Organized results
Algebra
Michael Artin

Contents

Chapter 1

Matrices

1.1 The basic operations

October 7, 2021

Definition 1.1.1 (Matrices over a field)**.** "A is an $m \times n$ matrix over $(F, +, \cdot)$" iff $(F, +, \cdot)$ is a field and $m, n \geq 1$ are naturals such that $A\colon \{1, \ldots, m\} \times \{1, \ldots, n\} \to F$.

"A is a matrix over $(F, +, \cdot)$" iff there exist m, n such that A is an $m \times n$ matrix over $(F, +, \cdot)$.

Remark 1.1.2. We'll deal with matrix over a given field $\mathbb{F}$, unless stated otherwise, thus replacing "let A be a matrix over $\mathbb{F}$" with "let A be a matrix".

We'll denote the set of scalars of $\mathbb{F}$ by $\mathfrak{F}$.

We'll write "a is a scalar" to mean that $a \in \mathfrak{F}$.

Abbreviation 1.1.3 (Entries of matrices)**.** For any matrix A of size $m \times n$ and for any $1 \leq i \leq m$ and any $1 \leq j \leq n$, we set $A_{i,j} := A_{(i,j)}$.

Lemma 1.1.4 (Size of a matrix)**.** *Let A be a matrix. Then there exist unique $m, n \in \mathbb{N}$ such that A is an $m \times n$ matrix.*

Lemma 1.1.5 (Zero matrices)**.** *Let $m, n \geq 1$ be naturals. Then there exists a unique $m \times n$ matrix A such that for each $1 \leq i \leq m$ and for each $1 \leq j \leq n$, we have $A_{i,j} = 0$.*

Remark 1.1.6. This allows to denote A by $0_{m \times n}$.

Definition 1.1.7 (Square matrices)**.** "A is a square matrix of size n" iff there A is an $n \times n$ matrix.

"A is a square matrix" iff there exists an n such that A is a square matrix of size n.

Lemma 1.1.8. *Let A be a square matrix. Then there exists a unique $n \in \mathbb{N}$ such that A is a square matrix of size n.*

Lemma 1.1.9 (Identity matrices)**.** *Let $n \geq 1$ be natural. Then there exists a unique square matrix A of size n such that for all $1 \leq i, j \leq n$, we have $A_{i,j} = 1$ if $i = j$, and $A_{i,j} = 0$ if $i \neq j$.*

Remark 1.1.10. This allows to denote A by I_n.

Lemma 1.1.11 (Operations on matrices)**.** *Let A and B be matrices of size $m \times n$ each, and C be a matrix of size $n \times p$ and λ be a scalar. Then there exist unique matrices W, X, Y, Z such that*

(a) (addition) *W is an $m \times n$ matrix such that for each $1 \leq i \leq m$ and for each $1 \leq j \leq n$, we have $W_{i,j} = A_{i,j} + Bi, j$,*
(b) (negation) *X is an $m \times n$ matrix such that for each $1 \leq i \leq m$ and for each $1 \leq j \leq n$, we have $X_{i,j} = -A_{i,j}$,*
(c) (matrix multiplication) *Y is an $m \times p$ matrix such that for each $1 \leq i \leq m$ and for each $1 \leq j \leq p$, we have $Y_{i,j} = \sum_{k=1}^{n} A_{i,k} C_{k,j}$, and*
(d) (scalar multiplication) *Z is an $m \times n$ matrix such that for each $1 \leq i \leq m$ and for each $1 \leq j \leq n$, we have $Z_{i,j} = \lambda A_{i,j}$.*

Remark 1.1.12. This along with Lemma 1.1.4 allows to denote W, X, Y, Z by $A + B$, $-A$, AB, λA.

Lemma 1.1.13 (Properties of matrices)**.** *Let $m, n, p, q \in \mathbb{N}$, and A, A', A'' be $m \times n$ matrices, and B, B' be $n \times p$ matrices and C be a $p \times q$ matrix and λ, μ be scalars. Then $A + A'$, A'', $A' + A''$, $-A$, λA are $m \times n$ matrices, and AB, AB', $A'B$ are $m \times p$, and BC is an $n \times q$ matrix, and λB is an $n \times p$ matrix, and*

$$
\begin{aligned}
A + A' &= A' + A, \\
(A + A') + A'' &= A + (A' + A''), \\
0_{m \times n} + A &= A, \\
(-A) + A &= 0_{m \times n},
\end{aligned}
$$

$$\begin{aligned}
(AB)C &= A(BC),\\
I_m A &= A I_n = A,\\
A(B+B') &= AB + AB',\\
(A+A')B &= AB + A'B,\\
1A &= A,\\
(\lambda\mu)A &= \lambda(\mu A),\\
\lambda(A+A') &= \lambda A + \lambda A', \textit{ and}\\
\lambda(AB) &= (\lambda A)B = A(\lambda B).
\end{aligned}$$

Definition 1.1.14 (Inverses and invertible matrices)**.** "B is an inverse of matrix A" iff there exists a natural $n \geq 1$ such that A, B are square matrices of size n and $AB = BA = I_n$.

"A is an invertible matrix" iff there exists a B such that B is an inverse of matrix A.

Corollary 1.1.15 (Simple properties of invertible matrices)**.**

(a) A is an inverse of matrix $B \iff B$ is an inverse of matrix A.

(b) Let A be an invertible matrix. Then there exists a unique $n \in \mathbb{N}$ such that A is a square matrix of size n.

(c) Let B be an inverse of matrix A and $n \in \mathbb{N}$ such that A is a square matrix of size n. Then B is also a square matrix of size n.

Lemma 1.1.16 (Uniqueness of inverses)**.** *Let A, L, R be square matrices of size n such that $LA = AR = I_n$. Then $L = R$.*

Hence, if A is an invertible matrix, then there exists a unique matrix B such that B is an inverse of A.

Lemma 1.1.17. *This allows to denote B by A^{-1}. (n is determined due to Lemma1.1.4.)*

Proposition 1.1.18 (Properties of invertible matrices)**.**

(a) Let A be an invertible matrix. Then A^{-1} is also invertible with $(A^{-1})^{-1} = A$.

(b) Let A, B be invertible matrices of size n. Then AB is invertible with the inverse being $B^{-1}A^{-1}$.

Remark 1.1.19. The notations like $A_1 + \cdots + A_k$ or $E_1 \cdots E_k$ are explained in the next chapter. They carry the usual meanings.

Proposition 1.1.20 (Inverses of nilpotent matrices)**.** *Let A be a matrix of size $n \times n$ and $k \geq 1$ such that $A^k = 0_{n\times n}$. Then $I - A$ is invertible with $(I - A)^{-1} = A^{k-1} + \cdots + I_n$.*

Definition 1.1.21. We will denote an $m\times n$ matrix A by $\begin{bmatrix} A_{1,1} & \dots & A_{1,n} \\ \vdots & & \vdots \\ A_{n,1} & \dots & A_{m,n} \end{bmatrix}$.

Lemma 1.1.22 (Inverses for 2×2 matrices)**.** *Let a, b, c, d be scalars. Then*

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = (ad - bc)I_2.$$

Also, $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *is invertible* $\iff ad - bc \neq 0.$

Lemma 1.1.23 (Rows and columns of matrices)**.** *Let $m, n \in \mathbb{N}$, and A be an $m \times n$ matrix, and $1 \leq i_0 \leq m$ and $1 \leq j_0 \leq n$. Then there exist unique matrices X, Y of sizes $1 \times n$ and $m \times n$ such that for all $1 \leq i \leq m$ and for all $1 \leq j \leq n$, we have $X_{1,j} = A_{i_0,j}$ and $Y_{i,1} = A_{i,j_0}$.*

Remark 1.1.24. This allows to denote X and Y by A_{i_0} and $A_{,j_0}$.

Lemma 1.1.25 (Square matrices with a zero row or column is not invertible)**.** *Let A be a square matrix of size n such that there exists a $1 \leq k \leq n$ so that $A_k = 0_{1\times n}$ or $A_{,k} = 0_{n\times 1}$. Then A is not invertible.*

Corollary 1.1.26 (Nonexistence of inverses for non-square matrices)**.** *Let L, A be $n \times m$ and $m \times n$ matrices with $m < n$. Then $LA \neq I_n$.*

Lemma 1.1.27 (Block matrices)**.**

(a) Let A, B be matrices of sizes $m_A \times n$ and $m_B \times n$. Then there exists a unique matrix C of size $(m_A + m_B) \times n$ such that for each $1 \leq i \leq m_A + m_B$, we have $C_i = A_i$ if $1 \leq i \leq m_A$, and $C_i = B_{i-m_A}$ if $m_A + 1 \leq i \leq m_A + m_B$.

(b) Let A', B' be matrices of sizes $m \times n_{A'}$ and $m \times n_{B'}$. Then there exists a unique matrix C' of size $m \times (n_{A'} + n_{B'})$ such that for each $1 \leq j \leq n_{A'} + n_{B'}$, we have $C'_{,j} = A'_{,j}$ if $1 \leq j \leq n_{A'}$, and $C'_{,j} = B_{,j-n_{A'}}$ if $1 + n_{A'} \leq j \leq n_{A'} + n_{B'}$.

Remark 1.1.28. This allows to denote C by $\begin{bmatrix} A \\ B \end{bmatrix}$ and C' by $\begin{bmatrix} A' & B' \end{bmatrix}$.

Corollary 1.1.29 (Block matrices)**.** *Let P, Q, R, S be matrices of sizes $m_1 \times n_1$ and $m_1 \times n_2$ and $m_2 \times n_1$ and $m_2 \times n_2$. Then $\begin{bmatrix} P & Q \end{bmatrix}$ and $\begin{bmatrix} R & S \end{bmatrix}$ are matrices of sizes $m_1 \times (n_1 + n_1)$ and $m_2 \times (n_1 + n_2)$, and $\begin{bmatrix} P \\ R \end{bmatrix}$ and $\begin{bmatrix} Q \\ S \end{bmatrix}$ are matrices of sizes $(m_1 + m_2) \times n_1$ and $(m_1 + m_2) \times n_2$ such that*

$$\begin{bmatrix} \begin{bmatrix} P & Q \end{bmatrix} \\ \begin{bmatrix} R & S \end{bmatrix} \end{bmatrix} = \begin{bmatrix} \begin{bmatrix} P \\ R \end{bmatrix} & \begin{bmatrix} Q \\ S \end{bmatrix} \end{bmatrix}.$$

Remark 1.1.30. This allows to denote the last matrix by $\begin{bmatrix} P & Q \\ R & S \end{bmatrix}$.

Lemma 1.1.31 (Block multiplication)**.**

(a) Let A, B, M be matrices of sizes $m_1 \times n$ and $m_2 \times n$ and $n \times p$. Then $\begin{bmatrix} A \\ B \end{bmatrix}$ and M are matrices of sizes $(m_1 + m_2) \times n$ and $n \times p$, and AM, BM are matrices of sizes $m_1 \times p$ and $m_2 \times p$, and

$$\begin{bmatrix} A \\ B \end{bmatrix} M = \begin{bmatrix} AM \\ BM \end{bmatrix}.$$

(b) Let M, A, B be matrices of sizes $m \times n$ and $n \times p_1$ and $n \times p_2$. Then M and $\begin{bmatrix} A & B \end{bmatrix}$ are matrices of sizes $m \times n$ and $n \times (p_1 + p_2)$, and MA, MB are matrices of sizes $m \times p_1$ and $m \times p_2$, and

$$M \begin{bmatrix} A & B \end{bmatrix} = \begin{bmatrix} MA & MB \end{bmatrix}.$$

(c) Let P, Q, R, S be matrices of sizes $m \times n_1$ and $m \times n_2$ and $n_1 \times p$ and $n_2 \times p$. Then $\begin{bmatrix} P & Q \end{bmatrix}$ and $\begin{bmatrix} R \\ S \end{bmatrix}$ are matrices of sizes $m \times (n_1 + n_2)$ and $(n_1 + n_2) \times p$, and PR, QS are matrices of sizes $m \times p$, and

$$\begin{bmatrix} P & Q \end{bmatrix} \begin{bmatrix} R \\ S \end{bmatrix} = PR + QS.$$

(d) Let P, Q, R, S be matrices of sizes $m_1 \times n$ and $m_2 \times n$ and $n \times p_1$ and $n \times p_2$. Then $\begin{bmatrix} P \\ Q \end{bmatrix}$ and $\begin{bmatrix} R & S \end{bmatrix}$ are matrices of sizes $(m_1 + m_2) \times n$ and

$n \times (p_1 + p_2)$, and PR, PS, QR, QS are matrices of sizes $m_1 \times p_1$ and $m_1 \times p_2$ and $m_2 \times p_1$ and $m_2 \times p_2$, and

$$\begin{bmatrix} P \\ Q \end{bmatrix} \begin{bmatrix} R & S \end{bmatrix} = \begin{bmatrix} PR & PS \\ QR & QS \end{bmatrix}.$$

Corollary 1.1.32 (Multiplication of 2×2 blocks)**.** *Let A, B, C, D be $m_1 \times n_1$ and $m_1 \times n_2$ and $m_2 \times n_1$ and $m_2 \times n_2$ matrices, and P, Q, R, S be $n_1 \times p_1$ and $n_1 \times p_2$ and $n_2 \times p_1$ and $n_2 \times p_2$ matrices. Then $\begin{bmatrix} A & B \\ C & D \end{bmatrix}$ and $\begin{bmatrix} P & Q \\ R & S \end{bmatrix}$ are $(m_1 + m_2) \times (n_1 + n_2)$ and $(n_1 + n_2) \times (p_1 + p_2)$ matrices, and $AP + BR$, $AQ + BS$, $CP + DR$, $CQ + DS$ are $m_1 \times p_1$ and $m_1 \times p_2$ and $m_2 \times p_1$ and $m_2 \times p_2$ matrices, and*

$$\begin{bmatrix} A & B \\ C & D \end{bmatrix} \begin{bmatrix} P & Q \\ R & S \end{bmatrix} = \begin{bmatrix} AP + BR & AQ + BS \\ CP + DR & CQ + DS \end{bmatrix}.$$

Lemma 1.1.33 (Matrix units)**.** *Let $m, n \geq 1$ be naturals and $1 \leq i_0 \leq m$ and $1 \leq j_0 \leq n$. Then there exists a unique matrix A of size $m \times n$ such that for all $1 \leq i \leq m$ and for all $1 \leq j \leq n$, we have $A_{i,j} = 1$ if $i = i_0$ and $j = j_0$ and $A_{i,j} = 0$ otherwise.*

Remark 1.1.34. This allows to denote A by $e_{i,j;m\times n}$.

Lemma 1.1.35 (Multiplication of matrix units)**.** *Let $m, n, p \geq 1$ be naturals and $1 \leq i \leq m$, and $1 \leq j, k \leq n$ and $1 \leq l \leq p$. Then*

$$e_{i,j;m\times n} e_{k,l;n\times p} = \begin{cases} e_{i,l;m\times p}, & j = k \\ 0_{m\times p}, & j \neq k \end{cases}.$$

Lemma 1.1.36 (Multiplication by matrix units)**.** *Let X be a matrix of size $m \times n$.*

(a) Let $l \geq 1$ be natural, and $1 \leq i \leq l$ and $1 \leq j \leq m$. Then for all $1 \leq \mu \leq l$,

$$(e_{i,j;l\times m} X)_\mu = \begin{cases} X_j, & \mu = i \\ 0_{1\times n}, & \mu \neq i \end{cases}.$$

(b) Let $p \geq 1$ be natural, and $1 \leq i \leq n$ and $1 \leq j \leq p$. Then for all $1 \leq \nu \leq p$,

$$(X e_{i,j;n\times p})_{,\nu} = \begin{cases} X_{,i}, & \nu = j \\ 0_{m\times 1}, & \nu \neq j \end{cases}.$$

Definition 1.1.37 (Commutativity of matrices)**.** "A, B are commuting matrices" iff there exist m, n such that A is a matrix of size $m \times n$ and B is a matrix of size $n \times m$ such that $AB = BA$.

Corollary 1.1.38 (Only square matrices commute)**.** *Let A, B be commuting matrices. Then there exists a unique $n \in \mathbb{N}$ such that A, B are square matrices of size n.*

Lemma 1.1.39 (Commutativity of matrix units)**.** *Let $n \geq 1$ be natural and $1 \leq i, j, k, l \leq n$. Then*

$$e_{i,j;n\times n}e_{k,l;n\times n} - e_{k,l;n\times n}e_{i,j;n\times n} = \begin{cases} e_{i,l;n\times n} - e_{k,j;n\times n}, & j = k, l = i \\ e_{i,l;n\times n}, & j = k, l \neq i \\ -e_{k,j;n\times n}, & j \neq k, l = i \\ 0_{n\times n}, & j \neq k, l \neq i \end{cases}.$$

Abbreviation 1.1.40 (Trace)**.** For any square matrix A of size n, we set $\operatorname{trace}(A) := \sum_{i=1}^{n} A_{i,i}$.

Proposition 1.1.41 (Properties of trace)**.** *Let A, B be $n \times n$ matrices. Then*

$$\begin{aligned} \operatorname{trace}(A + B) &= \operatorname{trace}(A) + \operatorname{trace}(B), \\ \operatorname{trace}(AB) &= \operatorname{trace}(BA), \text{ and} \\ \operatorname{trace}(A^t) &= \operatorname{trace}(A). \end{aligned}$$

Corollary 1.1.42. *Let A, B be $n \times n$ matrices. Then $AB - BA \neq I_n$.*

1.2 Row reduction

October 7, 2021

Lemma 1.2.1 (Rows and columns of matrix products)**.** *Let A, B be matrices of sizes $m \times n$ and $n \times p$. Then for all $1 \leq i \leq 1$ and for all $1 \leq j \leq p$, we have $(AB)_i = \sum_{k=1}^{n} A_{i,k} B_k$ and $(AB)_{,j} = \sum_{k=1}^{n} B_{k,j} A_{,k}$.*

Abbreviation 1.2.2 (Elementary matrices)**.** For any $n \geq 1$, and any $1 \leq i, j \leq n$ and any scalar c, we set

$$\mathcal{E}_{\mathbb{F},n;i\to i+cj} := I_n + ce_{i,j;n\times n},$$

$$\begin{aligned}\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j} &:= I_n - e_{i,i;n\times n} - e_{j,j;n\times n} + e_{i,j;n\times n} + e_{j,i;n\times n}, \text{ and}\\ \mathcal{E}_{\mathbb{F},n;i\to ci} &:= I_n + (c-1)e_{i,i;n\times n}.\end{aligned}$$

The above are called "elementary matrices of type (I or II or III) for size n" iff $i \neq j$ and $c \neq 0$.

Remark 1.2.3. Thus $\mathcal{E}_{\mathbb{F},n;i\to i+(-1)i}$ and $\mathcal{E}_{\mathbb{F},n;i\to 0i}$ are not elementary for any i and any n.

Proposition 1.2.4 (Type II in terms of types I and III)**.** *Let $n \geq 1$ and $1 \leq i < j \leq n$. Then $\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j} = \mathcal{E}_{\mathbb{F},n;j\to(-1)j}\,\mathcal{E}_{\mathbb{F},n;i\to i+1j}\,\mathcal{E}_{\mathbb{F},n;j\to j+(-1)i}\,\mathcal{E}_{\mathbb{F},n;i\to i+1j}$.*

Lemma 1.2.5 (Elementary matrices uniquely determine indices and scalars)**.** *Let $n \geq 1$ be natural and $1 \leq i, j, k, l \leq n$ and c, d be scalars. Then*

(a) $\mathcal{E}_{\mathbb{F},n;i\to i+cj} = \mathcal{E}_{\mathbb{F},n;k\to k+dk} \implies (c = d \text{ and } (c \neq 0 \implies i = k \text{ and } j = l))$,
(b) $\mathcal{E}_{\mathbb{F},n;i\to i+cj} = \mathcal{E}_{\mathbb{F},n;k\leftrightarrow l} \implies (c = 0 \text{ and } k = l)$,
(c) $\mathcal{E}_{\mathbb{F},n;i\to i+cj} = \mathcal{E}_{\mathbb{F},n;k\to dk} \implies (c = d-1 \text{ and } (c \neq 0 \implies i = j = k))$,
(d) $\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j} = \mathcal{E}_{\mathbb{F},n;k\leftrightarrow l} \implies ((i = j \iff k = l) \text{ and } (i \neq j \implies \{i, j\} = \{k, l\}))$,
(e) $\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j} = \mathcal{E}_{\mathbb{F},n;k\to ck} \implies (c = 1 \text{ and } i = j)$, *and*
(f) $\mathcal{E}_{\mathbb{F},n;i\to ci} = \mathcal{E}_{\mathbb{F},n;j\to dj} \implies (c = d \text{ and } (c \neq 0 \implies i = j))$.

Example 1.2.6. *Let $n \geq 1$ be natural. Then the sets of elementary matrices of type I, II, III of size n are pairwise disjoint.*

Lemma 1.2.7 (Multiplication by elementary matrices)**.** *Let X be a matrix of size $m \times n$ and c be a scalar. Then*

(a) for all $1 \leq i, j \leq m$,

$$\begin{aligned}(\mathcal{E}_{\mathbb{F},m;i\to i+cj}X)_k &= \begin{cases} X_i + cX_j, & k = i\\ X_k, & k \neq i\end{cases},\\ (\mathcal{E}_{\mathbb{F},m;i\leftrightarrow j}X)_k &= \begin{cases} X_j, & k = i\\ X_i, & k = j\\ X_k, & k \neq i, j\end{cases},\\ (\mathcal{E}_{\mathbb{F},m;i\to ci}X)_k &= \begin{cases} cX_i, & k = i\\ X_k, & k \neq i\end{cases}, \text{ and}\end{aligned}$$

(b) for all $1 \leq i, j \leq n$,

$$(X\mathcal{E}_{\mathbb{F},n;i\to i+cj})_{,k} = \begin{cases} X_{,j} + cX_{,i}, & k = j\\ X_{,k}, & k \neq j\end{cases},$$

$$(X\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j})_{,k} = \begin{cases} X_{,j}, & k=i \\ X_{,i}, & k=j \\ X_{,k}, & k\neq i,j \end{cases}, \text{ and}$$

$$(X\mathcal{E}_{\mathbb{F},n;i\to ci})_{,k} = \begin{cases} cX_{,i}, & k=i \\ X_{,k}, & k\neq i \end{cases}.$$

Lemma 1.2.8 (Elementary matrices are invertible)**.** *Let $n \geq 1$ be natural, and $1 \leq i, j \leq n$ and c be a scalar such that $i \neq j$ and $c \neq 0$. Then*

(a) $\mathcal{E}_{\mathbb{F},n;i\to i+cj}$ *is invertible with the inverse being* $\mathcal{E}_{\mathbb{F},n;i\to i+(-c)j}$*,*
(b) $\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j}$ *is invertible with itself being the inverse, and*
(c) $\mathcal{E}_{\mathbb{F},n;i\to ci}$ *is invertible with inverse being* $\mathcal{E}_{\mathbb{F},n;i\to(1/c)i}$*.*

October 14, 2021

Lemma 1.2.9 (Commutativity of elementary matrices)**.** *Let $n \geq 1$ be natural, and $1 \leq i, j, k, l \leq n$ and c, d be scalars. Then*

(a) $\mathcal{E}_{\mathbb{F},n;i\to i+cj}$ *and* $\mathcal{E}_{\mathbb{F},n;k\to k+dl}$ *commute* $\iff$ *one of these holds:*
  - *(i)* $c = 0$,
  - *(ii)* $d = 0$,
  - *(iii)* $i = j = k = l$,
  - *(iv)* $i \neq l$ *and* $j \neq k$;

(b) $\mathcal{E}_{\mathbb{F},n;i\to i+cj}$ *and* $\mathcal{E}_{\mathbb{F},n;k\leftrightarrow l}$ *commute* $\iff$ *one of these holds:*
  - *(i)* $c = 0$
  - *(ii)* $(j = k$ *or* $k = i)$ *and* $(j = l$ *or* $l = i)$,
  - *(iii)* $j \neq k$ *and* $k \neq i$ *and* $j \neq l$ *and* $l \neq i$;

(c) $\mathcal{E}_{\mathbb{F},n;i\to i+cj}$ *and* $\mathcal{E}_{\mathbb{F},n;k\to dk}$ *commute* $\iff$ *one of these holds:*
  - *(i)* $c = 0$,
  - *(ii)* $d = 1$,
  - *(iii)* $i = j = k$,
  - *(iv)* $j \neq k$ *and* $k \neq i$;

(d) $\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j}$ *and* $\mathcal{E}_{\mathbb{F},n;k\leftrightarrow l}$ *commute* $\iff$ *one of these holds:*
  - *(i)* $i = j$,
  - *(ii)* $k = l$,
  - *(iii)* $i \neq j$ *and* $k \neq l$ *and* $\{i, j\} \cap \{k, l\}$ *is not a singleton;*

(e) $\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j}$ *and* $\mathcal{E}_{\mathbb{F},n;k\to ck}$ *commute* $\iff$ *one of these holds:*
  - *(i)* $c = 1$,

(ii) $i = j = k$,
(iii) $i \neq k$ *and* $k \neq j$;

(f) $\mathcal{E}_{\mathbb{F},n;i\to ci}$ *and* $\mathcal{E}_{\mathbb{F},n;j\to dj}$ *commute.*

October 16, 2021

Definition 1.2.10 (Pivots of a matrix)**.** "(i, j) is a pivot of an $m \times n$ matrix A" iff A is a matrix of size $m \times n$ and $1 \leq i \leq m$ and $A_i \neq 0_{1\times n}$ (so that the set $S \neq \emptyset$) and $j = \min(S)$, where $S := \{1 \leq j \leq n : A_{i,j} \neq 0\}$.

Definition 1.2.11 (Row echelon matrices)**.** "A is an $m \times n$ row echelon matrix" iff A is an $m \times n$ matrix such that the following hold:

(a) For each $1 \leq i < m$, we have $(A_i = 0_{1\times n} \implies A_{i+1} = 0_{1\times n})$.
(b) For each $1 \leq i \leq m$ and for each $1 \leq j \leq n$, we have ((i, j) is a pivot of $A \implies A_{i,j} = 1$).
(c) For each $1 \leq i < m$ and for all $1 \leq j, j' \leq n$, we have ((i, j) and $(i + 1, j')$ are pivots of $A \implies j < j'$).
(d) For all $1 \leq i' < i \leq m$ and for all $1 \leq j \leq n$, we have ((i, j) is a pivot of $A \implies A_{i',j} = 0$).

