Abstract Algebra

I Groups

I 1. Binary structures, magmas, semigroups, monoids

Def 1: Let $M \neq \emptyset$. A binary structure on M is a map

$\tau : M \times M \to M$. $\mathrm{Map}(M \times M, M)$ is the set of binary structures on M.

For $\tau \in \mathrm{Map}(M \times M, M)$ we write $a \tau b$ for $\tau(a, b)$.

Ex: 1) $+ : \mathbb{N}^2 \longrightarrow \mathbb{N}$, $\mathbb{N} = \{1, 2, 3, \ldots\}$

2) $(\mathbb{R}^{>0} \times [0, 2\pi[) = M$

$((r_1, \varphi_1), (r_2, \varphi_2)) \longmapsto (r_1 r_2, \varphi_1 + \varphi_2)$ is not a binary structure on M

3) $X \neq \emptyset$ $\quad M = \mathrm{Map}(X) = \mathrm{Map}(X, X)$

$\circ : \mathrm{Map}(X) \times \mathrm{Map}(X) \longrightarrow \mathrm{Map}(X)$

$(f, g) \longmapsto f \circ g \qquad (f \circ g)(x) = f(g(x)), x \in X$

"composition of maps"

is a binary structure on M.

Def 2: A pair $(M, *)$ consisting of a non-empty set M and a binary structure $*$ on M is called "magma"

Ex: 1) Let V be an $\mathbb{R}$-vector space. Then

$$(\mathrm{End}_{\mathbb{R}} V = \{ f : V \to V \mid f \ \mathbb{R}\text{-linear} \}, \circ)$$

is a magma.

2) We can indicate the binary structure by using multiplication tables

$$M = \{a_0, \dots, a_{n-1}\} \quad a_i \neq a_{i+1}$$

	a_0	a_1	a_2	$\cdots$	a_{n-1}
a_0	$a_0 * a_0$	$a_0 * a_1$		$\cdots$	$a_0 * a_{n-1}$
a_1	$a_1 * a_0$	$a_1 * a_1$		$\cdots$	$a_1 * a_{n-1}$
$\vdots$					$\vdots$
a_{n-1}	$a_{n-1} * a_0$	$a_{n-1} * a_1$		$\cdots$	$a_{n-1} * a_{n-1}$

. There are n^2 many different binary structures on M

Def 3: 1) $M \neq \emptyset$. A binary structure $*$ on M is called
- associative if for all $a, b, c \in M$

$$(a * b) * c = a * (b * c)$$

- commutative (or abelian) if — " —

$$a * b = b * a$$

2) A magma $(M, *)$ is called
- semigroup if $*$ is associative.
- commutative (or abelian) if $*$ is commutative.

Let $(M,*)$ be a magma. For $a_1, a_2, \dots, a_m \in M$ we define inductively

$$P(a_1, a_2, a_3) := \{(a_1 * a_2) * a_3,\ a_1 * (a_2 * a_3)\}$$

$$P(a_1, a_2, \dots, a_m) := \{ b * c \mid \exists_{1 \le \ell \le m-1} \ b \in P(a_1, \dots, a_\ell) \text{ and } c \in P(a_{\ell+1}, \dots, a_m) \}$$

<u>Prop. 4:</u> Suppose $(M,*)$ is a semigroup. Then, for all $a_1, \dots, a_m \in M$, the set $P(a_1, \dots, a_m)$ is a singleton, i.e. only consists of one element.

<u>Proof.</u> (by induction m)

<u>$m=3$:</u> ✓, because $*$ is associative.

<u>$m>3$:</u> We define $a_1 * a_2 * \dots * a_m$

$$:= (((a_1 * a_2) * a_3) * \dots) * a_m)$$

Take $d \in P(a_1, \dots, a_m)$. To show $d = a_1 * \dots * a_m$

$\exists_{1 \le \ell \le m-1} \ \exists_1 b \in P(a_1, \dots, a_\ell) \ \exists_1 c \in P(a_{\ell+1}, \dots, a_m)$

$d = b * c$

Now $d = b * c \overset{(IH)}{=} (a_1 * \dots * a_\ell) * (a_{\ell+1} * \dots * a_m)$

(So we are done in case $\ell + 1 = m$)

in case $\ell < m-1$

$$\overset{\downarrow}{=} (a_1 * \dots * a_\ell) * ((a_{\ell+1} * a_{\ell+2}) * \dots * a_m)$$

$$\underset{(IH)}{=} (a_1 * \dots * a_\ell) * ((a_{\ell+1} * a_{\ell+2}) * (a_{\ell+3} * \dots * a_m))$$

$$\underset{(BC)}{=} ((a_1 * \dots * a_\ell) * (a_{\ell+1} * a_{\ell+2})) * (a_{\ell+3} * \dots * a_m)$$

base case

$$= (((a_1 * \dots * a_\ell) * a_{\ell+1}) * a_{\ell+2}) * (a_{\ell+3} * \dots * a_m)$$

$$\underset{(IH)}{=} (a_1 * \dots * a_{\ell+2}) * a_{\ell+3} * \dots * a_m. \qquad \square$$

The following proposition will be on the problem sheet

<u>Prop 5:</u> Let $(M, *)$ be an abelian semigroup. Then, for all $a_1, \dots, a_m \in M$ and for all $\tau \in \mathrm{Bij}(\{1, \dots, m\}) = \{f \in \mathrm{Map}(\{1, \dots, m\}) \mid f \text{ bijective}\}$, we have

$$a_1 * a_2 * \dots * a_m = a_{\tau(1)} * a_{\tau(2)} * \dots * a_{\tau(m)}.$$

<u>Def 6</u>: Let $(M,*)$ be a magma. An element a of M is called left-unit (right-unit) if $a*b=b \ \forall b\in M$

$(b*a=b \ \forall b\in M)$.

An element of M which is a left- and a right-unit is called a <u>unit</u>.

A semigroup having a unit is called a monoid.

<u>Prop 7</u>: Suppose $(M,*)$ is a semigroup containing a left-unit and a right-unit. Then $(M,*)$ is a monoid and all the left-units and the right-units agree.

<u>Proof</u>: Let e_l be a left-unit and e_r — " — right " of $(M,*)$.

$$\Rightarrow e_l \underset{e_r \text{ r-unit}}{=} e_l * e_r \underset{e_l \text{ left unit}}{=} e_r \qquad \square$$

<u>Ex.</u> 1) $(\mathbb{N} = \{1, 2, \ldots\}, +)$ is a semigroup, but not a monoid.

2) $(\mathcal{P}(M), \setminus)$ is a magma but not a semigroup if $|M| \geq 1$.

It has a right-unit.

3) $X \neq \emptyset$. $(\mathrm{Map}(X), \circ)$ is a monoid;

$$id_M \circ f = f = f \circ id_M,$$

and it is abelian iff $|X| \leq 2$.

I2 groups (definition)

Def 8: Let $(M,*)$ be a magma with a unit e and let $a \in M$. An element b of M is called a left-inverse (right-inverse) of a if $b*a = e$ $(a*b = e)$.

An element of M which is at the same time a left- and a right-inverse of a is called an <u>inverse of a</u>.

Prop 9: 1) If $(M,*)$ is a monoid and $a,b,c \in M$ s.t. $b*a = e = a*c$. Then $b = c$.

2) Suppose $(M,*)$ is a monoid and $a \in M$, s.t. a has a left-inverse. Then a satisfies the left-cancellation property (LCP)

$$\forall_{d_1,d_2 \in M} : (a*d_1 = a*d_2 \Rightarrow d_1 = d_2)$$

3) $(M,*)$ a monoid. Suppose M is finite and $a \in M$, s.t. a satisfies (LCP)

Then a has a left-inverse

<u>Proof:</u> 1) $b = b * e = b * (a * c) = (b * a) * c$
$= e * c = c.$

2) exercise.

3) $\{a^i \mid i \in \mathbb{N}_0\} \subseteq M$ is finite.

$\Rightarrow \exists_{0 \le i < j} : a^i = a^j$. Take i to be minimal.

. <u>Claim: $i = 0$:</u> If not then

$$a * a^{i-1} = a * a^{j-1}$$

$$\overset{(LCP)}{\Longrightarrow} a^{i-1} = a^{j-1} \quad \lightning \text{ to}$$

minimality of i.

. Thus $e = a^{j-1} * a$, so a has a left-inverse. $\square$

<u>Def 10:</u> A monoid $(M, *)$ is called a group if every element of M has an inverse.

$|M|$ is called the <u>order</u> of a group.

A group $(G, *)$ is called abelian if $*$ is abelian

<u>Ex.</u> 1) $(Bij(X), \circ)$ is a group.

2) $Isom(\mathbb{R}^n, |\cdot|_2) := \{ f : \mathbb{R}^n \to \mathbb{R}^n \mid$

$|f(\underline{u}) - f(\underline{v})|_2 = |\underline{u} - \underline{v}|_2 \ \forall \underline{u}, \underline{v} \in \mathbb{R}^n \}$

= " set of isometries of $\mathbb{R}^n$.

$(Isom(\mathbb{R}^n, |\cdot|_2), \circ)$ is a group.

3) $(\mathcal{P}(X), \Delta)$

$A \Delta B := (A \cup B) \setminus (A \cap B)$.

is an abelian group (exercise)

<u>Proof</u> 1) $Bij(X) = \{ f \in Map(X) \mid f \text{ bijective} \}$

i.e. injective and surjective

<u>Note</u> $f, g \in Map(X)$

If f, g injective, then $f \circ g$ too

— " — surjective — " —

So $Bij(X)$ is invariant under $\circ$.

$\Rightarrow$ $(\mathrm{Bij}(X), \circ)$ is a magma.

$(\mathrm{Map}(X), \circ)$ is a monoid and $\mathrm{Bij}(X) \ni \mathrm{id}_X$

$$\begin{array}{c} \cap\!| \\ \mathrm{Map}(X) \end{array}$$

$\Rightarrow$ $(\mathrm{Bij}(X), \circ)$ is a monoid.

For $f \in \mathrm{Bij}(X)$ and $y \in X$

$\exists x_y \in X : \quad f(x_y) = y$ (by surjectivity)

Define $g(y) := x_y$ (well-defined by injectivity.)

Then $(f \circ g)(y) = y \quad \forall y \in X.$

and $(g \circ f)(x) = x_{f(x)} \underset{\uparrow}{=} x$

$$\left(f(x) = f(x_{f(x)}) \overset{\text{inj}}{\Rightarrow} x = x_{f(x)} \right)$$

$\Rightarrow$ f has an inverse.

It is uniquely determined by Prop 9. Write f^{-1}.

2) $(\mathrm{Bij}(\mathbb{R}^n), \circ)$ is a group and

$\mathrm{Isom}(\mathbb{R}^n, \|\cdot\|_2) \subseteq \mathrm{Bij}(\mathbb{R}^n)$ (Why?)

So it is enough to show that

- the composition of isometries
- $id_{\mathbb{R}^n}$
- and the inverse in $Bij(\mathbb{R}^n)$ of an isometry

are isometries.

The associativity of $\circ$ still holds.

$\square$

<u>Def 11</u>: a) Let $(S,*)$ be a semigroup. $s \in S$ is said to be right- (left-) cancellative if

$$\forall_{t_1,t_2 \in S} : \quad t_1 s = t_2 s \Rightarrow t_1 = t_2$$

$$\left(\qquad st_1 = st_2 \Rightarrow t_1 = t_2. \right)$$

s is called <u>cancellative</u> if it satisfies both.

b) $(S,*)$ is called regular if $\forall_{s \in S} \exists_{t \in S} \; s = sts$.

c) $(S,*)$ — " — cancellative if all $s \in S$ are.

<u>Prop 12</u>: Let $(S,*)$ be a semigroup. Then are equivalent:

1° $(S,*)$ is cancellative and regular.

2° $(S,*)$ is a group.

<u>Proof</u>: Regularity $\Rightarrow \forall_{s \in S} \exists_{t_s \in S} : s = s t_s s$.

$$s_1 s_2 t_{s_2} s_2 = s_1 s_2 = s_1 t_{s_1} s_1 s_2$$

cancellation $\Rightarrow$ $s_2 t_{s_2} = s_1 t_{s_1}$ $\quad \forall_{s_1, s_2 \in S}$.

Call this element e. It is a unit

$\Rightarrow$ $(S, *)$ is a monoid.

$s t_s = t_s s = e \Rightarrow (S, *)$ is a group. $\square$

I3 Subgroups, - monoids, - semigroups

Def 13: a) Let $(G,*)$ be a magma (semigroup, group) and let $H \subseteq G$.

$(H, *|_{H\times H})$ is called a submagma (..., ...) if $(H, *|_{H\times H})$ is a magma (semigroup, group)

b) Suppose $(G,*)$ is a monoid and $H \subseteq G$. Then $(H, *|_{H\times H})$ is called a submonoid if $e_G \in H$ and $(H, *|_{H\times H})$ is a semigroup.

Ex: a) $(\mathbb{N},+)$ is a subsemigroup of $(\mathbb{R},+)$, but not a submonoid

b) $X \neq \emptyset$. $(\mathcal{P}(X), \cap)$ is a monoid. Take $Y \subsetneq X$. $(\mathcal{P}(Y), \cap)$ is a monoid too, but not a submonoid of $(\mathcal{P}(X), \cap)$, because $X \notin \mathcal{P}(Y)$.

<u>Prop 14</u>: (Subgroup criteria):

Let $(G,*)$ be a group and let H be a subset of G. Then are equivalent

1° $(H, *|_{H\times H})$ is a subgroup of $(G,*)$

2° $H \neq \emptyset$ and for all $h_1, h_2 \in H$ we have $h_1 h_2, h_1^{-1} \in H$

3° $H \neq \emptyset$ and for all $h_1, h_2 \in H$ we have $h_1 h_2^{-1} \in H$.

(Here h^{-1} means inverse in G)

<u>Proof</u>: 1° $\Rightarrow$ 2°. We have to show $e_H = e_G$

(Then the inverse in H is the inverse in G)

$e_H \cdot e_H = e_H = e_H \cdot e_G$.

cancellation $\Rightarrow e_H = e_G$.

