral Domains).
Let R be an integral domain and $a, b, c \in R$. Then $ac = bc$ and $c \neq 0$ implies $a = b$.
Hint: $ac = bc \Leftrightarrow (a - b)c = 0$.

Proposition 3.2.17.
Let $m \in \mathbb{N}$, then $\mathbb{Z}/m\mathbb{Z}$ is an integral domain if and only if m is prime.
Hint: ($\Leftarrow$) $\overline{k}, \overline{l}$ zero-divisors $\Rightarrow \overline{kl} = \overline{0} \Rightarrow m$ divides k or l as m prime, so $\overline{k} = 0$ or $\overline{l} = 0$, contradiction. ($\Rightarrow$) m not prime, then $m = kl$, $1 < k, l < m$, then $\overline{k} \neq 0$ or $\overline{l} \neq 0$ but $\overline{kl} = \overline{0}$.

Theorem 3.2.18.
Every ***finite*** integral domain is a field.
Hint: $\lambda_a : R \to R; b \mapsto ab$, cancellation law gives injectivity, finite gives surjectivity.

Lemma 3.3.3.

(i) If R has no zero-divisors, then $R[X]$ has no zero-divisors and $\deg(PQ) = \deg(P) + \deg(Q)$.
(ii) If R is an integral domain, so is $R[X]$.

Theorem 3.3.4 (Division and Remainder).
Let R be an integral domain and $P, Q \in R[X]$ with Q ***monic***. Then there exists ***unique*** $A, B \in R[X]$ s.t. $P = AQ + B$ and $\deg(B) < \deg(Q)$ or $B = 0$.
Hint: Choose A s.t. $\deg(P - AQ)$ minimal (possible as degree non-negative. Suppose $\deg(P - AQ) = r \geqslant \deg(Q) = d \Rightarrow \deg(P - A + a_r X^{r-d} Q) < \deg(P - AQ)$.

Exercise 42.
If R is an integral domain, then $R[X]^\times = R^\times$.

Exercise 43.
Let $R = \mathbb{F}_p$, where p is prime. Then the mapping $R[X] \to \text{Maps}(R, R)$ is not injective.
Hint: $X^p - X \in \mathbb{F}_p[X]$ & Fermat's Little Theorem.

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

Theorem 3.3.10.
Let R be an integral domain. Then a non-zero polynomial $P \in R[X]$ has at most $\deg(P)$ roots in R.
Hint: $\lambda_{1,\ldots,m}$ distinct roots of $P \Rightarrow i \geqslant 2$: $0 = P(\lambda_i) = A(\lambda_i)(\lambda_i - \lambda_1)$ and $\lambda_i - \lambda_1 \neq 0$, induction.

Theorem 3.3.13 (Fundamental Theorem of Algebra).
The field $\mathbb{C}$ is algebraically closed.

Theorem 3.3.14.
Let F be an algebraically closed field. Then every non-zero polynomial $P \in F[X]$ ***decomposes into linear factors***

$$P = c(X - \lambda_1) \ldots (X - \lambda_n)$$

with $n \geqslant 0$, $c \in F^\times$ and $\lambda_i \in F$. This decomposition is ***unique***, up to reordering.

Remark 3.4.4.
Let R, S be rings and $f : R \to S$ be a homomorphism. Then $f(1_R)$ is ***idempotent***, i.e. $f(1_R)^2 = f(1_R) \Leftrightarrow f(1_r)[f(1_R) - 1_S] = 0_S$. If S has no zero-divisors, then either $f(1_R) = 0_S$ or $f(1_R) = 1_S$.

Lemma 3.4.5.
Let $f : R \to S$ be a ring homomorphism. Then for all $x, y \in R$, $m \in \mathbb{Z}$:

(1) $f(0_R) = 0_S$;
(2) $f(-x) = -f(x)$;
(3) $f(x - y) = f(x) - f(y)$;
(4) $f(mx) = mf(x)$.

Remark 3.4.6.

(1) Let f be a homomorphism. Then $f(x^n) = (f(x))^n$ for all $n \in \mathbb{N}$.
(2) Let $f : \mathbb{R} \to \text{Mat}(2; \mathbb{R}); x \mapsto \left(\begin{smallmatrix} x & 0 \\ 0 & 0 \end{smallmatrix}\right)$, then f does not send identity to identity.

Example 3.4.10.
$I = \{\left(\begin{smallmatrix} 0 & b \\ 0 & d \end{smallmatrix}\right) : b, d \in \mathbb{R} \subset \text{Mat}(2; \mathbb{R})$ is not an ideal, it fails to satisfy $ir \in I$.

Proposition 3.4.14.
Let R be a commutative ring, $T \subseteq R$. Then ${}_R\langle T\rangle$ is the smallest ideal of R containing T.
Hint: Minimality: $I \trianglelefteq R, t_1, \ldots, t_m \in I \Rightarrow \sum_{i=1}^m r_i t_i \in I$.

Proposition 3.4.18.
Let $f : R \to S$ be a ring homomorphism. Then $\ker f \trianglelefteq R$.

Lemma 3.4.20.
f injective $\Leftrightarrow \ker f = \{0\}$.

Lemma 3.4.21.
$I, J \trianglelefteq R \Rightarrow I \cap J \trianglelefteq R$.

Lemma 3.4.21.
$I, J \trianglelefteq R \Rightarrow I + J = \{a + b : a \in I, b \in J\} \trianglelefteq R$.

Example 3.4.25.
If F is a field, then for any $m, n \in \mathbb{N}$, with $m \leqslant n$, $\text{Mat}(m; F)$ is a subring of $\text{Mat}(n, F)$. ***But***, identities are ***not*** equal, i.e. $\mathbb{I}_m \neq \mathbb{I}_n$.