"A is a row echelon matrix" iff there exist m, n such that A is an $m \times n$ row echelon matrix.

Lemma 1.2.12. *Let* $R \subseteq \mathbb{N} \times \mathbb{N}$ *such that for each* $i, j, j' \in \mathbb{N}$,

(a) $(i, j), (i + 1, j') \in R \implies j < j'$, *and*
(b) $i + 1 \in \operatorname{dom} R \implies i \in \operatorname{dom} R$.

Then for all $i, i', j, j' \in \mathbb{N}$,

(a) $i \in \operatorname{dom} R$ *and* $i' \leq i \implies i' \in \operatorname{dom} R$, *and*
(b) $(i, j), (i', j') \in R$ *and* $i < i' \implies j < j'$.

Lemma 1.2.13 (Pivots of row echelons)**.** *Let* A *be an* $m \times n$ *row echelon matrix and* (i_0, j_0) *be a pivot of* A*. Then*

(a) $i_0 \leq j_0$, *and*
(b) $A_{,j_0} = e_{i_0,1;m\times 1}$.

Lemma 1.2.14 (Preserving row echelon-ness)**.**

(a) Let A *be an* $m \times n$ *row echelon matrix. Then* $\begin{bmatrix} 0_{m,1} & A \end{bmatrix}$ *and* $\begin{bmatrix} A & 0_{m,1} \end{bmatrix}$ *are row echelon matrices.*

(b) *Let A, B be matrices of sizes $m \times n$ and $1 \times n$ such that for all $1 \leq i \leq m$ and for all $1 \leq j \leq n$, if (i, j) is a pivot for A, then $B_{1,j} = 0$. Then* $\begin{bmatrix} [1] & B \\ 0_{m,1} & A \end{bmatrix}$ *is a row echelon matrix.*

(c) *Let A, B be matrices of sizes $m_1 \times n$ and $m_2 \times n$ such that* $\begin{bmatrix} A \\ B \end{bmatrix}$ *is a row echelon matrix. Then A, B are each row echelon matrices.*

(d) *Let A, B be matrices of sizes $m \times n$ and $n \times 1$ such that $C := \begin{bmatrix} A & B \end{bmatrix}$ is a row echelon matrix. Then A is a row-echelon matrix.*

Lemma 1.2.15 (Square row echelons)**.** *Let A be a square row echelon matrix of size n. Then $A = I_n$ or $A_n = 0_{1\times n}$.*

Remark 1.2.16. See Proposition 2.1.9 for the precise meaning of $E_1 \cdots E_k$.

Definition 1.2.17 (Row equivalence)**.** "A, B are row equivalent matrices" iff there exist m, n such that A, B are matrices of size $m \times n$ and there exists a $k \geq 1$ and elementary matrices $E_1, \ldots, E_k$ each of size m such that $A = E_1 \cdots E_k B$.

Example 1.2.18. *Row equivalence is an equivalence relation on the set of matrices on $\mathbb{F}$.*

Lemma 1.2.19 (Preserving row equivalence)**.**

(a) *Let A, B be $m \times n_1$ and $m \times n_2$ matrices such that A and A' are row equivalent. Then $\begin{bmatrix} A & 0_{m\times 1} \end{bmatrix}$ and $\begin{bmatrix} A' & 0_{m\times 1} \end{bmatrix}$ are row equivalent.*

(b) *Let A, A' be $m \times n_1$ matrices and B, B' be $m \times n_2$ matrices such that $\begin{bmatrix} A & B \end{bmatrix}$ and $\begin{bmatrix} A' & B' \end{bmatrix}$ are row equivalent. Then A, A' and B, B' are row equivalent.*

Corollary 1.2.20 (Inverses of matrices using row reduction)**.** *Let A, B be square matrices of size n such that $\begin{bmatrix} A & I_n \end{bmatrix}$ is row equivalent to $\begin{bmatrix} I_n & B \end{bmatrix}$. Then $AB = BA = I_n$.*

Theorem 1.2.21 (Row reduction is possible)**.** *Let A be a matrix. Then there exists a row echelon matrix B such that A is equivalent to B.*

Lemma 1.2.22 (Equivalent systems of equations)**.** *Let A, A' be matrices of size $m \times n$, and B, B' be matrices of size $m \times 1$ and X be a matrix of size $n \times 1$ such that $\begin{bmatrix} A & B \end{bmatrix}$ and $\begin{bmatrix} A' & B' \end{bmatrix}$ are row equivalent. Then $AX = B \iff A'X = B'$.*

Proposition 1.2.23 (Solving linear systems using row echelons)**.** *Let A, B be matrices of sizes $m \times n$ and $m \times 1$ such that $M := \begin{bmatrix} A & B \end{bmatrix}$ is a row echelon matrix. We have the following cases:*

(a) *$(i, n+1)$ is a pivot of M for some i:*
Then $AX \neq B$ for any matrix X of size $n \times 1$.

(b) *$(i, n+1)$ is not a pivot of M for any i:*
Set $K := \{1 \leq i \leq m : A_i \neq 0_{1\times n}\}$ and $L := \{1 \leq j \leq n : (i,j)$ is not a pivot of A for any $i\}$. Then there exists a unique function $s\colon K \to \{1, \ldots, n\}$ such that for each $i \in K$, setting $X := \{1 \leq j \leq n : A_{i,j} \neq 0\}$, we have $X \neq \emptyset$ and $s(i) = \min(X)$. Further, for any such function s and any matrix X of size $n \times 1$,

(i) $L \cap s[K] = \emptyset$,
(ii) $L \cup s[K] = \{1, \ldots, n\}$, *and*
(iii) $AX = B \iff X_{s(i),1} + \sum_{j \in L, j > s(i)} A_{i,j} X_{j,1} = B'_{i,1}$ *for each* $i \in K$.

Remark 1.2.24. We'll write $m \times n$ matrix" instead of "matrix of size $m \times n$" from now on.

Corollary 1.2.25 (More variables than equations)**.** *Let $m < n$ be naturals and A be an $m \times n$ matrix. Then there exists an $n \times 1$ matrix X such that $X \neq 0_{n\times 1}$ and $AX = 0_{m\times n}$.*

October 17, 2021

Theorem 1.2.26 (Square matrices)**.** *Let A be a square matrix of size n. Then the following are equivalent:*

(a) *A is row equivalent to I_n.*
(b) *There exists a $k \geq 1$ and elementary matrices $E_1, \ldots, E_k$ each of size n such that $A = E_1 \cdots E_k$.*
(c) *A is invertible.*

Proposition 1.2.27 (A weaker condition for invertibility)**.** *Let A, B be square matrices of size n each such that $AB = I_n$. Then $BA = I_n$.*

Corollary 1.2.28. *Let A, B be $n \times n$ matrices such that AB is invertible. Then A and B are invertible.*

Theorem 1.2.29 (Square systems)**.** *Let A be a square matrix of size n. Then the following are equivalent:*

(a) *A is invertible.*

(b) *For each* $n \times 1$ *matrix* B*, there exists a unique* $n \times 1$ *matrix* X *such that* $AX = B$.
(c) *For each* $n \times 1$ *matrix* X*, if* $AX = 0_{n\times 1}$*, then* $X = 0_{n\times 1}$.

Proposition 1.2.30 (Left invertible matrices)**.** *Let* A *be an* $m \times n$ *matrix such that there exists an* $n \times m$ *matrix* L *so that* $LA = I_n$*. Let* B *be an* $m \times 1$ *matrix. Then*

(a) $m \geq n$*, and*
(b) $(AL)B = B \iff B = AX$ *for some* $n \times 1$ *matrix* X.

$m \geq n$.

Proposition 1.2.31 (Invertibility of $I - AB$)**.** *Let* A*,* B *be* $m \times n$ *and* $n \times m$ *matrices such that* $I_m - AB$ *is invertible. Then* $I_n - BA$ *is invertible with* $(I - BA)^{-1} = I + B(I - AB)^{-1}A$.

1.3 The matrix transpose

October 17, 2021

Lemma 1.3.1 (Transposes)**.** *Let* A *be a matrix. Then there exists a unique matrix* B *such that there exist* $m, n \in \mathbb{N}$ *so that* A*,* B *are* $m \times n$ *and* $n \times m$ *matrices such that for all* $1 \leq i \leq m$ *and* $1 \leq j \leq n$*, we have* $A_{i,j} = B_{j,i}$.

Remark 1.3.2. This allows to denote B by A^t.

Lemma 1.3.3 (Operations with transpose)**.** *Let* A*,* B *be* $m \times n$ *matrices, and* C *be an* $n \times p$ *matrix, and* λ *be a scalar. Then* A^t*,* B^t *are* $n \times p$ *matrices, and* C^t *is a* $p \times n$ *matrix, and*

$$\begin{aligned}(A+B)^t &= A^t + B^t,\\ (AC)^t &= C^t A^t,\\ (\lambda A)^t &= \lambda A^t, \text{ and}\\ (A^t)^t &= A.\end{aligned}$$

Lemma 1.3.4 (Some special transposes)**.**

(a) *Let* $m, n \in \mathbb{N}$*, and* $1 \leq i \leq m$ *and* $1 \leq j \leq n$*. Then* $(e_{i,j;,m\times n})^t = e_{j,i;n\times m}$.
(b) *Let* $n \geq 1$ *be natural. Then* $(I_n)^t = I_n$.

(c) Let A be an $m \times n$ matrix. Then A^t is an $n \times m$ matrix and

(i) $(A^t)_k = (A_{,k})^t$ for each $1 \leq k \leq n$, and

(ii) $(A^t)_{,l} = (A_l)^t$ for each $1 \leq l \leq m$.

Lemma 1.3.5 (Inverses of transposes)**.** *Let A be an invertible matrix. Then A^t is also invertible with $(A^t)^{-1} = (A^{-1})^t$.*

Lemma 1.3.6 (Transposes of elementary matrices)**.** *Let $n \geq 1$ be natural, and $1 \leq i, j \leq n$ and c be a scalar. Then*

$$\begin{aligned} (\mathcal{E}_{\mathbb{F},n;i\to i+cj})^t &= \mathcal{E}_{\mathbb{F},n;j\to j+ci}, \\ (\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j})^t &= \mathcal{E}_{\mathbb{F},n;i\leftrightarrow j}, \text{ and} \\ (\mathcal{E}_{\mathbb{F},n;i\to ci})^t &= \mathcal{E}_{\mathbb{F},n;i\to ci}. \end{aligned}$$

1.4 Determinants

October 18, 2021

Lemma 1.4.1 (Submatrices)**.** *Let A be an $m \times n$ matrix, and $1 \leq i_0 \leq m$ and $1 \leq j_0 \leq n$ such that $m, n \geq 2$. Then $m-1, n-1 \geq 1$ and there exists a unique $(m-1) \times (n-1)$ matrix B such that for all $1 \leq i \leq m-1$ and $1 \leq i \leq n-1$,*

$$B_{i,j} = \begin{cases} A_{i,j}, & i < i_0, j < j_0 \\ A_{i,j+1}, & i < i_0, j \geq j_0 \\ A_{i+1,j}, & i \geq i_0, j < j_0 \\ A_{i+1,j+1}, & i \geq i_0, j \geq j_0 \end{cases}.$$

Remark 1.4.2. This (along with Lemma 1.1.4) allows to denote B by $A_{\langle i_0, j_0\rangle}$.

Lemma 1.4.3 (Determinant function)**.** *Then there exists a unique function $\mathcal{F}$ on $\bigcup_{n\geq 1} \mathfrak{F}^{\mathrm{Mat}(n,n;\mathbb{F})}$ such that for all $f \in \bigcup_{n\geq 1} \mathfrak{F}^{\mathrm{Mat}(n,n;\mathbb{F})}$, there exists a $k \geq 1$ such that $f\colon \mathrm{Mat}(k,k;\mathbb{F}) \to \mathfrak{F}$ and $\mathcal{F}(f)\colon \mathrm{Mat}(k+1,k+1;\mathbb{F}) \to \mathfrak{F}$ so that for all $(k+1) \times (k+1)$ matrices A, we have that for all $1 \leq \nu \leq k+1$, we have that $A_{\langle \nu,1\rangle}$ is a $k \times k$ matrix, and*

$$(\mathcal{F}(f))(A) = \sum_{\nu=1}^{k+1} (-1)^{\nu+1} A_{\nu,1} f(A_{\langle \nu,1\rangle}).$$

Hence, there exists a unique function $\mathrm{Det}\colon \mathbb{N} \setminus \{0\} \to \bigcup_{n\geq 1} \mathfrak{F}^{\mathrm{Mat}(m,n;\mathbb{F})}$ such that *(a)* $\mathrm{Det}_1 \colon \mathrm{Mat}(1,1;\mathbb{F}) \to \mathfrak{F}$ *such that* $\mathrm{Det}_1(A) = A_{1,1}$ *for all* 1×1 *matrices* A*, and*

(b) for each $n \geq 1$*, we have that* $\mathrm{Det}_{n+1} = \mathcal{F}(\mathrm{Det}_n)$*.*

Hence, for any square matrix B*, there exists a unique* $x \in \mathfrak{F}$ *such that there exists an* $n \geq 1$ *so that* B *is an* $n \times n$ *matrix and* $x = \mathrm{Det}_n(B)$*.*

Remark 1.4.4. This allows to denote x by $\det(B)$.

Corollary 1.4.5 (Determinant of I_n)**.** *Let* $n \geq 1$*. Then* $\det(I_n) = 1$*.*

October 19, 2021

Definition 1.4.6 (Matrices differing in only one row)**.** "A and B are $m \times n$ matrices differing in only k-th row" iff A, B are $m \times n$ matrices, and $1 \leq k \leq m$ and for all $1 \leq i \leq m$, if $i \neq k$, then $A_i = B_i$.

Definition 1.4.7 (Matrices differing in only one column)**.** "A and B are $m \times n$ matrices differing in only k-th column" iff A, B are $m \times n$ matrices, and $1 \leq k \leq n$ and for all $1 \leq j \leq n$, if $j \neq k$, then $A_{,j} = B_{,j}$.

Lemma 1.4.8 (k-th row sum)**.** *Let* A*,* B *be* $m \times n$ *matrices differing in* k*-th row. Then there exists a unique* $m \times n$ *matrix* C *such that for each* $1 \leq i \leq m$*, we have* $C_i = A_i = B_i$ *if* $i \neq k$ *and* $C_i = A_i + B_i$ *if* $i = k$*.*

Remark 1.4.9. This (and Lemma 1.1.4) allow to denote C by $A +_k B$.

Lemma 1.4.10 (k-th column sum)**.** *Let* A*,* B *be* $m \times n$ *matrices differing only in* k*-th column. Then there exists a unique matrix* C *such that for each* $1 \leq j \leq n$*, we have* $C_{,j} = A_{,j} = B_{,j}$ *if* $j \neq k$ *and* $C_{,j} = A_{,j} + B_{,j}$ *if* $j = k$*.*

Remark 1.4.11. This (and Lemma 1.1.4) allow to denote C by $A +_{,k} B$.

Lemma 1.4.12. *Let* A*,* B *be* $m \times n$ *matrices differing only in* k*-th column. Then* A^t*,* B^t *are* $n \times m$ *matrices differing only in* k*-th row, and* $(A +_{,k} B)^t = A^t +_k B^t$*.*

Definition 1.4.13 (Determinant-like functions)**.** "δ is a determinant-like function on $n \times n$ matrices" iff $\delta \colon \mathrm{Mat}(n,n;\mathbb{F}) \to \mathfrak{F}$ such that the following hold:

(a) $\delta(I_n) = 1$.

(b) (i) For any $n \times n$ matrix A, for any scalar c and for any $1 \leq i \leq n$, we have that $\delta(\mathcal{E}_{\mathbb{F},n;i\to ci}A) = c\delta(A)$.

(ii) For any $n \times n$ matrices A, B differing in only i-th row, $\delta(A +_i B) = \delta(A) + \delta(B)$.

(c) For any $n \times n$ matrix A, if there exists a $1 \le i < n$ such that $A_i = A_{i+1}$, then $\delta(A) = 0$.

Lemma 1.4.14. *Let A, B be $m \times n$ matrices, and $1 \le i, j \le m$, and c be a scalar such that for each $1 \le k \le m$, we have $B_k = A_k$ if $k \neq i$ and $B_k = A_j$ if $k = i$. Then A and $\mathcal{E}_{\mathbb{F},n;i\to ci}B$ differ only in i-th rows and we have $\mathcal{E}_{\mathbb{F},n;i\to i+cj}A = A +_i \mathcal{E}_{\mathbb{F},n;i\to ci}B$.*

Lemma 1.4.15. *Let δ be a determinant-like function for $n \times n$ matrices, and A be an $n \times n$ matrix, and $1 \le i < n$, and $1 < j \le n$, and c be a scalar. Then*

(a) $\delta(\mathcal{E}_{\mathbb{F},n;i\to i+c(i+1)}A) = \delta(\mathcal{E}_{\mathbb{F},n;j\to j+c(j-1)}A) = \delta(A)$, and

(b) $\delta(\mathcal{E}_{\mathbb{F},n;i\leftrightarrow i+1}A) = \delta(\mathcal{E}_{\mathbb{F},n;j\leftrightarrow j-1}A) = -\delta(A)$.

Lemma 1.4.16. *Let δ be a determinant-like function on $n \times n$ matrices, and A be an $m \times n$ matrix and $1 \le i < j \le n$ such that $A_i = A_j$. Then*

(a) there exists a $k \ge 1$, and matrices $E_1, \ldots, E_k$, and a $1 \le i_0 < m$ such that for each $1 \le l \le k$, there exists a $1 \le a < m$ so that $E_l = \mathcal{E}_{\mathbb{F},n;a\leftrightarrow a+1}$, and $(E_1 \cdots E_k A)_{i_0} = (E_1 \cdots E_k A)_{i_0+1}$, and

(b) $m = n \implies \delta(A) = 0$.

Theorem 1.4.17 (Properties of determinant-like functions)**.** *Let δ be a determinant-like function on $n \times n$ matrices, and A be an $n \times n$ matrix, and c be a scalar, and $1 \le i, j \le n$ such that $i \neq j$. Then*

$$\begin{aligned}
&\delta(\mathcal{E}_{\mathbb{F},n;i\to i+cj}A) = \delta(A),\\
&\delta(\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j}A) \quad = -\delta(A),\\
&\delta(\mathcal{E}_{\mathbb{F},n;i\to ci}A) \quad = c\delta(A),\\
&A_i = 0_{1\times n} \qquad \implies \delta(A) = 0, \text{ and}\\
&A_i = cA_j \qquad \implies \delta(A) = 0.
\end{aligned}$$

Corollary 1.4.18 (Determinants of elementary matrices)**.** *Let δ be a determinant-like function on $n \times n$ matrices, A be an $n \times n$ matrix, and E be an elementary matrix of size n, and c be a scalar and $1 \le i, j \le n$ such that $i \neq j$. Then*

$$\begin{aligned}
&\delta(\mathcal{E}_{\mathbb{F},n;i\to i+cj}) = 1,\\
&\delta(\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j}) \quad = -1,
\end{aligned}$$

$$\begin{aligned}\delta(\mathcal{E}_{\mathbb{F},n;i\to ci}) &= c, \text{ and}\\ \delta(EA) &= \delta(E)\delta(A).\end{aligned}$$

Theorem 1.4.19 (Determinants are multiplicative)**.** *Let δ be a determinant-like function on $n \times n$ matrices and A, B be $n \times n$ matrices. Then $\delta(AB) = \delta(A)\delta(B)$.*

Theorem 1.4.20 (Uniqueness of determinant)**.** *Let $n \geq 1$. Then* Det_n *is the only determinant-like function on $n \times n$ matrices.*

Proposition 1.4.21 (Further properties of determinants)**.** *Let A be a square matrix of size n. Then the following hold:*

(a) *(i)* *A is invertible* $\iff \det(A) \neq 0$.
(ii) *A is invertible* $\implies \det(A) \neq 0$ *and* $\det(A^{-1}) = (\det(A))^{-1}$.

(b) *A^t is a square matrix of size n and* $\det(A^t) = \det(A)$.

(c) *For any scalar c and for any $1 \leq i, j \leq n$ such that $i \neq j$,*
(i) *(1)* $\det(A\mathcal{E}_{\mathbb{F},n;i\to ci}) = c\det(A)$,
(2) *for any square matrix B of size n differing from A only in the i-th column,* $\det(A +_{,i} B) = \det(A) + \det(B)$,
(ii) *(1)* $\det(A\mathcal{E}_{\mathbb{F},n;i\to i+cj}) = \det(A)$,
(2) $\det(A\mathcal{E}_{\mathbb{F},n;i\leftrightarrow j}) = -\det(A)$,
(3) $\det(A\mathcal{E}_{\mathbb{F},n;i\to ci}) = c\det(A)$,
(4) $A_{,i} = 0_{n\times 1} \implies \det(A) = 0$, *and*
(5) $A_{,i} = cA_{,j} \implies \det(A) = 0$.

Proposition 1.4.22 (Determinants of tridiagonal matrices)**.** *Let a, b, c be scalars and for all $n \geq 1$, let A_n be an $n \times n$ matrix such that for all $1 \leq i, j \leq n$,*

$$A_{i,j} = \begin{cases} a, & i = j \\ b, & j = i + 1 \\ c, & i = j + 1 \end{cases}.$$

Then for all $n \geq 1$, $\det(A_{n+1}) = a\det(A_{n+1}) - bc\det(A_n)$.

Proposition 1.4.23 (Determinants of block diagonals)**.** *Let A, B, D be $m \times m$ and $m \times n$ and $n \times n$ matrices. Then* $\det\left(\begin{bmatrix} A & B \\ 0_{n\times m} & D \end{bmatrix}\right) = \det(A)\det(D)$.

Corollary 1.4.24. *Let A, B, C, D be $n \times n$ matrices such that A is invertible and $AC = CA$. Then* $\det\left(\begin{bmatrix} A & B \\ C & D \end{bmatrix}\right) = \det(AD - CB)$.

Proposition 1.4.25 (Vandermonde determinant)**.** *Let $n \in \mathbb{N}$, and $t_0, \ldots, t_n$ be scalars and A be the $(n+1) \times (n+1)$ matrix such that $A_{i,j} = (t_{j-1})^{i-1}$ for all $1 \leq i, j \leq n+1$. Then $\det(A) = \prod_{k=0}^{n-1} \big(\prod_{l=k+1}^{n} (t_l - t_k) \big)$.*

Remark 1.4.26. We write "t_i's are distinct" to abbreviate that t is injective.

Corollary 1.4.27. *Let $n \in \mathbb{N}$ and $t_0, \ldots, t_n, b_0, \ldots, b_n$ be scalars such that t_i's are distinct. Then there exist unique $a_0, \ldots, a_n$ such that $a_0 + \ldots + a_n (t_i)^n = b_i$ for all $0 \leq i \leq n$.*

Remark 1.4.28. From this, it follows that a polynomial of degree n can not have $n+1$ distinct roots. That is, it has at most n distinct roots.

1.5 Permutations

October 22, 2021

Definition 1.5.1 (Permutations)**.** "p is a permutation on S" iff $p \colon S \to S$ and p is a bijection.

Lemma 1.5.2 (Permuting entries by p permutes indices by p^{-1})**.** *Let $n \geq 1$, and p be a permutation on $\{1, \ldots, n\}$ and X, Y be $n \times 1$ matrices such that $X_{i,1} = Y_{p(i),1}$ for all $1 \leq i \leq n$. Then for all $1 \leq i \leq n$, we have $Y_{i,1} = X_{p^{-1}(i),1}$.*

Lemma 1.5.3 (Permutation matrices)**.** *Let $n \geq 1$ and p be a permutation on $\{1, \ldots, n\}$. Then there exists a unique $n \times n$ matrix P such that for any $n \times 1$ matrix X, we have $X_{i,1} = (PX)_{p(i),1}$ for all $1 \leq i \leq n$.*

Remark 1.5.4. This allows to denote P by $\mathrm{PerMat}(p)$. (Functions uniquely determine their domains.)

Definition 1.5.5 (Permutation matrices)**.** "P is the permutation matrix for p on $\{1, \ldots, n\}$" iff $n \geq 1$, and p is a permutation on $\{1, \ldots, n\}$ and $P = \mathrm{PerMat}(p)$.

"P is an $n \times n$ permutation matrix" iff there exists a p such that P is the permutation matrix for p on $\{1, \ldots, n\}$.

Lemma 1.5.6 (Rows and columns of permutation matrices)**.** *Let P be the permutation matrix for p on $\{1, \ldots, n\}$. Then $P_{,k} = e_{p(k),1;,n \times 1}$ and $P_k = e_{1,p^{-1}(k);1 \times n}$ for all $1 \leq k \leq n$.*

Corollary 1.5.7 (Permutation matrix for identity)**.** *Let* $n \geq 1$*. Then* I_n *is the permutation matrix for* $\iota_{\{1,\dots,n\}\to\{1,\dots,n\}}$*.*

Corollary 1.5.8 (Permutation matrices permuting rows and columns)**.** *Let* P *be the permutation matrix for* p *on* $\{1,\dots,n\}$ *and* A*,* B *be* $n \times m$ *and* $m \times n$ *matrices. Then for all* $1 \leq i \leq n$*, we have* $(PA)_{p(i)} = A_i$ *and* $(BP)_{,p(i)} = B_{,i}$*.*

Proposition 1.5.9 (Characterizing permutation matrices)**.** *Let* P *be an* $n \times n$ *matrix. Then* P *is an* $n \times n$ *permutation matrix* $\iff$ *for each* $1 \leq k \leq n$*, there exist* $1 \leq i, j \leq n$ *such that* $P_k = e_{1,j;1\times n}$ *and* $P_{,k} = e_{i,1;n\times 1}$*.*

Lemma 1.5.10. *Let* $n \geq 1$ *and* P *be the permutation matrix for* p *on* $\{1,\dots,n+1\}$*. Then* $P_{\langle p(1),1\rangle}$ *is an* $n \times n$ *permutation matrix.*

Proposition 1.5.11 (Dtereminants of permutation matrices)**.** *Let* P *be an* $n \times n$ *permutation matrix. Then* $\det(P) = 1$ *or* $\det(P) = -1$*.*

Proposition 1.5.12 (Matrices of permutation compositions)**.** *Let* P*,* Q *be the permutation matrices for* p*,* q *each on* $\{1,\dots,n\}$*. Then* PQ *is the permutation matrix for* $p \circ q$ *on* $\{1,\dots,n\}$*.*

Lemma 1.5.13 (Inverses of permutation matrices)**.** *Let* P *be the permutation matrix for* p *on* $\{1,\dots,n\}$*. Then*

(a) P *is invertible,*
(b) $P^{-1} = P^t$*, and*
(c) P^{-1} *is the permutation matrix for* p^{-1} *on* $\{1,\dots,n\}$*.*

Lemma 1.5.14 (Transpositions)**.** *Let* $n \in \mathbb{N}$ *and* $1 \leq i, j \leq n$*. Then there exists a unique function* $f\colon \{1,\dots,n\} \to \{1,\dots,n\}$ *such that for all* $1 \leq k \leq n$*,*

$$f(k) = \begin{cases} j, & k = i \\ i, & k = j \\ k, & k \neq i, j \end{cases}.$$

Remark 1.5.15. This allows to denote f by $\tau_{n;i\leftrightarrow j}$.