2° $\Rightarrow$ 3° ✓

3° $\Rightarrow$ 1° 3° $\Rightarrow$ $e_G \in H$.

Therefore for all $h \in H$: $h^{-1} = e_G h^{-1} \in H$,

therefore for $h_1, h_2 \in H$: $h_1 h_2 = h_1 (h_2^{-1})^{-1} \in H$. □

<u>Ex</u>: 1) Let $S \subseteq \mathbb{R}^\times$ be a subgroup.

Then $H = \{A \in GL_n(\mathbb{R}) \mid \det(A) \in S\}$

is a subgroup of $GL_n(\mathbb{R})$

$\left[GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\} \right]$

<u>Pf</u>: Linear algebra $\Rightarrow$ $\forall A \in GL_n(\mathbb{R})$:

$\exists B \in M_n(\mathbb{R}) : AB = BA = I_n = (\times)$

$\circ$ assoc. / I_n a unit

$\Rightarrow (GL_n(\mathbb{R}), \circ)$ is a group.

Take $A, B \in H \ni I_n$.

Then $\det(AB^{-1}) = \underbrace{\det(A)}_{\in S} \underbrace{\det(B)^{-1}}_{\in S}$

$\in S$

$\uparrow$ subgroup criteria

Thus $AB^{-1} \in H$.

$\Rightarrow H$ is a subgroup of G

For example $S = \{1, -1\} = \mathbb{Z}^\times$

2) Let $q : V \longrightarrow \mathbb{R}$ be a quadratic form, i.e. q satisfies

on an $\mathbb{R}$ v.s. V

- $q(\lambda v) = \lambda^2 q(v) \quad \forall \lambda \in \mathbb{R}, v \in V$ and
- $q(v+w) - q(v) - q(w)$ is a bilinear form.

$$U(q) := \{ f \in \mathrm{Aut}_{\mathbb{R}}(V) \mid q(f(v)) = q(v) \}$$

is a subgroup of $\mathrm{Aut}_{\mathbb{R}}(V)$, because $\mathrm{id}_V \in U(q)$ and for $f_1, f_2 \in U(q)$ we have

- $q(f_1 \circ f_2(v)) = q(f_1(f_2(v)))$
  $= q(f_2(v)) = q(v)$
- $q(v) = q(f_1(f_1^{-1}(v)))$
  $= q(f_1^{-1}(v))$. $\square$

<u>Ex:</u> $V = \mathbb{R}^n$, • $q(\underline{x}) = \sum_{i=1}^{n} x_i^2$

$U(q) = O(n)$

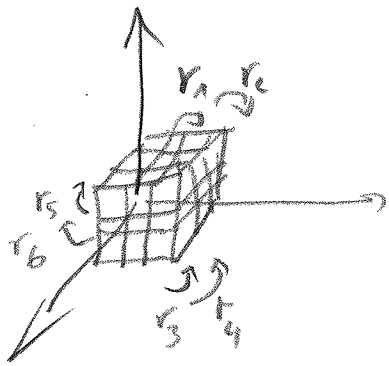
- $q(\underline{x}) = x_1^2 - x_2^2 - x_3^2 - x_4^2$

$U(q)$ = Lorentz group

$= O(1,3)$

$q(\underline{x}) = \sum_{i=1}^{\ell} x_i^2 - \sum_{i=\ell+1}^{n} x_i^2 \qquad U(q) = O(\ell, n-\ell)$

Symmetry group of a rubics cube



$C :=$ "Union of the open facets"

(There are 54 open facets)

We do not move the points on the 3 facets attached to $\underline{0}$.

We have 6 elementary maps $r_1, r_2, r_3, r_4, r_5, r_6$ (those are the rotations of the dices by $90°$)

$$\mathrm{Sym}(RC(3)) = \{ f \in \mathrm{Bij}(C) \mid \exists_m \exists_{s_1, \dots, s_m} \in \{r_1, \dots, r_6\}, \text{ s.t. } f = s_m \circ s_{m-1} \circ \dots \circ s_1 \}$$

$id_C \in \mathrm{Sym}(RC(3))$ and $r_i^4 = id_C$, i.e. $r_i^3 = r_i^{-1}$,

thus $\mathrm{Sym}(RC(3)) \neq \emptyset$ and $\forall f_1, f_2 \in \mathrm{Sym}(\ldots)$

$f_1 \circ f_2^{-1} \in \mathrm{Sym}(RC(3))$ and therefore

$\mathrm{Sym}(RC(3))$ is a subgroup of $\mathrm{Bij}(C)$.

I.4 permutation groups

If $1 \leq |X| < \infty$ then $(\mathrm{Bij}(X), \circ)$ is a finite group

If $X = \{1, 2, \ldots, n\}$, then we write

$$\mathfrak{S}_n := \mathrm{Bij}(X) = \text{"nth symmetric group"}$$

An element of $\mathfrak{S}_n$ is called <u>permutation of $\{1, \ldots, n\}$</u>. They can be written in the form

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \tau(1) & \tau(2) & \tau(3) & \cdots & \tau(n) \end{pmatrix}, \quad \tau \in \mathfrak{S}_n.$$

The set $\mathrm{supp}(\tau) := \{ i \in X \mid \tau(i) \neq i \}$ is called the support of τ. τ is called a <u>transposition</u> if $|\mathrm{supp}(\tau)| = 2$.

$$\begin{pmatrix} 1 & \cdots & a & \cdots & b & \cdots & n \\ 1 & & b & & a & & n \end{pmatrix} =: \langle a, b \rangle$$

<u>Prop 15:</u> Every $\sigma \in \mathfrak{S}_n$ is a product of transpositions.

<u>Proof:</u> (induction on n) <u>$n = 2$:</u> ✓

<u>$n > 2$:</u> If $\sigma(n) = n$ then apply (IH) on

$\sigma|_{\{1, \ldots, n-1\}} = \tilde{\sigma}$

$\tilde{\sigma} = \sigma|_{\{1,\dots,n-1\}} = \tilde{\tau}_1 \circ \tilde{\tau}_2 \circ \dots \circ \tilde{\tau}_t \qquad \tilde{\tau}_j \in \mathfrak{S}_{n-1}$ transposition

Extend $\tilde{\tau}_i$ to $\{1,\dots,n\}$: $\tau_i(x) := \begin{cases} \tilde{\tau}_i(x), & x < n \\ n, & x = n. \end{cases}$

$\Rightarrow \quad \sigma = \tau_1 \circ \dots \circ \tau_n.$

If $\sigma(n) \neq n$, Then consider $\langle \sigma(n), n \rangle \circ \sigma =: \rho$ satisfying $\rho(n) = n$.

So we find $\rho = \tau_1 \circ \dots \circ \tau_t$ and get

$$\sigma = \underbrace{\rho^{-1}}_{=\rho} \circ \tau_1 \circ \dots \circ \tau_t. \qquad \square$$

lecture 2

Ex: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 4 & 6 & 5 & 3 & 8 & 1 \end{pmatrix} = \langle 1,8 \rangle \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 4 & 6 & 5 & 3 & 1 & 8 \end{pmatrix}$

$= \langle 1,8 \rangle \circ \langle 1,7 \rangle \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 4 & 6 & 5 & 3 & 7 & 8 \end{pmatrix}$

$= \langle 1,8 \rangle \circ \langle 1,7 \rangle \circ \langle 6,3 \rangle \circ \langle 4,3 \rangle.$

Permutations can be decomposed in a canonical way: "cycle-decomposition".

For $\tau \in \mathfrak{S}_n$ the set $\{1,\dots,n\}$ is the union of the subsets $\{\tau^i(a) \mid i \in \mathbb{Z}\} =: \mathcal{O}_\tau(a)$ "τ-orbit of a".

Put $\text{orbits}(\tau) = \{ \mathcal{O}_\tau(a) \mid a \in \{1, \dots, n\} \}$.

<u>Def 16:</u> Let X be a set and $S \subseteq \mathcal{P}(X)$.
S is called a partition of X if

- $X = \bigcup_{Y \in S} Y$ and
- $\forall Y, Z \in S : Y \cap Z = \emptyset$

Write $\dot{\bigcup}_{Y \in S} Y = X$.

<u>Ex</u>: orbits(τ) is a partition of $\{1, \dots, n\}$:

$\mathcal{O}_\tau(a) \cap \mathcal{O}_\tau(b) \neq \emptyset \Rightarrow \exists\, i, j \in \mathbb{Z}$:
$(\tau^i(a) = b$ and $\tau^j(b) = a$.

$\Rightarrow \mathcal{O}_\tau(b) \subseteq \mathcal{O}_\tau(a) \subseteq \mathcal{O}_\tau(b)$

- concrete example:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 2 & 5 & 3 & 7 & 6 & 9 & 10 & 4 & 1 & 8 \end{pmatrix}$$

$\text{orbits}(\tau) = \{ \{1, 2, 5, 6, 9\}, \{4, 7, 10, 8\}, \{3\} \}$.

<u>Def 17:</u> $\tau \in S_n$ is called a cycle (or cyclic permutation) if τ has exactly one orbit $\mathcal{O}$ of size > 1.

$|\mathcal{O}|$ is then called the length of the cycle τ.

We say τ is an $|\mathcal{O}|$-cycle. With $\mathcal{O} = \text{orbit}(\tau)$ and $\tau = \langle a, \tau(a), \tau^2(a), \dots, \tau^{|\mathcal{O}|-1}(a) \rangle$, $a \in \mathcal{O}$.

<u>Ex:</u> $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 3 & 2 \end{pmatrix}$ has orbits $\{1\}$, $\{2,3,4,5\}$.

$\Rightarrow$ τ is a 4-cycle

$\tau = \langle 2, 4, 3, 5 \rangle$.

<u>Def 18:</u> We call an equation in S_n

$\tau = \sigma_1 \circ \sigma_2 \circ \dots \circ \sigma_\ell$ a "cycle-decomposition of τ" if

- each σ_i is a cycle and
- $\text{orbit}(\sigma_i) \cap \text{orbit}(\sigma_j) = \emptyset \ \forall i \neq j$.

<u>Prop 19:</u> Let τ be a permutation of $\{1, \dots, n\}$. Then: a) τ has a cycle-decomposition

b) if $\tau = \sigma_1 \circ \dots \circ \sigma_\ell = \sigma_1' \circ \dots \circ \sigma_{\ell'}'$ are two cycle-decompositions of τ

then $\ell = \ell'$ and $\exists f \in G_\ell$:

$\sigma_i = \sigma'_{f(i)}$ for all $i \in \{1, \dots, \ell\}$.

<u>Lemma 20:</u> Suppose $\tau_1, \tau_2 \in G_n$ are two permutation, s.t. $supp(\tau_1) \cap supp(\tau_2) = \emptyset$. We have

Then $\tau_1 \circ \tau_2 = \tau_2 \circ \tau_1$.

<u>Proof:</u> $x \in \{1, \dots, n\}$.

Case $x \in supp(\tau_1)$: ($\Rightarrow$ by assumption $x \notin supp(\tau_2)$)

$$\tau_1(\tau_2(x)) = \tau_1(x) \underset{\substack{\uparrow \\ \tau_1(x) \notin supp(\tau_2)\ (*)}}{=} \tau_2(\tau_1(x))$$

Proof of $(*)$: If $\tau_2(\tau_1(x)) \neq \tau_1(x)$

then by assumption $\tau_1(x) \notin supp(\tau_1)$

$\Rightarrow \tau_1^i(\tau_1(x)) = \tau_1(x)\ \forall i \in \mathbb{N}$.

But $\exists i > 0 : \tau_1^i(x) = x$.

So $\tau_1(x) = x$ ↯ □

□

other cases: exercise.

<u>Proof of Prop 19:</u> a) For $\sigma \in orbits(\tau)$ with $|\sigma| > 1$

we define $\tau_\sigma := \langle a, \tau(a), \tau^2(a), \dots, \tau^{|\sigma|-1}(a) \rangle$

Then put $\tilde{\tau} := \prod_{\substack{\sigma \in orbits(\tau) \\ |\sigma| > 1}} \tau_\sigma$. To show $\tau = \tilde{\tau}$.

Take $x \in \{1, \dots, n\}$.

<u>Case</u> $|\sigma_\tau(x)| > 1$. $\sigma_0 := \sigma_\tau(x)$

Lemma 20 $\Rightarrow \tilde{\tau} = \tau_{\sigma_0} \circ \left(\prod_{\substack{\sigma, |\sigma|>1 \\ \sigma \neq \sigma_0}} \tau_\sigma \right)$

x is not in the support of the right factor, because $\sigma \cap \sigma_0 = \emptyset$ for the involved τ-orbits.

$$\Rightarrow \tilde{\tau}(x) = \tau_{\sigma_0}(x) = \tau(x).$$

<u>Case: $\tau(x) = x$:</u> For every $\sigma \in \text{orbits}(\tau)$ with $|\sigma| > 1$ we have $\sigma \cap \underbrace{\sigma_\tau(x)}_{=\{x\}} = \emptyset$,

because orbits(τ) is a partition of $\{1, \dots, n\}$.

So $x \notin \text{supp}(\tilde{\tau})$. $\square$

b) We have $\underset{\text{of size}>1}{\text{orbits}}(\tau) = \{\text{orbit}(\sigma_1), \dots, \text{orbit}(\sigma_\ell)\}$
$= \{\text{orbit}(\sigma'_1), \dots, \text{orbit}(\sigma'_{\ell'})\}$

Compare cardinalities $\Rightarrow$ $\ell = \ell'$ and there is a bijection $f \in \mathfrak{S}_\ell$ s.t. $\text{orbit}(\sigma_i) = \text{orbit}(\sigma'_{f(i)})$ for all i.

