PERMUTATIONS

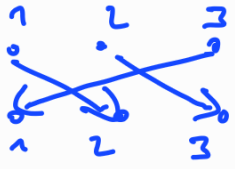
LA1 6/11/25

S_n - set of all permutations (bijective mappings) of $\{1,2,\dots,n\}$

The pair (i,j) is an **inversion pair** of $\pi \in S_n$ if $i < j$ and $\pi(i) > \pi(j)$.

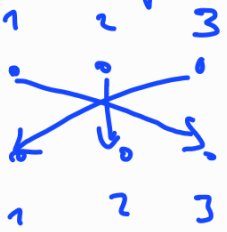
$I(\pi)$ ... the set of all inversion pairs of π

π_1:



$I(\pi_1) = \{(1,3),(2,3)\}$

π_2:

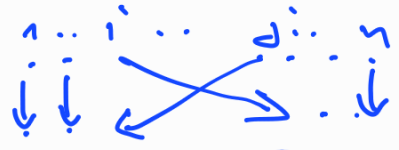


$I(\pi_2) = \{(1,2),(1,3),(2,3)\}$

the sign of a permutation π: ... parity of $|I(\pi)|$

$$\operatorname{sgn}(\pi) = (-1)^{|I(\pi)|} = \begin{cases} +1 & \text{for even } |I(\pi)| \\ -1 & \text{odd} \end{cases}$$

transposition - a permutation π that swaps two elements and fixes all other:



i.e., $\exists\, i \neq j : \pi(i) = j,\ \pi(j) = i,\ \pi(k) = k$ for $k \neq i, j$.

Eg. π_2.

Def: A **group** is a pair $(G, \oplus)$ where G is a set and $\oplus$ is a binary operation on G s.t.

1. $\forall a,b,c \in G : (a \oplus b) \oplus c = a \oplus (b \oplus c)$ associative property
2. $\exists n \in G\ \forall a \in G : a \oplus n = n \oplus a = a$ n ... neutral element of G
3. $\forall a \in G\ \exists b \in G : a \oplus b = b \oplus a = n$ b ... inverse element for a

If in addition

4. $\forall a,b \in G : a \oplus b = b \oplus a$ commutative prop.

holds, $(G, \oplus)$ is an **Abelian group**

(S_n with composition is a group)

$(T,+,\cdot)$

Def: A **field** is a set T with two binary operations on it, $+$ (addition) and $\cdot$ (multiplication) satisfying the following properties:

1. $(T,+)$ is an Abelian group, with neutral element 0; the inverse element for a is denoted $-a$.
2. $(T\setminus\{0\},\cdot)$ is an Abelian group, with neutral element 1; the inverse element for a is denoted a^{-1}.
3. $\forall a,b,c\in T$: $a\cdot(b+c)=a\cdot b+a\cdot c$ (distributive prop.)

Ex.: • $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$ with standard $+,\cdot$; • ~~$\mathbb{N}$~~, ~~$\mathbb{Z}$~~, no inverse elements for $+$, for $\cdot$

• $T=\{0,1\}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

HW: check that $(T,+,\cdot)$ is a field

The **smallest field** – two distinct neutral elements $0,1$ are needed

---

Derived binary operations: (inverse for b w.r.t. $+$)

$\forall a,b\in T$: $a-b=a+(-b)$ — subtraction

$\forall a\in T,\forall b\in T\setminus\{0\}$: $a/b=a\cdot(b^{-1})$ — division

---

Metatheorem: Everything we proved about real matrices holds for matrices over any field. (REF, Row reduction, …)

Proposition: 1. The elements 0 and 1 are unique.

2. $\forall a\in T$, the element $-a$ is unique, $\forall a\in T\setminus\{0\}$, a^{-1} unique.

Proof: 1. Assume there are neutral elements 0 and $\bar{0}$.

Then $0=0+\bar{0}=\bar{0}$; similarly for 1: $1=1\cdot\bar{1}=\bar{1}$.