Proposition 3.4.26 (Test for a Subring).
Let R' be a subset of ring R. Then R' is a subring of R if and only if:

(1) R' has a multiplicative identity;
(2) $a, b \in R' \Rightarrow a - b \in R'$; and
(3) R' is closed under multiplication.

Proposition 3.4.29.
Let $f : R \to S$ be a ring homomorphism and assume $f(1_R) = 1_S$. Then $x \in R^\times \Rightarrow f(x) \in S^\times$ and $(f(x))^{-1} = f(x^{-1})$.
Hint: $f(x)f(x^{-1}) = f(xx^{-1}) = f(1_R)$.

Exercise 52.
Let R be a ring and $I \trianglelefteq R$. If R is commutative, so is R/I.

Exercise 53.
Let R be a ring and $I \trianglelefteq R$. R/I is a non-zero ring if and only if $I \neq R$.

Exercise 54.
Let R be a ring and I be a ***proper*** ideal of R. If $r \in R^\times$, then $r + I \in (R/I)^\times$ with $(r + I)^{-1} = r^{-1} + I$.

Theorem 3.6.7 (The Universal Property of Factor Rings).
Let R be a ring and $I \trianglelefteq R$.

(1) $\text{can} : R \to R/I; r \mapsto r + I$ 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 exists a unique ring homomorphism $\overline{f} : R/I \to S$ such that $f = \overline{f} \circ \text{can}$.

Hint: $f(x + I) = f(x) + f(I) = \{f(x)\}$, so $\overline{f}(x + I) = f(x)$ only possible map.

Theorem 3.6.9 (First Isomorphism Theorem for Rings).
Let R, S be rings, then every homomorphism $f : R \to S$ induces an isomorphism:

$$\overline{f} : R/\ker f \xrightarrow{\sim} \text{im}\, f.$$

Hint: $\overline{f}$ from Universal Property, $\ker \overline{f} = \{0 + \ker f\}$ and Lemma 3.4.20.

Example 3.7.4.
A $\mathbb{Z}$-module is exactly the same as abelian group.

Example 3.7.6.
Let $I \trianglelefteq R$, then I is an R-module.

Example 3.7.7.
Let R be a ring, $M_1, \ldots, M_n$ be R-modules, then $M_1 \times M_2 \times \ldots \times M_n$ is an R-module with addition and scalar multiplication defined componentwise.

Example 3.7.9.
Let $R = \text{Mat}(2; \mathbb{C})$ and $M = \mathbb{C}^2$. Then $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right)$, so $\lambda\vec{v} = 0 \not\Rightarrow \lambda = 0$ or $\vec{v} = \vec{0}$.

Proposition 3.7.20 (Test for a Submodule).
Let R be a ring and let M be an R-module. Let M' be a subset of M, then M' is a submodule if and only if:

(1) $0_M \in M'$;
(2) $a, b \in M' \Rightarrow a - b \in M'$;
(3) $r \in R, a \in M' \Rightarrow ra \in M'$.

Lemma 3.7.21.
Let $f : M \to N$ be an R-homomorphism. Then $\ker f$ is a submodule of M and $\text{im}\, f$ is a submodule of N.

Lemma 3.7.28.
Let $T \subseteq M$. Then ${}_R\langle T\rangle$ is the smalles submodule of M containing T.

Lemma 3.7.29.
The intersection of ***any*** collection of submodules of M is a submodule of M.

Lemma 3.7.30.
Let M_1, M_2 be a submodule of M. Then $M_1 + M_2$ is a submodule of M.

Theorem 3.7.32 (The Universal Property of Factor Modules).
Let R be a ring, L, M R-modules and N a submodule of M.

(1) $\text{can} : M \to M/N; a \mapsto a + N$ is a surjective R-homomorphism with kernel N.
(2) If $f : M \to L$ is an R-homomorphism with $f(N) = \{0_L\}$, so that $N \subseteq \ker f$, then there exists a unique homomorphism $\overline{f} : M/N \to L$ such that $f = \overline{f} \circ \text{can}$.

Theorem 3.6.9 (First Isomorphism Theorem for Modules).
Let R be a ring, M, N be R-modules, then every R-homomorphism $f : M \to N$ induces an R-isomorphism:

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

Hint: $\overline{f}$ from Universal Property, $\ker \overline{f} = \{0 + \ker f\}$ for injectivity.

Exercise 59 (Second Isomorphism Theorem for Modules).
Let N, K be submodules of R-module M. Then K is submodule of $N + K$, $N \cap K$ is a submodule of N and

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

Exercise 60 (Third Isomorphism Theorem for Modules).
Let N, K be submodules of R-module M, s.t. $K \subseteq N$. Then N/K is a submodule of M/K and

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

Determinants and Eigenvalues Redux

Example 4.1.4.
The identity of $\mathfrak{S}_n$ has length 0. A transposition swapping i and j has length $2|i - j| - 1$.

Lemma 4.1.5 (Multiplicativity of Sign).
For each $n \in \mathbb{N}$, sign of permutation $\operatorname{sgn} : \mathfrak{S}_n \to \{\pm 1\}$ produces group homomorphism, i.e. $\forall \sigma, \tau \in \mathfrak{S}_n : \operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma)\operatorname{sgn}(\tau)$.

Exercise 61.
Let $\sigma \in \mathfrak{S}_n$ be permutation s.t. it moves i to the first place and leaves rest unchanged. Then σ has $i - 1$ inversions and $\operatorname{sgn}(\sigma) = (-1)^{i-1}$.