Take $x \in \text{orbit}(\sigma_i)$: $\sigma_i(x) = \tau(x) = \sigma'_{f(i)}(x)$. $\square$

Def 21: $\tau \in \mathfrak{S}_n$. By Prop 15 $\exists\, \tau_1, \dots, \tau_k$ transpositions: $\tau = \tau_1 \circ \dots \circ \tau_k$. We call $\operatorname{sign}(\tau) := (-1)^k$ the "sign of τ".

Prop 22: (exercise using Prop 19) $\operatorname{sign}(\tau)$ is well-defined.

Def 23: A pair $(i,j) \in \{1, \dots, n\}^2$ with $i \neq j$ is called an inversion of a permutation $\tau \in \mathfrak{S}_n$, if $\tau(i) > \tau(j)$

$$\operatorname{Inv}(\tau) := \{(i,j) \mid \tau(i) > \tau(j)\}$$

Ex: $\operatorname{Inv}\left(\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 3 & 6 & 1 & 4 \end{pmatrix}\right) = \{(1,5), (2,3), (2,5), (2,4), (3,5), (4,5), (4,6)\}$

Prop 24: Every element of $\mathfrak{S}_n$ can be written as a product of transpositions $\in \{\langle 1,2\rangle, \langle 2,3\rangle, \dots, \langle n-1, n\rangle\} =: S$

Proof: (induction on n)

$n \in \{1,2\}$ ✓

$n > 2$: We only need to consider transpositions $\langle a, b\rangle$, by Prop. 19, and only $b = n$ by

the induction hypothesis. If $a = n-1$ ✓.

<u>$a < n-1$:</u> $\langle a, n\rangle = \langle n, n-1\rangle \circ \langle a, n-1\rangle \circ \langle n, n-1\rangle$ and $\langle a, n-1\rangle$ is a product of elements of S by induction hypothesis. $\square$

<u>Def 25:</u> $\pi \in \mathfrak{S}_n$. The <u>length of π</u> is the number

$$\ell(\pi) := \min\{k \in \mathbb{N}_0 \mid \exists s_1, \dots, s_k \in S : \pi = s_1 \circ \dots \circ s_k\}$$

<u>Prop 25:</u> Let $\pi \in \mathfrak{S}_n$. Then

$$\ell(\pi) = |\mathrm{Inv}(\pi)| =: \mathrm{inv}(\pi).$$

<u>Proof</u> <u>Step 1:</u> We show $\ell(\pi) \leq \mathrm{inv}(\pi)$

$\pi = \mathrm{id}_{\{1,\dots,n\}}$: $\ell(\pi) = 0 = \mathrm{inv}(\pi)$

(induction on $\mathrm{inv}(\pi)$)

<u>$\mathrm{inv}(\pi) = 0$:</u> $\Rightarrow \pi = \mathrm{id} \Rightarrow \ell(\pi) = 0 = \mathrm{inv}(\pi)$

<u>$\mathrm{inv}(\pi) > 0$:</u> Put $k := \min\{j - i \mid (i,j) \in \mathrm{Inv}(\pi)\}$

<u>Claim:</u> $k = 1$. Proof (claim):

If $j_0 > i_0+1$, $(i_0, j_0) \in \mathrm{Inv}(I)$ and $k = j_0 - i_0$

Then $I(i_0+1) > I(i_0)$, because

$(i_0, i_0+1) \notin \mathrm{Inv}(I)$, and $I(i_0+1) < I(j_0)$,

because $(i_0+1, j) \notin \mathrm{Inv}(I)$.

$$\Rightarrow \quad I(i_0+1) < I(j_0) < I(i_0) < I(i_0+1) \quad ↯$$

□ (claim)

Take $(i_0, i_0+1) \in \mathrm{Inv}(I)$.

Then $\mathrm{Inv}(I \circ \langle i_0, i_0+1 \rangle)$

$$= \{(i,j) \in \mathrm{Inv}(I) \mid i, j \notin \{i_0, i_0+1\}\}$$

$$\dot\cup \{(i, i_0) \mid (i, i_0+1) \in \mathrm{Inv}(I), i \neq i_0\}$$

$$\dot\cup \{(i, i_0+1) \mid (i, i_0) \in \mathrm{Inv}(I)\}$$

$$\dot\cup \{(i_0, j) \mid (i_0+1, j) \in \mathrm{Inv}(I)\}$$

$$\dot\cup \{(i_0+1, j) \mid j > i_0+1 \text{ and } (i_0, j) \in \mathrm{Inv}(I)\}$$

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & i_0 & i_0+1 & \cdots & n \\ I(1) & I(2) & I(3) & & I(i_0) & I(i_0+1) & \cdots & I(n) \end{pmatrix} \circ \langle i_0, i_0+1 \rangle$$

$$= \begin{pmatrix} 1 & 2 & 3 & \cdots & i_0 & i_0+1 & \cdots & n \\ I(1) & I(2) & I(3) & & I(i_0+1) & I(i_0) & & I(n) \end{pmatrix}$$

So $|\mathrm{Inv}(I \circ \langle i_0, i_0+1 \rangle)| = \mathrm{inv}(I) - 1$.

$$(IH) \Rightarrow \quad \ell(I \circ \langle i_0, i_0+1 \rangle) \leq \mathrm{inv}(I \circ \langle i_0, i_0+1 \rangle) = \mathrm{inv}(I) - 1$$

$$\Rightarrow \quad \ell(I) \leq \mathrm{inv}(I).$$ □ (Step 1)

<u>Step 2:</u> $\ell(\tau) = \mathrm{inv}(\tau) \; \forall_{\tau \in \mathfrak{S}_n}$.
(exercise) $\square$

<u>Corollary 26:</u> $\forall_{\tau \in \mathfrak{S}_n}: \mathrm{sgn}(\tau) = (-1)^{\mathrm{inv}(\tau)}$
$= (-1)^{\ell(\tau)}$.

<u>Def 27:</u> A permutation $\tau \in \mathfrak{S}_n$ is called even (odd) if $\mathrm{sgn}(\tau) = 1$ ($= -1$).
$A_n := \{\tau \in \mathfrak{S}_n \mid \mathrm{sgn}(\tau) = 1\}$ is a group with "$\circ$" called the <u>alternating group.</u>

⌈ <u>Pf.</u> (A_n is a group): $\mathrm{id} \in A_n$, so $A_n \neq \emptyset$.
$\tau_1, \tau_2 \in A_n$. Write τ_1 and τ_2 as product of transpositions.

$$\tau_1 = \tau_1' \circ \dots \circ \tau_\ell'$$
$$\tau_2 = \tau_1'' \circ \dots \circ \tau_k''$$

$$\Rightarrow \quad \tau_1 \circ \tau_2^{-1} = \tau_1' \circ \dots \circ \tau_\ell' \, \tau_k''^{-1} \circ \dots \circ \tau_1''^{-1}$$

$$\Rightarrow \quad \mathrm{sgn}(\tau_1 \circ \tau_2^{-1}) = (-1)^{\ell + k}$$
$$= (-1)^\ell (-1)^k$$
$$= \mathrm{sgn}(\tau_1)\,\mathrm{sgn}(\tau_2^{-1})$$
$$\underset{\tau_1, \tau_2 \in A_n}{=} 1 \cdot 1 = 1$$

$\Rightarrow I_1 \circ I_2^{-1} \in A_n$

Subgroup criterion $\Rightarrow (A_n, \circ)$ is a subgroup of $(\mathfrak{S}_n, \circ)$.

Lecture 3 end

Prop 28: Every element of A_n is a product of 3-cycles.

Proof: (by induction on n)

$1 \leq n \leq 2$. ✓

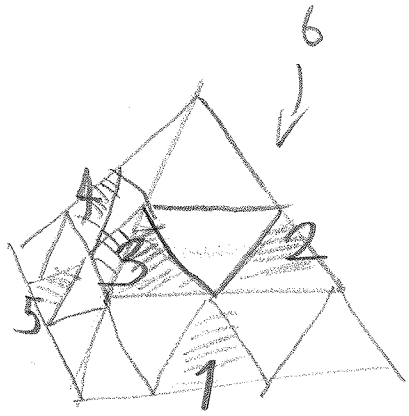
$n > 2$: Take $I \in A_n$. If $|supp(I)| < n$, say $i_0 \notin supp(I)$, then consider $I|_{\{1, \dots, \hat{i_0}, \dots, n\}}$ and apply the induction hypothesis and extend.

If $supp(I) = \{1, \dots, n\}$: Then $I(n) \neq n$, and take $i_0 \in \{1, \dots, n\} \setminus \{n, I(n)\}$ (which exists, because $n \geq 3$).

Then $(\langle I(n), n, i_0 \rangle \circ I)(n) = n$.

Now apply part one of the induction step to $\langle I(n), n, i_0 \rangle \circ I$. $\square$

Ex: A_6



6 stones.
There is a way to rotate the stones on one facet of the tetrahedron.

(1,2,3,4,5,6 are the positions!)

So we can perform

$\langle 1,3,2\rangle, \langle 5,4,3\rangle, \langle 1,5,6\rangle, \langle 4,6,2\rangle$

They are enough to generate A_6:

$\langle 1,2,3\rangle = \langle 1,3,2\rangle^2$

$\langle 1,2,4\rangle = \langle 3,4,5\rangle \circ \langle 1,2,3\rangle \circ \langle 5,4,3\rangle$

$\langle 1,2,5\rangle = \langle 3,4,5\rangle \circ \langle 1,2,4\rangle \circ \langle 5,4,3\rangle$

$\langle 1,3,4\rangle = \langle 4,6,2\rangle \circ \langle 1,3,2\rangle \circ \langle 2,6,4\rangle$

$\langle 1,3,5\rangle = \langle 1,2,4\rangle \circ \langle 5,4,3\rangle \circ \langle 4,2,1\rangle$

$\langle 1,3,6\rangle = \langle 4,6,2\rangle \circ \langle 1,3,4\rangle \circ \langle 2,6,4\rangle$

$\langle 1,2,6\rangle = \langle 1,3,4\rangle \circ \langle 2,6,4\rangle \circ \langle 4,3,1\rangle$

$\vdots$

$\langle 4,5,6\rangle =$ is given

$a<b<c$ $\quad \langle a,b,c\rangle = \langle 1,a,d\rangle \circ \langle 1,b,c\rangle \circ \langle a,1,d\rangle$

$d \notin \{a,b,c\}$

$1 \le d \le 6$

I.5. Cyclic groups

Def 29: Let $(G,*)$ be a monoid and $g \in G$.
The number (or ∞)
$$\operatorname{ord}(g) := \inf\{k \in \mathbb{N} \mid g^k = e_G\}$$
is called the order of g.

Note: $(\{g^i \mid i \in \mathbb{Z}\}, *)$ is a subgroup of G.
(Use the subgroup criterion.)

Def 30: Let $(G,*)$ be a group. G is called cyclic if $\exists\, g \in G$:
$$\langle g \rangle_G := \{g^i \mid i \in \mathbb{Z}\} = G.$$
We say "g generates G". Write $\langle g \rangle_G = G$.

Ex: 1) $(\mathbb{Z},+) = \langle 1 \rangle_{(\mathbb{Z},+)}$

$z \in \mathbb{Z}$. $z \geq 0$: $z = \overbrace{1+\dots+1}^{z \text{ times}}$

$z < 0$: $z = \underbrace{(-1)+\dots+(-1)}_{|z| \text{ times}}$.

2) $(\mathbb{Q}^\times, \cdot)$ is not cyclic.
If not, then $\exists\, g \in \mathbb{Q}^\times$: $\langle g \rangle_{\mathbb{Q}^\times} = \mathbb{Q}^\times$

$\Rightarrow \exists\, i,k \in \mathbb{Z}\setminus\{0\}: 2 = g^i \quad 3 = g^k$

$\Rightarrow \quad 2^k = 3^i \qquad (*)$

Either both sides have $|\cdot| > 1$ or
or — " — $|\cdot| < 1$.

$\Rightarrow$ Either $k, i \geq 1$ or $k, i \leq -1$.

W.l.o.g. $k, i \geq 1$. The left side of $(*)$ is even and the right side odd $\lightning$.

<u>Notation convention:</u>

a) If $(S, *)$ is an abelian semigroup and if we write $+$ for $*$, then we write ns for $\underbrace{s + \ldots + s}_{n \text{ times}}$ and $(-s)$ for the inverse of s (in the group case).

So if $(S, +)$ is an abelian group and $z \in \mathbb{Z}^{<0}$ then

$$zs := \underbrace{(-s) + \ldots + (-s)}_{-z \text{ times}}.$$

b) Let $(G, *)$ be a group and $H \subseteq G$. We write $H \leq G$ to say that

$(H, *)$ is a subgroup of $(G, *)$.

<u>Prop 31:</u> Let $(G, *)$ be a cyclic group and $H \leq G$.

a) H is cyclic

b) Suppose G to be finite.

Then

b1) For every generator g of G we have $\mathrm{ord}(g) = |G|$ and

$$G = \{e, g, g^2, \dots, g^{\mathrm{ord}(g)-1}\}$$

b2) There is a bijection

$$\{t \in \mathbb{N} \mid t \mid |G|\} \xrightarrow{\sim} \{H \mid H \leq G\}$$

<u>Proof:</u> a) $G = \langle g \rangle_G$. If $H = \{e_G\}$ ✓

If $H \neq \{e_G\}$ then $\exists\, i \in \mathbb{N}$:

$g^i \in H$. (and also $g \neq e_G$)

$i_0 := \min\{i \in \mathbb{N} \mid g^i \in H\}$

<u>Claim:</u> $H = \langle g^{i_0} \rangle_G$.

"$\supseteq$" ✓. "$\subseteq$" Take $h \in H \Rightarrow \exists\, j \in \mathbb{Z}: h = g^j$

To show $i_0 \mid j$.