2. Assume there are two inverse elements for a, $-a$, $\bar{-a}$:

$-a=-a+0=-a+(a+(\bar{-a}))=(-a+a)+(\bar{-a})=\bar{-a}$.

for a^{-1} in the same way. ∎

Proposition 2: 1. $\forall a \in T: 0 \cdot a = a \cdot 0 = 0$ not obvious!

2. $\forall a \in T: (-1) \cdot a = -a$ $(\Rightarrow \forall a,b \in T: (-b)\cdot a = -b\cdot a)$

3. If $a \cdot b = 0$, then $a = 0$ or $b = 0$.

Meaning!

Proof: 1. $0 \cdot a \overset{0}{=} 0 \cdot a + \overbrace{(0 \cdot a - 0 \cdot a)}^{=0} \overset{\text{asoc.}}{=} (0 \cdot a + 0 \cdot a) - 0 \cdot a =$

$\overset{\text{distr.}}{=} (0+0)\cdot a - 0 \cdot a \overset{0}{=} 0 \cdot a - 0 \cdot a = 0$

by commutativity of $\cdot$: $0 \cdot a = a \cdot 0$

2. $(-1)\cdot a + a \overset{1\text{ \& distr.}}{=} (-1+1)\cdot a = 0 \cdot a \overset{\text{point 1.}}{=} 0$,

i.e. $(-1)\cdot a$ has properties of $(-a)$. Thus, by uniqueness - Proposition 1: $(-1)\cdot a = -a$.

3. by a contradiction: Assume $a \neq 0$ & $b \neq 0$. Then $\exists\, a^{-1}, b^{-1}$.

$1 = 1 \cdot 1 = (a \cdot a^{-1}) \cdot (b \cdot b^{-1}) \overset{\text{asoc., komut.}}{=} \overbrace{(a \cdot b)}^{=0} \cdot (a^{-1} \cdot b^{-1}) \overset{\text{point 1.}}{=} 0$ contradiction! ∎

Ex. Let $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$.

For $c \in \mathbb{Z}$, $c \bmod n$ denotes $d \in \mathbb{Z}_n$ s.t. n divides $c - d$.

We define binary operations $\oplus$ and $\odot$ on $\mathbb{Z}_n$:

$\forall a,b \in \mathbb{Z}_n: a \oplus b = (a + b \bmod n) \quad a \odot b = (a \cdot b \bmod n)$

~ clock arithmetic: 10 am + 3 hours = 1 pm for $n = 12$

When is $(\mathbb{Z}_n, \oplus, \odot)$ a field?

Theorem: $\mathbb{Z}_n$ is a field $\Leftrightarrow$ n is a prime.

Proof: $\Rightarrow$ by a contradiction: Assume $n = a \cdot b$ for $a, b > 1$

Then $a \odot b = 0$. By Prop. 2(3), $a = 0$ or $b = 0$ - a contradiction.

$\Leftarrow$ $\oplus, \odot$ are binary operations on $\mathbb{Z}_n$

We have to check all the axioms of a field:

1. $(\mathbb{Z}_n, \oplus)$ group - easy - neutral element 0, ...

3. distributive property - easy ✓

2. $(\mathbb{Z}_n \setminus [0], \odot)$ group: assoc. ✓ neutral element 1 ✓

inverse elements ? $\forall a \in \mathbb{Z}_n \setminus \{0\}\ \exists a^{-1}$ s.t. $a \cdot a^{-1} = 1$?