Exercise 62.
Every permutation in $\mathfrak{S}_n$ can be written as product of transpositions of neighbouring numbers, i.e. permutations of form $(i\ i + 1)$.

Definition 4.2.1.
Let $A \in \operatorname{Mat}(n; R)$, where R is a ring. Then

$$\det A = \sum_{\sigma \in \mathfrak{S}_n} \operatorname{sgn}(\sigma) a_{1\sigma(a)} \ldots a_{n\sigma n}$$

In degenerate case $n = 0$, "empty matrix" is assigned determinant of 1.

Example 4.2.4.
The determinant of an upper triangular matrix is the product of the entries along the main diagonal.

Exercise 63.
Let $\mathbb{A}$ be a block-upper triangular matrix with diagonal entries $\mathbb{A}_{ii} = A_i$, for $A_i \in \operatorname{Mat}(n; R)$. Then $\det \mathbb{A} = \det(A_1)\det(A_2)\ldots\det(A_n)$.

Remark (unknown).
$|\det(L)|$ describes how much linear mapping L changes areas. If sign of $\det(L)$ is positive, then L preserves orientation, if negative, then L reverses orientation.

Remark 4.3.2.
If $H : U \times U \to W$, U, W being F-vector spaces, is an ***alternating*** bilinear form, then $\forall a, b \in U : H(a, b) = -H(b, a)$. If $1_F + 1_F \neq 0_F$, then $\forall a, b \in U : H(a, b) = -H(b, a)$ implies H is alternating. N.B.: this does ***not*** hold in $F = \mathbb{F}_2$!

Remark 4.3.5.
If $H : V \times V \times \ldots \times V \to W$, V, W being F-vector spaces, is an ***alternating*** bilinear form, then

$$H(\vec{v}_1, \ldots, \vec{v}_i, \ldots, \vec{v}_j, \ldots, \vec{v}_n) = -H(\vec{v}_1, \ldots, \vec{v}_j, \ldots, \vec{v}_i, \ldots, \vec{v}_n)$$

More generally, for $\sigma \in \mathfrak{S}_n$:

$$H(\vec{v}_{\sigma(1)}, \ldots, \vec{v}_{\sigma(n)}) = \operatorname{sgn}(\sigma) H(\vec{v}_1, \ldots, \vec{v}_n)$$

Converse is true provided $1_F + 1_F \neq 0_F$.

Theorem 4.3.6 (Characterisation of the Determinant).
Let F be a ***field***. The mapping $\det : \operatorname{Mat}(n; F) \to F$ is the unique alternating multilinear form on n-tuples of column vectors with values in F s.t. $\det \mathbb{I}_n = 1_F$.

Exercise 64.
Let $d : \operatorname{Mat}(n; F) \to F$ be an ***alternating*** multilinear form on n-tuples of column vectors in F^n, then $\forall A \in \operatorname{Mat}(n; F) : d(A) = d(e_1|\ldots|e_n)\det(A)$.

Theorem 4.4.1 (Multiplicativity of the Determinant).
Let R be a commutative ring, $A, B \in \operatorname{Mat}(n; R)$. Then $\det(AB) = (\det A)(\det B)$.

Theorem 4.4.2 (Determinantal Criterion for Invertibility).
Let F be a field, $A \in \operatorname{Mat}(n; F)$. Then $\det A \neq 0 \Leftrightarrow A$ invertible.
Hint: $(\Leftarrow)$ $B = A^{-1}$, $\det(AB) = 1$ by multiplicativity, $(\Rightarrow)$ A not invertible, then dependent column(s), then alternating form 0.

Remark 4.4.3.
From Theorem 4.4.2 follows that $\det A^{-1} = (\det A)^{-1}$ and $\det(A^{-1}BA) = \det B$. Latter asserts that there exists unique determinant for an endomorphism.

Theorem 4.4.7 (Laplace's Expansion of the Determinant).
Let $A = (a_{ij})$ with entries in commutative ring R. For fixed i, i-th row expansion is

$$\det A = \sum_{j=0}^{n} a_{ij} C_{ij}$$

and for fixed j, j-th column expansion is

$$\det A = \sum_{i=0}^{n} a_{ij} C_{ij}$$

Theorem 4.4.9 (Cramer's Rule).
Let $A \in \operatorname{Mat}(n; R)$, R being a commutative ring. Then $A \cdot \operatorname{adj}(A) = (\det A)\mathbb{I}_n$.

Corollary 4.4.11 (Invertibility of Matrices).
Let $A \in \operatorname{Mat}(n; R)$, R being a commutative ring. Then A invertible $\Leftrightarrow \det A \in R^\times$.

Theorem 4.5.4 (Existence of Eigenvalues).
Let $f : V \to V$ be an endomorphism, V a non-zero, finite dimensional vector space over F, where F is algebraically closed. Then f has an eigenvalue.

Remark 4.5.5.
Requirements in Theorem 4.5.4 are as tight as possible: consider infinite dimensional vector space $\mathbb{C}[X]$ with $f : P \mapsto X \cdot P$ and non-algebraically closed $\mathbb{R}^2$ with rotation by 90 degrees.

Theorem 4.5.8 (Eigenvalues and Characteristic Polynomials).
Let $A \in \operatorname{Mat}(n; F)$, F being a field. The eigenvalues of $A : F^n \to F^n$ are the roots of χ_A.
Hint: λ eigenvalue of $A \Leftrightarrow \exists \vec{v} \neq 0$ s.t. $A\vec{v} = \lambda\vec{v}$ $\Leftrightarrow \ker(A - \lambda\mathbb{I}_n) \neq \{\vec{0}\} \Leftrightarrow \det(A - \lambda\mathbb{I}_n)$.