If not then $\exists\, q \in \mathbb{Z},\ r \in \{1, \dots, i_0 - 1\}$:

$j = q i_0 + r$ (Euclidian algorithm)

$\Rightarrow g^r = g^j (g^{i_0})^{-q} \in H$ ↯ $(1 \leq r < i_0)$

b) If $G = \{e\}$ then there is nothing to show. Otherwise: $G = \langle g \rangle_G$ $g \neq e$

$G = \{g^i \mid i \in \mathbb{Z}\} = \{e, g, g^2, \dots, g^{\mathrm{ord}(g)-1}\}$

by the Euclidian algorithm (as above) dividing by $\mathrm{ord}(g)$. $\Rightarrow |G| \leq \mathrm{ord}(g)$

On the other hand for $0 \leq i < j \leq \mathrm{ord}(g)-1$

$$g^{j-i} \neq e \Rightarrow g^j \neq g^i.$$

So $|G| = \mathrm{ord}(g)$.

b2) $\{t \in \mathbb{N} \mid t \mid |G|\} \xrightarrow{\sim} \{H \mid H \leq G\}$

$$t \longmapsto \langle g^{\frac{|G|}{t}} \rangle_G$$

$$\langle g^{\frac{|G|}{t}} \rangle_G = \{e, g^{\frac{|G|}{t}}, \dots, g^{\frac{|G|}{t}(t-1)}\}$$

is a subgroup of order t, so the map is injective.

Take $H \leq G \overset{a)}{\Rightarrow} \exists\, j \in \mathbb{N} : \langle g^j \rangle_G = H$

Take j minimal. <u>Claim</u>: $j = \frac{|G|}{|H|}$.

In the next Lemma we show $|H| \mid |G|$. Take $j_0 := \frac{|G|}{|H|}$.

b1) $\Rightarrow |H| = \mathrm{ord}(g^j)$ and thus $g^{j \cdot |H|} = e$ and thus $\mathrm{ord}(g) \mid \underbrace{j \cdot |H|}_{j \cdot \frac{|G|}{j_0}}$. (Eucl. alg.)

Thus $j_0 \mid j$ and thus

$$\langle g^{j_0} \rangle_G \supseteq \langle g^j \rangle_G = H$$

and $|\langle g^{j_0}\rangle_G| = \frac{|G|}{d_0} = |H|$.

so $H = \langle g^{j_0}\rangle_G$.

$\Longrightarrow$ $j_0 = j$. $\square$

$1 \leq j_0 \leq j$, j minima

<u>Lemma 32</u> (Lagrange) Let $(G,*)$ be a group and $(H,*)$ a subgroup. then

$$\{ \underbrace{gH}_{\{gh \mid h \in H\}} \mid g \in G \}$$ is a partition

of G. If further G is finite, then $|H| \mid |G|$.

<u>Proof:</u> <u>Partition:</u> $g_1 H \cap g_2 H \neq \emptyset$

$\Longrightarrow \exists\, h_1, h_2 \in H: g_1 h_1 = g_2 h_2$

$\Longrightarrow \forall h \in H: g_1 h = g_2 g_2^{-1} g_1 h$

$= g_2 h_2 h_1^{-1} h \in g_2 H$

$\Longrightarrow g_1 H \subseteq g_2 H$.

$g_2 H \subseteq g_1 H$ similarly.

$g \in G \Rightarrow g = g \circ_G e \in gH$.

$\underline{|H| \mid |G|}$ (G finite): By part one we have

$$G = g_1 H \dot\cup g_2 H \dot\cup \dots \dot\cup g_\ell H$$

for some $g_1, \dots, g_\ell$, and the map $H \xrightarrow{l_g|_H} gH$ is bijective
$h \longmapsto gh$
for all $g \in G$. (The inverse is $l_{g^{-1}}|_{gH}$)

$$\Rightarrow |G| = |H| \cdot \ell \qquad \square$$

<u>Def/Remark:</u> Let $(G, *)$ be a group and $S \subseteq G$.

If $\langle S \rangle_G = G$, then we say "S is a set of generators for G".

Then $\langle S \rangle_G := \bigcap_{S \subseteq H \leq G} H$ is a subgroup of G by the subgroup criterion.

We have $\langle S \rangle_G = \{ g \in G \mid \exists_{\ell \in \mathbb{N}_0} \exists_{s_1, \dots, s_\ell \in S} \exists_{\varepsilon_1, \dots, \varepsilon_\ell \in \{\pm 1\}} : g = s_1^{\varepsilon_1} * \dots * s_\ell^{\varepsilon_\ell} \} =: \mathcal{L}(S)$

<u>Proof:</u> $\mathcal{L}(S) \supseteq S$ and $\mathcal{L}(S)$ is a subgroup of G by the subgroup criterion. So $\mathcal{L}(S) \supseteq \langle S \rangle_G$.

I.6 Homomorphisms

Def 33: 1) Let $(M_i, *_i)$, $i = 1,2$ be two magmas. A map $f: M_1 \to M_2$ is called a magma homomorphism if

$$\forall x, y \in M_1 : f(x *_1 y) = f(x) *_2 f(y).$$

(similar: semigroup homom. and group homom.)

Write $\mathrm{Hom}_{magma}(M_1, M_2) = \{f: M_1 \to M_2 \mid f \text{ magma homom.}\}$

2) Let $(M_i, *_i)$ be monoids, $i = 1,2$.

$f \in \mathrm{Hom}_{magma}(M_1, M_2)$ is called monoid homomorphism if $f(e_1) = e_2$ for the units.

Write $\mathrm{Hom}_{monoid}(M_1, M_2)$ for the set of those.

Notation: $\mathrm{Hom}_{sg}(S_1, S_2) = \{f: S_1 \to S_2 \mid f \in \mathrm{Hom}_{magma}(S_1, S_2)\}$

$\mathrm{Hom}_{gp}(G_1, G_2) = \mathrm{Hom}_{magma}(G_1, G_2)$

for semigroups S_1, S_2 and groups G_1, G_2.

<u>Ex:</u> 1) $f : (\mathbb{N}, +) \to (\mathbb{R}^{>0}, \cdot)$

$$f(n) := \left(\frac{1}{7}\right)^n .$$

$$f(n_1 + n_2) = \left(\frac{1}{7}\right)^{n_1+n_2} = \left(\frac{1}{7}\right)^{n_1} \cdot \left(\frac{1}{7}\right)^{n_2}$$
$$= f(n_1)\, f(n_2). \quad f \in \mathrm{Hom}_{sg}((\mathbb{N},+),(\mathbb{R}^{>0},\cdot))$$

2) $X \neq \emptyset$, $Y \subsetneq X$

$$f : (\mathcal{P}(X), \cap) \longrightarrow (\mathcal{P}(X), \cap)$$
$$f(A) := A \cap Y$$
$$f(A \cap B) = A \cap B \cap Y = (A \cap Y) \cap (B \cap Y)$$
$$= f(A) \cap f(B), \text{ but}$$
$$f(X) = X \cap Y = Y \neq X, \text{ so}$$
$$f \in \mathrm{Hom}_{sg}((\mathcal{P}(X),\cap),(\mathcal{P}(X),\cap)) \text{ and}$$
$$f \notin \mathrm{Hom}_{monoid}((\mathcal{P}(X),\cap),(\mathcal{P}(X),\cap)).$$

3) $\mathrm{vec}_{<\infty} = \{ [V]_{\cong} \mid V \text{ an } \mathbb{R} \text{ vector space of finite dimension} \}$

$[V]_{\cong}$ = "isomorphy class of V."
$= \{ W \mid W \ \mathbb{R}\text{ v.s.}\ W \cong V \}$

$$f : \mathrm{vec}_{<\infty} \longrightarrow \mathbb{N}_0$$

$$f([V]_{\cong}) := \dim_{\mathbb{R}} V$$

is a semigroup homomorphism w.r.t.

$(\mathrm{vec}_{<\infty}, \oplus)$ and $(\mathbb{N}_0, +)$.

4) · $f \in \mathrm{Hom}_{\mathbb{R}}(V,V) = \mathrm{End}_{\mathbb{R}}(V) =$ "$\mathbb{R}$-linear endomorphisms of V"

is a group homomorphism of $(V,+)$.

· $A \in M_n(\mathbb{R})$. $g(\underline{x}) := A\underline{x}$, $g : \mathbb{R}^n \to \mathbb{R}^n$

$$g(\underline{x}+\underline{y}) = A(\underline{x}+\underline{y}) = A\underline{x} + A\underline{y}$$
$$= g(\underline{x}) + g(\underline{y}).$$

<u>Def 34:</u> A homomorphism $f : M_1 \to M_2$ is called an isomorphism if $\exists\, g : M_2 \to M_1$ homomorphism: $f \circ g = id_{M_2}$ and $g \circ f = id_{M_1}$.

<u>Remark:</u> $f : (M_1, *_1) \to (M_2, *_2)$ is an isomorphism iff f isobijective homomorphism.

<u>Pf:</u> "$\Rightarrow$" ✓

"$\Leftarrow$" f bijective, so has an inverse $g : M_2 \to M_1$. Then for $x, y \in M_2$:

$$g(X *_2 Y) = g(f(g(X)) *_2 f(g(Y)))$$

$$\overset{f \in \mathrm{Hom}(N,M)}{=} g(f(g(X) *_1 g(Y)))$$

$$= g(X) *_1 g(Y). \qquad \square$$

<u>Remark:</u> Let G, G' be groups

1. $f \in \mathrm{Hom}_{gp}(G, G') \Rightarrow f(e) = e'$
2. $(f(x))^{-1} = f(x^{-1}) \quad \forall x \in G_1$
3. f injective $\Leftrightarrow \ker(f) = \{e\}$, where
   $\ker(f) := \{g \in G \mid f(g) = e'\}$
   "kernel of f".
4. $H \leq G,\ H' \leq G' \Rightarrow f(H) \leq G',\ f^{-1}(H') \leq G$.

<u>Proof:</u> 1. $f(e) = f(e * e) = f(e) * f(e)$

$$\underset{e' * f(e)}{\parallel} \underset{\text{cancellation}}{\Rightarrow} e' = f(e)$$

2. $f(x) * f(x^{-1}) = f(x * x^{-1}) = f(e) = e'$

$f(x^{-1}) * f(x) = \ldots = e'$

3. "$\Rightarrow$" f injective $\Rightarrow \underset{\ker(f)}{\underset{\parallel}{f^{-1}(e')}} = \{e\}$

"$\Leftarrow$" Suppose $\ker(f) = \{e\}$. Take $g_1, g_2 \in G$

s.t. $f(g_1) = f(g_2) \Rightarrow f(g_1)(f(g_2))^{-1} = e'$

$\underset{2.}{\Rightarrow} e' = f(g_1) f(g_2^{-1}) = f(g_1 g_2^{-1}) \underset{\ker(f) = \{e\}}{\Rightarrow} g_1 g_2^{-1} = e \Rightarrow g_1 = g_2$

4. We only show $f^{-1}(H) \leq G$.

$e \in f^{-1}(H) \Rightarrow f^{-1}(H) \neq \emptyset$

$g_1, g_2 \in f^{-1}(H) \Rightarrow f(g_1) \in H'$ and $f(g_2) \in H$

$\Rightarrow f(g_2^{-1}) = (f(g_2))^{-1} \in H'$, because $H' \leq G'$.

So $f(g_1 g_2^{-1}) = f(g_1) f(g_2^{-1}) \in H'$

$\Rightarrow g_1 g_2^{-1} \in H'$ $\square$

<u>Ex</u>: · $\mathcal{M}_f^{2,cp,c} := \{ [S]_{homeo} \mid S$ compact, closed surface $\}$

$[S]_{homeo} = \{ S' \mid S'$ compact, closed surface homeomorphic to $S \}$

· Given two surfaces S_1, S_2, remove small discs $D_1 \subseteq S_1$ and $D_2 \subseteq S_2$

and glue them along the discs, more precisely take $D_i' \subsetneq D_i^\circ$

The result is a surface $S_1 \# S_2$

$$\rightsquigarrow \quad [S_1] \# [S_2] := [S_1 \# S_2]$$

"connected sum" (well-defined)

$(\mathcal{M}^{2,CP,c}, \#)$ is a monoid, abelian

<u>Fact:</u> Every $[S]$ is a connected sum of $[S^2]$, $[\bigcirc]$, $[\mathbb{P}^2] = [$  $]$

antipodal identification.

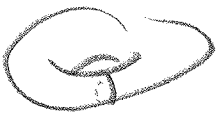
<u>Genus of S:</u> maximal number of simple closed curves on S, one can choose, s.t. after removing them S doesn't fall apart.

<u>Ex:</u> S^2 

Take any closed simple curve

$\Rightarrow S^2$ falls into 2 pieces.

$\Rightarrow \text{genus}(S^2) = 0$

T^2 

$\text{genus}(T^2) = 1$

$$f : \mathcal{M}^{2,CP,c} \longrightarrow \mathbb{N}_0 \quad f([S]) = \text{genus}([S])$$

is not a homomorphism, but when restricted to orientable surfaces:

$[$  $]^{\#n}$, then it is a homomorphism.

<u>Not</u> $\mathrm{End}(G) = \mathrm{Hom}(G,G)$, $\mathrm{Aut}(G) = \{f \in \mathrm{End}(G) \mid f \text{ bijective}\}$

$\mathrm{Iso}(G_1,G_2) = \{f \in \mathrm{Hom}(G_1,G_2) \mid f \text{ bij.}\}$

<u>Ex</u> 1) $\mathrm{End}(\mathbb{Z},+) = \{f : \mathbb{Z} \to \mathbb{Z} \mid f \text{ group homom}\}$

$\overset{\Phi}{\underset{\sim}{\sim}} \mathbb{Z}$, via

$\Phi(f) := f(1)$

In fact $\mathrm{End}(\mathbb{Z},+)$ forms a group w.r.t.

$(f+g)(z) := f(z) + g(z)$ (exercise)

Φ is a group isomorphism. $(\mathrm{End}(\mathbb{Z}),+) \simeq (\mathbb{Z},+)$

- $\Phi(f+g) = (f+g)(1) = f(1) + g(1)$
  $= \Phi(f) + \Phi(g)$

- $\ker \Phi = \{f \in \mathrm{End}(\mathbb{Z},+) \mid \Phi(f) = 0\}$

  $= \{ \quad " \quad f(1) = 0\}$

  $= \{0\}$ zero map.