Definition 1.5.16 ((Proper) transpositions)**.** "T is a (proper) transposition on $\{1,\dots,n\}$" iff $n \in \mathbb{N}$ and there exist $1 \leq i, j \leq n$ such that ($i \neq j$ and) $T = \tau_{n;i\leftrightarrow j}$.

Lemma 1.5.17 (Transpositions are permutations)**.** *Let $n \in \mathbb{N}$ and T be a transposition on $\{1, \dots, n\}$. Then T is a permutation on $\{1, \dots, n\}$.*

Lemma 1.5.18 (Permutation matrices for transpositions)**.** *Let $n \geq 1$ and $1 \leq i, j \leq n$. Then* $\operatorname{PerMat}(\tau_{n;i\leftrightarrow j}) = \mathcal{E}_{\mathbb{F},n;i\leftrightarrow j}$.

Remark 1.5.19. We don't define empty function composition.

Proposition 1.5.20 (Permutations as transposition compositions)**.** *Let $n \in \mathbb{N}$ and p be a permutation on $\{1, \dots, n\}$. Then there exists a $k \geq 1$ and transpositions $T_1, \dots, T_k$ on $\{1, \dots, n\}$ such that $p = T_1 \circ \cdots \circ T_k$.*

Abbreviation 1.5.21 (Signs of permutations)**.** For any $n \geq 1$ and for any permutation p on $\{1, \dots, n\}$, we set $\operatorname{sign}(p) := \det(\operatorname{PerMat}(p))$.

Proposition 1.5.22 (Odd and even permutations)**.** *Let $n \geq 1$, and $k \geq 1$ and $T_1, \dots, T_k$ be proper transpositions on $\{1, \dots, n\}$. Set $p := T_1 \circ \cdots \circ T_k$. Then p is a permutation on $\{1, \dots, n\}$, and*

(a) k *is even* $\implies \operatorname{sign}(p) = 1$, *and*
(b) k *is odd* $\implies \operatorname{sign}(p) = -1$.

Lemma 1.5.23 (Cycles)**.** *Let $n, k \in \mathbb{N}$ such that $k \leq n$. Then there exists a unique function $p\colon \{1, \dots, n\} \to \{1, \dots, n\}$ such that for each $1 \leq i \leq n$,*

$$p(i) = \begin{cases} i+1, & i < k \\ 1, & i = k \\ i, & i > k \end{cases}.$$

Remark 1.5.24. This allows to denote p by $(1 \cdots k)_n$.

Corollary 1.5.25. *Let $n, k \in \mathbb{N}$ such that $k \leq n$. Set $p := (1 \cdots k)_n$. Then*

(a) $p \in \mathrm{S}_n$, *and*
(b) $k = 0$ *or* $k = 1 \implies p = \iota_{\{1,\dots,n\}\to\{1,\dots,n\}}$.

Lemma 1.5.26 (Sign of cycles)**.** *Let $1 < k \leq n$ and set $p := (1 \cdots k)_n$. Then*

(a) $p = \tau_{n;1\leftrightarrow 2} \circ \cdots \circ \tau_{n;k-1\leftrightarrow k}$, *and*
(b) $\operatorname{sign}(p) = (-1)^{k-1}$.

1.6 Other formulas for the determinant

October 24, 2021

Proposition 1.6.1 (Expanding det on arbitrary rows and columns)**.** *Let $n \geq 1$, and A be an $(n+1) \times (n+1)$ matrix and $1 \leq i_0, j_0 \leq n+1$. Then*

$$\begin{aligned}\det(A) &= \sum_{i=1}^{n+1} (-1)^{i+j_0} A_{i,j_0} \det(A_{\langle i,j_0 \rangle}) \\ &= \sum_{j=1}^{n+1} (-1)^{i_0+j} A_{i_0,j} \det(A_{\langle i_0,j \rangle}).\end{aligned}$$

Lemma 1.6.2 (Embedding permutations doesn't change sign)**.** *Let $n \geq 1$, and p be a permutation on $\{1, \ldots, n\}$ and $q \colon \{1, \ldots, n+1\} \to \{1, \ldots, n+1\}$ such that for each $1 \leq i \leq n+1$,*

$$q(i) = \begin{cases} p(i), & i \leq n \\ n+1, & i = n+1 \end{cases}.$$

Then q is a permutation on $\{1, \ldots, n+1\}$ and $\operatorname{sign}(p) = \operatorname{sign}(q)$.

Lemma 1.6.3. *Let $n \geq 1$, and p be a permutation on $\{1, \ldots, n\}$ and $q \colon \{1, \ldots, n+1\} \to \{1, \ldots, n+1\}$ such that for all $1 \leq i \leq n+1$,*

$$q(i) = \begin{cases} 1, & i = 1 \\ p(i-1)+1, & i > 1 \end{cases}.$$

Then q is a permutation on $\{1, \ldots, n+1\}$ and $\operatorname{sign}(p) = \operatorname{sign}(q)$.

Proposition 1.6.4 (Complete expansion of det)**.** *Let $n \geq 1$ and A be an $n \times n$ matrix. Then*

$$\det(A) = \sum_{p \in X} \operatorname{sign}(p) A_{1,p(1)} \cdots A_{n,p(n)}$$

where $X := \{p : p \text{ is a permutation on } \{1, \ldots, n\}\}$.

Lemma 1.6.5 (Co-factor matrix)**.** *Let A be an $n \times n$ matrix. Then there exists a unique $n \times n$ matrix C such that*

(a) $n = 1 \implies C = [1]$, *and*
(b) $n > 1 \implies C_{i,j} = (-1)^{i+j} \det(A_{\langle j,i \rangle})$ *for all* $1 \leq i, j \leq n$.

Remark 1.6.6. This allows to denote C by $\operatorname{cof}(A)$.

Theorem 1.6.7 (Inverse using co-factor matrix)**.** *Let A be an $n \times n$ matrix. Then* $A \operatorname{cof}(A) = \operatorname{cof}(A) A = \det(A) I_n$.

Remark 1.6.8. We'll write $x = \pm k$ for abbreviating "$x = k$ or $x = -k$".

Example 1.6.9. *Let A be an invertible matrix with integer entries. Then* A^{-1} *has integer entries* $\iff \det(A) = \pm 1$.

Chapter 2

Groups

2.1 Laws of composition

October 28, 2021

Definition 2.1.1 (Identity)**.** "e is an identity for $+$ on S" iff S is a set, and $+\colon S \times S \to S$, and $e \in S$ and $e + x = x + e = x$ for each $x \in S$.

"$+$ on S has an identity" iff there is an e such that e is an identity for $+$ on S.

Lemma 2.1.2 (Uniqueness of identity)**.** *Let $+$ on S have an identity. Then there exists a unique e such that e is the identity for $+$ on S.*

Remark 2.1.3. This allows to denote e by Id_+. (S determined by $+$.)

Definition 2.1.4 (Inverses)**.** "a is an inverse of b for $+$ on S with identity" iff $+$ on S has an identity, and $b \in S$ and $a + b = b + a = \mathrm{Id}_+$.

"b is invertible for $+$ on S" iff there exists an a such that a is an inverse of b for $+$ on S with identity.

Definition 2.1.5 (Associativity)**.** "$+$ on S is associative" iff S is a set and $+\colon S \times S \to S$ and $(a + b) + c = a + (b + c)$ for all $a, b, c \in S$.

Lemma 2.1.6 (Uniqueness of inverses)**.** *Let $+$ on S have an identity and be associative and $a, l, r \in S$. Then*

(a) $a + l = a + r \implies l = r$*, and*
(b) *a is invertible for $+$ on S $\implies$ there exists a unique b such that b is the inverse of a.*

Remark 2.1.7. This allows to denote b by $\mathrm{Inv}_+(a)$.

Lemma 2.1.8 (Inverses of products and inverses)**.** *Let + on S have an identity and be associative, and $a, b \in S$ be invertible. Then $a+b$ and $\mathrm{Inv}_+(a)$ are invertible with*

$$\begin{aligned} \mathrm{Inv}_+(a+b) &= \mathrm{Inv}_+(b) + \mathrm{Inv}_+(a), \text{ and} \\ \mathrm{Inv}_+(\mathrm{Inv}_+(a)) &= a. \end{aligned}$$

Proposition 2.1.9 (Strings for associative operations)**.** *Let + on S be associative. Then there exists a unique function $\mathcal{F}\colon \mathbb{N} \setminus \{0\} \to \bigcup_{n\geq 1} S^{(S^{\{1,\ldots,n\}})}$ such that*

(a) $\mathcal{F}_m\colon S^{\{1,\ldots,m\}} \to S$ for each $m \geq 1$,
(b) $\mathcal{F}_1(a) = a$ for each $a \in S^{\{1,\ldots,1\}}$, and
(c) for all $1 \leq i < m$ and for each $b \in S^{\{1,\ldots,m-i\}}$ such that $b_k = a_{k+i}$ for each $1 \leq k \leq m-i$, we have $\mathcal{F}_m(a) = \mathcal{F}_i\big(a \circ \iota_{\{1,\ldots,i\}\to\{1,\ldots,m\}}\big) + \mathcal{F}_{m-i}(b)$.

Remark 2.1.10. This allows to denote $\mathcal{F}_m(a)$ by $a_1 + \cdots + a_m$ for each $a \in S^{\{1,\ldots,m\}}$ and for each $m \geq 1$. (S and m are determined by a.)

This also allows, for each $a \in S$ and for each $m \geq 1$, to denote $\mathcal{F}_m(b)$ by $\mathrm{Iter}_{+,m}(a)$ where b is the unique function (determined by a and m) such that $b\colon \{1, \ldots, m\} \to S$ so that $b_k = a$ for all $1 \leq k \leq m$.

Lemma 2.1.11 (Adding constant strings, and strings of a string)**.** *Let + on S be associative, and $a \in S$ and $r, s \geq 1$. Then $rs, r+s \geq 1$, and*

$$\begin{aligned} \mathrm{Iter}_{+,r}(a) + \mathrm{Iter}_{+,s}(a) &= \mathrm{Iter}_{+,r+s}(a), \text{ and} \\ \mathrm{Iter}_{+,s}(\mathrm{Iter}_{+,r}(a)) &= \mathrm{Iter}_{+,rs}(a). \end{aligned}$$

Lemma 2.1.12. *Let + on S be associative and have an identity, and $a \in S$. Then there exists a unique function $f\colon \mathbb{N} \to S$ such that for each $n \in \mathbb{N}$,*

$$f((a,n)) = \begin{cases} \mathrm{Id}_+, & n = 0 \\ \mathrm{Iter}_{+,n}(a), & n \geq 1 \end{cases}.$$

Remark 2.1.13. This allows to set $f(n)$ by $\mathrm{IterId}_{+,n}(a)$ for each $n \in \mathbb{N}$.

Corollary 2.1.14. *Let + on S be associative and have an identity, and $a \in S$, and $n \in \mathbb{N}$. Then*

(a) $\mathrm{IterId}_{+,n}(\mathrm{Id}_+) = \mathrm{Id}_+$,
(b) $\mathrm{IterId}_{+,0}(a) = \mathrm{Id}_+$, *and*
(c) $n \geq 1 \implies \mathrm{IterId}_{+,n}(a) = \mathrm{Iter}_{+,n}(a)$.

Lemma 2.1.15. *Let $+$ on S have an identity and be associative, and $a \in S$, and $r, s \in \mathbb{N}$. Then $rs, r+s \in \mathbb{N}$ and analogue of Lemma 2.1.11 holds.*

Lemma 2.1.16. *Let $+$ on S have an identity and be associative, and $a \in S$ be invertible. Then there exists a unique function $f\colon \mathbb{Z} \to S$ such that for each $p \in \mathbb{Z}$,*

$$f(p) = \begin{cases} \mathrm{IterId}_{+,p}(a), & p \geq 0 \\ \mathrm{Iter}_{+,-p}(\mathrm{Inv}_+(a)) & p < 0 \end{cases}.$$

Remark 2.1.17. This allows to denote $f(p)$ by $\mathrm{Itr}_{+,p}(a)$ for each $p \in \mathbb{Z}$.

Corollary 2.1.18. *Let $+$ on S be associative and have an identity, and $a \in S$ be invertible and $n \in \mathbb{N}$. Then*
(a) $\mathrm{Itr}_{+,n}(a) = \mathrm{IterId}_{+,n}(a)$,
(b) $\mathrm{Itr}_{+,-1}(a) = \mathrm{Inv}_+(a)$, *and*
(c) $\mathrm{IterId}_{+,n}(a)$ *is invertible and* $\mathrm{Itr}_{+,-n}(a) = \mathrm{Inv}_+(\mathrm{IterId}_{+,n}(a))$.

Lemma 2.1.19. *Let $+$ on S have an identity and be associative, and $a \in S$ be invertible and $r, s \in \mathbb{Z}$. Then $r+s, rs \in \mathbb{Z}$ and analogue of Lemma 2.1.11 holds.*

Lemma 2.1.20 (Restriction of binary operations)**.** *Let G be a set, and $\cdot\colon G \times G \to G$ and $H \subseteq G$ such that $a \cdot b \in H$ for each $a, b \in H$. Then there exists a unique function $*\colon H \times H \to H$ such that $a * b = a \cdot b$ for all $a, b \in H$.*

Remark 2.1.21. This allows to denote $*$ by $\cdot_H$. (This is poor notation if ordered pairs are considered as Kuratowski pairs.)

2.2 Groups and subgroups

October 29, 2021

Definition 2.2.1 (Groups)**.** "$(G, \cdot)$ is a group" iff $\cdot$ on G has an identity and is associative, and each $a \in G$ is invertible.

Proposition 2.2.2. *Let $+$ on S be associative and have an identity. Set $G := \{x \in S : x$ is invertible for $+$ on $S\}$. Then $(G, +_G)$ is a group.*

Proposition 2.2.3. *Let* $(G, \cdot)$ *be a group, and* $a, b \in G$ *and* $n \in \mathbb{Z}$*. Then* $\mathrm{Iter}_{\cdot,n}(a \cdot b) = \mathrm{Id}_{\cdot} \iff \mathrm{Iter}_{\cdot,n}(b \cdot a) = \mathrm{Id}_{\cdot}$*.*

Definition 2.2.4 (Finite groups)**.** "$(G, \cdot)$ is a finite group" iff $(G, \cdot)$ is a group and G is a finite set.

Definition 2.2.5 (Abelian groups)**.** "$(G, \cdot)$ is an abelian group" iff $(G, \cdot)$ is a group and $a \cdot b = b \cdot a$ for all $a, b \in G$.

Corollary 2.2.6 (A condition for commuting elements)**.** *Let* $(G, \cdot)$ *be a group and* $a, b \in G$ *such that* $\mathrm{Iter}_{\cdot,2}(a) = \mathrm{Iter}_{\cdot,2}(b) = \mathrm{Iter}_{\cdot,2}(ab) = \mathrm{Id}_{\cdot}$*. Then* $a \cdot b = b \cdot a$*.*

Proposition 2.2.7 (Cancellation law)**.** *Let* $(G, \cdot)$ *be a group and* $a, b, c \in G$*. Then*

(a) $(ab = ac$ *or* $ba = ca) \implies b = c$*, and*
(b) $(ab = a$ *or* $ba = a) \implies b = \mathrm{Id}_{\cdot}$*.*

Abbreviation 2.2.8 (General linear, symmetric and alternating groups)**.** For any $n \geq 1$, we set $\mathrm{GL}_n(\mathbb{F}) := \{A \in \mathrm{Mat}(n, n; \mathbb{F}) : A \text{ is invertible}\}$ and for any $m \in \mathbb{N}$, we set $\mathrm{S}_m := \{p \in \{1, \ldots, m\}^{\{1,\ldots,m\}} : p \text{ is bijective}\}$ and $\mathrm{A}_m := \{p \in S_m : \mathrm{sign}(p) = 1\}$.

Lemma 2.2.9 (Cardinality of S_n)**.** *Let* $n \in \mathbb{N}$*. Then* $\#(\mathrm{S}_n) = n!$*.*

Example 2.2.10 (Groups)**.** *For any* $m, n \in \mathbb{N}$ *such that* $n \geq 1$*, we have that* $(\mathrm{S}_m, \circ)$ *and* $(\mathrm{GL}_n(\mathbb{F}), \textit{matrix multiplication})$ *are groups.*

Example 2.2.11 (Characterizing S_3)**.** *Set* $x := (123)$*, and* $y := (12)$*. Then, in multiplicative notation,*

$$\begin{aligned} x, y &\neq 1, \\ x^3 &= 1, \\ y^2 &= 1, \\ yx &= x^2 y, \text{ and} \\ \mathrm{S}_3 &= \{1, x, x^2, y, xy, x^2 y\}. \end{aligned}$$

Definition 2.2.12 (Subgroups)**.** "H is a subgroup of $(G, \cdot)$" iff the following hold:

(a) $H \subseteq G$.

(b) $a \cdot b \in H$ for each $a, b \in H$.
(c) $(H, \cdot_H)$ is a group.

Proposition 2.2.13 (An equivalent condition for being a subgroup). *Let $(G, \cdot)$ be a group and H be a set. Then H is a subgroup of $(G, \cdot)$ $\iff$ the following hold:*

(a) $H \subseteq G$.
(b) $a \cdot b \in H$ *for all* $a, b \in H$.
(c) $\mathrm{Id.} \in H$.
(d) $\mathrm{Inv.}(a) \in H$ *for each* $a \in H$.

Proposition 2.2.14 (Subgroups of subgroups). *Let H be a subgroup of $(G, \cdot)$ and K be a subgroup of $(H, \cdot_H)$. Then K is a subgroup of $(H, \cdot)$.*

Proposition 2.2.15 (Intersection of subgroups). *Let H and K be subgroups of $(G, \cdot)$. Then $H \cup K$ is a subgroup of $(G, \cdot)$.*

Lemma 2.2.16 (Trivial subgroups). *Let $(G, \cdot)$ be a group. Then G, $\{\mathrm{Id.}\}$ are subgroups of $(G, \cdot)$.*

Definition 2.2.17 (Proper subgroups). "H is a proper subgroup of $(G, \cdot)$" iff H is a subgroup of $(G, \cdot)$, and $H \neq G$ and $H \neq \{\mathrm{Id.}\}$.

Abbreviation 2.2.18 (Special linear groups). For any $n \geq 1$, we set $\mathrm{SL}_n(\mathbb{F}) := \{A \in \mathrm{GL}_n(\mathbb{F}) : \det(A) = 1\}$.

Example 2.2.19 (Examples of subgroups).

(a) $\mathrm{SL}_n(\mathbb{F})$ *is a subgroup of* $(\mathrm{GL}_n(\mathbb{F}),$ *matrix multiplication*$)$ *for any* $n \geq 1$.
(b) $\{z \in \mathbb{C} : |z| = 1_{\mathbb{R}}\}$ *is a subgroup of* $(\mathbb{C},$ *complex multiplication*$)$.
(c) The set of upper triangular matrices is a subgroup of $(\mathrm{GL}_n(\mathbb{F}),$ *matrix multiplication*$)$ *for each* $n \geq 1$.
(d) Let $1 \leq r < n$. *Then* $\left\{\begin{bmatrix} A & B \\ 0_{(n-r)\times r} & D \end{bmatrix} : A \in \mathrm{GL}_r(\mathbb{F}), D \in \mathrm{GL}_{n-r}(\mathbb{F})\right\}$ *is a subgroup of* $(\mathrm{GL}_n(\mathbb{F}),$ *matrix multiplication*$)$.

Definition 2.2.20 (Subgroups generated by sets). "H is a smallest subgroup of $(G, \cdot)$ generated by S" iff H is the minimal set such that $S \subseteq H$ and H is a subgroup of $(G, \cdot)$.

Corollary 2.2.21 (Uniqueness of the subgroups generated by sets). *Let H, H' be subgroups of $(G, \cdot)$ generated by S. Then $H = H'$.*

Example 2.2.22. *The group generated by a subset contains exactly all the finite products (including empty products which evaluate to identity) of the elements of U and their inverses.*

Proposition 2.2.23 (Product set of subgroups being a subgroup)**.** *Let H, K be subgroups of $(G, \cdot)$. Set $A := \{h \cdot k : h \in H, k \in K\}$ and $B := \{k \cdot h : k \in K, h \in H\}$. Then A is a subgroup of $(G, \cdot) \iff A = B$.*

Proposition 2.2.24 (Type I and type III generate $\mathrm{GL}_n(\mathbb{F})$)**.** *Let $n \geq 1$. Then $\mathrm{GL}_n(\mathbb{F})$ is the smallest subgroup of $\mathrm{GL}_n(\mathbb{F})$ generated by $\{E \in \mathrm{Mat}(n, n; \mathbb{F}) :$ E is type I or type III elementary matrix of size $n\}$.*

Proposition 2.2.25 (Type I generates $\mathrm{SL}_n(\mathbb{F})$)**.** *Let $n \geq 1$. Then $\mathrm{SL}_n(\mathbb{F})$ is the smallest subgroup of $\mathrm{GL}_n(\mathbb{F})$ generated by $\{E \in \mathrm{Mat}(n, n; \mathbb{F}) : E$ is a type I elementary matrix of siz*

Proposition 2.2.26 ((Proper) transpositions generate S_n)**.** *Let $n \in \mathbb{N}$. Then S_n is the smallest subgroup of S_n generated by $\{p \in \mathrm{S}_n : p$ is a proper transposition$\}$.*

Proposition 2.2.27 (3-cycles generate A_n)**.** *Let $n \geq 3$. Then A_n is the smallest subgroup of S_n generated by $\{p \circ (1 \cdots 3)_n \circ p^{-1} : p \in \mathrm{S}_n\}$.*

Abbreviation 2.2.28 (Subgroups generated by singletons)**.** For any group $(G, \cdot)$ and any $x \in G$, we set $\langle x \rangle_{\cdot} := \{\mathrm{Itr}_{\cdot, m}(x) : m \in \mathbb{Z}\}$.

Lemma 2.2.29. *Let $(G, \cdot)$ be a group and $x \in G$. Then $\langle x \rangle_{\cdot}$ is the smallest subgroup of $(G, \cdot)$ generated by $\{x\}$.*

Definition 2.2.30 (Path connections in subsets of $\mathbb{R}^k$)**.** "a and b are connected in S of $\mathbb{R}^k$" iff $k \geq 1$, and $a, b \in \mathbb{R}^k$, and $S \subseteq R^k$, and there exists a $\phi \colon [0_{\mathbb{R}}, 1_{\mathbb{R}}] \to \mathbb{R}^k$ such that

(a) $\phi(0_{\mathbb{R}}) = a$ and $\phi(1_{\mathbb{R}}) = b$,
(b) ϕ is conitnuous, and
(c) $\phi(x) \in S$ for all $0_{\mathbb{R}} \leq x \leq 1_{\mathbb{R}}$.

Definition 2.2.31 (Path-connected subsets)**.** "S is path-connected in $\mathbb{R}^k$" iff S is a set such that for every $a, b \in S$, we have that a and b are connected in S of $\mathbb{R}^k$.

Proposition 2.2.32 (Path connections form an equivalence relation)**.** *Let $k \geq 1$, and $S \subseteq \mathbb{R}^k$ and $a \in S$. Set $R := \{(a, b) : a$ and b are connected in S of $\mathbb{R}^k\}$. Then*

(a) R is an equivalence relation on S, and
(b) $[a]_R$ is path-connected in $\mathbb{R}^k$.

Example 2.2.33 (Examples of path-connected subsets)**.** *$\{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$ and $\{(x,y) \in \mathbb{R}^2 : xy = 0\}$ are path-connected in $\mathbb{R}^2$, whereas $\{(x,y) \in \mathbb{R}^2 : xy = 1\}$ is not.*

Remark 2.2.34. From Definition 2.2.35 to Example 2.2.39, we'll fix an $n \geq 1$ and a bijection $f\colon \{1,\ldots,n\} \times \{1,\ldots,n\} \to \{1,\ldots,n^2\}$.

We'll set g to be the unique function $g\colon \mathrm{Mat}(n,n;\mathbb{R}) \to \mathbb{R}^{n^2}$ such that $g(A)_{f((i,j))} = A_{i,j}$ for any $A \in \mathrm{Mat}(n,n;\mathbb{R})$ and for all $1 \leq i,j \leq n$.

We'll also shorten $\mathrm{GL}_n(\mathbb{R}, +, \text{real multiplication})$ to $\mathrm{GL}_n(\mathbb{R})$.

Definition 2.2.35 (Path connections in subsets of $\mathrm{GL}_n(\mathbb{R})$)**.** "$A$ and B are connected in S of $\mathrm{GL}_n(\mathbb{R})$" iff $S \subseteq \mathrm{GL}_n(\mathbb{R})$, and $g(A)$ and $g(B)$ are connected in $g[S]$ of $g[\mathrm{GL}_n(\mathbb{R})]$.

"S is path-connected in $\mathrm{GL}_n(\mathbb{R})$" iff S is a set such that for every $A, B \in S$, we have that A and B are connected in S of $\mathrm{GL}_n(\mathbb{R})$.

Example 2.2.36 (Connected components are normal subgroups)**.** *Let G be a subgroup of $(\mathrm{GL}_n(\mathbb{R}), \text{matrix multiplication})$, and A and B, and C and D be connected in G of $\mathrm{GL}_n(\mathbb{R})$. Then*

(a) AC and BD are connected in G of $\mathrm{GL}_n(\mathbb{R})$, and
(b) $\{M \in \mathrm{GL}_n(\mathbb{R}) : M$ and I_n are connected in G of $\mathrm{GL}_n(\mathbb{R})\}$ is a normal subgroup of $(\mathrm{GL}_n(\mathbb{R}), \text{matrix multiplication})$.