Exercise 67.
Let $A \in \operatorname{Mat}(n; F)$, F being a field. Then $\chi_A(x) = (-x)^n + \operatorname{tr}(A)(-x)^{n-1} + \ldots + \det(A)$.

Remark 4.5.9.

(2) Let $A, B \in \operatorname{Mat}(n; R)$ be representing matrices of $f : V \to V$ with respect to different bases. Then A and B are conjugate.
(3) Let $A, B \in \operatorname{Mat}(n; R)$, R being a commutative ring, be ***conjugate***. Then $\chi_A = \chi_B$.
(4) Let $f : V \to V$, V being an n-dimensional vector space over field F and let A be the representing matrix for f with respect to ***any*** basis. Then $\chi_f = \chi_A$.

Exercise 68.
Let $A, B \in \operatorname{Mat}(n; F)$, F begin a field. Then A and B are conjugate $\Leftrightarrow \exists f : V \to V$ s.t. A and B are representing matrices of f.

Proposition 4.6.1 (Triangularisability).
Let $f : V \to V$, V being a finite dimensional F-vector space. Then the following is equivalent:

(1) f is ***triangularisable***.
(2) χ_f decomposes into linear factors in $F[X]$.

Remark 4.6.2.

(1) Endomorphism $A : F^n \to F^n$ is triangularisable $\Leftrightarrow$ A is conjugate to an upper triangular matrix.
(3) Endomorphism $f : F^n \to F^n$ is triangularisable $\Leftrightarrow$ there exists sequence of subspaces $\{0\} = V_0 \subset V_1 \subset V_2 \subset \ldots \subset V_n = V$ s.t. V_i is i-dimensional and $f(V_i) \subseteq V_i$.

Remark 4.6.4.
Let $A \in \operatorname{Mat}(n; F)$, then A ***nilpotent*** $\Leftrightarrow$ $\chi_A(x) = (-x)^n$.

Lemma 4.6.8 (Linear Independence of Eigenvectors).
Let $f : V \to V$ with eigenvectors $\vec{v}_1, \ldots, \vec{v}_n$ with pairwise different eigenvalues $\lambda_1, \ldots, \lambda_n$. Then $\vec{v}_1, \ldots, \vec{v}_n$ are linearly independent.
Hint: Consider $(f - \lambda_2 \operatorname{id}_V) \circ \ldots \circ (f - \lambda_n \operatorname{id}_V)(\vec{v}_j) = \prod_{i=2}^{n}(\lambda_i - \lambda_j)\vec{v}_i$, 0 if $i \neq 1$ and $\prod_{i=2}^{n}(\lambda_1 - \lambda_j)\vec{v}_1$ if $i = 1$. Apply to $\sum_{i=1}^{n} \alpha_i \vec{v}_i = \vec{0} \Rightarrow \alpha_1 \prod_{i=2}^{n}(\lambda_1 - \lambda_j)\vec{v}_1 = \vec{0} \Rightarrow \alpha_1 = 0$. Repeat for rest.

Remark 4.6.3.
Let $A \in \operatorname{Mat}(n; F)$, then A nilpotent $\Leftrightarrow \chi_A(x) = (-x)^n$.

Theorem 4.6.9 (The Cayley-Hamilton Theorem).
Let $A \in \operatorname{Mat}(n; R)$, with ***commutative ring*** R. Then $\chi_A(A) = 0$, the zero matrix.
Hint: $B = A - x\mathbb{I} \in \operatorname{Mat}(n, R[x])$, Cramer's Rule $\Rightarrow B \cdot \operatorname{adj}(B) = \det(B)\mathbb{I} = \chi_A(x)\mathbb{I}$, $\operatorname{adj}(B) \in \operatorname{Mat}(n, R[x])$. Equally $\operatorname{adj}(B) \in \operatorname{Mat}(n, R)[x] \Rightarrow \operatorname{adj}(B) = \sum_{i \geqslant 0} x^i K_i$. Substitute s.t. $\chi_A(x)\mathbb{I} = AK_0 + \sum_{i \geqslant 1} x^i(AK_i - K_{i-1})$.

Evaluate at A and cancel s.t. $\chi_A(x)\mathbb{I} = A^{n+1}C_n$. Degree of cofactors of $\operatorname{adj}(B)$ at most $n-1$, so $C_n = 0$.

Lemma 4.7.6.
Let $M \in \mathrm{Mat}(n;\mathbb{R})$ be a Markov matrix. Then $\lambda = 1$ is an eigenvalue of M.

Hint: Columns of $M - \mathbb{I}_n$ sum to 0 $\Rightarrow$ sum of row vectors is $\vec{0} \Rightarrow$ linear dependence $\Rightarrow \det(M - \mathbb{I}_n) = 0 \Rightarrow \chi_M(1) = 0$.

Theorem 4.7.10 (Perron, 1907).
Let $M \in \mathrm{Mat}(n;\mathbb{R})$ be a Markov matrix with ***positive*** entries, then eigenspace $\mathrm{E}(1, M)$ is one dimensional. There exists a unique basis vector $\vec{v} \in \mathrm{E}(1, M)$ whose entries are positive and sum to 1.

Inner Product Spaces

Example 5.1.4.
Let $\vec{v}, \vec{w}\mathbb{C}^n$, then ***standard inner product*** is $(\vec{v}, \vec{w}) = \vec{v}^T \circ \overline{\vec{w}}$. N.B.: Conjugate on second.

Example 5.1.6.
Let $\vec{v}, \vec{w}$ be orthogonal. Then Pythagoras' Theorem holds: $\|\vec{v} + \vec{w}\|^2 = \|\vec{v}\|^2 + \|\vec{w}\|^2$.