$\left(f(1) = 0 \Rightarrow 0 = z f(1) = \begin{cases} f(1) + \dots + f(1) \\ (-f(1)) + \dots + f(-1) \end{cases} \overset{z \in \mathbb{Z}}{=} f(z).\right)$

- Surjectivity: $z \in \mathbb{Z}$

$f(x) := zx$

$\Rightarrow f(x+y) = z(x+y) = zx + zy = f(x) + f(y)$

and $\Phi(f) = f(1) = z\,1 = z$.

If $\Phi(f) = z$, then $\operatorname{im} f = z\mathbb{Z}$ and $\ker(f) = \begin{cases} 0, & z \neq 0 \\ \mathbb{Z}, & z = 0. \end{cases}$

2) G a group. $f \in \operatorname{Aut}(G)$ is called inner automorphism if $\exists\, g \in G\ \forall_{x \in G}$

$f(x) = gxg^{-1} =: \operatorname{int}(g)(x)$.

$\operatorname{Inn}(G) := \{\operatorname{int}(g) \mid g \in G\}$

$(\operatorname{Aut}(G), \circ) \leq (\operatorname{Bij}(G), \circ)$ by the subgroup criterion.

- $\operatorname{int}(g) \in \operatorname{End}(G)$ with inverse $\operatorname{int}(g^{-1})$

$\ulcorner \operatorname{int}(g)(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \operatorname{int}(g)(x)\,\operatorname{int}(g)(y)$.

$(\operatorname{int}(g) \circ \operatorname{int}(g^{-1}))(x) = gg^{-1}xgg^{-1} = x = \mathrm{id}_G = \operatorname{int}(e)$.

$= \operatorname{int}(g^{-1}) \circ \operatorname{int}(g)(x)$ $\lrcorner$

- Consider $G \xrightarrow{\operatorname{int}} \operatorname{Aut}(G)$

$g \longmapsto \operatorname{int}(g)$

int is a group homomorphism

$$\mathrm{int}(g_1 g_2)(x) = g_1 g_2 x g_2^{-1} g_1^{-1}$$
$$= \mathrm{int}(g_1)(\mathrm{int}(g_2)(x))$$
$$= (\mathrm{int}(g_1) \circ \mathrm{int}(g_2))(x).$$

$\Rightarrow$ $\mathrm{Inn}(G) = \mathrm{Im}(\mathrm{int})$ and

$$C(G) = \mathrm{Ker}(\mathrm{int})$$
$$= \{g \in G \mid \mathrm{int}(g) = \mathrm{id}_G\}$$
$$= \{g \in G \mid gxg^{-1} = x \ \forall x \in G\}$$
$$= \text{"center of } G\text{"}$$

are subgroups of $\mathrm{Aut}(G)$, resp. G.

lecture 5

Ex: · G abelian $\Rightarrow C(G) = G$

· $C(S_n) = \begin{cases} S_n, & n = 1,2,3 \\ \{id\}, & n \geq 4 \end{cases}$

· $C(GL_2(\mathbb{R})) = \left\{ \begin{pmatrix} \lambda & \\ & \lambda \end{pmatrix} \middle| \lambda \in \mathbb{R} \right\}$

· $C(U_2(\mathbb{C}/\mathbb{R})) = C(\{A \in GL_2(\mathbb{C}) \mid \bar{A}^t = A^{-1}\}) \simeq S^1$.

I.7 Factor groups

<u>Recap</u>: (equivalence relation)
$M \neq \emptyset$. A relation on M is a set $R \subseteq M \times M$. Instead of $(x,y) \in R$ we write xRy.

<u>Def 35</u>: R is called an <u>equivalence relation</u> if

(E1) $\forall x \in M: xRx$ (reflexive)

(E2) $\forall x,y \in M: (xRy \Rightarrow yRx)$ (symmetric)

(E3) $\forall x,y,z \in M: (xRy\,Rz \Rightarrow xRz)$ (transitive)

<u>Prop 36</u>: $\exists$ bijection

$$\{R \mid R \text{ equiv. relation on } M\} \xrightarrow{\sim} \{P \subseteq \mathcal{P}(M) \mid P \text{ partition of } M\}$$

<u>Proof</u>: Given R, define

$$P_R = \{ [x]_R \mid x \in M \}$$

where $[x]_R = \{ y \in M \mid yRx \}$

"R-equivalence class of x"

$[x]_R \cap [y]_R \neq \emptyset \Rightarrow \exists z \in M$

$xRz \wedge zRy \Rightarrow xRy \Rightarrow y \in [x]_R$

transitivity $\Rightarrow [y]_R \subseteq [x]_R$

"$\supseteq$" similar.

Conversely let P be a partition of M. Define

$$R_P = \{ (x,y) \mid \exists S \in P : x,y \in S \}$$

Notice: This set S is unique, because P is a partition.

So R_P is an equivalence relation $\square$

<u>Def 37</u>: Let G be a group, $H \leq G$, $g \in G$.

$$gH = \{gh \mid h \in H\}$$ "<u>left-coset</u>" <u>H-left-coset for g</u>"

$$Hg = \{hg \mid h \in H\}$$ – " – with right.

$x \in gH$ is called a "coset representative".

$$G/H := \{gH \mid g \in G\}$$ <u>left factor set</u>

$$H\backslash G := \{Hg \mid g \in G\}$$ ...

Lagrange $\Rightarrow$ G/H and $H\backslash G$ are partitions. So let's describe the equivalence relations $\sim_H$ and $_H\sim$.

<u>$\sim_H$</u>: $g_1 \sim_H g_2 \Leftrightarrow \exists\, g \in G \;\; g_1, g_2 \in gH$

$\Leftrightarrow \exists g \in G \; \exists h_1, h_2 \in H: \quad g_1 = g h_1$

$g_2 = g h_2$

$\Leftrightarrow \quad g_1^{-1} g_2 \in H$

("$\Rightarrow$" ✓ "$\Leftarrow$" Take $g = g_2$)

$g_1 \underset{H}{\sim} g_2 \Leftrightarrow g_1 g_2^{-1} \in H.$

$(G:H) := |G/H| =$ "index of H in G".

<u>Example</u>: 1) $G = \mathfrak{S}_3 =$ 3rd symmetric group.

$A_3 \leq \mathfrak{S}_3$

1a) $\mathfrak{S}_3 / A_3 = \{ \langle 1,2 \rangle A_3, A_3 \}$

1b) $A_3 \backslash \mathfrak{S}_3 = \{ A_3 \langle 1,2 \rangle, A_3 \}$

<u>Proof</u> 1a) $\sigma \in \mathfrak{S}_3$ even:

$\sigma A_3 \subseteq A_3$ and $\sigma^{-1} A_3 \subseteq A_3$

So $\sigma A_3 \subseteq A_3 \subseteq \sigma A_3 = A_3$.

$\sigma \in \mathfrak{S}_3$ odd: Then $\langle 1,2 \rangle \circ \sigma$ is even

So $(\langle 1,2\rangle \circ \sigma) A_3 = A_3$,

so $\sigma A_3 = \underbrace{\langle 1,2\rangle}_{(\langle 1,2\rangle^{-1})} A_3$. $\square$

Both are partitions of $\mathfrak{S}_3$, so

$\langle 1,2\rangle A_3 = A_3 \langle 1,2\rangle$.

1 c) $\tau := \langle 1,2\rangle \in \mathfrak{S}_3$. $H := \langle \tau \rangle_{\mathfrak{S}_3}$

$= \{ id, \tau \}$

<u>Claim</u>: $\mathfrak{S}_3 / H = \{ \sigma H \mid \sigma \in A_3 \}$

$= \{ \langle 1,2,3\rangle H, \langle 1,3,2\rangle H, H \}$

Check: This is a partition of $\mathfrak{S}_3$ by H-left-cosets.

2) $G = (\mathbb{Z}, +)$, $H \leq \mathbb{Z}$

Prop 31 $\Rightarrow \exists\, n \in \mathbb{N}_0$: $H = \langle n \rangle_{(\mathbb{Z},+)}$

$= \{ \underbrace{n + \dots + n}_{z \text{ times}} \mid z \in \mathbb{Z} \}$

$= \{ \underbrace{z + \dots + z}_{n \text{-times}} \mid z \in \mathbb{Z} \} = n\mathbb{Z}$.

What is $\sim_{n\mathbb{Z}}$.

$$\mathbb{Z}/n\mathbb{Z} = \{ z + n\mathbb{Z} \mid z \in \mathbb{Z} \} = \mathbb{Z}/n\mathbb{Z}$$

$$z + n\mathbb{Z} = \{ z + n\tilde{z} \mid \tilde{z} \in \mathbb{Z} \} = \{ n\tilde{z} + z \mid \tilde{z} \in \mathbb{Z} \}$$

$$= n\mathbb{Z} + z.$$

$$z_1 \sim_{n\mathbb{Z}} z_2 \Leftrightarrow (-z_1) + z_2 \in n\mathbb{Z}$$

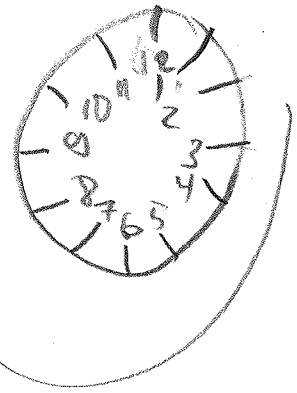
$$\Leftrightarrow \exists \tilde{z} \in \mathbb{Z} : z_2 - z_1 = n\tilde{z}$$

$$\Leftrightarrow n \mid z_2 - z_1.$$

$$\overset{\text{def.}}{\Leftrightarrow} z_2 \equiv_n z_1$$

"z_2 is congruent to z_1 modulo n".

How to view this:



$$\cdots \equiv_{12} 42 \equiv_{12} 30 \equiv_{12} 18 \cdots$$

$$\equiv_{12} 6 \equiv_{12} -6 \equiv_{12} \cdots$$

Also write $z_1 \equiv z_2 \mod n$.

$[z_1]_n = [z]_{\sim_n}$ Congruence class of z. mod n.

$\mathbb{Z}/n\mathbb{Z}$ "$\underbrace{\text{set of integers}}_{\mathbb{Z}}$ $\underbrace{\text{modulo } n}_{/n\mathbb{Z}}$"

<u>Def 38</u>: Let G be a group. $H \leq G$ is called a <u>normal</u> subgroup of G (write $H \trianglelefteq G$) if $\forall_{g \in G}$: $gHg^{-1} := \{ghg^{-1} \mid h \in H\} = H$

<u>Prop 39</u>: Let G be a group and $H \leq G$.

<u>T.a.e.</u>: 1° $H \trianglelefteq G$

2° $G/H = H\backslash G$

3° $\forall_{g \in G}$: $gH = Hg$

4° $\exists$ $\bar{*}$: $G/H \times G/H \to G/H$

s.t. the diagram

$$\begin{tikzcd}
(x,y) \; G \times G \arrow[r, mapsto] \arrow[d] & x*y \; G/H \\
(xH, yH) \; G/H \times G/H \arrow[ur, "\bar{*}"] &
\end{tikzcd}$$

is commutative.

<u>Proof:</u> <u>$3^\circ \Rightarrow 2^\circ$:</u> ✓

<u>$2^\circ \Rightarrow 3^\circ$:</u> $gH \cap Hg \ni g$

$G/H \underset{2^\circ}{=} G$ is a partition

$gH = Hg$.

$1^\circ \Rightarrow 3^\circ$ $\Rightarrow$ $gH = \{ghg^{-1}g \mid h \in H\}$

$= (gHg^{-1})g \underset{1^\circ}{=} Hg$

$3^\circ \Rightarrow 1^\circ$ Exercise.

$1^\circ \Rightarrow 4^\circ$ Define

$$\bar{*}(\underbrace{[x]_H}_{xH}, \underbrace{[y]_H}_{yH}) := \underbrace{[xy]_H}_{xyH}$$

<u>Claim</u> $\bar{*}$ is well-defined.

<u>Proof:</u> $[x]_H = [\tilde{x}]_H$, $[y]_H = [\tilde{y}_H]$

$\Rightarrow \exists\, h_x, h_y \in H$: $x = \tilde{x} h_x$

$y = \tilde{y} h_y$

$$xy = \tilde{x} h_x \tilde{y} h_y = \tilde{x}\tilde{y} \underbrace{\tilde{y}^{-1} h_x \tilde{y}}_{\in H} h_y$$

So $xyH = \tilde{x}\tilde{y}H$.

$\square$ (Claim)

$4^\circ \Rightarrow 1^\circ$ Take $g \in G$, $h \in H$. To show

$$ghg^{-1} \in H.$$

We have

$$\bar{*}([h]_H, [g^{-1}]_H) = *([1]_H, [g^{-1}]_H)$$

$$\begin{array}{ccc} \| & & \| \\ hg^{-1}H & & g^{-1}H \end{array}$$

$$\Rightarrow \quad ghg^{-1} \in H \qquad \square$$

$\sim_H$

<u>Corollary 40:</u> $H \trianglelefteq G$. Then

$(G/H, \bar{*})$ is a group. "Factor group of G by H"

<u>Proof:</u> associativity:

$$([x] \bar{*} [y]) \bar{*} [z]$$

$$= [x * y] \bar{*} [z] = [(x * y) * z]$$

$$= [x * (y * z)] = [x] \bar{*} [y * z] = [x] \bar{*} ([y] \bar{*} [z])$$

unit: $[e] \bar{*} [x] = [x] = [x * e]$

$$= [x] \bar{*} [e]$$

inverses: $[x] \bar{*} [x^{-1}] = [x^{-1}] \bar{*} [x] = [e]$

$\square$

<u>Ex</u> 1) $(\mathbb{Z},+) \trianglerighteq (n\mathbb{Z},+)$

$(\mathbb{Z}/n\mathbb{Z},+)$ $\quad [z]_n + [\tilde{z}]_n$

$$\overset{\shortparallel}{[z+\tilde{z}]_n}.$$

2) $(G,*)$ a group.