Proposition 2.2.37 ($\mathrm{SL}_n(\mathbb{R})$ is path-connected)**.** *$\mathrm{SL}_n(\mathbb{R})$ is path-connected in $\mathrm{GL}_n(\mathbb{R})$.*

Example 2.2.38 (Generators of $\mathrm{GL}_n(\mathbb{R})$)**.** *$\mathrm{GL}_n(\mathbb{R})$ is the smallest subgroup of $(\mathrm{GL}_n(\mathbb{R}), \text{matrix multiplication})$ generated by $\{E \in \mathrm{Mat}(n,n;\mathbb{R}) : (E$ is type I elementary m $\mathcal{E}_{\mathbb{F},n;i\to ci}$ for some $c > 0$ and some $1 \leq i \leq n)$ or $(E = I_n - 2e_{1,1})\}$.*

Example 2.2.39 ($\mathrm{GL}_n(\mathbb{R})$'s connected subsets)**.** *Let $A \in \mathrm{GL}_n(\mathbb{R})$. Set*

$$\begin{aligned}
X &:= \{B \in \mathrm{GL}_n(\mathbb{R}) : \det(B) > 0\},\\
Y &:= \{B \in \mathrm{GL}_n(\mathbb{R}) : \det(B) < 0\},\\
W &:= \{B \in \mathrm{GL}_n(\mathbb{R}) : B \text{ and } I_n \text{ are connected in } \mathrm{GL}_n(\mathbb{R}) \text{ of } \mathrm{GL}_n(\mathbb{R})\}, \text{ and}\\
Z &:= \{B \in \mathrm{GL}_n(\mathbb{R}) : B \text{ and } I_n - 2e_{1,1} \text{ are connected in } \mathrm{GL}_n(\mathbb{R}) \text{ of } \mathrm{GL}_n(\mathbb{R})\}.
\end{aligned}$$

Then

(a) $X = W$ *and* $Y = Z$,
(b) $\{X, Y\}$ *is a partition of* $\mathrm{GL}_n(\mathbb{R})$,
(c) W *and* Z *are path-connected in* $\mathrm{GL}_n(\mathbb{R})$, *and*
(d) P *and* Q *are not connected in* $\mathrm{GL}_n(\mathbb{R})$ *of* $\mathrm{GL}_n(\mathbb{R})$ *for any* $P \in W$ *and any* $Q \in Z$.

2.3 Subgroups of the additive group of integers

October 29, 2021

Lemma 2.3.1 (Euclid's division lemma for $\mathbb{Z}$). *Let* $a, b \in \mathbb{Z}$ *such that* $b \neq 0$. *Then there exist unique* $q, r \in \mathbb{Z}$ *such that* $0 \leq r < |b|$ *and* $a = bq + r$.

Abbreviation 2.3.2. For any $a \in \mathbb{Z}$, we set $\mathbb{Z}a := \{ka : k \in \mathbb{Z}\}$.

Corollary 2.3.3.

(a) *Let* $a \in \mathbb{Z}$. *Then* $\mathbb{Z}a = \mathbb{Z}(-a) = \mathbb{Z}(|a|)$.
(b) $\mathbb{Z}1 = \mathbb{Z}$.
(c) $\mathbb{Z}0 = \{0\}$.

Lemma 2.3.4 (Strings in $(\mathbb{Z}, +)$). *Let* $m, n \in \mathbb{Z}$. *Then* $\mathrm{Itr}_{+,m}(n) = mn$.

Corollary 2.3.5 (a generates $\mathbb{Z}a$). *Let* $a \in \mathbb{Z}$. *Then* $\mathbb{Z}a = \langle a \rangle_+$.

Lemma 2.3.6. *Let* $a, b \geq 0$ *such that* $\mathbb{Z}a = \mathbb{Z}b$. *Then* $a = b$.

Theorem 2.3.7 (Characterizing subgroups of $\mathbb{Z}$). *Let* S *be a subgroup of* $(\mathbb{Z}, +)$. *Then, setting* $X := \{m \in S : m > 0\}$

(a) $X = \emptyset \implies S = \{0\}$, *and*
(b) $X \neq \emptyset \implies S = \mathbb{Z}(\min(X))$.

Abbreviation 2.3.8. For any $a, b \in \mathbb{Z}$, we set $\mathbb{Z}a + \mathbb{Z}b := \{x + y : x \in \mathbb{Z}a, y \in \mathbb{Z}b\}$.

Lemma 2.3.9 (a, b generate $\mathbb{Z}a + \mathbb{Z}b$). *Let* $a, b \in \mathbb{Z}$. *Then* $\mathbb{Z}a + \mathbb{Z}b$ *is the smallest subgroup of* $(G, \cdot)$ *generated by* $\{a, b\}$.

Lemma 2.3.10 (gcd). *Let* $a, b \in \mathbb{Z}$ *such that not both are zero. Then there exists a unique* $m > 0$ *such that* $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}m$.

Remark 2.3.11. This allows to denote m by $\gcd(a, b)$.

Corollary 2.3.12. *Let $a, b \in \mathbb{Z}$ such that not both are zero. Then $|a|, |b|$ are not both zero and* $\gcd(a, b) = \gcd(|a|, |b|)$.

Proposition 2.3.13 (Euclid's algorithm)**.** *Let $a, b \in \mathbb{N}$ not both be zero. Then there exist unique functions $A, B \colon \mathbb{N} \to \mathbb{N}$ such that $A_0 = \max(a, b)$, and $B_0 = \min(a, b)$ and for all $n \in \mathbb{N}$,*

$$(A_{n+1}, B_{n+1}) = \begin{cases} (B_n, \textit{remainder on dividing } A_n \textit{ by } B_n), & B_n \neq 0 \\ (A_n, 0), & B_n = 0 \end{cases}.$$

Further, for any such functions A, B, the following hold:

(a) *For each $n \in \mathbb{N}$,*
  - *(i)* $A_n > 0$ *and* $B_n \geq 0$,
  - *(ii)* $B_n \neq 0 \implies B_{n+1} < B_n$, *and*
  - *(iii)* $\mathbb{Z}A_n + \mathbb{Z}B_n = \mathbb{Z}a + \mathbb{Z}b$.

(b) *Setting $K := \{n \in \mathbb{N} : B_n = 0\}$, we have $K \neq \emptyset$. Set $N := \min(K)$. Also, $A_n = A_N$ and $B_n = 0$ for each $n \geq N$.*

(c) $\gcd(a, b) = A_N$.

Definition 2.3.14 (Divisors)**.** "a is a divisor of b" or "a divides b" or b is a multiple of a" iff $a, b \in \mathbb{Z}$ and $b \in \mathbb{Z}a$.

Lemma 2.3.15 (Quotients)**.** *Let m divide n such that $m \neq 0$. Then there exists a unique $q \in \mathbb{Z}$ such that $n = qm$.*

Remark 2.3.16. This allows to denote q by n/m.

Proposition 2.3.17 (Characterizing gcd)**.** *Let $a, b, d \in \mathbb{Z}$ such that a, b are not both zero. Then*

(a) $\gcd(a, b)$ *is a divisor of a, b,*
(b) *d is a divisor of a, b $\implies$ d is a divisor of* $\gcd(a, b)$, *and*
(c) $\gcd(a, b) = ra + sb$ *for some $r, s \in \mathbb{Z}$.*

Proposition 2.3.18 (gcd of quotients)**.** *Let $a, b, k \in \mathbb{Z}$ such that a, b are not both zero and k divides both a and b. Set $d := \gcd(a, b)$. Then*

(a) *k divides d and $k \neq 0$,*
(b) $\mathbb{Z}(a/k) + \mathbb{Z}(b/k) = \mathbb{Z}(d/k)$, *and*

(c) $\gcd(a,b) = d/|k|$.

Definition 2.3.19 (Co-primes)**.** "a, b are co-primes" iff $a, b \in \mathbb{Z}$ and $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}$.

Proposition 2.3.20 (Characterizing co-primes)**.** *Let $a, b \in \mathbb{Z}$. Then the following are equivalent:*

(a) a, b are co-primes.
(b) There exist $r, s \in \mathbb{Z}$ such that $ra + rb = 1$.
(c) For any $d > 0$, if d divides a, b, then $d = 1$.

Definition 2.3.21 (Primes)**.** "p is a prime" iff $p \in \mathbb{Z}$, and $p \neq 1$, and $p \neq -1$ and for any a, if a divides p, then $a \in \{1, -1, p, -p\}$.

Corollary 2.3.22. 0 *is not prime.*

Proposition 2.3.23. *Let p be a prime and $a, b \in \mathbb{Z}$ such that p divides ab. Then p divides a or p divides b.*

Lemma 2.3.24 (lcm)**.** *Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then there exists a unique $m > 0$ such that $\mathbb{Z}a \cap \mathbb{Z}b = \mathbb{Z}m$.*

Remark 2.3.25. This allows to denote m by $\operatorname{lcm}(a,b)$.

Proposition 2.3.26 (Characterizing lcm)**.** *Let $a, b, m \in \mathbb{Z}$ such that a, b are each nonzero. Then*

(a) $\operatorname{lcm}(a,b)$ *is a positive multiple of a, b,*
(b) m is a multiple of a, b and $m > 0 \implies m$ is a multiple of $\operatorname{lcm}(a,b)$.

Proposition 2.3.27 (lcm of quotients)**.** *Let $a, b, k \in \mathbb{Z}$ such that $a, b \neq 0$ and k divides both a and b. Set $m := \operatorname{lcm}(a,b)$. Then*

(a) k divides m and $k \neq 0$,
(b) $\mathbb{Z}(a/k) \cap \mathbb{Z}(b/k) = \mathbb{Z}(m/k)$, and
(c) $\operatorname{lcm}(a/k, b/k) = m/|k|$.

Lemma 2.3.28. *Let $a, b \geq 0$ such that a divides b and b divides a. Then $a = b$.*

Proposition 2.3.29 (Product of gcd and lcm)**.** *Let $a, b \geq 1$. Then* $\gcd(a,b)\operatorname{lcm}(a,b) = ab$.

Corollary 2.3.30. *Let $m, n > 0$ and $k \in \mathbb{Z}$ such that n divides mk. Then n divides* $m\gcd(n,k)$.

Corollary 2.3.31 (lcm of co-primes)**.** *Let $r, s \geq 1$ be co-primes. Then* $\operatorname{lcm}(r,s) = rs$.

2.4 Cyclic groups

October 29, 2021

Definition 2.4.1 (Cyclic groups)**.** "$(G, \cdot)$ is a cyclic group" iff $(G, \cdot)$ is a group and there exists an $a \in G$ such that $\langle x \rangle_{\cdot} = G$.

Corollary 2.4.2 (Cyclic groups are abelian)**.** *Let $(G, \cdot)$ be a cyclic group. Then $(G, \cdot)$ is an abelian group.*

Example 2.4.3. $(\mathrm{S}_3, \circ)$ *is non-abelian and non-cyclic.*

Proposition 2.4.4 (Subgroups of cyclic groups)**.** *Let $(G, \cdot)$ be a cyclic group and H be a subgroup of $(G, \cdot)$. Then $(H, \cdot_H)$ is a cyclic group.*

Definition 2.4.5 (Order of elements)**.** "x has order n in $(G, \cdot)$" iff $(, \cdot)$ is a group and, setting $S := \{m > 0 : \mathrm{Itr}_{\cdot,m}(x) = \mathrm{Id}_{\cdot}\}$, we have $S \neq \emptyset$ and $n = \min(S)$.

Proposition 2.4.6 (Finite groups have finite orders)**.** *Let $(G, \cdot)$ be a finite group and $x \in G$. Then there exists a unique $n \geq 1$ such that x has order n in $(G, \cdot)$.*

Remark 2.4.7. We write $P(i)$'s are distinct for each $i \in X$" to mean that there exists a set Y and a function $f \colon X \to Y$ such that $f(i) = P(i)$ for each $x \in X$, and that any such f is injective.

Proposition 2.4.8 (Cyclic subgroups)**.** *Let $(G, \cdot)$ be a group, and $x \in \mathbb{G}$, and $r, s \in \mathbb{Z}$ and $n \geq 1$. Set $S := \{k \in \mathbb{Z} : \mathrm{Itr}_{\cdot,k}(x) = \mathrm{Id}_{\cdot}\}$. Then*

- *(a) S is a subgroup of $(\mathbb{Z}, +)$,*
- *(b) $x^r = x^s \iff r - s \in S$, and*
- *(c) the following are equivalent:*
  - *(i) $S = \mathbb{Z}n$.*
  - *(ii) $\langle x \rangle_{\cdot} = \{\mathrm{Itr}_{\cdot,i}(x) : 0 \leq i < n\}$ and $\mathrm{Itr}_{\cdot,i}(x)$'s are distinct for $0 \leq i < n$.*
  - *(iii) $\langle x \rangle_{\cdot}$ has n elements.*
  - *(iv) x has order n in $(G, \cdot)$.*

Proposition 2.4.9 (Order of x^k)**.** *Let x have order n in $(G, \cdot)$ and $k \in \mathbb{Z}$. Then x^k has order $n/\gcd(n, k)$ in $(G, \cdot)$.*

Proposition 2.4.10 (Elements with no finite order). *Let $(G, \cdot)$ be a group and $a \in G$. Then $\langle a \rangle_{\cdot}$ is a finite set $\iff$ there exists an $n \in \mathbb{Z} \setminus \{0\}$ such that* $\mathrm{Iter}_{\cdot,n}(a) = \mathrm{Id}_{\cdot}$.

Proposition 2.4.11 (Characterizing groups with no proper subgroups). *Let $(G, \cdot)$ be a group. Then there are no proper subgroups of $(G, \cdot)$ $\iff$ G is a finite set such that $\#(G) = 1$ or $\#(G)$ is prime.*

Example 2.4.12 (Order of elements in S_4).

n	*Number of elements of order n in* S_4
1	1
2	9
3	8
4	6

Example 2.4.13 (Product of finite ordered elements need not be finite ordered). *Let b be a nonzero scalar. Then* $\begin{bmatrix} 1 & b \\ 0 & -1 \end{bmatrix}$ *and* $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ *have order* 2 *in* $(\mathrm{GL}_n(\mathbb{F}), \textit{matrix multiplication})$, *but* $\left(\begin{bmatrix} 1 & b \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \right)^n \neq I_n$ *for any* $n \geq 1$.

2.5 Homomorphisms

October 30, 2021

Definition 2.5.1 (Homomorphisms). "ϕ is a homomorphism from $(G, \cdot)$ to $(G', *)$ " iff $(G, \cdot)$, $(G', *)$ are groups, and $\phi \colon G \to G'$ and $\phi(a \cdot b) = \phi(a) * \phi(b)$ for all $a, b \in G$.

Example 2.5.2 (Homomorphisms).

(a) *For any $n \geq 1$, we have that* det *is a homomorphism from* $(\mathrm{GL}_n(\mathbb{F}), \textit{matrix multiplication})$ *to* $(\mathfrak{F} \setminus \{0\}, \textit{field multiplication})$.

(b) *For any $n \geq 1$, we have that* sign *is a homomorphism from* $(\mathrm{S}_n, \circ)$ *to* $(\{-1, 1\}, \textit{field multiplication})$.

(c) exp *is a homomorphism from* $(\mathbb{R}, +)$ *to* $(\mathbb{R} \setminus \{0_{\mathbb{R}}\}, \textit{real multiplication})$.

(d) *Let $(G, \cdot)$ be a group and $a \in G$. Then* $n \mapsto \mathrm{Itr}_{\cdot,n}(a)$ *is a homomorphism from* $(\mathbb{Z}, +)$ *to* $(G, \cdot)$.

(e) $x \mapsto |x|$ *is a homomorphism from* $(\mathbb{C} \setminus \{0_{\mathbb{C}}\},$ *complex multiplication) to* $(\mathbb{R} \setminus \{0_{\mathbb{R}}\},$ *real multiplication).*

Lemma 2.5.3 (Trivial and inclusion homomorphisms)**.**

(a) *Let* $(G, \cdot)$, $(G', *)$ *be groups and* $\phi\colon G \to G'$ *such that* $\phi(a) = \mathrm{Id}_*$ *for all* $a \in G$. *Then* ϕ *is a homomorphism from* $(G, \cdot)$ *to* $(G', *)$.

(b) *Let* H *be a subgroup of* $(G, \cdot)$. *Then* $\iota_{H \to G}$ *is a homomorphism from* $(H, \cdot_H)$ *to* $(G, \cdot)$.

Proposition 2.5.4 (Properties of homomorphisms)**.** *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$. *Then*

(a) *for all* $k \geq 1$ *and for all functions* $a\colon \{1, \ldots, k\} \to G$, *we have* $\phi(a_1 \cdot \cdots \cdot a_k) = (\phi \circ a)_1 * \cdots * (\phi \circ a)_k$.

(b) $\phi(\mathrm{Id}_.) = \mathrm{Id}_*$, *and*

(c) $\phi(\mathrm{Inv}_.(a)) = \mathrm{Inv}_*(\phi(a))$ *for all* $a \in G$.

Abbreviation 2.5.5 (Kernels)**.** For any homomorphism ϕ from $(G, \cdot)$ to $(G, *)$, we set $\ker_*(\phi) := \phi^{-1}[\{\mathrm{Id}_*\}]$.

Proposition 2.5.6 (Images and kernels form subgroups)**.** *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$. *Then* $\phi[G]$ *and* $\ker_*(\phi)$ *are subgroups of* $(G', *)$ *and* $(G, \cdot)$ *respectively.*

Proposition 2.5.7 (Subgroup conservation under homomorphisms)**.** *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$ *and* H *be a subgroup of* $(G, \cdot)$. *Then* $\phi[H]$ *is a subgroup of* $(G', *)$.

Abbreviation 2.5.8 (Cosets)**.** For any subgroup H of $(G, \cdot)$ and any $a \in G$, we set $\mathrm{coset}(a \cdot H) := \{a \cdot h : h \in H\}$ and $\mathrm{coset}(H \cdot a) := \{h \cdot a : h \in H\}$.

Example 2.5.9 (Solutions of linear systems)**.** *Let* A, B *be* $m \times n$ *and* $m \times 1$ *matrices. Set* $S := \{X \in \mathrm{Mat}(n, 1; \mathbb{F}) : AX = B\}$ *and* $W := \{X \in \mathrm{Mat}(n, 1; \mathbb{F}) : AX = 0_{m \times 1}\}$. *Then*

(a) W *is a subgroup of* $(\mathrm{Mat}(n, 1; \mathbb{F}), +)$, *and*

(b) $S = \emptyset$ *or* $S = \mathrm{coset}(X_0 + W)$ *for some* $n \times 1$ *matrix* X_0

Lemma 2.5.10. *Let* H *be a subgroup of* $(G, \cdot)$ *and* $a, b \in G$. *Then* $\mathrm{Inv}_.(a) \cdot b \in H \iff b \in \mathrm{coset}(a \cdot H)$.

Proposition 2.5.11 (Properties of kernels)**.** *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$ *and* $a, b \in G$. *Then, setting* $K := \ker_*(\phi)$ *the following are equivalent:*

(a) $\phi(a) = \phi(b)$.
(b) $\text{Inv.}(a) \cdot b \in K$.
(c) $b \in \text{coset}(a \cdot K)$.
(d) $\text{coset}(a \cdot K) = \text{coset}(b \cdot K)$.

Corollary 2.5.12 (Injectivity and kernels)**.** *Let ϕ be a homomorphism from $(G, \cdot)$ to $(G', *)$. Then ϕ is injective $\iff$ $\ker_*(\phi) = \{\text{Id.}\}$.*

Lemma 2.5.13 (Conjugation)**.** *Let $(G, \cdot)$ be a group and $g \in G$. Then there exists a unique function $f\colon G \to G$ such that $f(x) = g \cdot x \cdot \text{Inv.}(g)$ for all $x \in G$.*

Remark 2.5.14. This allows to denote f by $\text{conj}_{\cdot,g}$.

Proposition 2.5.15 (Conjugation is a homomorphism)**.** *Let $(G, \cdot)$ be a group and $g \in G$. Then $\text{conj}_{\cdot,g}$ is a homomorphism from $(G, \cdot)$ to $(G, \cdot)$.*

Corollary 2.5.16 (Subgroup conservation under conjugation)**.** *Let H be a subgroup of $(G, \cdot)$ and $g \in G$. Then $\text{conj}_{\cdot,g}[H]$ is a subgroup of $(G, \cdot)$.*

Definition 2.5.17 (Normal subgroups)**.** "N is a normal subgroup of $(G, \cdot)$" iff N is a subgroup of $(G, \cdot)$ and $\text{conj}_{\cdot,g}[N] \subseteq N$ for all $g \in G$.

Example 2.5.18. *In Example 2.2.11, the subgroup $\langle y \rangle$ of S_3 is not normal.*

Proposition 2.5.19 (Intersections of cosets)**.** *Let H, K be subgroups of $(G, \cdot)$ and $x, y \in G$. Then*
(a) *H is a normal subgroup of $(G, \cdot)$ $\implies$ $H \cap K$ is a normal subgroup of $(K, \cdot_H)$, and*
(b) *there exists a $z \in G$ such that $\text{coset}(x \cdot H) \cap \text{coset}(y \cdot K) = \text{coset}(z \cdot (H \cap K))$.*

Definition 2.5.20 (Centers of groups)**.** "Z is the center of $(G, \cdot)$" iff $(G, \cdot)$ is agroup and $Z = \{a \in G : a \cdot g = g \cdot a \text{ for all } g \in G\}$.

Example 2.5.21 (Examples of centers)**.**
(a) *For each $n \geq 3$, the center of $(\mathrm{S}_n, \circ)$ is $\{\iota_{\{1,\ldots,n\} \to \{1,\ldots,n\}}\}$.*
(b) *For each $n \geq 1$, the center of $(\mathrm{GL}_n(\mathbb{F}), \textit{matrix multiplication})$ is $\{\lambda I_n : \lambda \textit{ is a nonzero scalar}\}$.*

Corollary 2.5.22.
(a) *Let Z be the center of $(G, \cdot)$. Then Z is a normal subgroup of $(G, \cdot)$.*

(b) *Let* $(G, \cdot)$ *be an abelian group and* H *be a subgroup of* $(G, \cdot)$*. Then* H *is a normal subgroup of* $(G, \cdot)$*.*

(c) *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$*. Then* $\ker_*(\phi)$ *is a normal subgroup of* $(G, \cdot)$*.*

Proposition 2.5.23 (A condition for a set to be a group)**.** *Let* $(G, \cdot)$ *be a group, and* G' *be a set, and* $*\colon G' \times G' \to G'$ *and* $\phi\colon G \to G'$ *be surjective such that* $\phi(a \cdot b) = \phi(a) * \phi(b)$ *for all* $a, b \in G$*. Then*

(a) $(G', *)$ *is a group,*

(b) $\mathrm{Id}_* = \phi(\mathrm{Id}_\cdot)$*,*

(c) $\mathrm{Inv}_*(\phi(a)) = \phi(\mathrm{Inv}_\cdot(a))$ *for all* $a \in G$*,*

(d) $(G, \cdot)$ *is a cyclic group* $\Longrightarrow$ $(G', *)$ *is a cyclic group, and*

(e) $(G, \cdot)$ *is an abelian group* $\Longrightarrow$ $(G', *)$ *is an abelian group.*

2.6 Isomorphisms

October 31, 2021

Definition 2.6.1 (Isomorphisms)**.** "ϕ is an isomorphism from $(G, \cdot)$ to $(G', *)$" iff ϕ is a homomorphism from $(G, \cdot)$ to $(G', *)$ and ϕ is a bijection.

Example 2.6.2 (Examples of isomorphisms)**.**

(a) $\exp$ *is an isomorphism from* $(\mathbb{R}, +)$ *to* $(\mathbb{R}^+, \textit{real multiplication})$*.*

(b) *Let* $(G, \cdot)$ *be a group and* $a \in G$ *such that* a *has infinite order. Then* $n \mapsto \mathrm{Itr}_{\cdot,n}(a)$ *is an isomorphism from* $(\mathbb{Z}, +)$ *to* $(\langle a \rangle_\cdot, \cdot)$*.*

(c) *For each* $n \geq 1$*, we have that* $p \mapsto \mathrm{PerMat}(p)$ *is an isomorphism from* $(\mathrm{S}_n, \circ)$ *to* $(\{\mathrm{PerMat}(p) : p \in \mathrm{S}_n\}, \textit{matrix multiplication})$*.*

(d) *For each* $n \geq 1$*, we have that* $x \mapsto I_n + xe_{n\times n;1,n}$ *is an isomorphism from* $(\mathfrak{F}, +)$ *to* $(\{\mathcal{E}_{\mathbb{F},n;1\to 1+cn} : c \textit{ is a scalar}\}, \textit{matrix multiplication})$*.*

Definition 2.6.3 (Automorphisms)**.** "ϕ is an automorphism on $(G, \cdot)$" iff ϕ is an isomorphism from $(G, \cdot)$ to $(G, \cdot)$.

Example 2.6.4 (Examples of automorphisms)**.**

(a) *For any group* $(G, \cdot)$*, identity map and conjugation by any element are automorphisms on it.*

(b) $A \mapsto (A^t)^{-1}$ *is an automorphism on* $(\mathrm{GL}_n(\mathbb{F}), \textit{matrix multiplication})$ *for each* $n \geq 1$*.*

(c) There are 6 automorphisms on $(S_3, \circ)$.

Proposition 2.6.5 ($x \mapsto x^2$ on finite groups)**.** *Let $(G, \cdot)$ be a finite group and $\phi\colon G \times G \to G$ such that $\phi(x) = \mathrm{Iter}_{\cdot,2}(x)$ for each $x \in G$. Then ϕ is an automorphism on $(G, \cdot) \iff (G, \cdot)$ is an abelian group and there is no a such that a has order 2 in $(G, \cdot)$.*

Definition 2.6.6 (Isomorphic groups)**.** "$(G, \cdot)$ and $(G', *)$ are isomorphic groups" iff there exists a ϕ such that ϕ is an isomorphism from $(G, \cdot)$ to $(G', *)$.