Theorem 5.1.10.
Every ***finite*** dimensional inner product space V has an ***orthonormal*** basis.

Hint: Induction on $\dim V$. Base Case $\dim V = 0$ trivial. $\dim V = n > 0 \Rightarrow \exists \vec{v} \in V$, normalize to $\vec{v}_1$ and consider $(-, \vec{v}_1) : V \to \mathbb{R}; \vec{w} \to (\vec{w}, \vec{v}_1)$. Kernel of that has dim. $n-1$ by Rank-Nullity.

Exercise 73.
Let V be an inner product space, then $\forall T \subseteq V$ $T^\perp$ is a subspace and $T^\perp = \langle T\rangle^\perp$.

Proposition 5.2.2.
Let $U \subseteq V$ be finite dimensional subspace of inner product space V. Then $U, U^\perp$ are complementary, i.e. $V = U \oplus U^\perp$.

Hint: Exercise 19. $\vec{v} \in U \cap U^T \Rightarrow (\vec{v}, \vec{v}) = 0 \Rightarrow \vec{v} = \vec{0}$. Want $\vec{v} = \vec{p} + \vec{r}$ s.t. $\vec{p} \in U$, $\vec{r} \in U^\perp$. Thrm 5.1.10 $\Rightarrow U$ has orthonormal basis $\{\vec{v}_i$ s.t. $\vec{p} = \sum_{i=1}^n (\vec{v}, \vec{v}_i)\, \vec{v}_i$. Take $\vec{r} = \vec{v} - \vec{p}$ s.t. $(\vec{r}, \vec{v}_j) = 0 \Rightarrow \vec{r} \in U^\perp$.

Proposition 5.2.4.
Let $U \subseteq V$ be finite dimensional subspace of inner product space V.

(1) π_U is a linear mapping with $\operatorname{im}(\pi_u) = U$, $\ker(\pi_U) = U^\perp$;
(2) if $\{\vec{v}_1, \dots, \vec{v}_n\}$ ***orthonormal*** basis of U, then for $\vec{v} \in V$: $\pi_U(\vec{v}) = \sum_{i=1}^n (\vec{v}, \vec{v}_i)\, \vec{v}_i$;
(3) $\pi_U^2 = \pi_U$, i.e. π_U idempotent.

Theorem 5.2.5 (Cauchy-Schwarz Inequality).
Let $\vec{v}, \vec{w} \in V$, inner product space. Then

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

with ***equality*** $\Leftrightarrow \vec{v}, \vec{w}$ ***linearly dependent***.

Hint: $\vec{w} = \vec{0}$ trivially true; $\vec{w} \neq 0$, $W = \langle \vec{w} \rangle$, $\vec{x} = \vec{v} - \pi_W(\vec{v}) \Rightarrow \vec{x} \perp \pi_W(\vec{v})$ so Pythagoras holds: $\|\vec{v}\|^2 = \|\vec{x} + \pi_W(\vec{v})\|^2 = \|\vec{x}\|^2 + \|\pi_W(\vec{v})\|^2$, $\pi_W(\vec{v})$ from Prop. 5.2.4.

Corollary 5.2.6.
Let $\|\cdot\|$ be the norm on inner product space V, then $\forall \vec{v}, \vec{w} \in V$:

(1) $\|\vec{v}\| \geqslant 0$, equality $\Leftrightarrow \vec{v} = 0$;
(2) $\|\lambda \vec{v}\| = |\lambda|\, \|\vec{v}\|$;
(3) ***Triangle Inequality:*** $\|\vec{v} + \vec{w}\| = \|\vec{v}\| + \|\vec{w}\|$

Exercise 75.
Let T^* be adjoint of T. Then $(T^*)^* = T$.

Theorem 5.3.4.
Let $T : V \to V$, V begin a finite dimensional inner product space. Then T^* exists and is ***unique***.

Hint: $\phi := (T(-), \vec{w}) : V \to F$, linear as $(-, \vec{w})$, T are. Thrm 5.1.10 $\Rightarrow \exists \{\vec{e}_i\}_{1 \leqslant i \leqslant n}$ orthonormal basis of $V \Rightarrow$ for $\vec{v} = \sum_{i=1}^n (\vec{v}, \vec{e}_i)\, \vec{e}_i \Rightarrow \phi(\vec{v}) = \sum_{i=1}^n (\vec{v}, \vec{e}_i)\, \phi(\vec{e}_i) = \left(\vec{v}, \sum_{i=1}^n \overline{\phi(\vec{e}_i)} \vec{e}_i\right) \Rightarrow \exists\, \vec{u}$ s.t. $\phi(\vec{v}) = (\vec{v}, \vec{u}) = (\vec{v}, T^*(\vec{w})) \Rightarrow T^*$ exists. $(\vec{v}, \vec{u} - \vec{u}') = \phi(\vec{v}) - \phi\vec{v}$ for uniqueness & show linearity with uniqueness.

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

(1) every eigenvalue of T is real;
(2) if λ, μ are distinct eigenvalues of T, then the corresponding eigenvectors are orthogonal;
(3) T has an eigenvalue.