$\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$

(exercise)

$\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G)$

"outer automorphism group"

<u>Ex</u> a) $\mathrm{Out}(\mathbb{Z}/n\mathbb{Z}) \simeq \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$

because $\mathrm{Inn}(\mathbb{Z}/n\mathbb{Z}) = \{\mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}\}$

b) $\mathrm{Out}(\mathfrak{S}_3) = \{[\mathrm{id}_{\mathfrak{S}_3}]_{\mathrm{Inn}(\mathfrak{S}_3)}\}$

<u>lecture 6</u>

For an automorphism $\varphi \in \mathrm{Aut}(\mathfrak{S}_3)$

it is enough to know

$$\underbrace{\varphi(\langle 1,2\rangle)}_{\substack{3\text{-choices}\\ (\text{order } 2)}} \text{ and } \underbrace{\varphi(\langle 1,2,3\rangle)}_{\substack{2 \text{ choices}\\ (\text{order } 3)}}$$

$\Rightarrow$ At most 6 automorphisms.

$$C(\mathfrak{S}_3) = \ker(\mathrm{int})$$

$$= \{\tau \in \mathfrak{S}_3 \mid \forall \sigma \in \mathfrak{S}_3 : \sigma\tau = \tau\sigma\}$$

$$= \{\mathrm{id}_{\{1,2,3\}}\}.$$

exercise

$\Rightarrow$ int is injective $\Rightarrow |\mathrm{Im}(G)| = 6$.

$\mathrm{Aut}(G) \setminus \mathrm{Im}(\mathrm{int}) =$ "set of outer automorphisms

I.8. Isomorphism theorems

Theorem 41: Let G, G' be groups and $H \trianglelefteq G$. Then, for every $f \in \mathrm{Hom}_{gp}(G, G')$, are equivalent:

1° $\exists\, \bar{f} : G/H \to G'$

s.t. $\bar{f} \circ \pi_H = f$ $\left(\pi_H : G \to G/H,\ g \mapsto [g]\right)$

2° $\exists!\, \bar{f}$ ... (as in 1°)

3° $H \subseteq \mathrm{Ker}(f)$

Proof: $2° \Rightarrow 1°$ ✓

$1° \Rightarrow 3°$: $h \in H \Rightarrow f(h) = \bar{f}([h])$

$$\overset{\shortparallel}{e' = f(e) = \bar{f}([e])}$$

$\Rightarrow h \in \mathrm{Ker}(f)$

$3° \Rightarrow 2°$: Uniqueness:

$$\bar{f}_1([g]) = (\bar{f}_1 \circ \pi)(g) = f(g)$$

$$\bar{f}_2([g]) = (\bar{f}_2 \circ \pi)(g) = f(g)$$

<u>Existence:</u> Define $\bar{f}([g]) := f(g)$.

<u>Well-defined:</u> $[g] = [\tilde{g}]$

$$\Rightarrow \quad g^{-1}\tilde{g} \in H \underset{\uparrow 3^\circ}{\subseteq} \ker(f)$$

$$\Rightarrow e' = f(g^{-1}\tilde{g}) = f(g)^{-1} f(\tilde{g})$$

$$\Rightarrow f(\tilde{g}) = f(g).$$

Homomorphism: exercise. $\square$

<u>Corollary 42:</u> Let $H \leq \ker(f)$ and $H \trianglelefteq G$.

Then $\bar{f} \in \mathrm{Iso}(G/H, \mathrm{im}(f)) \Leftrightarrow$

$$\ker(f) = H.$$

<u>Proof:</u> $\ker(\bar{f}) = \{[g] \mid f(g) = e\}$

$$= \ker(f)/H. \quad \square$$

$e_1 = (1,0)$
$e_2 = (0,1)$

Ex: 1) $\mathbb{R}$-vector spaces

$$V := \mathbb{R} \oplus \mathbb{R} \xrightarrow{f} \mathbb{R} \oplus \mathbb{R}$$

$$f(\underbrace{x,y}_{xe_1 + ye_2}) := (x+y, x+y) = (x+y)(e_1+e_2)$$

$$\ker(f) = \{(x,y) \in \mathbb{R}^2 \mid x+y = 0\}$$
$$= \{(x,-x) \mid x \in \mathbb{R}\}$$
$$= \mathbb{R}(e_1 - e_2)$$

$$\operatorname{im} f = \{(x+y)\cdot(e_1+e_2) \mid x,y \in \mathbb{R}\}$$
$$= \mathbb{R}(e_1+e_2)$$

Corollary 42 $\Rightarrow$ $V/\mathbb{R}(e_1-e_2) \cong \mathbb{R}(e_1+e_2)$

as groups "+". (In fact as $\mathbb{R}$-vector spaces)

2) $\mathfrak{S}_4$ has 3 cyclic subgroups of order 4:

$$X_1 = \langle \langle 1,2,3,4 \rangle \rangle_{\mathfrak{S}_4}$$
$$X_2 = \langle \langle 1,3,2,4 \rangle \rangle_{\mathfrak{S}_4}$$
$$X_3 = \langle \langle 1,3,4,2 \rangle \rangle_{\mathfrak{S}_4}$$

We have for $\tau \in \mathfrak{S}_4$ a map on $S = \{X_1, X_2, X_3\}$

$$c_\tau : S \longrightarrow S \quad X \longmapsto \tau X \tau^{-1}$$

(permuting the cyclic subgroups of order 4)

$$f : \mathfrak{S}_4 \xrightarrow{\tau \mapsto c_\tau} \mathrm{Bij}(S) \text{ is a group}$$

homomorphism

$$\begin{aligned} f(\tau_1 \tau_2)(X) &= \tau_1 \tau_2 X \tau_2^{-1} \tau_1^{-1} \\ &= \tau_1 f(\tau_2)(X) \tau_1^{-1} \\ &= (f(\tau_1) \circ f(\tau_2))(X) \end{aligned}$$

$$\Rightarrow f(\tau_1 \tau_2) = f(\tau_1) \circ f(\tau_2).$$

<u>Claim:</u>

$\mathrm{Ker}(f) = K_4 = \{id, \langle 1,2\rangle\langle 3,4\rangle, \langle 3,1\rangle\langle 2,4\rangle, \langle 1,4\rangle\langle 2,3\rangle\}$ and f is surjective

$$\Rightarrow \mathfrak{S}_4 / K_4 \simeq \mathfrak{S}_3$$

<u>Proof:</u> $\langle 1,2,3,4\rangle \overset{L}{=} \langle 1,3\rangle\langle 2,4\rangle$

Take $\tau \in \mathrm{Ker}(f)$.

$$\tau \langle 1,3\rangle\langle 2,4\rangle \tau^{-1}$$

$$= \langle \tau(1),\tau(3)\rangle \circ \langle \tau(2),\tau(4)\rangle \quad \mathrm{I}$$

$$= \langle 1,3\rangle\langle 2,4\rangle$$

If $\tau(1)=1$, then $\tau(3)=3$

$$\tau\langle 1,2\rangle\langle 3,4\rangle\tau^{-1} \qquad \mathrm{II}$$

$$= \langle 1,2\rangle\langle 3,4\rangle$$

$\Rightarrow \tau(2)=2$ or $\tau(4)=4$, so $\tau = id$

If $\tau(1)=2$, then Then (II) $\tau(2)=1$ and

(I) $\tau(3)=4$. $\quad \tau = \langle 1,2\rangle\langle 3,4\rangle$

If $\tau(1)=3$: $\quad \tau = \langle 1,3\rangle\langle 2,4\rangle$

If $\tau(1)=4$ $\quad \tau = \langle 1,4\rangle\langle 2,3\rangle$

Check: They also are in the kernel.

So $\ker(f) = \{id, \langle 1,2\rangle\langle 3,4\rangle, \langle 1,3\rangle\langle 2,4\rangle, \langle 1,4\rangle\langle 2,3\rangle\} = K_4$

$\overset{42}{\Rightarrow}$ $\mathfrak{S}_4/K_4 \simeq \mathrm{im} f$ and

$$|\mathrm{im} f| = \frac{|\mathfrak{S}_4|}{|K_4|} = \frac{24}{4} = 6 = |Bij(S)|$$

So $\mathrm{im} f = Bij(S) \simeq \mathfrak{S}_3$ $\square$

<u>Theorem 43:</u> (Noether) Let G be a group, $G \geq N, H$

① If $N \supseteq H$ and $G \trianglerighteq N$, $G \trianglerighteq H$

then $$\frac{G/H}{N/H} \simeq G/N$$

② If $N \trianglelefteq G$, then $HN \leq G$
$$HN = \{hn \mid h \in H, n \in N\}$$

and $$HN/N \simeq H/H \cap N$$

(as groups)

<u>Proof:</u> ① homework

② HN is a group: $e = ee \in HN$

$h_1 n_1, h_2 n_2 \in HN$

$$\Rightarrow h_1 n_1 n_2^{-1} h_2^{-1} = h_1 h_2^{-1} \overbrace{h_2 n_1 n_2^{-1} h_2^{-1}}^{\in N}$$
$$\in HN$$

subgroup criterion $\Rightarrow HN \leq G$

Define $f : H \longrightarrow HN/N$ $\quad f(h) = [h]_N$

$$\ker(f) = \{h \in H \mid f(h) = [e]_N\} = \{h \in H \mid [h]_N = [e]_N\}$$

$$f(h_1 h_2) = [h_1 h_2]_N = [h_1]_N [h_2]_N = f(h_1) f(h_2)$$

$= \{h \in H \mid e'h \in N\} = H \cap N$

$\mathrm{im}(f) = \{f(h) \mid h \in H\} = \{[h]_N \mid h \in H\}$

$= \{hN \mid h \in H\} \underset{nN=N}{=} \{hnN \mid h \in H, n \in N\}$

$= HN/N$

Corollary 4.2 $\Rightarrow$ $H/H\cap N \cong HN/N$ $\square$

<u>Example</u>: $DA_4 \subseteq S_4$ $\quad K_4 \subseteq A_4$ Kleinian 4 group. $K_4 = \{id, \langle 1,2\rangle\circ\langle 3,4\rangle, \langle 1,3\rangle\circ\langle 2,4\rangle, \langle 1,4\rangle\circ\langle 2,3\rangle\}$

$H := \{\langle 1,2,3\rangle, \langle 1,3,2\rangle, id\}$

$= \langle \langle 1,2,3\rangle \rangle_{S_4}$.

$K_4 \trianglelefteq S_4$, because it is a kernel of a homomorphism $S_4 \to G'$.
(in fact we can take $G' = S_3$)

and $K_4 \cap H = \{id\}$ (*)

because this intersection has order $|4$ and $|3$.

$$K_4H / K_4 \simeq H / H \cap K_4 \simeq H.$$

Because of (*) we have a bijection of sets

$$K_4 \times H \simeq K_4H \leq A_4$$
$$(k, h) \longmapsto kh$$

$(k_1h_1 = k_2h_2 \Rightarrow k_2^{-1}k_1 = h_2h_1^{-1} \in K_4 \cap H = \{id\}$
$\Rightarrow k_1 = k_2$ and $h_1 = h_2$.)

Thus $|K_4H| = 4 \cdot 3 = 12 = |A_4|$

$\Rightarrow K_4H = A_4$.

$\Rightarrow A_4 / K_4 \simeq H.$

2) $n, m \in \mathbb{Z}$. $n\mathbb{Z}, m\mathbb{Z} \leq \mathbb{Z}$

$$n\mathbb{Z} + m\mathbb{Z} / m\mathbb{Z} \simeq n\mathbb{Z} / n\mathbb{Z} \cap m\mathbb{Z}.$$

(I) $n\mathbb{Z} \cap m\mathbb{Z} = \operatorname{lcm}(n,m)\mathbb{Z}$

(II) $n\mathbb{Z} + m\mathbb{Z} = \gcd(n,m)\mathbb{Z}$

<u>Proof (II)</u>: Bezout's lemma $\Rightarrow \exists\, a, b \in \mathbb{Z}$:

so $\gcd(n,m) = an + bm$.

Thus we have "$\supseteq$".

On the other hand: $\gcd(n,m)\mathbb{Z} \supseteq n\mathbb{Z}$

and $\supseteq m\mathbb{Z}$ $\square$

Thus $$\gcd(n,m)\mathbb{Z} / m\mathbb{Z} \simeq n\mathbb{Z} / \operatorname{lcm}(n,m)\mathbb{Z}.$$

$n = 4$, $m = 6$ $\quad 2\mathbb{Z}/6\mathbb{Z} \simeq 4\mathbb{Z}/12\mathbb{Z}.$

I.8. Structure theorem for ~~abel~~ f.g. abelian groups

Def 4.4: A group G is called <u>finitely generated</u> if $\exists\, S \subseteq G$ finite: $\langle S \rangle_G = G$.

Thm 45: (elementary divisor thm) Let G be a finitely generated abelian group. Then $\exists!\, m, \ell \in \mathbb{N}_0$ $\exists!\, n_1, \dots, n_\ell \in \mathbb{N}^{>1}$: $n_1 | n_2 | n_3 | \dots | n_\ell$ and $G \simeq \mathbb{Z}^m \times \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \times \dots \times \mathbb{Z}/n_\ell\mathbb{Z}$.

Def 46: Let $(G, *)$ be an abelian group.
$\mathrm{Tor}(G) := \{ g \in G \mid \exists\, n \in \mathbb{Z} : g^n = e \}$
is called the torsion subgroup of G.

Rem 47: 1) $\mathrm{Tor}(G) \trianglelefteq G$.
2) $G_1 \simeq G_2$ abelian $\Rightarrow \mathrm{Tor}(G_1) \simeq \mathrm{Tor}(G_2)$.

Lecture 7

Ex: $(G, +) = (\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, +)$

Take $(z_1, [z_2]_6) \in G$.

$(z_1, [z_2]_6) \in \mathrm{Tor}(G) \Leftrightarrow \exists\, n \in \mathbb{N} : \underbrace{(n z_1, [n z_2]_6)}_{= (0, [0]_6)}$

$\Leftrightarrow z_1 = 0$ and $z_2 \in \mathbb{Z}$.