Proposition 2.6.7 (Isomorphic cyclic groups)**.** *Let $(G, \cdot)$ and $(G', *)$ be cyclic groups such that one of the following holds:*

(a) G and G' are finite sets such that $\#(G) = \#(G')$.
(b) G and G' are infinite sets.

Then $(G, \cdot)$ and $(G', *)$ are isomorphic groups.

Proposition 2.6.8 (Homomorphisms between cyclic groups)**.** *Let ϕ be a homomorphism from $(G, \cdot)$ to $(G', *)$, and $a \in G$ such that $\langle a \rangle_{\cdot} = G$. Then the following hold:*

(a) ϕ is a surjection $\iff \langle \phi(a) \rangle_{\cdot} = G'$.
(b) If G is a finite set, then
  - *(i) ϕ is injective $\iff$ ϕ is surjective, and*
  - *(ii) ϕ is injective and $\#(G) \geq 2 \implies \phi(a) \neq \mathrm{Id}_*$.*

(c) If G is an infinite set, then
  - *(i) ϕ is injective $\iff \phi(a) \neq \mathrm{Id}_*$, and*
  - *(ii) ϕ is surjective $\implies$ ϕ is injective.*

Definition 2.6.9 (Semigroups, their generators and their isomorphisms)**.** "$(S, \cdot)$ is a semigroup" iff $\cdot$ on S has an identity and is associative.

"s is a generator of the semigroup $(S, \cdot)$" iff $(S, \cdot)$ is a semigroup and $S = \{\mathrm{IterId}_{\cdot,m}(s) : m \geq 0\}$.

"ϕ is a semigroup isomorphism from $(S, \cdot)$ to $(S', *)$" iff $\phi\colon S \to S'$ is a bijection and $\phi(a \cdot b) = \phi(a) * \phi(b)$ for all $a, b \in S$.

"$(S, \cdot)$ and $(S', *)$ are isomorphic semigroups" iff there exists a ϕ such that ϕ is a semigroup isomorphism from $(S, \cdot)$ to $(S', *)$.

Lemma 2.6.10. *Let s be a generator of the semigroup $(S, \cdot)$ and S be a finite set. Set $n := \#(S)$. Then*

(a) $S = \{\text{IterId}_{\cdot,m}(s) : 0 \le m < n\}$,
(b) $\text{IterId}_{\cdot,n}(s) = \text{Id}_{\cdot} \iff (S, \cdot)$ *is a group,*
(c) $\text{IterId}_{\cdot,n}(s) = \text{IterId}_{\cdot,i}(s)$ *for some* $2 \le i < n$ *and* t *is a generator of the semigroup* $(S, \cdot) \implies s = t$, *and*
(d) $\text{IterId}_{\cdot,n}(s) = s$ *and* t *is a generator of the semigroup* $(S, \cdot) \implies \text{IterId}_{\cdot,n}(t) = t$.

Proposition 2.6.11 (Classification of semigroups generated by single element)**.** *Let* s, t *be generators of semigroups* $(S, \cdot)$, $(S', *)$. *Then*

(a) S, T *have* n *elements and* $0 \le i < j = n$ *such that* $\text{IterId}_{\cdot,n}(s) = \text{IterId}_{\cdot,i}(s)$ *and* $\text{IterId}_{*,n}(t) = \text{IterId}_{*,j}(t) \implies (S, \cdot)$ *and* $(S', *)$ *are not isomorphic semigroups, and*
(b) S *is an infinite set* $\implies (S, \cdot)$ *and* $(\mathbb{N}, +)$ *are isomorphic semigroups.*

Proposition 2.6.12 (Finite semigroups with cancellation)**.** *Let* $(S, \cdot)$ *be a semigroup such that* S *is a finite set and for all* $a, b \in S$ *let* $a \cdot b = a \cdot c \implies b = c$ *hold. Then* $(S, \cdot)$ *is a group.*

2.7 Equivalence relations and partitions

November 3, 2021

Definition 2.7.1 (Relation induced by conjugation)**.** "R is the relation on $(G, \cdot)$ induced by conjugation" iff $(G, \cdot)$ is a group and $R = \{(a, b) \in G \times G : b = g \cdot a \cdot \text{Inv}_{\cdot}(g) \text{ for some } g \in G\}$.

Proposition 2.7.2 (Conjugation is an equivalence relation)**.** *Let* R *be the relation on* $(G, \cdot)$ *induced by conjugation. Then* R *is an equivalence relation on* G.

Definition 2.7.3 (Relations and partitions induced by functions)**.** "R is the relation on X induced by $f \colon X \to Y$" iff $f \colon X \to Y$ and $R = \{(a, b) \in X \times X : f(a) = f(b)\}$.

"$\mathcal{C}$ is the partition induced by $f \colon X \to Y$" iff $f \colon X \to Y$ and $\mathcal{C} = \{f^{-1}[\{y\}] : y \in Y\} \setminus \{\emptyset\}$.

Proposition 2.7.4 (Equivalence relations induced by functions)**.** *Let* R *be the relation on* X *and* $\mathcal{C}$ *be the partition, both induced by* $f \colon X \to Y$ *and let* $x \in X$. *Then*

(a) R *is an equivalence relation on* X *and* $\mathcal{C} = \{[x]_R : x \in R\}$,
(b) $[x]_R = f^{-1}[\{f(x)\}]$, *and*
(c) *there exists a unique function* $g\colon f[X] \to \mathcal{C}$ *such that* $g(y) = f^{-1}[\{y\}]$ *for all* $y \in f[X]$*; further, any such function* g *is a bijection.*

Corollary 2.7.5 (Partitions induced by homomorphisms)**.** *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$*, and* $\mathcal{C}$ *be the partition induced by* $\phi\colon G \to G'$*, and* $f \in \mathcal{C}$*, and* $a \in G$ *such that* $a \in f$ *and set* $K := \ker_*(\phi)$*. Then*

(a) $f = \operatorname{coset}(a \cdot K)$*, and*
(b) $\mathcal{C} = \{\operatorname{coset}(a \cdot K) : a \in G\}$.

2.8 Cosets

November 4, 2021

Remark 2.8.1. We'll work with only left cosets. Analogues of all the results also hold for right cosets.

Proposition 2.8.2 (Cosets of a subgroup form a partition)**.** *Let* H *be a subgroup of* $(G, \cdot)$ *and set* $R := \{(a, b) \in G \times G : \operatorname{Inv.}(a) \cdot b \in H\}$ *and* $\mathcal{C} := \{\operatorname{coset}(a \cdot H) : a \in G\}$*. Then* R *is an equivalence relation on* G *and* $\mathcal{C} = \{[x]_R : x \in G\}$*, and* $[a]_R = \operatorname{coset}(a \cdot H)$ *for all* $a \in G$.

Proposition 2.8.3 (A condition for a set to be subgroup)**.** *Let* $(G, \cdot)$ *be a group and* $S \subseteq G$ *such that* $1 \in S$ *and* $\{\{a \cdot x : x \in S\} : a \in G\}$ *is a partition of* G*. Then* S *is a subgroup of* $(G, \cdot)$.

Lemma 2.8.4 (Cosets of a subgroup are equinumerous)**.** *Let* H *be a subgroup of* $(G, \cdot)$ *and* $a \in G$*. Then there exists a bijection from* H *to* $\operatorname{coset}(a \cdot H)$.

Abbreviation 2.8.5 (Index of subgroups)**.** For any subgroup H of $(G, \cdot)$, such that $A := \{\operatorname{coset}(a \cdot H) : a \in G\}$ is a finite set, we set $[(G, \cdot) : H] := \#(A)$.

Proposition 2.8.6 (Intersection of finite index subgroups)**.** *Let* H*,* K *be subgroups of* $(G, \cdot)$ *such that* $\{\operatorname{coset}(a \cdot H) : a \in G\}$ *and* $\{\operatorname{coset}(a \cdot K) : a \in G\}$ *are finite sets. Then* $\{\operatorname{coset}(a \cdot (H \cap K)) : a \in G\}$ *is a finite set.*

Corollary 2.8.7. *Let* H *be a subgroup of* $(G, \cdot)$ *such that* $[(G, \cdot) : H] = 2$*. Then* H *is a normal subgroup of* $(G, \cdot)$.

Corollary 2.8.8 (Counting formula)**.** *Let H be a subset of a group $(G, \cdot)$ such that G is a finite set. Then H and $\{\mathrm{coset}(a \cdot H) : a \in G\}$ are finite sets, and $\#(G) = [(G, \cdot) : H]\#(H)$.*

Theorem 2.8.9 (Lagrange's theorem)**.** *Let H be a subset of $(G, \cdot)$ such that G is a finite set. Then H is a finite set and $\#(H)$ divides $\#(G)$.*

Corollary 2.8.10 (Order divides $\#(G)$)**.** *Let a have order n in $(G, \cdot)$ such that G is a finite set. Then n divides $\#(G)$.*

Corollary 2.8.11 (Groups with prime number of elements)**.** *Let $(G, \cdot)$ be a group, and $a \in G \setminus \{\mathrm{Id.}\}$, and $p > 0$ be prime such that G has p elements. Then a has order p in $(G, \cdot)$ and $\langle a \rangle_{\cdot} = G$.*

Proposition 2.8.12 (Groups with prime-power number of elements)**.** *Let $(G, \cdot)$ be a group, and $p > 0$ be prime and $k \geq 1$ such that G has p^k elements. Then*

(a) there exists an a such that a has order p in $(G, \cdot)$, and
(b) if there exists exactly one subgroup H of $(G, \cdot)$ such that H contains p elements, then there exists an a such that a has order p^l for some $1 < l \leq k$.

Proposition 2.8.13 (Groups with prime-product elements)**.** *Let $(G, \cdot)$ be a group and $p, q \geq 2$ be primes such that G has pq elements. Let $x, y \in G$ such that $x \neq \mathrm{Id.}$ and $y \notin \langle a \rangle_{\cdot}$, and let H be a subgroup of $(G, \cdot)$ such that $x, y \in H$. Then $H = G$.*

Example 2.8.14 (Subgroups of S_3)**.** *The subgroups of $(\mathrm{S}_3, \circ)$ are $\langle 1 \rangle$, $\langle x \rangle$, $\langle y \rangle$, $\langle xy \rangle$, $\langle x^2 y \rangle$ and S_3.*

Proposition 2.8.15 (Groups with 35 elements)**.** *Let $(G, \cdot)$ be a group such that G has 35 elements. Then there exist $a, b \in G$ such that a, b have orders 5, 7 in $(G, \cdot)$.*

Corollary 2.8.16 (Counting formula for homomorphisms)**.** *Let ϕ be a homomorphism from $(G, \cdot)$ to $(G', *)$ and set $K := \ker_*(\phi)$. Then*

(a) there exists a bijection from $\{\mathrm{coset}(a \cdot K) : a \in G\}$ to $\phi[G]$, and
(b) G and $\phi[G]$ are finite sets $\implies$ K is a finite set and $\#(G) = \#(K)\#(\phi[G])$.

Example 2.8.17 (Half of S_n is even)**.** *Let $n \geq 2$. Then $\#(\mathrm{A}_n) = n!/2$.*

Lemma 2.8.18. *Let $f\colon X \to Y$ and $f[X]$ have n elements. Then there exists a function $x\colon \{1, \cdots, n\} \to X$ such that $f[X] = x[\{1, \cdots, n\}]$.*

Lemma 2.8.19. *Let H be a subgroup of $(G, \cdot)$, and $A \subseteq G$ such that $\bigcup_{a \in A} \operatorname{coset}(a \cdot H)$ is a subgroup of $(G, \cdot)$. Then $\operatorname{coset}\big(g \cdot \big(\bigcup_{a \in A} \operatorname{coset}(a \cdot H)\big)\big) = \bigcup_{a \in A} \operatorname{coset}((g \cdot a) \cdot H)$.*

Proposition 2.8.20 (Indices are multiplicative)**.** *Let H, K be subgroups of $(G, \cdot)$ such that G is a finite set and $K \subseteq H$. Then K is a subgroup of $(H, \cdot_H)$, and $\{\operatorname{coset}(a \cdot K) : a \in G\}$ and $\{\operatorname{coset}(a \cdot H) : a \in G\}$ and $\{\operatorname{coset}(b \cdot_H H) : b \in H\}$ are finite sets and $[(G, \cdot) : K] = [(G, \cdot) : H][(H, \cdot_H) : K]$.*

Lemma 2.8.21 (Sufficient conditions for a group being finite)**.** *Let $(G, \cdot)$, $(G', *)$ be groups. Then G is a finite set if one of the following holds:*

- *(a) There exists a subgroup H of $(G, \cdot)$ such that H and $\{\operatorname{coset}(a \cdot H) : a \in G\}$ are finite sets.*
- *(b) There exists a homomorphism ϕ from $(G, \cdot)$ to $(G', *)$ such that $\ker_*(\phi)$ and $\phi[G]$ are finite sets.*
- *(c) There exist subgroups H, K of $(G, \cdot)$ such that $K \subseteq H$, and K and $\{\operatorname{coset}(a \cdot H) : a \in G\}$ and $\{\operatorname{coset}(b \cdot K) : b \in H\}$ are finite sites.*

Lemma 2.8.22. *Let H be a subgroup of $(G, \cdot)$ and $g, g' \in G$ such that $\operatorname{coset}(g \cdot H) = \operatorname{coset}(H \cdot g')$. Then $\operatorname{coset}(g \cdot H) = \operatorname{coset}(g' \cdot H)$ and $\operatorname{coset}(H \cdot g) = \operatorname{coset}(H \cdot g')$.*

Proposition 2.8.23 (Equivalent conditions for a normal subgroup)**.** *Let H be a subgroup of $(G, \cdot)$. Then the following are equivalent:*

- *(a) H is a normal subgroup of $(H, \cdot)$.*
- *(b) $\operatorname{conj}_{\cdot, g}[H] = H$ for all $g \in G$.*
- *(c) $\operatorname{coset}(g \cdot H) = \operatorname{coset}(H \cdot g)$ for all $g \in G$.*
- *(d) For each $g \in G$, there exists a $g' \in G$ such that $gH = Hg'$.*

Corollary 2.8.24. *Let $n \geq 1$ and H be the unique subgroup of $(G, \cdot)$ such that $\#(H) = n$. Then H is a normal subgroup of $(G, \cdot)$.*

2.9 Modular arithmetic

November 7, 2021

Abbreviation 2.9.1 ($\mathbb{Z}/\mathbb{Z}n$)**.** For any $n \in \mathbb{Z}$, we set $\mathbb{Z}/\mathbb{Z}n := \{\operatorname{coset}(a + \mathbb{Z}n) : a \in \mathbb{Z}\}$.

Definition 2.9.2 (Equality mod n)**.** We write "$a \equiv b \mod n$" iff $a, b \in \mathbb{Z}$ and n divides $a - b$.

Proposition 2.9.3 (mod n equivalence relation)**.** *Let $n \in \mathbb{Z}$ and set $R := \{(a,b) \in \mathbb{Z} \times \mathbb{Z} : a \equiv b \mod n\}$. Then R is an equivalence relation on $\mathbb{Z}$, and $\mathbb{Z}/\mathbb{Z}n = \{[a]_R : a \in \mathbb{Z}\}$, and $[a]_R = \operatorname{coset}(a + \mathbb{Z}n)$ for each $a \in \mathbb{Z}$.*

Proposition 2.9.4 (Cardinality of $\mathbb{Z}/\mathbb{Z}n$)**.** *Let $n \geq 1$. Then $\mathbb{Z}/\mathbb{Z}n = \{\operatorname{coset}(a + \mathbb{Z}n) : 0 \leq a < n\}$ and $\operatorname{coset}(a + \mathbb{Z}n)$'s are distinct for each $0 \leq a < n$.*

Lemma 2.9.5 (Sum and products of equivalent integers)**.** *Let $n \in \mathbb{Z}$, and $a \equiv a' \mod n$ and $b \equiv b' \mod n$. Then $a + b \equiv a' + b' \mod n$ and $ab \equiv a'b' \mod n$.*

Corollary 2.9.6 (Operations on $\mathbb{Z}/\mathbb{Z}n$)**.** *Let $n \in \mathbb{Z}$ and $A, B \in \mathbb{Z}/\mathbb{Z}n$. Then there exist unique $C, D \in \mathbb{Z}/\mathbb{Z}n$ such that for all $a, b \in \mathbb{Z}$ so that $A = \operatorname{coset}(a + \mathbb{Z}n)$ and $B = \operatorname{coset}(b + \mathbb{Z}n)$, we have $C = \operatorname{coset}((a + b) + \mathbb{Z}n)$ and $D = \operatorname{coset}((ab) + \mathbb{Z}n)$.*

Remark 2.9.7. This allows to denote C and D by $A +_n B$ and $A \cdot_n B$. (Since sets (here as cosets) are not functions (here as matrices), no notational collision.)

Corollary 2.9.8. *Let $n \in \mathbb{Z}$ and $a, b \in \mathbb{Z}$. Then $(\operatorname{coset}(a + \mathbb{Z}n)) +_n (\operatorname{coset}(b + \mathbb{Z}n)) = \operatorname{coset}((a + b) + \mathbb{Z}n)$ and $(\operatorname{coset}(a + \mathbb{Z}n)) \cdot_n (\operatorname{coset}(b + \mathbb{Z}n)) = \operatorname{coset}((ab) + \mathbb{Z}n)$.*

Corollary 2.9.9 ($\mathbb{Z}/\mathbb{Z}n$ forms a ring)**.** *Let $n \in \mathbb{Z}$ and $A, B, C \in \mathbb{Z}/\mathbb{Z}n$. Then*

$$\begin{aligned}
(A +_n B) +_n C &= A +_n (B +_n C), \\
A +_n B &= B +_n A, \\
A +_n \operatorname{coset}(0 + \mathbb{Z}n) &= A, \\
A +_n D &= \operatorname{coset}(0 + \mathbb{Z}n) \text{ for some } D \in \mathbb{Z}/\mathbb{Z}n, \\
(A \cdot_n B) \cdot_n C &= A \cdot_n (B \cdot_n C), \\
A \cdot_n B &= B \cdot_n A, \\
A \cdot_n \operatorname{coset}(1 + \mathbb{Z}n) &= A, \text{ and} \\
A \cdot_n (B +_n C) &= (A \cdot_n B) +_n (A \cdot_n C).
\end{aligned}$$

Proposition 2.9.10. *Let $n \in \mathbb{Z}$. Then $2a \equiv 1 \mod n$ for some $a \in Z \iff n$ is odd.*

Example 2.9.11. *Let $n \geq 0$ and $a \colon \{0, \dots, n\} \to \{0, \dots, 9\}$. Then $(a_0 10^0 + \dots + a_n 10^n) \equiv (a_0 + \dots + a_n) \mod 9$.*

Proposition 2.9.12 (Chinese remainder theorem)**.** *Let $a, b, u, v \in \mathbb{Z}$ such that not both of a, b are zero and $\gcd(a, b) = 1$. Then there exists an $x \in Z$ such that $x \equiv u \mod a$ and $x \equiv v \mod b$.*

Abbreviation 2.9.13 ($a \bmod b$)**.** For any $a, b \in \mathbb{Z}$ such that $b \neq 0$, we set $a \bmod b :=$ remainder on dividing a by b.

Proposition 2.9.14 (Properties of $a \bmod b$)**.** *Let $n, a, b \in \mathbb{Z}$ such that $n \neq 0$. Then*

(a) $a \bmod n = b \bmod n \iff a \equiv b \mod n$,
(b) $a \equiv (a \bmod n) \mod n$, *and hence* $(a \bmod n) \bmod n = a \bmod n$,
(c) $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$, *and*
(d) $(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$.

Corollary 2.9.15. *Let $n, k \in \mathbb{Z}$ such that $n \neq 0$ and $k \geq 0$ and $a \colon \{1, \dots, n\} \to \mathbb{Z}$. Then*

(a) $(a_1 + \dots + a_k) \bmod n = ((a_1 \bmod n) + \dots + (a_k \bmod n)) \bmod n$, *and*
(b) $(a_1 \cdots a_k) \bmod n = ((a_1 \bmod n) \cdots (a_k \bmod n)) \bmod n$.

Lemma 2.9.16. *Let $n, a \in \mathbb{Z}$ such that $n \neq 0$. Then $\operatorname{coset}((a \bmod n) + \mathbb{Z}n) = \operatorname{coset}(a + \mathbb{Z}n)$.*

Example 2.9.17 (Ring isomorphism between $\mathbb{Z}/\mathbb{Z}n$ and $\{0, \dots, n-1\}$)**.** *Let $n \geq 1$. Then $a \mapsto \operatorname{coset}(a + \mathbb{Z}n)$ is an isomorphism from $(\{0, \dots, n-1\}, \text{addition} \bmod n)$ to $(\mathbb{Z}/\mathbb{Z}n, +_n)$. Also, for any $0 \leq a, b < n$, we have $\operatorname{coset}((ab \bmod n) + \mathbb{Z}n) = \operatorname{coset}(a + \mathbb{Z}n) \cdot_n \operatorname{coset}(b + \mathbb{Z}n)$*

Corollary 2.9.18 ($\mathbb{Z}/\mathbb{Z}n$ is cyclic)**.** *Let $n \in \mathbb{Z}$. Then $(\mathbb{Z}/\mathbb{Z}n, +_n)$ is a cyclic group.*

Example 2.9.19 (Automorphisms on $\mathbb{Z}/\mathbb{Z}n$)**.** *Let $n \geq 1$. Set $\mathcal{G} := (\{0, \dots, n-1\}, \text{addition} \bmod n)$ and ϕ be a homomorphism from $\mathcal{G}$ to $\mathcal{G}$. Then ϕ is an automorphism on $\mathcal{G} \iff \gcd(\phi(1), n) = 1$.*

Example 2.9.20 (Order of a k-cycle)**.** *Let $1 \leq k \leq n$ and $l \geq 1$. Then*

(a) *for all* $1 \le i \le n$, *we have* $((1 \cdots k)_n)^l(i) = \begin{cases} ((i + l - 1) \bmod k) + 1, & i \le k \\ i, & i > k \end{cases}$,
and

(b) *order of* $(1 \cdots k)_n$ *in* $(S_n, \circ)$ *is* k.

2.10 The correspondence theorem

November 9, 2021

Lemma 2.10.1 (Restriction of a homomorphism)**.** *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$ *and* H *be a subgroup of* $(G, \cdot)$. *Then* $\phi \circ \iota_{H \to G}$ *is a homomorphism from* $(H, \cdot_H)$ *to* $(G', *)$, *and* $\ker_*(\phi \circ \iota_{H \to G}) = (\ker_*(\phi)) \cap H$.

Proposition 2.10.2. *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$ *and* H *be a subgroup of* $(G, \cdot)$ *such that* H *and* G' *are finite sets and* $\gcd(\#(H), \#(G')) = 1$. *Then* $H \subseteq \ker_*(\phi)$.

Example 2.10.3 (Subgroups of S_n with odd cardinality)**.** *Let* $n \in \mathbb{N}$ *and* H *be a subgroup of* $(\mathrm{S}_n, \circ)$ *such that* $\#(H)$ *is odd. Then* $H \subseteq \mathrm{A}_n$

Proposition 2.10.4 (Inverse images of subgroups under homomorphisms)**.** *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$ *and* H' *be a subgroup of* $(G', *)$. *Then*

(a) $\ker_*(\phi) \subseteq \phi^{-1}[H']$,

(b) $\phi^{-1}[H']$ *is a subgroup of* $(G, \cdot)$,

(c) H' *is a normal subgroup of* $(G', *)$ $\implies$ $\phi^{-1}[H']$ *is a normal subgroup of* $(G, \cdot)$, *and*

(d) ϕ *is surjective and* $\phi^{-1}[H']$ *is a normal subgroup of* $(G, \cdot)$ $\implies$ H' *is a normal subgroup of* $(G', *)$.

Lemma 2.10.5. *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$ *and* $H' \subseteq G'$ *such that* ϕ *is a surjection and* $\phi^{-1}[H']$ *is a subgroup of* $(G, \cdot)$. *Then* H' *is a subgroup of* $(G', *)$.

Theorem 2.10.6 (Correspondence theorem)**.** *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$ *such that* ϕ *is surjective, and let* H, H' *be subgroups of* $(G, \cdot)$, $(G', *)$ *such that* $\ker_*(\phi) \subseteq H$. *Set* $K := \ker_*(\phi)$. *Then the following hold:*

(a) (i) $\phi[H]$ *is a subgroup of* $(G', *)$.

(ii) $\phi^{-1}[H']$ *is a subgroup of* $(G,\cdot)$ *and* $K \subseteq \phi^{-1}[H']$.

(b) $\phi^{-1}[\phi[H]] = H$ *and* $\phi[\phi^{-1}[H']] = H'$.

(c) (i) H *is a normal subgroup of* $(G,\cdot) \iff \phi[H]$ *is a normal subgroup of* $(G',*)$.

(ii) H' *is a normal subgroup of* $(G',*) \iff \phi^{-1}[H']$ *is a normal subgroup of* $(G,\cdot)$.

(d) (i) H *is a finite set* $\iff \phi[H]$ *and* K *are finite sets.*

(ii) $\phi^{-1}[H']$ *is a finite set* $\iff H'$ *and* K *are finite sets.*

(e) (i) H, K, $\phi[H]$ *are finite sets* $\implies \#(H) = \#(\phi[H])\#(K)$.

(ii) $\phi^{-1}[H']$, K, H' *are finite sets* $\implies \#(\phi^{-1}[H']) = \#(H')\#(K)$.

(f) (i) *There exists a bijection between* $\{\mathrm{coset}(a\cdot H) : a \in G\}$ *and* $\{\mathrm{coset}(a' * \phi[H]) : a' \in G'\}$.

(ii) *There exists a bijection between* $\{\mathrm{coset}(a\cdot \phi^{-1}[H']) : a \in G\}$ *and* $\{\mathrm{coset}(a' * H') : a' \in G'\}$.

2.11 Product groups

November 11, 2021

Lemma 2.11.1. *Let* $(G,\cdot)$, $(G',*)$ *be groups. Then there exists a unique function* $f\colon (G\times G')\times(G\times G') \to (G\times G')$ *such that* $f(((a,a'),(b,b'))) = (a\cdot b, a'*b')$ *for all* $a,b\in G$ *and for all* $a',b'\in G'$.

Remark 2.11.2. This allows to denote f by $\binom{\mathrm{P}}{\cdot,*}$.