Hint: (1) $\lambda(\vec{v}, \vec{v}) = (T\vec{v}, \vec{v}) = (\vec{v}, T\vec{v}) = \overline{\lambda}(\vec{v}, \vec{v})$. (2) $\lambda(\vec{v}, \vec{w}) = (T\vec{v}, \vec{w}) = (\vec{v}, T\vec{w}) = \mu(\vec{v}, \vec{w})$. (3) Over $\mathbb{R}$. $R(\vec{v}) = \frac{(T\vec{v}, \vec{v})}{(\vec{v}, \vec{v})}$ restricted to unit sphere, Heine-Borel Thrm $\Rightarrow$ maximum at $\vec{v}_+$ in unit sphere & $R(\lambda\vec{v}) = R(\vec{v}) \Rightarrow \vec{v}_+$ is max. overall. $R_{\vec{w}}(t) = R(\vec{v}_+ + t\vec{w})$ is well-defined and

$$R'_{\vec{w}}(0) = \frac{(T\vec{w}, \vec{v}_+) + (T\vec{v}_+, \vec{w})}{(\vec{v}_+, \vec{v}_+)} - \frac{2\,(T\vec{v}_+, \vec{v}_+)\,(\vec{v}_+, \vec{w})}{(\vec{v}_+, \vec{v}_+)^2}.$$

Use $\vec{w}^\perp \in V$ s.t. $\vec{v}_+ \perp \vec{w}^\perp \Rightarrow$ $R'_{\vec{w}^\perp}(0) = \frac{\left(T\vec{w}^\perp, \vec{v}_+\right) + \left(T\vec{v}_+, \vec{w}^\perp\right)}{(\vec{v}_+, \vec{v}_+)} = 0 \Rightarrow$ $\left(T\vec{w}^\perp, \vec{v}_+\right) = -\left(T\vec{v}_+, \vec{w}^\perp\right) \Rightarrow \vec{w}^\perp \perp T\vec{v}_+ \Rightarrow$ $T\vec{v}_+ \in (\langle \vec{v}_+ \rangle^\perp)^\perp = \langle \vec{v}_+ \rangle \Rightarrow$ $\exists \lambda \in \mathbb{R} : T\vec{v}_+ = \lambda \vec{v}_+$.

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

Hint: Induction on $\dim V$. $\dim V = 1$ holds by Thrm 5.3.7. For $\dim V = n > 1$ take any eigenvalue λ of T, exists by Thrm 5.3.7, and ***normalized*** eigenvector $\vec{u}$. $U = \langle \vec{u} \rangle$, $\vec{v} \in U^\perp$. $(\vec{u}, T\vec{v}) = \lambda(\vec{u}, \vec{v}) = 0 \Rightarrow T(U^\perp) \subseteq U^\perp$, so $T|_{U^\perp} : U^\perp \to U^\perp$ self-adjoint, induction hypothesis $\Rightarrow \exists$ orthonormal basis $B \Rightarrow$ $B \cup \{\vec{u}\}$ orthonormal basis V.

Exercise 76.
Let $P \in \mathrm{Mat}(n;\mathbb{R})$, then $P^T P = \mathbb{I}_n \Leftrightarrow$ columns of P form orthonormal basis for $\mathbb{R}^n$.

Corollary 5.3.12 (The Spectral Theorem for Real Symmetric Matrices).
Let $A \in \mathrm{Mat}(n, \mathbb{R})$ be ***symmetric***. Then there exists $P \in \mathrm{Mat}(n, \mathbb{R})$ ***orthogonal*** s.t.

$$P^T A P = P^{-1} A P = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$$

where $\lambda_1, \dots, \lambda_n \in \mathrm{R}$ are eigenvalues of A, repeated accordingly.

Hint: Spectral Theorem & Exercise 76.

Exercise 78.
Let $P \in \mathrm{Mat}(n;\mathbb{C})$, then $\overline{P}^T P = \mathbb{I}_n \Leftrightarrow$ columns of P form orthonormal basis for $\mathbb{C}^n$.

Corollary 5.3.15 (The Spectral Theorem for Hermitian Matrices).
Let $A \in \mathrm{Mat}(n, \mathbb{C})$ be ***hermitian***. Then there exists $P \in \mathrm{Mat}(n, \mathbb{C})$ ***unitary*** s.t.

$$P^T A P = P^{-1} A P = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$$

where $\lambda_1, \dots, \lambda_n \in \mathrm{R}$ are eigenvalues of A, repeated accordingly.

Exercise Hw.6, Ex.3.
Let $T : V \to V$ be an endomorphism of a finite-dimensional inner product space. Let T^* be the adjoint of T. Then

(1) T^*T is self-adjoint; and
(2) if $T^*T = 0$, then $T = 0$.

Exercise Hw.6, Ex.4.

(1) Let $A \in \mathrm{Mat}(n;\mathbb{R})$ be an orthogonal matrix. Then $\det A \in \{\pm 1\}$.
(2) Let $A \in \mathrm{Mat}(n;\mathbb{C})$ be a unitary matrix. Then $\det A$ lies on the unit circle in $\mathbb{C}$.

Hint: Spectral Theorem & Exercise 78.

Miscellaneous

Remark (unknown). Let $\sim$ be an equivalence relation on X, $x, y \in X$ and $E(x), E(y)$ equivalence classes for x, y respectively. The following are equivalent:

(1) $x \sim y$;
(2) $E(x) = E(y)$;
(3) $E(x) \cap E(y) \neq \emptyset$.

Proposition (unknown).
A, B matrices, then $(A + B)^T = A^T + B^T$.

Proposition (unknown).
$A \in \mathrm{Mat}(n;\mathbb{C})$, then $\det(\overline{A}^T) = \overline{\det(A)}$.

Theorem (Lagrange's Theorem).
Let G be a finite group and H a subgroup, then $|H|$ divides $|G|$.

Definitions

Definition (unknown).
Let U, W be subspace of V, then $U + W := \langle U \cup W \rangle$, i.e. subspace generated by U and W together.