$\mathrm{Tor}(G) = \{ (0, [z]_6) \mid z \in \mathbb{Z} \} = \{0\} \times \mathbb{Z}/6\mathbb{Z}$.

$\{0\} \times \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$.

<u>Not:</u> $(G,+)$ $\operatorname{maxord}(G) := \max\{\operatorname{ord}(a) \mid a \in G\}$

<u>Lemma 48:</u> Suppose $\ell \in \mathbb{N}$ and $2 \leq n_1 \mid n_2 \mid \dots n_{\ell-1} \mid n_\ell$

$n_i \in \mathbb{N}$ and H_1 and H_2 be cyclic subgroups

of $G := \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_\ell\mathbb{Z}$.

Then $\operatorname{maxord}(G/H_1) = \operatorname{maxord}(G/H_2)$.

and $G/H_1 \simeq G/H_2$.

<u>Proof:</u> $H = \langle \underbrace{([z_1]_{n_1}, \dots, [z_\ell]_{n_\ell})}_{h} \rangle_G$

Because of $\operatorname{ord}(h) = n_\ell$ we can assume w.l.o.g.

$\gcd(z_\ell, n_\ell) = 1$. Then we get a group isomorphism

$G \xrightarrow{\sim} G$ which maps ~~H onto~~ $\mathbb{Z}/n_\ell\mathbb{Z}$ onto H.

$$\varphi((([a_1]_{n_1}, \dots, [a_\ell]_{n_\ell})) := ([a_1 + z_1 a_\ell]_{n_1}, [a_2 + z_2 a_\ell]_{n_2}, \dots, [z_\ell a_\ell]_{n_\ell})$$

Exercise: φ is a well-defined group isomorphism.

$\varphi(\mathbb{Z}/n_\ell\mathbb{Z}) = H$.

Thus $G/H \simeq G/(\mathbb{Z}/n_\ell\mathbb{Z}) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_{\ell-1}\mathbb{Z}$. $\square$

Lemma 49: (uniqueness of $n_1 | \cdots n_{\ell-1} | n_\ell$)

Suppose $\ell, \ell' \in \mathbb{N}_0$, $2 \leq n_1 | n_2 | \cdots n_{\ell-1} | n_\ell$, $n_i \in \mathbb{N}$
$2 \leq n_1' | n_2' | \cdots n_{\ell'-1} | n_{\ell'}'$, $n_j' \in \mathbb{N}$

s.t. $G := \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_\ell\mathbb{Z} \overset{\varphi}{\simeq} \mathbb{Z}/n_1'\mathbb{Z} \times \cdots \times \mathbb{Z}/n_{\ell'}'\mathbb{Z} =: G'$

Then $\ell = \ell'$ and $n_1 = n_1', n_2 = n_2', \ldots, n_\ell = n_{\ell'}'$.

Proof: If $\ell = 0$ then $\ell' = 0$, because otherwise
$|G'| \geq n_1' \geq 2 \neq 1 = |G|$.

Suppose $\ell, \ell' \geq 1$.

$\Rightarrow \quad n_\ell = \operatorname{maxord}(G) = \operatorname{maxord}(G') = n_{\ell'}'$

$\underset{\text{Lemma before}}{\Rightarrow} \quad G/(\mathbb{Z}/n_\ell\mathbb{Z}) \simeq G/\varphi^{-1}(\mathbb{Z}/n_{\ell'}'\mathbb{Z}) \overset{\varphi}{\simeq} G'/(\mathbb{Z}/n_{\ell'}'\mathbb{Z})$

(IH) $\Rightarrow \quad \ell - 1 = \ell' - 1$ and $n_1 = n_1', \ldots, n_{\ell-1} = n_{\ell-1}'$. $\square$

Def 50: $m \in \mathbb{N}$. $B = \{\underline{z}^{(1)}, \ldots, \underline{z}^{(m)}\} \subseteq \mathbb{Z}^m$ is called a $\mathbb{Z}$-basis of $\mathbb{Z}^m$ if B is a $\mathbb{Q}$ ~~[illegible]~~ - linear independent and $\langle \underline{z}^{(1)}, \ldots, \underline{z}^{(m)} \rangle_{\mathbb{Z}^m} = \mathbb{Z}^m$.

<u>Proof (Thm 45):</u> $(A,+)$ finitely generated by

$S = \{s_1, \dots, s_k\}$.

$$\Longrightarrow \quad \mathbb{Z}^k \xrightarrow{\varphi} A$$

$$\underset{(0,\dots,\overset{(i)}{1},\dots,0)}{} \longmapsto s_i$$

$$\overset{42}{\Longrightarrow} \quad \mathbb{Z}^k / \ker(\varphi) \xrightarrow[\sim]{\bar{\varphi}} A. \qquad M := \ker(\varphi)$$

<u>Existence: Induction on k:</u>

If $M = \{0\}$ then $\mathbb{Z}^k \simeq A$.

Otherwise $2 \le n_1 := \min\{t \in \mathbb{N} \mid \exists\ \mathbb{Z}\text{ basis of } \mathbb{Z}^k: \underline{z}^{(1)}, \dots, \underline{z}^{(k)}$

$\exists\ a_1, \dots, a_k : \ a_1 \underline{z}^{(1)} + \dots a_k \underline{z}^{(k)} \in M\}$

$a_1 = t$

So we have a_i and $\underline{z}^{(i)}$ s.t. $a_1 = n_1$

and $\sum_{i=1}^{k} a_i \underline{z}^{(i)} \in M$.

(*) Exercise: By the Euclidian algorithm: $n_1 \mid a_2, \dots, n_1 \mid a_k$.

$n_1 b_i = a_i$

$\underline{z}^{(1)} + b_2 \underline{z}^{(2)} + \dots + b_k \underline{z}^{(k)}, \underline{z}^{(2)}, \dots, \underline{z}^{(k)}$

is a $\mathbb{Z}$ basis still. So we can take the $\mathbb{Z}$-basis s.t. $a_2 = \dots = a_k = 0$.

$$\Longrightarrow \quad n_1 \mathbb{Z} \underline{z}^{(1)} \subseteq M.$$

$$\Rightarrow \quad M = \underbrace{\mathbb{Z}(n_1 \underline{z}^{(1)})}_{\subseteq M} \oplus \left(M \cap \left(\bigoplus_{i=2}^{k} \mathbb{Z}\, \underline{z}^{(i)}\right)\right)$$

$\ulcorner$ "$\supseteq$" ✓

"$\subseteq$" $x \in M \Rightarrow \exists\, a_1, \dots, a_k \in \mathbb{Z} : x = \sum_{i=1}^{k} a_i \underline{z}^{(i)}$

$\Rightarrow n_1 \mid a_1$, ~~$i = 1, \dots, k$ by Euclidian Algo-~~

rithm. <u>Proof:</u> $a_1 = n_1 \cdot q_1 + r_1 \qquad 0 \le r_1 < n_1$

$$x - q_1 n_1 \underline{z}^{(1)} = r_1 \underline{z}^{(1)} + a_2 \underline{z}^{(2)} + \dots + a_k \underline{z}^{(k)} \in M$$

$\underset{\substack{\text{def. of } n_1 \\ 0 \le r_1 < n_1}}{\Rightarrow} \quad r_1 = 0. \quad \Rightarrow x \in \mathbb{Z} n_1 \underline{z}^{(1)} + \left(M \cap \left(\bigoplus_{j=2}^{k} \mathbb{Z}\, \underline{z}^{(j)}\right)\right) \lrcorner$

By induction we get $\underline{z}^{(1)}, \underline{z}^{(2)}, \dots, \underline{z}^{(k)}$ s.t.

$$M = \mathbb{Z} n_1 \underline{z}^{(1)} \oplus \mathbb{Z} n_2 \underline{z}^{(2)} \oplus \dots \oplus \mathbb{Z} n_k \underline{z}^{(k)}.$$

$$n_1 \underline{z}^{(1)} + n_2 \underline{z}^{(2)} \in M$$

$\underset{(*)}{\Rightarrow} \quad n_1 \mid n_2. \quad$ So $n_1 \mid n_2 \mid \dots \mid n_k$. by induction.

<u>base case:</u> $k = 1$ and $A \neq \{0\}$ $\Rightarrow A \cong \mathbb{Z}/n_1\mathbb{Z}$ for some $n_1 \in \{0, 2, 3, 4, \dots\} = \mathbb{N}_0 \setminus \{1\}$.

<u>uniqueness:</u>

$$\mathrm{Tor}\left(\mathbb{Z}^m \times \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_\ell\mathbb{Z}\right)$$

$$\cong \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_\ell\mathbb{Z} \qquad 2 \le n_1 \mid n_2 \mid \dots \mid n_\ell$$

$$\cong \mathbb{Z}/n_1'\mathbb{Z} \times \dots \times \mathbb{Z}/n_{\ell'}'\mathbb{Z} \qquad 2 \le n_1' \mid n_2' \mid \dots \mid n_{\ell'}'$$

Take

$$\frac{\mathbb{Z}^m \times \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_\ell\mathbb{Z}}{\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_\ell\mathbb{Z}} \cong \mathbb{Z}^m$$

$$\cong \frac{\mathbb{Z}^{m'} \times \mathbb{Z}/n_1'\mathbb{Z} \times \dots \times \mathbb{Z}/n_{\ell'}'\mathbb{Z}}{\mathbb{Z}/n_1'\mathbb{Z} \times \dots \times \mathbb{Z}/n_{\ell'}'\mathbb{Z}} \cong \mathbb{Z}^{m'}$$

$$\Rightarrow \mathbb{Z}^m \overset{f}{\cong} \mathbb{Z}^{m'}$$

Suppose $\underline{z}^{(1)}, \dots, \underline{z}^{(m)}$ $\mathbb{Z}$-basis of $\mathbb{Z}^m$

$\Rightarrow f(\underline{z}^{(1)}), \dots, f(\underline{z}^{(m)})$ are $\mathbb{Q}$-linear independent $\subseteq \mathbb{Q}^{m'}$

and $\dim_{\mathbb{Q}} \mathbb{Q}^{m'} = m'$

So $m \le m'$ ($m' \le m$ similarly)

We also have $\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_\ell\mathbb{Z} = \mathrm{Tor}(\dots)$

$\cong$

$\mathbb{Z}/n_1'\mathbb{Z} \times \dots \times \mathbb{Z}/n_{\ell'}'\mathbb{Z} = \mathrm{Tor}(\dots)$

Lemma 49 $\square$

How to get abelian groups from non-abelian ones?

Def 50: G a group. The commutator with $x, y \in G$ is $[x,y] = xyx^{-1}y^{-1}$.

The group $[G,G] := \langle [x,y] \mid x,y \in G \rangle_G$ is called the <u>commutator subgroup of G</u>

Remark 51: 1) $[G,G] \trianglelefteq G$.

Proof: $g \in G$. $g[x,y]g^{-1} = [gxg^{-1}, gyg^{-1}]$

$$\Rightarrow g[G,G]g^{-1} \supseteq \{[gxg^{-1}, gyg^{-1}] \mid x,y \in G\}$$

$$= \{[x,y] \mid x,y \in G\}$$

$$\Rightarrow g[G,G]g^{-1} \supseteq [G,G].$$

g arbitrary $\Rightarrow [G,G] \trianglelefteq G$ □

2) $G/[G,G]$ is abelian

3) $G \xrightarrow{f} A$ homomorphism of groups and A abelian

then $[G,G] \leq \ker(f)$.

Ex 1) $[(\mathbb{Z},+),(\mathbb{Z},+)] = \{0\}$ $(z_1+z_2-z_1-z_2=0)$

2) $[S_3, S_3] = A_3$ $[\langle 1,2\rangle, \langle 1,2,3\rangle] = \langle 2,1,3\rangle \circ \langle 3,2,1\rangle = \langle 1,2,3\rangle$

"$\subseteq$" ✓ (even permutations)

An extra example for the Commutator subgroup:

$$[GL_n(\mathbb{R}), GL_n(\mathbb{R})] = SL_n(\mathbb{R})$$
$$= \{A \in GL_n(\mathbb{R}) \mid \det A = 1\}$$

Proof: "$\subseteq$" ✓

"$\supseteq$" $\begin{pmatrix} 1 & r \\ & 1 \end{pmatrix} = \begin{pmatrix} \alpha & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & s \\ & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & -s \\ & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & \alpha s - s \\ & 1 \end{pmatrix}$ for $\alpha = 2$, $s = r$.

$\begin{pmatrix} \alpha & \\ & \alpha^{-1} \end{pmatrix} = \begin{pmatrix} \alpha & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \begin{pmatrix} \alpha^{-1} & \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ & 1 \end{pmatrix}$

$\square$

I.9. Free groups

Every f.g. abelian group is isomorphic to a factor group of $\mathbb{Z}^n$ for some $n \in \mathbb{N}$.

What about non-abelian groups?

$\rightsquigarrow$ Here we construct the free groups.

Let S be a set.

$$\mathcal{M}(S) := \{ (s_1, \dots, s_\ell) \mid \ell \in \mathbb{N}_0,\ s_1, \dots, s_\ell \in S \}.$$

We have a binary structure on $\mathcal{M}(S)$

$$(s_1, \dots, s_\ell) * (s'_1, \dots, s'_{\ell'}) := (s_1, \dots, s_\ell, s'_1, \dots, s'_{\ell'})$$

$(\mathcal{M}(S), *)$ is a monoid with unit $()$.