For a prime n, and $\forall a \in \mathbb{Z}_n \setminus \{0\}$, the numbers

$1 \odot a, 2 \odot a, \dots, (n-1) \odot a$ are all different.

proof: by a contradiction: Assume $c \odot a = d \odot a$, for $c \neq d$

then $0 = c \odot a - d \odot a \overset{\text{Prop 2(2)}}{=} c \odot a + (-d) \odot a \overset{\text{distri.}}{=} (c-d) \odot a$

By Proposition 2, point 3, $c - d = 0$, or $a = 0$ -

- a contradiction as $c \neq d$ and $a \neq 0$ ∎

$\Rightarrow$ For every $a \in \mathbb{Z}_n \setminus \{0\}$, $\{1 \odot a, \dots, (n-1) \odot a\} = \{1, \dots, n-1\}$ -

$n-1$ different numbers from $\mathbb{Z}_n \setminus \{0\}$ -

- one of them has to be 1, i.e.,

for some $b \in \{1, \dots, n-1\}$, $b \odot a = 1$ ... $b = a^{-1}$ ∎

Note: An existential proof - we proved that a^{-1} exists,

but do not know which number it is. HW!

Let $(F, \oplus, \odot)$ be a field. $\forall a, b, c \in F : a = b \Rightarrow a \odot c = b \odot c$.

Fermat's little theorem: If p is a prime and $a \in \mathbb{Z}_n \setminus \{0\}$

then $\underbrace{a \odot a \odot \cdots \odot a}_{\text{a product } n-1 \text{ numbers } a} = 1$ $\qquad (a^{n-1} = 1 \bmod n)$

Proof: By the above :

$\{1, 2, \dots, n-1\} = \{1 \odot a, 2 \odot a, \dots, (n-1) \odot a\}$

$\Rightarrow$ The product of numbers in both sets is equal:

$$\underbrace{1 \odot 2 \odot \cdots \odot (n-1)}_{=b} = 1 \odot a \odot 2 \odot a \odot \cdots \odot (n-1) \odot a \overset{\text{asoc., comut.}}{=}$$

$$= \underbrace{1 \odot 2 \odot \cdots \odot (n-1)}_{=b} \odot \underbrace{a \odot \cdots \odot a}_{n-1 \text{ times}}$$

We know : As $b \neq 0$, $\exists b^{-1}$ s.t. $b^{-1} \cdot b = 1$

by ☝ $\Rightarrow 1 = a \odot a \odot \cdots \odot a \cdot \underbrace{a^{n-2} \cdot \dots \cdot a^{n-2}}_{n-2 \text{ times}}$ ∎

Corollary : $a^{-1} = \underbrace{a \odot a \odot \cdots \odot a}_{n-2 \text{ times}}$ inverse elem. for a.

Def: The characteristic of a Field F is the smallest $n \in \mathbb{N}$, if it exists, s.t. $\overbrace{1+1+\dots+1}^{n\text{-times}} = 0$ (where 0 and 1 are the neutral elements of F w.r.t. $+$ and $\cdot$).
If no such n exists, then the characteristic is 0.

Theorem: The characteristic of a field is 0 or a prime.

Proof: By a contradiction: Assume that F is a field of characteristic $n = a \cdot b$, $a, b > 1$.

Then

$$0 = \overbrace{\underbrace{1+1+\dots+1}_{a\text{-times}} + \underbrace{1+1+\dots+1}_{a\text{-times}} + \dots + \underbrace{1+1+\dots+1}_{a\text{-times}}}^{a\cdot b\text{-times}}$$

$$= \underbrace{(1+1+\dots+1)}_{a\text{-times}} \cdot \underbrace{(1+1+\dots+1)}_{b\text{-times}}$$

(distributivity)

$\neq 0$ $\quad$ $\neq 0$

- a contradiction - 0 as a product of 2 non-zeros. ∎

Example: field with 4 elements

$T = \{0, 1, x, (x+1)\}$

$\oplus$ as addition of polynomials, coefficient mod 2

$\odot$ as multiplication of polynomials, mod x^2+x+1

characteristic = 2

$\oplus$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\odot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

$x^2 \bmod x^2+x+1 =$
"$x^2+2x+2 \bmod x^2+x+1$" $= x+1$

$x^2 + x \bmod x^2+x+1 = 1$

$(x+1)^2 \bmod x^2+x+1 = x$

It holds: a field with n elements exists iff n is a power of a prime number, i.e., $n = p^k$ where p is a prime and $k \in \mathbb{N}$