Proposition 2.11.3 (Product groups)**.** *Let* $(G,\cdot)$, $(G',*)$ *be groups. Set* $\star := \binom{P}{\cdot,*}$ *Then*

(a) $(a,a')\star(b,b') = (a\cdot b, a'*b')$ *for all* $a,b\in G$ *and all* $a',b'\in G'$,

(b) $(G\times G',\star)$ *is a group,*

(c) $\mathrm{Id}_\star = (\mathrm{Id}_\cdot, \mathrm{Id}_*)$, *and*

(d) $\mathrm{Inv}_\star((a,a')) = (\mathrm{Inv}_\cdot(a), \mathrm{Inv}_*(a'))$ *for all* $a\in G$ *and all* $a'\in G'$.

Proposition 2.11.4 (Orders in product groups)**.** *Let* x, y *have rders* r, s *in* $(G,\cdot)$, $(G',*)$. *Then* (x,y) *has order* rs *in* $(G\times G', \binom{P}{\cdot,*})$.

Proposition 2.11.5 (Product of subgroups)**.** *Let* H *be a subgroup of* $(G,\cdot)$ *and* H' *be a subgroup of* $(G',*)$. *Then* $H\times H'$ *is a subgroup of* $(G\times G', \binom{P}{\cdot,*})$.

Proposition 2.11.6 (Product of isomorphic groups)**.** *Let* $(G,\cdot)$, $(G',\cdot')$ *and* $(H,*)$, $(H',*')$ *be isomorphic groups. Then* $\big(G\times H, \binom{P}{\cdot,*}\big)$ *and* $\big(G'\times H', \binom{P}{\cdot',*'}\big)$ *are isomorphic groups.*

Proposition 2.11.7 (Factors of a product group)**.** *Let* $(G, \cdot)$*,* $(G', *)$ *be groups. Set* $\star := \binom{P}{\cdot,*}$*. Then*

(a) *(i)* $(G, \cdot)$ *and* $\big(G \times \{\mathrm{Id}_*\}, \star_{G \times \{\mathrm{Id}_*\}}\big)$ *are isomorphic,*
(ii) $(G', *)$ *and* $\big(\{\mathrm{Id.}\} \times G', \star_{\{\mathrm{Id.}\} \times G'}\big)$ *are isomorphic,*

(b) *(i)* $\pi_{G \times G' \to G}$ *is a homomorphism from* $(G \times G', \star)$ *to* $(G, \cdot)$ *and* $\ker.(\pi_{G \times G' \to G}) = \{\mathrm{Id.}\} \times G'$*, and*
(ii) $\pi_{G \times G' \to G'}$ *is a homomorphism from* $(G \times G', \star)$ *to* $(G', *)$ *and* $\ker_*(\pi_{G \times G' \to G'}) = G \times \{\mathrm{Id}_*\}$*.*

Proposition 2.11.8 (Center of a product group)**.** *Let* Z*,* Z' *be centers of* $(G, \cdot)$*,* $(G', *)$*. Then* $Z \times Z'$ *is the center of* $(G \times G', \binom{P}{\cdot,*})$*.*

Proposition 2.11.9 (Products of cyclic groups with co-prime cardinalities)**.** *Let* $(G, \cdot)$*,* $(G', *)$ *be cyclic groups such that* G*,* G' *are finite sets and* $\#(G)$*,* $\#(G')$ *are co-primes. Then* $(G \times G', \binom{P}{\cdot,*})$ *is a cyclic group.*

Proposition 2.11.10 ($C_2 \times C_2$ is not cyclic)**.** *Let* $(G, \cdot)$ *be a cyclic group such that* G *is a finite set and* $\#(G) = 2$*. Then* $(G \times G, \binom{P}{\cdot,\cdot})$ *is not a cyclic group.*

Proposition 2.11.11 (Product of infinite cyclic groups)**.** $(\mathbb{Z} \times \mathbb{Z}, \binom{P}{+,+})$ *is not a cyclic group.*

Proposition 2.11.12 (Properties of product groups)**.** *Let* H*,* K *be subgroups of* $(G, \cdot)$ *and* $f \colon H \times K \to G$ *such that* $f((h, k)) = h \cdot k$ *for all* $h \in H$ *and all* $k \in K$*. Then*

(a) f *is injective* $\iff$ $H \cap K = \mathrm{Id.}$*,*

(b) f *is a homomorphism from* $\Big(H \times K, \binom{P}{\cdot,\cdot}_{H \times K}\Big)$ *to* $(G, \cdot)$ $\iff$ $hk = kh$ *for all* $h \in H$ *and all* $k \in K$*,*

(c) H *is a normal subgroup of* $(G, \cdot)$ $\implies$ $f[H \times K]$ *is a subgroup of* $(G, \cdot)$*, and*

(d) f *is an isomorphism from* $\Big(H \times K, \binom{P}{\cdot,\cdot}_{H \times K}\Big)$ *to* $(G, \cdot)$ $\iff$ *the following hold:*
(i) $H \cap K = \{\mathrm{Id.}\}$*.*
(ii) $f[H \times K] = G$*.*
(iii) H*,* K *are normal subgroups of* $(G, \cdot)$*.*

Proposition 2.11.13 (Classification of groups with cardinality 4)**.** *Let* $(G, \cdot)$ *be a finite group such that* $\#(G) = 4$*. Then exactly one of the following holds:*

(a) *$(G, \cdot)$ is a cyclic group.*
(b) *There exists a cyclic group $(H, *)$ such that H is a finite set with $\#(H) = 2$ and $(G, \cdot)$ is isomorphic to $\big(H \times H, \binom{P}{*,*}\big)$.*

Example 2.11.14 (A condition for the group to contain an element of prime-product order)**.** *Let $p, q \geq 2$ be primes such that $p \neq q$. Let x, y have orders p, q in $(G, \cdot)$ such that $\langle x \rangle_\cdot$, $\langle y \rangle_\cdot$ are normal subgroups of $(G, \cdot)$. Set $\star := \binom{P}{\cdot,\cdot}$ and $H := \langle x \rangle_\cdot \times \langle y \rangle_\cdot$ and $K := \{a \cdot b : a \in \langle x \rangle_\cdot, b \in \langle y \rangle_\cdot\}$. Then*
(a) *K is a subgroup of $(G, \cdot)$,*
(b) *$(a, b) \mapsto a \cdot b$ is an isomorphism from $(H, \star_H)$ to $(K, \cdot_K)$, and*
(c) *$x \cdot y$ has order pq in $(G, \cdot)$.*

Example 2.11.15. *Let H be a subgroup of $(G, \cdot)$ and ϕ be a homomorphism from $(G, \cdot)$ to $(H, \cdot_H)$ such that $\phi \circ \iota_{H \to G} = \iota_{H \to H}$. Then $(a, b) \mapsto a \cdot b$ is a bijection from $H \times \ker_{\cdot_H}(\phi)$ to G.*

2.12 Quotient groups

November 11, 2021

Abbreviation 2.12.1 (Quotient set)**.** For a normal subgroup N of $(G, \cdot)$, we set $(G, \cdot)/N := \{\operatorname{coset}(a \cdot N) : a \in G\}$.

Lemma 2.12.2 (Operation on quotient sets)**.** *Let N be a normal subgroup of $(G, \cdot)$. Then there exists a unique function $f\colon ((G, \cdot)/N) \times ((G, \cdot)/N) \to (G, \cdot)/N$ such that $f((\operatorname{coset}(a \cdot N), \operatorname{coset}(b \cdot N))) = \operatorname{coset}((a \cdot b) \cdot N)$ for all $a, b \in G$.*

Remark 2.12.3. This allows to denote f by $\binom{\mathrm{Q}}{\cdot,N}$.

Proposition 2.12.4 (Operation on quotient groups coincides with product of cosets)**.** *Let N be a normal subgroup of $(G, \cdot)$. Set $\star := \binom{Q}{\cdot,N}$. Then for any $A, B \in (G, \cdot)/N$, we have $A \star B = \{a \cdot b : A \in A, b \in B\}$.*

Proposition 2.12.5 (Only normal groups form quotient groups)**.** *Let H be a subgroup of $(G, \cdot)$ such that H is not a normal subgroup of $(G, \cdot)$. Then there exist $x, y \in G$ such that $\{a \cdot b : a \in \operatorname{coset}(x \cdot H), b \in \operatorname{coset}(y \cdot H)\} \neq \operatorname{coset}(z \cdot H)$ for any $z \in G$.*

Proposition 2.12.6 (Quotient groups)**.** *Let N be a normal subgroup of $(G, \cdot)$. Set $\star := \binom{Q}{\cdot,N}$. Then* *(a)* $\operatorname{coset}(a \cdot N) \star \operatorname{coset}(b \cdot N) = \operatorname{coset}((a \cdot b) \cdot N)$ *for all* $a, b \in G$,

(b) $((G, \cdot)/N, \star)$ *is a group,*

(c) $\mathrm{Id}_\star = N$, *and*

(d) $\mathrm{Inv}_\star(\operatorname{coset}(a \cdot N)) = \operatorname{coset}(\mathrm{Inv}.(a) \cdot N)$ *for each* $a \in G$.

Example 2.12.7. *Let* $n \geq 2$. *Set* $H := \{A \in \mathrm{GL}_n(\mathbb{F}) : A$ *is upper triangular with diagonal ent* *and* $K := \{\mathcal{E}_{\mathbb{F},n;1\to 1+cn} : c$ *is a scalar*$\}$. *Let* $A, B \in H$. *Then*

(a) H *is a subgroup of* $(\mathrm{GL}_n(\mathbb{F}),$ *matrix multiplication*$)$,

(b) K *is a normal subgroup of* $(H,$ *matrix multiplication*$)$,

(c) A, B *lie in some same coset of* $K \iff A$, B *(possibly) differ only in* $(1, n)$*-th entry, and*

(d) K *is the center of* H.

Proposition 2.12.8 (A condition for a subset to be a normal subgroup)**.** *Let* $(G, \cdot)$ *be a group and* P *be a partition of* G *such that for any* $A, B \in P$, *there exists a* $C \in P$ *such that* $\{a \cdot b : a \in A, b \in B\} \subseteq C$. *Let* $N \in P$ *such that* $1 \in N$. *Then*

(a) N *is a normal subgroup of* $(G, \cdot)$, *and*

(b) $P = \{\operatorname{coset}(a \cdot N) : a \in G\}$.

Corollary 2.12.9. *Let* N *be a normal subgroup of* $(G, \cdot)$ *and* $\phi \colon G \to (G, \cdot)/N$ *such that* $\phi(a) = \operatorname{coset}(a \cdot N)$ *for all* $a \in G$. *Set* $\star := \binom{Q}{\cdot, N}$. *Then*

(a) ϕ *is a surjection,*

(b) ϕ *is a homomorphism from* $(G, \cdot)$ *to* $((G, \cdot)/N, \star)$,

(c) $\ker_\star(\phi) = N$, *and*

(d) *for all* $a, b \in G$ *such that* $a \cdot b \in N$, *we have* $\phi(a) \star \phi(b) = N$.

Theorem 2.12.10 (First isomorphism theorem)**.** *Let* ϕ *be a homomorphism from* $(G, \cdot)$ *to* $(G', *)$ *such that* ϕ *is surjective. Set* $K := \ker_*(\phi)$. *Then there exists a unique function* $\psi \colon (G, \cdot)/N \to G'$ *such that* $\psi(\operatorname{coset}(a \cdot K)) = \phi(a)$ *for all* $a \in G$. *Further, any such function* ψ *is an isomorphism from* $\big((G, \cdot)/N, \binom{Q}{\cdot, K}\big)$ *to* $(G', *)$.

Chapter 3

Vector spaces

3.2 Fields

November 23, 2021

Definition 3.2.1 (Fields)**.** "$(F, +, \cdot)$ is a field" iff each of the following hold:

(a) $(F, +)$ is an abelian group.
(b) $\cdot\colon F \times F \to F$.
(c) $a \cdot b \in F \setminus \{\mathrm{Id}_+\}$ for all $a, b \in F \setminus \{\mathrm{Id}_+\}$.
(d) $(F \setminus \{\mathrm{Id}_+\}, \cdot_F)$ is an abelian group.
(e) $a \cdot (b + c) = (a \cdot b) + (a \cdot b)$ for all $a, b, c \in F$.

Remark 3.2.2. We'll always assume (unless otherwise stated) the precedence of "multiplicative symbols" over "additive symbols", so that $a \cdot b + c$ will mean $(a \cdot b) + c$ and not $a \cdot (b + c)$.

Lemma 3.2.3 (Properties of fields)**.** *Let $(F, +, \cdot)$ be a field, and $a \in F$ and $r \in \mathbb{Z}$. Then*

(a) $\mathrm{Id}_+ \neq \mathrm{Id}_\cdot$*,*
(b) $a \cdot \mathrm{Id}_+ = \mathrm{Id}_+ \cdot a = \mathrm{Id}_+$*,*
(c) $\cdot$ *on* F *is associative and commutative,*
(d) $a \cdot \mathrm{Id}_\cdot = \mathrm{Id}_\cdot \cdot a = a$*,*
(e) $\mathrm{Inv}_+(\mathrm{Id}_\cdot) \cdot a = \mathrm{Inv}_+(a)$*, and*
(f) $\mathrm{Iter}_{+,r}(a) = \mathrm{Iter}_{+,r}(\mathrm{Id}_\cdot) \cdot a$*.*

Lemma 3.2.4. *Let p be prime and $a, b \in Z$ such that $ab \equiv 0 \mod p$. Then $a \equiv 0 \mod p$ or $b \equiv 0 \mod p$.*

Theorem 3.2.5 (Prime fields)**.** *Let p be prime. Then $(\mathbb{Z}/\mathbb{Z}p, +_p, \cdot_p)$ is a field.*

Abbreviation 3.2.6 (Prime fields)**.** Let p be prime. Then we set $\mathbb{F}_p := (\mathbb{Z}/\mathbb{Z}p, +_p, \cdot_p)$.

Example 3.2.7. $(\mathrm{GL}_2(\mathbb{F}_2)$, *matrix multiplication*$)$ *is isomorphic to* $(\mathrm{S}_3, \circ)$.

Definition 3.2.8 (Field characteristic)**.** "p is a characteristic of $(F, +, \cdot)$" iff, $(F, +, \cdot)$ is a field and setting $S := \{m > 0 : \mathrm{Iter}_{+,m}(\mathrm{Id}_{\cdot}) = \mathrm{Id}_+\}$ one of the following holds:

(a) $S = \emptyset$ and $p = 0$.
(b) $S \neq \emptyset$ and $p = \min(S)$.

Lemma 3.2.9 (Permissible characteristics)**.** *Let p be the characteristic of $(F, +, \cdot)$. Then $p = 0$ or p is prime.*

Definition 3.2.10 (Primitive roots)**.** "r is a primitive root of $(F, +, \cdot)$" iff $(F, +, \cdot)$ is a field and $\langle r \rangle_{\cdot} = F \setminus \{\mathrm{Id}_+\}$.

Example 3.2.11 (Some primitive roots)**.**

(a) 3, 5 *are the primitive roots of* $\mathbb{F}_7$.
(b) 2, 6, 7, 8 *are the primitive roots of* $\mathbb{F}_{11}$.

Proposition 3.2.12 (Fermat's and Wilson's theorems)**.** *Let $p > 0$ be prime and $(\mathbb{Z}/\mathbb{Z}p \setminus \{\mathbb{Z}p\}, +_p, \cdot_p)$ be a cyclic group. Let $a \in \mathbb{Z}$. Then*

(a) $a^p \equiv a \mod p$, *and*
(b) $(p-1)! \equiv -1 \mod p$.

Proposition 3.2.13 $(\{a + \sqrt{n}b : a, b \in \mathbb{F}\}$ is a field$)$**.** *Let $(F, +, \cdot)$ be a field and $n \in F \setminus \{a \cdot a : a \in F\}$. Let $\oplus, \odot \colon F \times F \to F$ such that for all $a, b, c, d \in F$, we have $(a, b) \oplus (c, d) = (a + c, b + d)$ and $(a, b) \odot (c, d) = (a \cdot c + n \cdot b \cdot d, a \cdot d + b \cdot c)$. Then $(F \times F, \oplus, \odot)$ is a field.*

Proposition 3.2.14 $(\{a + \sqrt{n}b + \sqrt[3]{n}c : a, b, c \in \mathbb{F}\}$ is a field$)$**.** *Let $(F, +, \cdot)$ be a field and $n \in F \setminus \{a \cdot a \cdot a : a \in F\}$. Let $\oplus, \odot \colon F \times F \times F \to F$ such that for all $a, b, c, a', b', c' \in F$, we have $(a, b, c) \oplus (a', b', c') = (a + a', b + b', c + c')$ and $(a, b, c) \odot (a', b', c') = (a \cdot a' + n \cdot b \cdot c' + n \cdot c \cdot b', a \cdot b' + b \cdot a' + n \cdot c \cdot c', a \cdot c' + b \cdot b' + c \cdot a')$. Then $(F \times F \times F, \oplus, \odot)$ is a field.*

Example 3.2.15 (A field with non-prime order and infinite characteristic)**.** $\left\{0_{2\times 2}, I_2, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\right\}$ *forms a field with entries in* $\mathbb{F}_2$.

3.3 Vector spaces

November 23, 2021

Definition 3.3.1 (Vector spaces)**.** "$(V, (F, \oplus, \odot), +, \cdot)$ is a vector space" iff the following hold:

(a) $(V, +)$ is an abelian group.
(b) $(F, \oplus, \odot)$ is a field.
(c) $\cdot \colon F \times V \to V$.
(d) $\mathrm{Id}_{\odot} \cdot v = v$ for all $v \in V$.
(e) $(a \odot b) \cdot v = a \cdot (b \cdot v)$ for all $a, b \in F$ and all $v \in V$.
(f) $(a \oplus b) \cdot v = (a \cdot v) + (b \cdot v)$ for all $a, b \in F$ and all $v \in V$.
(g) $a \cdot (v + w) = (a \cdot v) + (a \cdot w)$ for all $a \in F$ and all $v, w \in V$.

Example 3.3.2 (Examples of vector spaces)**.** *In the following, the vector addition and scalar multiplication are defined usually.*

(a) $\mathrm{Mat}(m, n; \mathbb{F})$ *over* $\mathbb{F}$ *for any* $m, n \geq 1$*.*
(b) $\mathbb{C}$ *over* $(\mathbb{R}, +, \textit{real multiplication})$*.*
(c) Set of polynomials of degree at most n *with coefficients in* $\mathfrak{F}$ *over* $\mathbb{F}$*.*
(d) Set of continuous functions on $\mathbb{R}$ *over* $(\mathbb{R}, +, \textit{real multiplication})$*.*

Lemma 3.3.3 (Properties of vector spaces)**.** *Let* $(V, (F, \oplus, \odot), +, \cdot)$ *be a vector space and* $v \in V$*. Then*

(a) $\mathrm{Id}_{\oplus} \cdot v = \mathrm{Id}_{+}$*, and*
(b) $\mathrm{Inv}_{\oplus}(\mathrm{Id}_{\odot}) \cdot v = \mathrm{Inv}_{+}(v)$*.*

Remark 3.3.4. For any $m \geq 1$ and any field $\mathbb{F} := (F, \cdot, +)$, we'll abbreviate $\big(\mathrm{Mat}(m, 1; \mathbb{F}), \mathbb{F}, \tilde{+}, \tilde{\cdot}\big)$ as "F^m over $\mathbb{F}$", where $\tilde{+}$ and $\tilde{\cdot}$ are the susal operations of matrix addition and scalar multiplication respectively on $\mathrm{Mat}(m, 1; \mathbb{F})$.

Proposition 3.3.5 (F^m is a vector space)**.** *Let* $m \geq 1$ *and* $\mathbb{F} := (F, +, \cdot)$ *be a field. Then* F^m *over* $\mathbb{F}$ *is a vector space.*

Proposition 3.3.6 (Linear combinations in F^m)**.** *Let* $m \geq 1$ *and* $\mathbb{F} := (F, +, \cdot)$ *be a field. Let* $n \geq 1$*, and* $v_1, \ldots, v_n \in \mathrm{Mat}(m, 1; \mathbb{F})$ *and* $x_1, \cdots, x_n \in F$*. Let* $A \in \mathrm{Mat}(m, n; \mathbb{F})$ *such that* $A_{,j} = v_j$ *for all* $1 \leq j \leq n$*, and* $X \in \mathrm{Mat}(m, 1; \mathbb{F})$ *such that* $X_{i,1} = x_i$ *for all* $1 \leq i \leq m$*. Then* $x_1 v_1 + \cdots + x_n v_n = AX$*.*

Lemma 3.3.7 (Restriction of scalar multiplication). *Let F, V be sets and $\cdot\colon F \times V \to V$. Let $W \subseteq V$ such that $c \cdot w \in W$ for all $c \in F$ and all $w \in W$. Then there exists a unique function $*\colon F \times W \to W$ such that $c * w = c \cdot w$ for all $c \in F$ and all $w \in W$.*

Remark 3.3.8. This allows to denote $*$ by $\cdot_W$. (Poor notation since possible collision with the notation for restriction of binary operations (besides the case when ordered pairs are considered as Kuratowski pairs); when $V = F$ such that the above condition is fulfilled, then $\cdot$ is also a binary operation and $W \subseteq F$ is closed under $\cdot$.)

So, we will follow the convention that if $\cdot$ is the scalar multiplication for some vector space, then $\cdot_W$ will always denote the above.

Definition 3.3.9 (Subspace). "W is a subspace of $(V, (F, \oplus, \odot), +, \cdot)$" iff $(V, (F, \oplus, \odot), +, \cdot)$ is a vector space and the following hold:

(a) $w + v \in W$ for all $w, v \in W$.
(b) $c \cdot w \in W$ for each $c \in F$ and for each $w \in W$.
(c) $(W, (F, \oplus, \odot), +_W, \cdot_W)$ is a vector space.

Corollary 3.3.10 (An equivalent condition for being a subspace). *Let $(V, (F, \oplus, \odot), +, \cdot)$ be a vector space and W be a set. Then W is a subspace of $(V, (F, \oplus, \odot), +, \cdot)$ $\iff$ the following hold:*

(a) $W \subseteq V$.
(b) $w_1 + w_2 \in W$ *for all* $w_1, w_2 \in W$.
(c) $c \cdot w \in W$ *for all* $c \in F$ *and all* $w \in W$.
(d) $\mathrm{Id}_+ \in W$.

Proposition 3.3.11 (Subspaces of subspaces). *Let W be a subspace of $(V, (F, \oplus, \odot), +, \cdot)$ and U be a subspace of $(W, (F, \oplus, \odot), +_W, \cdot_W)$. Then U is a subspace of $(V, (F, \oplus, \odot), +, \cdot)$.*

Proposition 3.3.12 (Intersection of subspaces). *Let U and W be subspaces of $(V, (F, \oplus, \odot), +, \cdot)$. Then $U \cap W$ is a subspace of $(V, (F, \oplus, \odot), +, \cdot)$.*

Definition 3.3.13 (Proper subspaces). "W is a proper subspace of $(V, (F, \oplus, \odot), +, \cdot)$" iff W is a subspace of $(V, (F, \oplus, \odot), +, \cdot)$ and $W \neq \{\mathrm{Id}_+\}, V$.

Example 3.3.14 (Proper subspaces of $\mathbb{F}^2$). *Let W be a set and W_1, W_2 be proper subspaces of $(\mathrm{Mat}(2, 1; \mathbb{F}), \mathbb{F}$, matrix addition, scalar multiplication$)$. Then* *(a)* *W is a proper subspace of* $(\mathrm{Mat}(2,1;\mathbb{F}),\mathbb{F},$ *matrix addition, scalar multiplication*$)$ $\iff$ *there exists a* $w \in W \setminus \{\mathrm{Id}_+\}$ *such that* $W = \{c \cdot w : c \in F\}$,

(b) $\{c \cdot w : c \in F\} = W_1$ *for all* $w \in W_1 \setminus \{\mathrm{Id}_+\}$,

(c) *there exists a bijection between* W_1 *and* W_2*, and*

(d) $W_1 \neq W_2 \implies W_1 \cap W_2 = \{\mathrm{Id}_+\}$.

Example 3.3.15 (Number of proper subspaces of $\mathbb{F}^2$)**.** *Let* $\mathbb{F}$ *have* n *scalars. Then there are* $n+1$ *proper subspaces of* $(\mathrm{Mat}(2,1;\mathbb{F}),\mathbb{F},$ *matrix addition, scalar multiplication*$)$.

Definition 3.3.16 (Isomorphisms)**.** "ϕ is an isomorphism from $(V,+,\cdot)$ to $(V',+',\cdot')$ over $(F,\oplus,\odot)$" iff $(V,(F,\oplus,\odot),+,\cdot)$ and $(V',(F,\oplus,\odot),+',\cdot')$ are vector spaces the following hold:

(a) $\phi\colon V \to V'$ is a bijection.

(b) $\phi(v+w) = \phi(v) +' \phi(w)$ for all $v,w \in V$.

(c) $\phi(c \cdot v) = c \cdot' \phi(v)$ for all $c \in F$ and all $v \in V$.

Definition 3.3.17 (Isomorphic vector spaces)**.** "$(V,+,\cdot)$ and $(V',+',\cdot')$ are isomorphic over $(F,\oplus,\odot)$" iff there exists a ϕ such that ϕ is an isomorphism from $(V,+,\cdot)$ to $(V',+',\cdot')$ over $(F,\oplus,\odot)$.

Example 3.3.18 (Examples of isomorphic vector spaces)**.** *In the following, vector addition and scalar multiplication are defined in the usual way.*

(a) $\mathrm{Mat}(m,n;\mathbb{F})$ *is isomorphic to* $\mathrm{Mat}(mn,1;\mathbb{F})$ *over* $\mathbb{F}$.

(b) $(a,b) \mapsto a+bi$ *is an isomorphism from* $\mathbb{R}^2$ *to* $\mathbb{C}$ *over* $(\mathbb{R},+,$ *real multiplication*$)$.

3.4 Bases and dimension

November 30, 2021

Definition 3.4.1 (Span)**.** For any vector space $(V,\mathbb{F},+,\cdot)$ and $S \subseteq V$, $\mathcal{U} := \{U \subseteq V : S \subseteq V \text{ and } U \text{ is a subspace of } (V,\mathbb{F},+,\cdot)\} \neq \emptyset$, and we set $\mathrm{span}_{\mathbb{F},+,\cdot}(S) := \bigcap \mathcal{U}$.