Definition 1.7.6.
Two vector spaces V_1 and V_2 are ***complementary*** if addition defines a bijection $V_1 \times V_2 \xrightarrow{\sim} V$. This produces a bijection $V_1 \oplus V_2 \xrightarrow{\sim} V$, we say $V = V_1 \oplus V_2$ is the ***(internal) direct sum*** of V_1, V_2.

Definition 2.2.2.
An ***elementary matrix*** is a matrix which differs from the identity in at most one entry.

Definition 2.2.4.
A matrix with only 0's except possibly along the diagonal, where first only 1's then 0's, is in ***Smith Normal Form***.

Definition 2.2.6.
Column/Row rank of a matrix is dimension of subspace spanned by columns/rows of said matrix.

Definition 2.2.8.
Rank of a matrix A, $\mathrm{rk}A$, is column/row rank. If rank of a matrix is equal to number of rows/columns, then matrix has ***full rank***.

Definition 32.
Endomorphism $f : V \to V$ is ***nilpotent*** if there exists $d \in \mathbb{N}$ s.t. $f^d = 0$.

Definition 2.4.6.
The ***trace*** of a matrix A, $\mathrm{tr}(A)$, is the ***sum*** of the diagonal entries.

Definition 3.1.8.
A ***field*** is a non-zero, commutative ring F in which every non-zero element $a \in F$ has an inverse $a^{-1} \in F$.

Definition 3.1.9.
A ***skewfield*** or ***division ring*** is a non-zero ring F in which every non-zero element $a \in F$ has an inverse $a^{-1} \in F$. N.B.: does ***not*** have to be commutative.

Definition 3.2.6. Let R be a ring. Element $a \in R$ is a ***unit*** if $a^{-1} \in R$, i.e. a is ***invertible***.

Definition 3.2.12. Let R be a ring. Element $a \in R$ is a ***zero-divisor*** if $a \neq 0$ and $\exists\, b \in R$ s.t. $b \neq 0$ and either $ab = 0$ or $ba = 0$.

Definition 3.2.13. An ***integral domain*** is a ***non-zero, commutative*** ring with ***no zero-divisors***.

Definition 3.3.11.
A field F is algebraically closed if each non-constant polynomial with coefficients in F has a root in F.

Definition 3.4.7.
Let R be a ring and $I \subseteq R$. Then I is an ***ideal*** of R, $I \trianglelefteq R$, if:

(1) $I \neq \emptyset$;
(2) $a, b \in I \Rightarrow a - b \in I$;
(3) $\forall i \in I, r \in R : ri, ir \in I$.

E.g. $m\mathbb{Z} \trianglelefteq \mathbb{Z}$, $R \trianglelefteq R$, $\{0\} \trianglelefteq R$.

Definition 3.4.11.
Let R be a commutative ring, $T \subset R$. Then the ***ideal of*** R ***generated by*** T is the set:

$$_R\langle T\rangle = \{r_1t_1 + \ldots + r_mt_m : t_i \in T, r_i \in R\}$$

including 0_R in case $T = \emptyset$.

Definition 3.4.15.
Let R be a commutative ring. Then $I \trianglelefteq R$ is a ***principal ideal*** if $\exists t \in R : I = \langle t\rangle$.

Definition 3.5.7.
A map $g : (X/\sim) \to Z$ is ***well-defined*** if there exists a map $f : X \to Z$ with property $x \sim y \Rightarrow f(x) = f(y)$ and $g = \overline{f}$, where $\overline{f}(E(x)) = f(x)$.

Definition 3.6.1.
Let $I \trianglelefteq R$, $x \in R$ then the set

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

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

Definition 3.6.3.
Let R be a ring, $I \trianglelefteq R$ and $\sim$ an 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/I) of cosets of I in R.

Definition 4.1.1.
A ***transposition*** is a permutation swapping exactly two elements.

Definition 4.1.2.
An ***inversion*** of a permutation $\sigma \in \mathfrak{S}_n$ is a pair (i, j) s.t. $1 \leqslant i < j \leqslant n$ and $\sigma(i) > \sigma(j)$. The number of inversions of the permutation σ is ***length of*** σ, $\ell(\sigma)$:

$$\ell(\sigma) = |\{(i, j) : 1 \leqslant i < j \leqslant n \,\text{but}\, \sigma(i) > \sigma(j)\}|$$

The ***sign of*** σ is $\mathrm{sgn}(\sigma) = (-1)^{\ell(\sigma)}$.

Definition 4.3.1.
Let U, V, W be F-vector spaces. A ***bilinear form*** $H : U \times V \to W$ is a mapping s.t. for all $a, b \in U$ and $c, d \in V$ and all $\lambda \in F$:

$$H(a + b, c) = H(a, c) + H(b, c)$$
$$H(\lambda a, c) = \lambda H(a, c)$$
$$H(a, c + d) = H(a, c) + H(a, d)$$
$$H(a, \lambda c) = \lambda H(a, c)$$

A bilinear form is ***symmetric*** if $U = V$ and

$$\forall a, b \in U : H(a, b) = H(b, a)$$

and ***alternating*** or ***antisymmetric*** if $U = V$ and

$$\forall a \in U : H(a, a) = 0.$$

Definition 4.3.4.
Let V, W be F-vector spaces, $H : V \times \ldots \times V$ multilinear form. Then H is ***alternating*** if it vanishes on any n-tuple of elements of V where at least two entries are equal:

$$(\exists i \neq j : v_i = v_j) \Rightarrow H(v_1, \ldots, v_n) = 0.$$

Definition 4.4.6.
Let $A \in \mathrm{Mat}(n; R)$, R commutative ring. Let $1 \leqslant i, j \leqslant n$. 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 A with row i and column j removed.