Corollary 3.4.2 (Spans are minimal subspaces)**.** *Let* $(V,\mathbb{F},+,\cdot)$ *be a vector space and* $S \subseteq V$*. Then* $\mathrm{span}_{\mathbb{F},+,\cdot}(S)$ *is a subspace of* $(V,\mathbb{F},+,\cdot)$ *and for any subspace* W *of* $(V,\mathbb{F},+,\cdot)$ *such that* $S \subseteq W$*, we have that* $S \subseteq W$.

Corollary 3.4.3 (Span of $\emptyset$)**.** *Let* $(V,\mathbb{F},+,\cdot)$ *be a vector space. Then* $\mathrm{span}_{\mathbb{F},+,\cdot}(\emptyset) = \{\mathrm{Id}_+\}$.

Remark 3.4.4. From now on, for a set X which has on itself an associative binary operation $+$, and for a function $f\colon \{1,\cdots,n\} \to X$ for $n \geq 1$, we'll set $f(1)+\cdots+f(n)$ to be the obvious object.

If $+$ has an identity too, then $n=0$ will also be allowed.

Proposition 3.4.5 (Characterizing span)**.** *Let* $(V,\mathbb{F},+,\cdot)$ *be a vector space and* $S \subseteq V$*. Then* $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = \bigcup_{n\in\mathbb{N}}\{\operatorname{span}_{\mathbb{F},+,\cdot}(\{v_1,\ldots,v_n\}) : v\colon \{1,\cdots,n\} \to S$ *is an injection*$\}$.

Proposition 3.4.6 (Spans of finite sets)**.** *Let* $\mathbb{F} := (F,\oplus,\odot)$ *be a field and* $(V,\mathbb{F},+,\cdot)$ *be a vector space. Let* $n \in \mathbb{N}$ *and* $v_1,\ldots,v_n \in V$*. Then* $\operatorname{span}_{\mathbb{F},+,\cdot}(\{v_1,\cdots,v_n\}) = \{x_1\cdot v_1+\cdots+x_n\cdot v_n : x_1,\ldots,x_n \in F\}$.

Abbreviation 3.4.7 (Column space of matrices)**.** For any field $\mathbb{F} := (F,\oplus,\odot)$, and any $m,n \geq 1$ and any $A \in \operatorname{Mat}(m,n;\mathbb{F})$, we set $\operatorname{colSpan}_{\mathbb{F}}(A) := \operatorname{span}_{\mathbb{F},\tilde{+},\tilde{\cdot}}(\{A_{,1},\ldots,A_{,n}\})$ where $\tilde{+}$ and $\tilde{\cdot}$ are the matrix addition and matrix multiplication respectively on $\operatorname{Mat}(m,1;\mathbb{F})$.

Corollary 3.4.8 (Consistency of linear system)**.** *Let* $\mathbb{F}$ *be a field, and* $m,n \geq 1$ *and* $A \in \operatorname{Mat}(m,n;\mathbb{F})$ *and* $B \in \operatorname{Mat}(m,1;\mathbb{F})$*. Then* $B \in \operatorname{colSpan}_{\mathbb{F}}(A) \iff$ *there exists an* $X \in \operatorname{Mat}(n,1;\mathbb{F})$ *such that* $AX = B$.

Definition 3.4.9 (Independent and dependent sets)**.** "L of $(V,(F,\oplus,\odot),+,\cdot)$ is independent" or "L is independent in $(V,(F,\oplus,\odot),+,\cdot)$" iff $(V,(F,\oplus,\odot),+,\cdot)$ is a vector space, and $L \subseteq V$ and for every $n \in \mathbb{N}$ and for every injection $v\colon \{1,\ldots,n\} \to L$ and for all $x_1,\ldots,x_n \in F$, we have that $x_1\cdot v_1+\cdots+x_n\cdot v_n = \mathrm{Id}_+ \implies x_1,\ldots,x_n = \mathrm{Id}_\oplus$.

"L of $(V,(F,\oplus,\odot),+,\cdot)$ is dependent" or "L is dependent in $(V,(F,\oplus,\odot),+,\cdot)$" iff $(V,(F,\oplus,\odot),+,\cdot)$ is a vector space, and $L \subseteq V$ but L of $(V,(F,\oplus,\odot),+,\cdot)$ is not independent.

Corollary 3.4.10 ($\emptyset$ is independent)**.** *Let* $(V,\mathbb{F},+,\cdot)$ *be a vector space. Then* $\emptyset$ *of* $(V,\mathbb{F},+,\cdot)$ *is independent.*

Proposition 3.4.11 (Finite independent sets)**.** *Let* $(V,(F,\oplus,\odot),+,\cdot)$ *be a vector space. Let* $n \in \mathbb{N}$ *and* $v_1,\ldots,v_n \in V$*. Then the following are equivalent:*

(a) v_i*'s are distinct and* $\{v_1,\ldots,v_n\}$ *of* $(V,(F,\oplus,\odot),+,\cdot)$ *is independent.*

(b) For all $x_1,\ldots,x_n \in F$*, we have that* $x_1\cdot v_1+\cdots x_n\cdot v_n = \mathrm{Id}_+ \implies x_1,\cdots,x_n = \mathrm{Id}_\oplus$.

Lemma 3.4.12 (Properties of independent sets). *Let $(V,(F,\oplus,\odot),+,\cdot)$ be a vector space, and $L', L \subseteq V$ and $v, w \in V$. Then,*

(a) L is independent in $(V,(F,\oplus,\odot),+,\cdot)$ and $L' \subseteq L \implies \mathrm{Id}_+ \notin L$ and L' is independent in $(V,(F,\oplus,\odot),+,\cdot)$,
(b) $\{v\}$ is independent in $(V,(F,\oplus,\odot),+,\cdot) \iff v \neq \mathrm{Id}_+$, and
(c) $\{v,w\}$ is independent in $(V,(F,\oplus,\odot),+,\cdot) \iff v \notin \{c \cdot w : c \in F\}$ and $w \notin \{c \cdot v : c \in F\}$.

Definition 3.4.13 (Bases). "B is a basis of $(V,\mathbb{F},+,\cdot)$" iff B is independent in $(V,\mathbb{F},+,\cdot)$ and $\mathrm{span}_{\mathbb{F},+,\cdot}(B) = V$.

Remark 3.4.14. If $+$ on X is associative and commutative, and has an identity, then for any finite set K and any function $f\colon K \to X$, we'll set $\sum_{k\in K} f(k)$ to be the obvious object.

Lemma 3.4.15. *Let $(V,\mathbb{F},+,\cdot)$ be a vector space and $S \subseteq V$ such that S is a finite set. Let $x\colon S \to F$. Then*

(a) $\sum_{v\in S} x_v \cdot v \in \mathrm{span}_{\mathbb{F},+,\cdot}(S)$, and
(b) S is independent in $(V,\mathbb{F},+,\cdot)$ and $\sum_{v\in S} x_v \cdot v = \mathrm{Id}_+ \implies x_v = \mathrm{Id}_\oplus$ for all $v \in S$.

Proposition 3.4.16 (Characterizing bases). *Let $(V,\mathbb{F},+,\cdot)$ be a vector space and $B \subseteq V$. Then B is a basis of $(V,\mathbb{F},+,\cdot) \iff$ for every $w \in V$, there exists a unique function $x\colon B \to F$ such that, setting $B' := \{v \in B : x_v \neq \mathrm{Id}_\oplus\}$,*

(a) B' is finite, and
(b) $w = \sum_{v\in B'} x_v \cdot v$.

Proposition 3.4.17 (Finite bases). *Let $(V,\mathbb{F},+,\cdot)$ be a vector space. Let $n \in \mathbb{N}$ and $v_1,\ldots,v_n \in V$. Then the following are equivalent:*

(a) v_i's are distinct and $\{v_1,\ldots,v_n\}$ is a basis of $(V,\mathbb{F},+,\cdot)$.
(b) For all $w \in V$, there exist unique $x_1,\ldots,x_n \in F$ such that $w = x_1 \cdot v_1 + \cdots + x_n \cdot v_n$.

Proposition 3.4.18 (Standard basis for F^m). *Let $m \geq 1$. Then $\{e_{1,1;m\times 1},\ldots,e_{m,1;m\times 1}\}$ is a basis of F^m over $\mathbb{F}$.*

Proposition 3.4.19 (Spans and independence upon adding single elements). *Let $(V,\mathbb{F},+,\cdot)$ be a vector space. Let $S \subseteq V$ and $w \in V$. Then* *(a)* $\operatorname{span}_{\mathbb{F},+,\cdot}(S \cup \{w\}) = \operatorname{span}_{\mathbb{F},+,\cdot}(S) \iff w \in \operatorname{span}_{\mathbb{F},+,\cdot}(S)$*, and*

(b) S *is independent in* $(V, \mathbb{F}, +, \cdot) \implies (S \cup \{w\}$ *is independent in* $(V, \mathbb{F}, +, \cdot)$ *and* $w \notin S \iff w \notin \operatorname{span}_{\mathbb{F},+,\cdot}(S))$*.*

Definition 3.4.20 (Finite-dimensional vector spaces)**.** "$(V, \mathbb{F}, +, \cdot)$ is a finite-dimensional vector space" iff $(V, \mathbb{F}, +, \cdot)$ is a vector space and there exists a finite set $S \subseteq V$ such that $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = V$.

Corollary 3.4.21 (Spanning sets in finite dimensions can be reduced to finite sets)**.** *Let* $(V, \mathbb{F}, +, \cdot)$ *be a finite-dimensional vector space and* $S \subseteq V$ *such that* $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = V$*. Then there exists an* $S' \subseteq S$ *such that* S' *is a finite set and* $\operatorname{span}_{\mathbb{F},+,\cdot}(S') = V$*.*

Proposition 3.4.22 (Making an independent set a basis in finite dimensions)**.** *Let* L *be independent in* $(V, \mathbb{F}, +, \cdot)$ *and* $S \subseteq V$ *be a finite set such that* $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = V$*. Then there exists an* $S' \subseteq S$ *such that* $S' \cup L$ *is a basis of* $(V, \mathbb{F}, +, \cdot)$*.*

Corollary 3.4.23 (Making a finite spanning set into a basis)**.** *Let* $(V, \mathbb{F}, +, \cdot)$ *be a vector space and* $S \subseteq V$ *be a finite set such that* $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = V$*. Then there exists an* $S' \subseteq S$ *such that* S' *is a basis of* $(V, \mathbb{F}, +, \cdot)$*.*

Corollary 3.4.24 (Finite-dimensional spaces have a basis)**.** *Let* $(V, \mathbb{F}, +, \cdot)$ *be a finite-dimensional vector space. Then there exists a basis of* $(V, \mathbb{F}, +, \cdot)$*.*

Theorem 3.4.25 (Finite spanning sets have more elements than finite independent ones)**.** *Let* L *be independent in* $(V, \mathbb{F}, +, \cdot)$ *and* $S \subseteq V$ *such that* $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = V$*, and* S *and* L *are finite sets. Then* $\#(S) \geq \#(L)$*.*

Proposition 3.4.26 (Independent sets in finite dimensions are finite)**.** *Let* $(V, \mathbb{F}, +, \cdot)$ *be a finite-dimensional vector space and* L *be independent in* $(V, \mathbb{F}, +, \cdot)$*. Then* L *is a finite set.*

Proposition 3.4.27 (Dimension of finite-dimensional spaces)**.** *Let* $(V, \mathbb{F}, +, \cdot)$ *be a finite-dimensional vector space. Then there exists a unique* $n \in \mathbb{N}$ *such that for any basis* B *of* $(V, \mathbb{F}, +, \cdot)$*, we have that* B *has* n *elements.*

Remark 3.4.28. This allows to denote n by $\dim_{\mathbb{F},+,\cdot}(V)$.

Corollary 3.4.29. *Let* $(V, \mathbb{F}, +, \cdot)$ *be a finite-dimensional vector space. Let* L *be independent in* $(V, \mathbb{F}, +, \cdot)$ *and* $S \subseteq V$ *be a finite set such that* $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = V$*. Then* L *is a finite set and* $\#(L) \leq \dim_{\mathbb{F},+,\cdot}(V) \leq \#(S)$*. Further,* $\#(L) = \dim_{\mathbb{F},+,\cdot}(V) = \#(S) \iff L$ *and* S *are bases of* $(V, \mathbb{F}, +, \cdot)$*.*

Example 3.4.30 (Dimension of F^n). *Let $m \geq 1$ and $\mathbb{F} := (F, +, \cdot)$ be a field. Then F^m over $\mathbb{F}$ is a finite-dimensional vector space with dimension m.*

Proposition 3.4.31 (Independent spanning set for a subspace in finite dimensions). *Let $(V, \mathbb{F}, +, \cdot)$ be a finite-dimensional vector space and W be a subspace of $(V, \mathbb{F}, +, \cdot)$. Then there exists an independent L in $(V, \mathbb{F}, +, \cdot)$ such that $\operatorname{span}_{\mathbb{F},+,\cdot}(L) = W$.*

Lemma 3.4.32 (Independence and spans in subspaces). *Let W be a subspace of $(V, \mathbb{F}, +, \cdot)$. Let $L, S \subseteq W$. Then*

(a) L is independent in $(V, \mathbb{F}, +, \cdot) \iff L$ is independent in $(W, \mathbb{F}, +_W, \cdot_W)$, and
(b) $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = \operatorname{span}_{\mathbb{F},+_W,\cdot_W}(S)$.

Proposition 3.4.33 (Dimensions of subspaces of finite dimensional spaces). *Let $(V, \mathbb{F}, +, \cdot)$ be a finite-dimensional vector space and W be a subspace of $(V, \mathbb{F}, +, \cdot)$. Then*

(a) $(W, \mathbb{F}, +_W, \cdot_W)$ is a finite-dimensional vector space,
(b) $\dim_{\mathbb{F},+_W,\cdot_W}(W) \leq \dim_{\mathbb{F},+,\cdot}(V)$, and
(c) $\dim_{\mathbb{F},+_W,\cdot_W}(W) = \dim_{\mathbb{F},+,\cdot}(V) \iff V = W$.

Example 3.4.34. *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field and $m, n \geq 1$. Let $\{X_1, \ldots, X_m\}$ and $\{Y_1, \ldots, Y_n\}$ be bases of $\operatorname{Mat}(m, 1; \mathbb{F})$ and $\operatorname{Mat}(n, 1; \mathbb{F})$ respectively. Then $\{X_i(Y_j)^t : 1 \leq i \leq m, 1 \leq j \leq n\}$ is a basis of $\operatorname{Mat}(m, n; \mathbb{F})$.*

Proposition 3.4.35 (Basis of $\mathbb{F}^n$ and invertible matrices). *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field and $n \geq 1$. Let $v_1, \ldots, v_n \in \operatorname{Mat}(n, 1; \mathbb{F})$ and $A \in \operatorname{Mat}(n, n; \mathbb{F})$ such that $A_i = (v_i)^t$ for each $1 \leq i \leq n$. Then $\{v_1, \ldots, v_n\}$ is a basis for F^n over $\mathbb{F} \iff A$ is invertible.*

Proposition 3.4.36 (Subspaces as solutions of homogeneous systems). *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field and $n \geq 1$. Let W be a subspace of F^n over $\mathbb{F}$. Then there exists an $A \in \operatorname{Mat}(n, n; \mathbb{F})$ such that $W = \{X \in \operatorname{Mat}(n, 1; \mathbb{F}) : AX = 0_{m\times 1}\}$.*

Proposition 3.4.37. *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field, and $n \geq 1$ and $A \in \operatorname{Mat}(n, n; \mathbb{F})$. Then there exist $c_0, \ldots, c_{n^2} \in F$ such that $c_i \neq \operatorname{Id}_\oplus$ for some $0 \leq i \leq n^2$ and $c_0 A^0 + \cdots + c_{n^2} A^{n^2} = 0_{n\times n}$.*

Proposition 3.4.38 (Vector spaces over infinite fields can't be finitely covered). *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field such that F is an infinite set. Let $n \in \mathbb{N}$ and $U_1, \ldots, U_n$ be subspaces of $(V, \mathbb{F}, +, \cdot)$. Then $V \neq \bigcup_{i=1}^n U_i$.*

3.5 Computing with bases

December 6, 2021

Proposition 3.5.1 (Morphisms from F^n to V)**.** *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field and $(V, \mathbb{F}, +, \cdot)$ be a vector space. Let $n \in \mathbb{N}$ and $v_1, \ldots, v_n \in V$. Let $\psi\colon \mathrm{Mat}(n, 1; \mathbb{F}) \to V$ such that $\psi(X) = X_{1,1} \cdot v_1 + \cdots + X_{n,1} \cdot v_n$ for all $X \in \mathrm{Mat}(n, 1; \mathbb{F})$. Then*

(a) $\psi(X + Y) = \psi(X) + \psi(Y)$ *and* $\psi(cX) = c \cdot \psi(X)$ *for all* $X, Y \in \mathrm{Mat}(n, 1; \mathbb{F})$ *and all* $c \in F$*,*

(b) ψ *is injective* $\iff$ v_i*'s are distinct and* $\{v_1, \ldots, v_n\}$ *is independent in* $(V, \mathbb{F}, +, \cdot)$*, and*

(c) ψ *is surjective* $\iff$ $\mathrm{span}_{\mathbb{F},+,\cdot}(\{v_1, \ldots, v_n\}) = V$.

Corollary 3.5.2 (Classification of finite-dimensional vector spaces)**.** *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field.*

(a) Let $(V, \mathbb{F}, +, \cdot)$ be a finite-dimensional vector space such that $n := \dim_{\mathbb{F},+,\cdot}(V) \geq 1$. Then $(V, +, \cdot)$ and F^n over $\mathbb{F}$ are isomorphic over $\mathbb{F}$.

(b) Let $m, n \geq 1$ such that $m \neq n$. Then F^m over $\mathbb{F}$ and F^n over $\mathbb{F}$ are not isomorphic over $\mathbb{F}$.

Proposition 3.5.3 (Basechange)**.** *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field and $(V, \mathbb{F}, +, \cdot)$ be a vector space. Let $m, n \geq 1$ with $v_1, \ldots, v_m, v'_1, \ldots, v'_n \in V$ such that v_i's are distinct and $B := \{v_1, \ldots, v_m\}$ is a basis of $(V, \mathbb{F}, +, \cdot)$. Set $B' := \{v'_1, \ldots, v'_n\}$. Let $P \in \mathrm{Mat}(m, n; \mathbb{F})$ such that $v'_j = P_{1,j} \cdot v_1 + \cdots + P_{m,j} \cdot v_j$ for all $1 \leq j \leq n$. Then the following hold:*

(a) The following are equivalent:

- *(i) v'_i's are distinct and B' is a basis of $(V, \mathbb{F}, +, \cdot)$.*
- *(ii) $m = n$ and P is invertible.*

(b) If v'_i's are distinct and B' is a basis of $(V, \mathbb{F}, +, \cdot)$, and $Q \in \mathrm{Mat}(n, m; \mathbb{F})$ such that $v_j = Q_{1,j} \cdot v'_1 + \cdots + Q_{n,j} \cdot v'_n$ for all $1 \leq j \leq m$, and $X, X' \in \mathrm{Mat}(m, 1; \mathbb{F})$, then

- *(i) $m = n$*
- *(ii) P is invertible with $P^{-1} = Q$, and*
- *(iii) $X_{1,1} \cdot v_1 + \cdots + X_{m,1} \cdot v_m = X'_{1,1} \cdot v'_1 + \cdots + X'_{m,1} \cdot v'_m \iff PX' = X$.*

Example 3.5.4 (Rowspans of row equivalent matrices)**.** *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field and $m, n \geq 1$. Let $A, B \in \mathrm{Mat}(m, n; \mathbb{F})$ be row equivalent. Set*

$V := \mathrm{Mat}(1, n; \mathbb{F})$, and $X := \{A_1, \ldots, A_m\}$ and $Y := \{B_1, \ldots, B_m\}$. Let $\tilde{+}$ and $\tilde{\cdot}$ be the usual operations of matrix addition and scalar multiplication on V. Then

(a) $\mathrm{span}_{\mathbb{F},\tilde{+},\tilde{\cdot}}(X) = \mathrm{span}_{\mathbb{F},\tilde{+},\tilde{\cdot}}(Y)$, *and*
(b) *A_i's are distinct and X is independent in $(V, \tilde{+}, \tilde{\cdot}) \iff B_i$'s are distinct and Y is independent in $(V, \tilde{+}, \tilde{\cdot})$.*

Lemma 3.5.5 (Elementary actions)**.** *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field and $\mathcal{V} := (V, \mathbb{F}, +, \cdot)$ be a vector space. Let $n \geq 1$. Let $1 \leq i, j \leq n$ and $c \in F$. Then there exist unique functions $f, g, h\colon V^{\{1,\ldots,n\}} \to V^{\{1,\ldots,n\}}$ such that for each $v \in V^{\{1,\ldots,n\}}$, we have that for each $1 \leq k \leq n$,*

(a) $(f(v))_k = \begin{cases} v_k, & k \neq i \\ v_i + c \cdot v_j, & k = i \end{cases}$,
(b) $(g(v))_k = \begin{cases} v_k, & k \neq i, j \\ v_j, & k = i \\ v_i, & k = j \end{cases}$, *and*
(c) $(h(v))_k = \begin{cases} v_k & k \neq i \\ c \cdot v_i & k = i \end{cases}$.

Remark 3.5.6. This allows to denote f, g, h by $\mathfrak{a}_{\mathcal{V},n;i\to i+cj}$, $\mathfrak{a}_{\mathcal{V},n;i\leftrightarrow j}$, $\mathfrak{a}_{\mathcal{V},n;i\to ci}$ respectively.

Further, we'll call them "type I, or II, or III elementary actions for n vectors of $\mathcal{V}$" iff $i \neq j$ and $c \neq 0$.

Proposition 3.5.7 (Elementary actions preserve spans and independence)**.** *Let $\mathcal{V} := (V, \mathbb{F}, +, \cdot)$ be a vector space. Let $n \geq 1$ and $v\colon \{1, \ldots, n\} \to V$. Let a be an elementary action for n vectors of $\mathcal{V}$ and set $w := a \circ v$. Then*

(a) $\mathrm{span}_{\mathbb{F},+,\cdot}(\{w_1, \ldots, w_n\}) = \mathrm{span}_{\mathbb{F},+,\cdot}(\{v_1, \ldots, v_n\})$, *and*
(b) *v_i's are distinct and $\{v_1, \ldots, v_n\}$ is independent in $(V, \mathbb{F}, +, \cdot) \implies w_i$'s are distinct and $\{w_1, \ldots, w_n\}$ is independent in $(V, \mathbb{F}, +, \cdot)$.*

Lemma 3.5.8. *Let $(V, (F, \oplus, \odot), +, \cdot)$ be a vector space. Let $n \geq 1$ and $u\colon \{1, \ldots, n\} \to V$ be such that $\{u_1, \ldots, u_n\}$ is a basis for $(V, \mathbb{F}, +, \cdot)$ and u_i's are distinct. Let $A \in \mathrm{Mat}(n, n; \mathbb{F})$. Let E, a be such that there exist $1 \leq i, j \leq n$ and $c \in F$ so that one of the following holds:*

(a) $E = \mathcal{E}_{\mathbb{F},n;i\to i+cj}$ *and* $a = \mathfrak{a}_{\mathcal{V},n;i\to i+cj}$.
(b) $E = \mathcal{E}_{\mathbb{F},n;i\leftrightarrow j}$ *and* $a = \mathfrak{a}_{\mathcal{V},n;i\leftrightarrow j}$.

(c) $E = \mathcal{E}_{\mathbb{F},n;i\to ci}$ *and* $a = \mathfrak{a}_{\mathcal{V},n;i\to ci}$.

Then for each $1 \leq k \leq n$, *we have that* $(EA)_{k,1}\cdot u_1 + \cdots + (EA)_{k,n}\cdot u_k = (a \circ v)_k$.

Proposition 3.5.9 (Any two bases related by elementary actions)**.** *Let* $\mathcal{V} := (V, \mathbb{F}, +, \cdot)$ *be a vector space. Let* $n \geq 1$ *and* $u, v \colon \{1, \ldots, n\} \to V$ *such that* $\{u_1, \ldots, u_n\}$ *and* $\{v_1, \ldots, v_n\}$ *are bases of* $(V, \mathbb{F}, +, \cdot)$ *and* u_i*'s and* v_i*'s are distinct. Then there exists a* $k \in \mathbb{N}$ *and elementary actions* $a_1, \ldots, a_k$ *each for* n *vectors of* $\mathcal{V}$ *such that* $v = (a_1 \circ \cdots \circ a_k) \circ u$.

Example 3.5.10 (Number of independent ordered sets)**.** *Let* $p > 0$ *be prime and* $n \geq m \geq 1$. *Set* $F := \mathbb{Z}/\mathbb{Z}p$, *and* $\mathbb{F} := (F, +_p, \cdot_p)$ *and* $S := \{v \in \mathrm{Mat}(n,1;\mathbb{F})^{\{1,\ldots,m\}} : \{v_1, \ldots, v_m\}$ *is independent in* F^n *over* $\mathbb{F}$ *and* v_i*'s are distinct*$\}$. *Let* $\tilde{+}$ *and* $\tilde{\cdot}$ *be the usual operations of matrix addition and scalar multiplication on* $\mathrm{Mat}(n,1;\mathbb{F})$. *Then*

(a) $S = \{v \in \mathrm{Mat}(n,1;\mathbb{F})^{\{1,\ldots,m\}} : v_1 \neq \mathrm{Id}_{\tilde{+}}$ *and* $v_{k+1} \notin \mathrm{span}_{(F,\oplus,\odot),\tilde{+},\tilde{\cdot}}(\{v_1, \ldots, v_k\})$ *for all* $1 \leq k < m\}$, *and*

(b) $\#(S) = \prod_{i=0}^{m-1}(p^n - p^i)$.

Corollary 3.5.11 (Cardinality of $\mathrm{GL}_n(\mathbb{F}_p)$)**.** *Let* $p > 0$ *be prime and* $n \geq 1$. *Then* $\#(\mathrm{GL}_n(\mathbb{F}_p)) = \prod_{i=0}^{n-1}(p^n - p^i)$.

Proposition 3.5.12 (Number of subspaces of $\mathbb{F}_p^n$)**.** *Let* $p > 0$ *be prime and* $n \geq 1$ *and* $0 \leq m \leq n$. *Set* $F := \mathbb{Z}/\mathbb{Z}p$, *and* $\mathbb{F} := (F, +_p, \cdot_p)$. *Let* $\tilde{+}$ *and* $\tilde{\cdot}$ *be the usual operations of matrix addition and scalar multiplication on* $\mathrm{Mat}(n,1;\mathbb{F})$. $S := \{W : W$ *is a subspace of* F^n *over* $\mathbb{F}$ *and* $\dim_{\mathbb{F},\tilde{+},\tilde{\cdot}}(W) = m\}$. *Then* $\#(S)\big(\prod_{i=0}^{m-1}(p^m - p^i)\big) = \prod_{i=0}^{m-1}(p^n - p^i)$.

Proposition 3.5.13 (Number of 2×2 matrices with a given determinant in $\mathbb{F}_p$)**.** *Let* $p > 0$ *be prime. Set* $F := \mathbb{Z}/\mathbb{Z}p$ *and* $\mathbb{F} := (F, +_p, \cdot - p)$. *Then*

$$\#(\{A \in \mathrm{Mat}(2,2;\mathbb{F}) : \det(A) = \mathbb{Z}/\mathbb{Z}n\}) = \begin{cases} (p-1)p(p+1), & n \neq 0 \\ p(p^2+p-1), & n = 0 \end{cases}$$

for every $0 \leq n < p$.

3.6 Direct sums

December 6, 2021

Abbreviation 3.6.1 (Sum of subspaces)**.** For any set vector space $(V, \mathbb{F}, +, \cdot)$ and any set $\mathcal{W}$ of subspaces of $(V, \mathbb{F}, +, \cdot)$, we set $\mathrm{SubspSum}_{\mathbb{F},+,\cdot}(\mathcal{W}) := \mathrm{span}_{\mathbb{F},+,\cdot}(\bigcup \mathcal{W})$.

Proposition 3.6.2 (Characterizing sums)**.** *Let $(V, \mathbb{F}, +, \cdot)$ be a vector space and $\mathcal{W}$ be a set of subspaces of $(V, \mathbb{F}, +, \cdot)$. Then $\mathrm{SubspSum}_{\mathbb{F},+,\cdot}(\mathcal{W}) = \bigcup_{n\in\mathbb{N}}\{\mathrm{SubspSum}_{\mathbb{F},+,\cdot}(\{W_1, \dots, W_n\}) : W : \{1, \dots, n\} \to \mathcal{W}$ is an injection$\}$.*

Proposition 3.6.3 (Finite sums)**.** *Let $(V, \mathbb{F}, +, \cdot)$ be a vector spcae, and $n \in \mathbb{N}$ and $W_1, \dots, W_n$ be subspaces of $(V, \mathbb{F}, +, \cdot)$. Then $\mathrm{SubspSum}_{\mathbb{F},+,\cdot}(\{W_1, \dots, W_n\}) = \{w_1 + \cdots + w_n : w_i \in W_i$ for all $1 \le i \le n\}$.*

Definition 3.6.4 (Independent subspaces)**.** "$\mathcal{W}$ contains independent subspaces of $(V, \mathbb{F}, +, \cdot)$" iff $(V, \mathbb{F}, +, \cdot)$ is a vector space, and $\mathcal{W}$ is a set of subspaces of $(V, \mathbb{F}, +, \cdot)$, and for any $n \in \mathbb{N}$ and for any injection $W : \{1, \dots, n\} \to \mathcal{W}$ and for any $w_1, \dots, w_n \in V$ such that $w_i \in W_i$ for all $1 \le i \le n$, we have that $w_1 + \cdots + w_n = \mathrm{Id}_+ \implies w_1, \dots, w_n = \mathrm{Id}_+$.

Corollary 3.6.5 (Independence of zero subspace)**.** *Let $\mathcal{W}$ contain independent subspaces of $(V, \mathbb{F}, +, \cdot)$. Then $\mathcal{W} \cup \{\{\mathrm{Id}_+\}\}$ contains independent subspaces of $(V, \mathbb{F}, +, \cdot)$.*

Corollary 3.6.6 (Independence of two subspaces)**.** *Let U, W be subspaces of $(V, \mathbb{F}, +, \cdot)$. Then $\{U, W\}$ contains independent subspaces of $(V, \mathbb{F}, +, \cdot)$ $\iff U \cap W = \{\mathrm{Id}_+\}$ or $U = W$.*

Proposition 3.6.7 (Finite set of independent subspaces)**.** *Let $(V, \mathbb{F}, +, \cdot)$ be a vector space, and $n \in \mathbb{N}$ and $W_1, \dots, W_n$ be subspaces of $(V, \mathbb{F}, +, \cdot)$. Then the following are equivalent:*

(a) $\{W_1, \dots, W_n\}$ contains independent subspaces of $(V, \mathbb{F}, +, \cdot)$ and W_i's are distinct.

(b) For any $w_1, \dots, w_n \in V$ such that $w_i \in W_i$ for all $1 \le i \le n$, we have that $w_1 + \cdots + w_n = \mathrm{Id}_+ \implies w_1, \dots, w_n = \mathrm{Id}_+$.

(c) W_i's are distinct and $\big(\mathrm{SubspSum}_{\mathbb{F},+,\cdot}(\{W_1, \dots, W_k\})\big) \cap W_{k+1} = \{\mathrm{Id}_+\}$ for all $1 \le k < n$.

Proposition 3.6.8 (Independence of vectors and subspaces)**.** *Let $(V, \mathbb{F}, +, \cdot)$ be a vector space and $L \subseteq V$. Then L is independent in $(V, \mathbb{F}, +, \cdot)$ $\iff$ $\mathrm{Id}_+ \notin L$ and $\{\mathrm{span}_{\mathbb{F},+,\cdot}(\{v\}) : v \in L\}$ contains independent subspaces of $(V, \mathbb{F}, +, \cdot)$.*

Lemma 3.6.9 (Results on finite sums)**.** *Let $+$ on X be associative, commutative and have an identity 0. Let I be a finite set.*

(a) *Let X be a finite set and Π be a partition of X. Then Π is a finite set, and P is a finite set for all $P \in \Pi$, and $\sum_{x\in X} x = \sum_{P\in\Pi}\big(\sum_{x\in P} x\big)$.*

(b) *Let $\{A_i\}_{i\in I}$ and $\{f_i\}_{i\in I}$ be such that A_i is a finite set and $f_i \colon A_i \to X$ for all $i \in I$, and $g \colon I \times \big(\bigcup_{i\in I} A_i\big) \to X$ such that*

$$g((i,a)) = \begin{cases} f_i(a), & a \in A_i \\ 0, & a \notin A_i \end{cases}.$$

Set $\mathcal{A} := \bigcup_{i\in I} A_i$. Then $\sum_{i\in I}\big(\sum_{a\in A_i} f_i(a)\big) = \sum_{i\in I}\big(\sum_{a\in\mathcal{A}} g((i,a))\big)$.

Lemma 3.6.10. *Let $\mathbb{F} := (F, \oplus, \odot)$ be a field, and $(V, \mathbb{F}, +, \cdot)$ be a vector space and $S, S' \subseteq V$. Let $u \in \operatorname{span}_{\mathbb{F},+,\cdot}(S)$ and $v \in \operatorname{span}_{\mathbb{F},+,\cdot}(S')$, and $a, b \in F$. Then $a \cdot u + b \cdot v \in \operatorname{span}_{\mathbb{F},+,\cdot}(S \cup S')$.*

Remark 3.6.11. Let $\{B_i\}_{i\in I}$ be a family of sets. We'll say that "B_i's are pairwise disjoint" to mean the obvious.

Definition 3.6.12 (Direct sums)**.** "$(V, \mathbb{F}, +, \cdot)$ is a direct sum of $\mathcal{W}$" iff $\mathcal{W}$ contains independent subspaces of $(V, \mathbb{F}, +, \cdot)$, and $\operatorname{SubspSum}_{\mathbb{F},+,\cdot}(\mathcal{W}) = V$.

Proposition 3.6.13 (Characterizing direct sums)**.** *Let $(V, \mathbb{F}, +, \cdot)$ be a vector space and $\mathcal{W}$ be a set of subspaces of $(V, \mathbb{F}, +, \cdot)$. Let $\{B_W\}_{W\in\mathcal{W}}$ be a family of sets such that B_W is a basis of $(W, \mathbb{F}, +_W, \cdot_W)$ for each $W \in \mathcal{W}$. Then the following are equivalent:*

(a) *$(V, \mathbb{F}, +, \cdot)$ is a direct sum of $\mathcal{W}$.*

(b) *$\bigcup_{W\in\mathcal{W}} B_W$ is a basis of $(V, \mathbb{F}, +, \cdot)$ and B_W's are pairwise disjoint.*

(c) *For every $v \in V$, there exists a unique function $w \colon \mathcal{W} \to \bigcup \mathcal{W}$ such that*

  (i) *$w_W \in W$ for each $w \in \mathcal{W}$,*

  (ii) *$\mathcal{U} := \{W \in \mathcal{W} : w_W \neq \operatorname{Id}_+\}$ is a finite set, and*

  (iii) *$v = \sum_{W\in\mathcal{U}} w_W$.*

Proposition 3.6.14 (Subspaces of independent subspaces)**.** *Let $\mathcal{W}$ contain independent subspaces of $(V, \mathbb{F}, +, \cdot)$. Let $\{U_W\}_{W\in\mathcal{W}}$ be a family of sets such that U_W is a subspace of $(W, \mathbb{F}, +_W, \cdot_W)$ for all $W \in \mathcal{W}$. Then $\{U_W : W \in \mathcal{W}\}$ contains independent subspaces of $(V, \mathbb{F}, +, \cdot)$.*

Remark 3.6.15. We'll talk of "finite-dimensional subspaces" to talk of the obvious.

Proposition 3.6.16 (Dimension of a subspace sum)**.** *Let* $n \in \mathbb{N}$ *and* $W_1, \ldots, W_k$ *be finite-dimensional subspaces of* $(V, \mathbb{F}, +, \cdot)$*. Then* $\dim_{\mathbb{F},+,\cdot}\big(\mathrm{SubspSum}_{\mathbb{F},+,\cdot}(\{W_1, \ldots, W_n\})\big) \leq \dim_{\mathbb{F},+,\cdot}(W_1) + \ldots + \dim_{\mathbb{F},+,\cdot}(W_n)$ *with equality holding* $\iff$ $\{W_1, \ldots, W_n\}$ *contains independent subspaces of* $(V, \mathbb{F}, +, \cdot)$ *and* W_i*'s are distinct.*

Lemma 3.6.17. *Let* $(V, \mathbb{F}, +, \cdot)$ *be a vector space and* $S, S' \subseteq V$*. Then* $\mathrm{span}_{\mathbb{F},+,\cdot}\big(S \cup \mathrm{span}_{\mathbb{F},+,\cdot}(S')\big) = \mathrm{span}_{\mathbb{F},+,\cdot}(S \cup S')$*.*

Proposition 3.6.18 (Basis from two subspaces)**.** *Let* U*,* W *be subspaces of* $(V, \mathbb{F}, +, \cdot)$ *such that* $\mathrm{SubspSum}_{\mathbb{F},+,\cdot}(\{U, W\}) = V$*. Let* $B, C, D \subseteq V$ *such that* B *is a basis of* $(U \cap W, \mathbb{F}, +_{U\cap W}, \cdot_{U\cap W})$*, and* $B \cup C$ *is a basis of* $(U, \mathbb{F}, +_U, \cdot_U)$*, and* $B \cup D$ *is a basis of* $(W, \mathbb{F}, +_W, \cdot_W)$*, and* $B \cap C = B \cap D = \emptyset$*. Then*

- *(a)* $B \cup C \cup D$ *is a basis of* $(V, \mathbb{F}, +, \cdot)$*,*
- *(b)* $C \cap D = \emptyset$*, and*
- *(c)* $(V, \mathbb{F}, +, \cdot)$ *is a direct sum of* $\{U \cap W, \mathrm{span}_{\mathbb{F},+,\cdot}(C), \mathrm{span}_{\mathbb{F},+,\cdot}(D)\}$*.*

Corollary 3.6.19. *Let* U, W *be finite-dimensional subspaces of* $(V, \mathbb{F}, +, \cdot)$*. Then* $\mathrm{SubspSum}_{\mathbb{F},+,\cdot}(\{U, W\})$ *and* $U \cap W$ *are finite-dimensional subspaces of* $(V, \mathbb{F}, +, \cdot)$*, and* $\dim_{\mathbb{F},+,\cdot}(U) + \dim_{\mathbb{F},+,\cdot}(W) = \dim_{\mathbb{F},+,\cdot}\big(\mathrm{SubspSum}_{\mathbb{F},+,\cdot}(\{U, W\})\big) + \dim_{\mathbb{F},+,\cdot}(U \cap W)$*.*

Example 3.6.20 (Matrix decompositions)**.** *Let* p *be the characteristic of* $\mathbb{F} := (F, \oplus, \odot)$ *and* $n \geq 1$*. Let* $\tilde{+}$ *and* $\tilde{\cdot}$ *be the usual operations of matrix addition and scalar multiplication on* $\mathrm{Mat}(n, n; \mathbb{F})$*. Set* $U := \{A \in \mathrm{Mat}(n, n; \mathbb{F}) : A^t = A\}$ *and* $W := \{A \in \mathrm{Mat}(n, n; \mathbb{F}) : A^t = -A\}$*. Set* $U' := \{A \in \mathrm{Mat}(n, n; \mathbb{F}) : \mathrm{trace}(A) = \mathrm{Id}_{\oplus}\}$ *and* $W' := \{\lambda e_{n,n;n\times n} : \lambda \in F\}$*. Then*

- *(a)* $p \neq 2 \implies (\mathrm{Mat}(n, n; \mathbb{F}), \tilde{+}, \tilde{\cdot})$ *is the direct sum of* $\{U, W\}$*, and*
- *(b)* $(\mathrm{Mat}(n, n; \mathbb{F}), \tilde{+}, \tilde{\cdot})$ *is the direct sum of* $\{U', W'\}$*.*

3.7 Infinite-dimensional spaces

December 29, 2021

Remark 3.7.1. We'll use AC in this section.

Proposition 3.7.2 (Making independent sets into bases given a spanning set)**.** *Let L be independent in $(V, \mathbb{F}, +, \cdot)$ and $S \subseteq V$ such that* $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = V$*. Then there exists an $S' \subseteq S$ such that $L \cup S'$ is a basis of $(V, \mathbb{F}, +, \cdot)$.*

Corollary 3.7.3 (Existence of basis and making spanning sets into bases)**.** *Let $(V, \mathbb{F}, +, \cdot)$ be a vector space and $S \subseteq V$ such that* $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = V$*. Then there exist $B \subseteq V$ and $S' \subseteq S$ such that B and S' are bases for $(V, \mathbb{F}, +, \cdot)$.*

Proposition 3.7.4 (Independent sets of countably infinite-dimensional spaces)**.** *Let L be independent over $(V, \mathbb{F}, +, \cdot)$ and $S \subseteq V$ be countably infinite such that* $\operatorname{span}_{\mathbb{F},+,\cdot}(S) = V$*. Then L is finite or countably infinite.*

Chapter 4

Linear operators

4.1 The dimension formula

January 4, 2022

Remark 4.1.1. For any field $\mathbb{F}$, we'll write "F is the set of scalars of $\mathbb{F}$" to mean the obvious.

Definition 4.1.2 (Linear transformation)**.** "T is a linear transformation from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$" iff $(V, \mathbb{F}, +, \cdot)$ and $(W, \mathbb{F}, \boxplus, *)$ are vector spaces, and $T\colon V \to W$ such that for all $u, v \in V$ and for all $x \in F$, where F is the set of scalars of $\mathbb{F}$, we have that $T(u + v) = T(u) \boxplus T(v)$, and $T(x \cdot v) = x * T(v)$.

Corollary 4.1.3 (Linear transformation on arbitrary linear combinations)**.** *Let T be a linear transformation from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$ and F be the set of scalars of $\mathbb{F}$. Let $n \geq 1$ and $x_1, \ldots, x_n \in F$ and $v_1, \ldots, v_n \in V$. Then $T(x_1 \cdot v_1 + \cdots + x_n \cdot v_n) = x_1 * T(v_1) \boxplus \cdots \boxplus x_n * T(v_n)$.*

Abbreviation 4.1.4. For any linear transformation T from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$, we'll set $\mathrm{Ker}_{\mathbb{F},\boxplus,*}(T) := T^{-1}[\{\mathrm{Id}_{\boxplus}\}]$.

Proposition 4.1.5 (Kernel and image are subspaces)**.** *Let T be a linear transformation from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$. Then $\mathrm{Ker}_{\mathbb{F},\boxplus,*}(T)$ and $T[V]$ are subspaces of $(V, \mathbb{F}, +, \cdot)$ and $(W, \mathbb{F}, \boxplus, *)$.*

Theorem 4.1.6 (The dimension formula)**.** *Let T be a linear transformation from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$ and set $K := \mathrm{Ker}_{\mathbb{F},\boxplus,*}(T)$ and $I := T[V]$. Then the following hold:*

(a) $(V,\mathbb{F},+,\cdot)$ *is finite-dimensional* $\iff$ $(K,\mathbb{F},{}_K,\cdot_K)$ *and* $(I,\mathbb{F},\boxplus_I,*_I)$ *are finite-dimensional.*

(b) *All the above three are finite-dimensional* $\implies \dim_{\mathbb{F},+_K,\cdot_K}(K)+\dim_{\mathbb{F},\boxplus_I,*_I}(I) = \dim_{\mathbb{F},+,\cdot}(V)$.

4.2 The matrix of a linear transformation

January 4, 2022

Abbreviation 4.2.1. For any field $\mathbb{F}$ and any $m \geq 1$, we'll set $\mathrm{VecSp}_n(\mathbb{F}) := (\mathrm{Mat}(m,1;\mathbb{F}),\tilde{+},\tilde{\cdot})$, as in Remark 3.3.4.

Lemma 4.2.2 (Linear transformations from $\mathbb{F}^n$ to $\mathbb{F}^m$)**.** *Let* $\mathbb{F}$ *be a field and* $m,n \geq 1$. *Let* T *be a linear transformation from* $\mathrm{VecSp}_n(\mathbb{F})$ *to* $\mathrm{VecSp}_m(\mathbb{F})$ *and* $A \in \mathrm{Mat}(m,n;\mathbb{F})$ *such that* $A_{,j} = T(e_{j,1;n,1})$ *for each* $1 \leq j \leq n$. *Then* $T(X) = AX$ *for all* $X \in \mathrm{Mat}(n,1;\mathbb{F})$.

Remark 4.2.3. "$(v_1,\ldots,v_n)$ is an ordered basis of $(V,\mathbb{F},+,\cdot)$" iff $(V,\mathbb{F},+,\cdot)$ is a finite-dimensional vector space, and $\dim_{\mathbb{F},+,\cdot}(V) = n \geq 1$, and $v_1,\ldots,v_n \in V$ such that v_i's are distinct and $\{v_1,\ldots,v_n\}$ is a basis of $(V,\mathbb{F},+,\cdot)$.

Proposition 4.2.4 (Matrix of a linear transformation for given bases)**.** *Let* T *be a linear transformation from* $(V,\mathbb{F},+,\cdot)$ *to* $(W,\mathbb{F},\boxplus,*)$, *and* $(v_1,\ldots,v_n)$ *and* $(w_1,\ldots,w_m)$ *be ordered bases of* $(V,\mathbb{F},+,\cdot)$ *and* $(W,\mathbb{F},\boxplus,*)$. *Let* $A \in \mathrm{Mat}(m,n;\mathbb{F})$. *Then the following are equivalent:*

(a) *For all* $X \in \mathrm{Mat}(n,1;\mathbb{F})$, *we have* $T(X_{1,1}\cdot v_1+\cdots+X_{n,1}\cdot v_n) = (AX)_{1,1}*w_1\boxplus\cdots\boxplus(AX)_{m,1}*w_m$.

(b) *For all* $1 \leq j \leq n$, *we have that* $T(v_j) = A_{1,j}*w_1\boxplus\cdots\boxplus A_{m,j}*w_m$.

Remark 4.2.5. We'll abbreviate "A is the matrix of the linear transformation T from $(V,\mathbb{F},+,\cdot)$ to $(W,\mathbb{F},\boxplus,*)$ for the ordered bases $(v_1,\ldots,v_n)$ and $(w_1,\ldots,w_m)$" iff $(v_1,\ldots,v_n)$ and $(w_1,\ldots,w_m)$ are ordered bases of $(V,\mathbb{F},+,\cdot)$ and $(W,\mathbb{F},\boxplus,*)$, and $A \in \mathrm{Mat}(m,n;\mathbb{F})$ such that $T(v_j) = A_{1,j}*w_1\boxplus\cdots\boxplus A_{m,j}*w_m$ for all $1 \leq j \leq n$.

Proposition 4.2.6 (Matrix of linear transformation upon basechange)**.** *Let* A *be the matrix of linear transformation* T *from* $(V,\mathbb{F},+,\cdot)$ *to* $(W,\mathbb{F},\boxplus,*)$ *for ordered bases* $(v_1,\ldots,v_n)$ *and* $(w_1,\ldots,w_m)$. *Let* $P \in \mathrm{GL}_n(\mathbb{F})$ *and* $Q \in \mathrm{GL}_m(\mathbb{F})$. *Set* $v'_j := P_{1,j}\cdot v_1+\cdots+P_{n,j}\cdot v_n$ *and* $w'_i := Q_{1,i}*w_1\boxplus\cdots\boxplus Q_{m,i}*w_m$

for all $1 \leq j \leq n$ and all $1 \leq i \leq m$. Then $Q^{-1}AP$ is the matrix of the linear transformation T from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$ for ordered bases $(v'_1, \ldots, v'_n)$ and $(w'_1, \ldots, w'_m)$.

Corollary 4.2.7 (Matrices of a given linear map)**.** *Let A be the matrix of a linear transformation T from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$ for ordered bases $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_m)$ and $M \in \mathrm{Mat}(m, n; \mathbb{F})$. Then the following are equivalent:*

(a) There exist $v'_1, \ldots, v'_n \in V$ and $w'_1, \ldots, w'_m \in W$ such that M is the matrix of the linear transformation T from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$ for ordered bases $(v'_1, \ldots, v'_n)$ and $(w'_1, \ldots, w'_m)$.
(b) There exist $P \in \mathrm{GL}_n(\mathbb{F})$ and $Q \in \mathrm{GL}_m(\mathbb{F})$ such that $M = Q^{-1}AP$.

Abbreviation 4.2.8. For any $n \geq 1$ and any subspaces U of $\mathrm{VecSp}_n(\mathbb{F})$, we'll set $\dim_{\mathrm{VecSp}_n(\mathbb{F})}(U) := \dim_{\mathbb{F}, \tilde{+}_U, \tilde{\cdot}_U}(U)$ where $\tilde{+}$, $\tilde{\cdot}$ are as in Remark 3.3.4.

Remark 4.2.9. No notational collisions.

Proposition 4.2.10 (Ranks of linear transformation and its matrix)**.** *Let A be the matrix of the linear transformation T from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$ for ordered bases $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_m)$. Set $I := T[V]$ and $I' = T'[\mathrm{Mat}(n, 1; \mathbb{F})]$. Then $\dim_{\mathbb{F}, \boxplus_I, *_I}(I) = \dim_{\mathrm{VecSp}_m(\mathbb{F})}(\mathrm{colSpan}_{\mathbb{F}}(A))$.*

Corollary 4.2.11 (Rank of a matrix upon multiplication by invertible matrices)**.** *Let $\mathbb{F}$ be a field and $m, n \geq 1$. Let $A \in \mathrm{Mat}(m, n; \mathbb{F})$, and $P \in \mathrm{GL}_n(\mathbb{F})$ and $Q \in \mathrm{GL}_m(\mathbb{F})$. Then $\dim_{\mathrm{VecSp}_m(\mathbb{F})}(\mathrm{colSpan}_{\mathbb{F}}(A)) = \dim_{\mathrm{VecSp}_m(\mathbb{F})}(\mathrm{colSpan}_{\mathbb{F}}(Q^{-1}AP))$.*

Theorem 4.2.12 (Special form of the matrix of a linear map)**.**

(a) Let $(V, \mathbb{F}, +, \cdot)$ and $(W, \mathbb{F}, \boxplus, *)$ be finite-dimensional vector spaces. Set $n := \dim_{\mathbb{F}, +, \cdot}(V)$ and $m := \dim_{\mathbb{F}, \boxplus, *}(W)$. Let T be a linear transformation from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$. Set $I := T[V]$ and $r := \dim_{\mathbb{F}, \boxplus_I, *_I}(I)$. Let $A \in \mathrm{Mat}(m, n; \mathbb{F})$ such that

$$A_{,j} = \begin{cases} e_{j,j;m,1}, & j \leq r \\ 0_{m,1}, & j > r \end{cases}.$$

Then there exist $v_1, \ldots, v_n \in V$ and $w_1, \ldots, w_m \in W$ such that A is the matrix of linear transformation T from $(V, \mathbb{F}, +, \cdot)$ to $(W, \mathbb{F}, \boxplus, *)$ for ordered bases $(v_1, \ldots, v_n)$ and $(w_1, \ldots, w_m)$.

(b) *Let* $\mathbb{F}$ *be a field, and* $m, n \geq 1$*, and* $A \in \mathrm{Mat}(m, n; \mathbb{F})$*. Set* $r := \dim_{\mathrm{VecSp}_m(\mathbb{F})}(\mathrm{colSpan}_{\mathbb{F}}(A))$*. Then there exist* $P \in \mathrm{GL}_n(\mathbb{F})$ *and* $Q \in \mathrm{GL}_m(\mathbb{F})$ *such that* $B = Q^{-1}AP$ *is so that*

$$A_{,j} = \begin{cases} e_{j,j;m,1}, & j \leq r \\ 0_{m,1}, & j > r \end{cases}.$$

Corollary 4.2.13 (Row and column ranks are equal)**.** *Let* $\mathbb{F}$ *be a field and* $m, n \geq 1$*. Let* $A \in \mathrm{Mat}(m, n; \mathbb{F})$*. Then* $\dim_{\mathrm{VecSp}_m(\mathbb{F})}(\mathrm{colSpan}_{\mathbb{F}}(A)) = \dim_{\mathrm{VecSp}_n(\mathbb{F})}(\mathrm{colSpan}_{\mathbb{F}}(A^t))$*.*