Definition 4.4.8.
Let $A \in \mathrm{Mat}(n; R)$, R being a commutative ring. Let C_{ji} be the (j, i)-cofactor of A, then the ***adjugate matrix*** $\mathrm{adj}(A)$ is the matrix with entries $\mathrm{adj}(A)_{ij} = C_{ji}$.

Definition 4.5.6.
Let $A \in \mathrm{Mat}(n; R)$, R being a commutative ring. Then the ***characteristic polynomial of*** A is $\chi_A(x) := \det(A - x\mathbb{I}_n)$.

Definition 4.5.9.
Let $A, B \in \mathrm{Mat}(n; R)$, R being a commutative ring. Then A, B are ***conjugate*** if there exists invertible $P \in \mathrm{GL}(n; R)$ s.t. $B = P^{-1}AP$.

Definition 4.6.1.
Let $f : V \to V$, V being a finite dimensional F-vector space. Then f is ***triangularisable*** if there exists an ordered basis for V s.t. the representing matrix of f with respect to the basis is triangular.

Definition 4.6.5.
An endomorphism $f : V \to V$ of F-vector space V is ***diagonalisable*** if and only if there exists a basis of V consisting of eigenvectors of f. For finite dimensional V this is equivalent to representing matrix being diagonal with eigenvalues of f as entries.

Definition 4.7.5.
A ***Markov matrix*** or ***stochastic matrix***, is a matrix M s.t. each entry is non-negative and the columns sum to 1.

Definition 5.1.1. V vector space over $\mathbb{R}$, ***inner product*** is mapping $(-, -) : V \times V \to \mathbb{R}$ such that for $\vec{x}, \vec{y}, \vec{z} \in V$, $\lambda, \mu \in \mathbb{R}$:

(1) $(\lambda\vec{x} + \mu\vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$;
(2) $(\vec{x}, \vec{y}) = (\vec{y}, \vec{z})$;
(3) $(\vec{x}, \vec{x}) \geqslant 0$ and $0 \Leftrightarrow \vec{x} = \vec{0}$.

Definition 5.1.1. V vector space over $\mathbb{C}$, ***inner product*** is mapping $(-, -) : V \times V \to \mathbb{C}$ such that for $\vec{x}, \vec{y}, \vec{z} \in V$, $\lambda, \mu \in \mathbb{C}$:

(1) $(\lambda\vec{x} + \mu\vec{y}, \vec{z}) = \lambda(\vec{x}, \vec{z}) + \mu(\vec{y}, \vec{z})$;
(2) $(\vec{x}, \vec{y}) = \overline{(\vec{y}, \vec{z})}$;
(3) $(\vec{x}, \vec{x}) \geqslant 0$ and $0 \Leftrightarrow \vec{x} = \vec{0}$.

N.B.: Complex inner product is hermitian, and so sesquilinear.

Definition 5.1.4.
A map $f : V \to W$, V, W complex vector spaces, is ***skew-linear*** if for $\vec{v}, \vec{u} \in V$, $\lambda \in \mathbb{C}$:

(i) $f(\vec{v} + \vec{u}) = f(\vec{v}) + f(\vec{u})$;
(ii) $f(\lambda\vec{v}) = \overline{\lambda}f(\vec{v})$.

Definition 5.1.4.
A map $f : V_1 \times V_2 \to W$, complex vector spaces, that is linear in its first and skew-linear in its second variable is a ***sesquilinear form***, i.e.:

(i) $f(\lambda\vec{v}, \vec{u}) = \lambda f(\vec{v}, \vec{u})$
(ii) $f(\vec{v}, \lambda\vec{u}) = \overline{\lambda}f(\vec{v}, \vec{u})$

Definition 5.1.4.
Let f be a sesquilinear form and let $f(\vec{v}, \vec{u}) = \overline{f(\vec{u}, \vec{v})}$, then f is ***hermitian***.

Definition 5.1.5.
In complex or real inner product space, the ***length*** or ***inner product norm*** $\|\vec{v}\| \in \mathbb{R}$ is defined $\|\vec{v}\| = \sqrt{(\vec{v}, \vec{v})}$.

Definition 5.1.7.
A family $(\vec{v}_i)_{i \in I}$ of vectors in an inner product space is an ***orthonormal family*** if all $\vec{v}_i$ have length 1 and are pairwise orthogonal, i.e. $(\vec{v}_i, \vec{v}_j) = \delta_{ij}$.
If an orthonormal family is a basis, it is an ***orthonormal basis***.

Definition 5.2.1.
Let V inner product space, $T \subseteq V$. Then

$$T^{\perp} = \{\vec{v} \in V : \vec{v} \perp \vec{t}, \forall \vec{t} \in T\}$$

is the ***orthogonal*** to T.

Definition 5.2.3.
Let $U \subseteq V$ be finite dimensional subspace of inner product space V. $U^{\perp}$ is ***orthogonal complement to*** U.
The map $\pi_U : V \to V; \vec{v} = \vec{p} + \vec{r} \mapsto \vec{p}$, $\vec{p} \in U$, $\vec{r} \in U^{\perp}$ is the ***orthogonal projection from V onto U***.

Definition 5.3.6.
Let $A \in \mathrm{Mat}(n, \mathbb{C})$ s.t. $A = \overline{A}^T$, then A is ***hermitian***.

Definition 5.3.11.
Let $P \in \mathrm{Mat}(m, \mathbb{R})$. P is ***orthogonal*** if $P^TP = \mathbb{I}_n$, i.e. $P^{-1} = P^T$.

Definition 5.3.14.
Let $P \in \mathrm{Mat}(m, \mathbb{C})$. P is ***unitary*** if $\overline{P}^TP = \mathbb{I}_n$, i.e. $P^{-1} = \overline{P}^T$.