Let T be a set and $S := T \dot\cup \{t^{-1} \mid t \in T\}$ (t^{-1} formal notation)

We define on $\mathcal{M}(S)$ an incidence relation

(just ~~reflexive~~ symmetric)

$$(s_1, \dots, s_\ell) \overset{1}{\sim} (s'_1, \dots, s'_{\ell'}) \iff \text{if} \Big(\ell' = \ell - 2 \text{ and}$$

$$\exists i \in \{1, \dots, \ell-1\} : s_i = s_{i+1}^{-1} \text{ or } s_i^{-1} = s_{i+1}$$

$$\text{and } s_1 = s'_1, s_2 = s'_2, \dots, s_{i-1} = s'_{i-1}$$

$$\text{and } s_{i+2} = s'_i, \dots, s_\ell = s'_{\ell'} \Big)$$

$$\text{or } \Big(\ell' - 2 = \ell \text{ and } \dots \Big)$$

<u>Ex:</u> $(s_1, s_2, s_2^{-1}, s_3) \overset{r}{\sim} (s_1, s_3)$.

We use the incidence relation r to define an equivalence relation R

$m_1, m_2 \in M(S)$.

$$m_1 \overset{R}{\sim} m_2 \iff \underset{\ell \in \mathbb{N}_0}{\exists} \exists\, \tilde{m}_1 = m_1, \tilde{m}_2, \dots, \tilde{m}_{\ell-1}, \tilde{m}_\ell = m_2 :$$

$$\forall_{i=1,\dots,\ell-1} : \tilde{m}_i \overset{r}{\sim} \tilde{m}_{i+1}.$$

We put $F(T) := M(S)/\sim$.

$[m_1]_\sim * [m_2]_\sim := [m_1 * m_2]_\sim$ is well-defined:

<u>Proof:</u>
$$m_1 \overset{r}{\sim} u_2 \overset{r}{\sim} u_3 \overset{r}{\sim} \dots \overset{r}{\sim} u_{\ell-1} \sim m_1'$$
$$m_2 \overset{r}{\sim} v_2 \overset{r}{\sim} v_3 \sim \dots \overset{r}{\sim} v_{k-1} \sim m_2'$$

$$\Rightarrow \quad m_1 * m_2 \overset{r}{\sim} u_2 * m_2 \overset{r}{\sim} u_3 * m_2 \overset{r}{\sim} \dots \overset{r}{\sim} m_1' * m_2$$
$$\overset{r}{\sim} m_1' * v_2 \overset{r}{\sim} m_1' * v_3 \overset{r}{\sim} \dots \overset{r}{\sim} m_1' * v_{k-1} \overset{r}{\sim} m_1' * m_2'$$

$\square$

<u>Def. 52:</u> Let R be an equivalence relation on M. A subset N of M is called system of representatives of R if the map

$$N \longrightarrow M/R \qquad x \longmapsto [x]_R$$

is bijective.

<u>Ex:</u> 1) On $\mathbb{Z} =: M$ take $R = \sim_n$ $(n \in \mathbb{N})$.

$\{1, \dots, n\}$ is a system of representatives of R.

[<u>Pf:</u> $\{1, \dots, n\} \xrightarrow{i \mapsto [i]_n} \mathbb{Z}/n\mathbb{Z}$ is bijective.]

2) $M = \mathbb{R}^2$ $\quad (x,y) \sim (x',y') \Leftrightarrow_{\text{def}} x - x' \in \mathbb{Z}$ and $y - y' \in \mathbb{Z}$

$\sim$ is an equivalence relation and

$N :=$  $= [0,1) \times [0,1)$ is a system of

representatives of $\sim$: <u>Proof:</u>

- Take $(x,y) \in \mathbb{R}^2$. Then $\exists\, k, l \in \mathbb{Z}$:

  $k \leq x < k+1$ and $l \leq y < l+1$

  $\Rightarrow [(x,y)]_\sim = [(x-k, y-l)]_\sim$

  and $(x-k, y-l) \in N$

- $(x,y), (x',y') \in N$ s.t. $(x,y) \sim (x',y')$

  $\Rightarrow$ $x - x' \in \mathbb{Z}$ and $y - y' \in \mathbb{Z}$

  and $-1 < x - x' < 1$ and

  $-1 < y - y' < 1$

  $\Rightarrow$ $x = x'$ and $y = y'$ $\square$

<u>Prop 53:</u> $(F(T), *)$ is a group and

$N = \{(s_1, \dots, s_l) \mid l \in \mathbb{N}_0, s_i \in T \dot{\cup} T^{-1}$

such that $s_i^{-1} \neq s_{i+1}$ and $s_{i+1}^{-1} \neq s_i$ for $i = 1, \dots, l-1\}$

is a system of representatives for $M(T \dot{\cup} T^{-1})/\sim_R$

$(F(T), *)$ is called the free group determined by T.

Prop 53 $\Rightarrow$ $T \dot{\cup} T \longrightarrow F(T)$ is injective.

$$s \longmapsto [s]_{\sim_R}$$

So later we write s instead of $[s]_{\sim_R}$

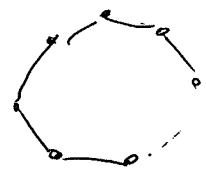
<u>Proof of Prop. 53:</u> The group property is trivial.

We consider the following tree:

V = vertices = $\cancel{\{(t_1, \dots, t_\ell) \mid \ell \in \mathbb{N}_0, t_1, \dots, t_\ell \in T\}}$ N

edges: $E = \{ \{n, n * s\} \mid n \in N, s \in T \dot{\cup} T^{-1}, n$ does not end on $s^{-1}. \}$

Firstly (V, E) is a tree, so there are no circles in (V, E)



(In one orientation the tuple of the vertex get more components. ↯)

- and (V, E) is connected. $\forall v_1, v_2$ $\exists$ path $v_1 \to v_2$

An element of $M(T \dot{\cup} T^{-1})$ defines a path in (V, E) from $()$ to some $v \in V$, say $v(m)$ for $m \in M(T \dot{\cup} T^{-1})$.

For $m_1 \sim m_2$ we get $v(m_1) = v(m_2)$

Take $n_1, n_2 \in N$. Then $v(n_1) = n_1$ and $v(n_2) = n_2$. If $n_1 \sim n_2$ then $v(n_1) = v(n_2)$ so $n_1 = n_2$. $\square$

<u>Def 54:</u> For a group G and $R \subseteq G$ we ~~put~~ write

$$\langle\langle R \rangle\rangle_G := \bigcap_{R \subseteq N \trianglelefteq G} N$$

for the normal subgroup generated by R.

Let T be a set an $R \subseteq F(T)$.

$$F(T) / \langle\langle R \rangle\rangle$$

is called the group determined ~~generated~~ by T and the relations R.

We also write $\langle T \mid R \rangle$

<u>Ex:</u> $\langle a \mid a^2 \rangle = \langle a \mid a^2 = 1 \rangle \cong C_2$

cyclic group of order 2

<u>Proof:</u> $a^{\mathbb{Z}} = F(\{a\}) \xrightarrow{\varphi} C_2 = \{1, b\}$

$a^z \longmapsto b^z$

$\ker(\varphi) = \{a^z \mid b^z = 1\} = \langle a^2 \rangle_{F(\{a\})}$

$\langle a^2 \rangle_{F(\{a\})} \trianglelefteq F(\{a\})$

So $\langle\langle a^2 \rangle\rangle \subseteq \langle a^2 \rangle_{F(\{a\})}$ ~~$\ker(\varphi)$~~

$\subseteq \langle\langle a^2 \rangle\rangle$

$\Rightarrow \dfrac{F(\{a\})}{\langle\langle a^2 \rangle\rangle} = \dfrac{F(\{a\})}{\ker(\varphi)} \simeq C_2.$ $\square$

<u>Ex:</u> $\langle a, b \mid \underbrace{b^n = 1,\ a^2 = 1,\ aba = b^{-1}}_{R} \rangle$

$=: D_{2n}$ the dihedral group with $2n$ elements.

How to show that ~~this~~ D_{2n} has $2n$ elements?

$F(a,b) \xrightarrow{\varphi} G$ (from the homework)

$G = \Gamma(V,E)$

$\ker(\varphi) \supseteq R$, so $\ker(\varphi) \supseteq \langle\langle R \rangle\rangle$

$\Rightarrow \dfrac{F(a,b)}{\langle\langle R \rangle\rangle} \xrightarrow{\bar{\varphi}} G$

$\dfrac{F(a,b)}{\langle\langle R \rangle\rangle} = D_{2n}$

By the relations R one can show that

$|D_{2n}| \leq 2n$. $\Rightarrow$ $\bar{\varphi}$ bijective, because $|G| = 2n$.

<u>Ex</u>: $SL_2(\mathbb{Z}) / \{\pm I_2\} =: G = PSL_2(\mathbb{Z})$

Claim $G \simeq \langle S, T \mid \underbrace{S^2 = e,\ (ST)^3 = e}_{R} \rangle$

<u>Proof</u>: $F(\tilde{S}, \tilde{T}) \xrightarrow{\varphi} G$

$$\tilde{S} \longmapsto \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$$

$$\tilde{T} \longmapsto \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}$$

Then $\varphi(\tilde{S}\tilde{T}) = \left[\begin{pmatrix} & -1 \\ 1 & 1 \end{pmatrix}\right]$

$$\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}^3 = \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & \\ & -1 \end{pmatrix}$$

$$\Rightarrow \left[\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}^3\right] = \left[\begin{pmatrix} 1 & \\ & 1 \end{pmatrix}\right]$$

(<u>Fact</u>: $SL_2(\mathbb{Z}) = \langle \begin{pmatrix} & -1 \\ 1 & \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix} \rangle_{SL_2(\mathbb{Z})}$.)

We have

$$S, T \in F(\tilde{S}, \tilde{T}) / \langle\langle R \rangle\rangle \xrightarrow{\bar{\varphi}} G$$

<u>To show</u>: $\bar{\varphi}$ is injective.

$S = [\tilde{S}]$, $T = [\tilde{T}]$.

We have $STSTST = E \Rightarrow STS^{-1} = TST^{-1}$

Write $A := ST$.

If there is a relation

$$\bar{\varphi}(SA^{\varepsilon_1} S A^{\varepsilon_2} \cdots A^{\varepsilon_\ell} S) = \varphi(E)$$

or $\varphi(A^{\varepsilon_1} S \cdots A^{\varepsilon_\ell} S) = \varphi(E)$

or $\bar{\varphi}(SA^{\varepsilon_1} S \cdots A^{\varepsilon_\ell}) = \varphi(E)$

$\varepsilon_i \in \{\pm 1\}$

note that $\bar{\varphi}(SA) = \left[\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}\right] = \left[\begin{pmatrix} -1 & -1 \\ & -1 \end{pmatrix}\right]$

$$\cong \left[\begin{pmatrix} 1 & 1 \\ & 1 \end{pmatrix}\right] \text{ mod } \varphi(\pm I_2).$$

and $\bar{\varphi}(SA^{-1}) = \left[\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}\right] = \left[\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\right]$

So if $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in M_2(\mathbb{Z})$ s.t.

(*) $\begin{cases} \text{all } b_{ij} \text{ are non-negative or non-positive} \\ \text{and both rows are non-zero.} \end{cases}$

$[C] = \bar{\varphi}(SA^{\varepsilon_1} \cdots SA^{\varepsilon_\ell})[B]$ fulfills (*)

and $|C_{11}| + |C_{12}| + |C_{21}| + |C_{22}| \geq 2 + \ell$.

So $[C \cdot I_2] \neq [I_2]$ and $[C \cdot I_2] \neq \left[\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}\right]$. ↯.

I 10 Dual of a group

Def 55: $m \in \mathbb{N}$ is called an exponent of an element g of a group G if $g^m = e$, and m is called an exponent of a group G if it is an exponent for every $g \in G$.

Rk: If G has exponent m, then m is divisible by the lcm of all $\mathrm{ord}(g)$, $g \in G$.

(use division by $\mathrm{lcm}(\mathrm{ord}(g) \mid g \in G)$)

Def 56: Suppose $(A, +)$ is an abelian group of lowest exponent m. We call $\mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z}) =: A^\wedge$ the dual group of A.

We have $\mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z}) \xrightarrow{\phi} \mathrm{Hom}(A, \mathbb{Z}/km\mathbb{Z})$

, for $k \in \mathbb{N}$, $f \longmapsto (a \mapsto [kt]_{km})$

if $f(a) = [t]_m$.

ϕ is injective, because

$\ker(\phi) = \{ f \in \mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z}) \mid [kt]_{km} = [0]_{mk}$

$\forall t \in \mathbb{Z}$ s.t. $\exists a \in A$ $f(a) = [t]_m \}$

$(km \mid kt \Rightarrow m \mid t \Rightarrow [t]_m = [0]_m)$

$= \{ 0_{\mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z})} \}$

Surjectivity $f_1 \in \mathrm{Hom}(A, \mathbb{Z}/km\mathbb{Z})$

$= m f_1(a) = f_1(ma) = f_1(0) = 0$,

so $\mathrm{im}(f_1) \subseteq k\mathbb{Z}/km\mathbb{Z}$.

So ϕ is surjective. $\square$

<u>Prop 57:</u> A, B abelian groups with exponent m. Then $(A \times B)^\wedge \cong A^\wedge \times B^\wedge$

<u>Proof:</u> $\mathrm{Hom}(A \times B, \mathbb{Z}/m\mathbb{Z}) \simeq \mathrm{Hom}(A, \mathbb{Z}/m\mathbb{Z}) \times \mathrm{Hom}(B, \mathbb{Z}/m\mathbb{Z})$.

$$f \longmapsto \left(f|_{A \times \{0\}}, f|_{\{0\} \times B}\right)$$

$$\left((a,b) \mapsto f_1(a) + f_2(b)\right) \longleftarrow\!\shortmid (f_1, f_2)$$

$\square$

<u>Prop 58:</u> Every finite abelian group is $\simeq$ to its dual.

<u>Proof:</u> A finite group is a product of finite cyclic groups $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_\ell\mathbb{Z}$.

$$(\mathbb{Z}/n_1\mathbb{Z})^\wedge \simeq \mathrm{Hom}(\mathbb{Z}/n_1\mathbb{Z}, \mathbb{Z}/n_1\mathbb{Z})$$

$$\simeq \frac{\frac{n_1}{\gcd(n_1,n_1)}\mathbb{Z}}{n_1\mathbb{Z}} = \mathbb{Z}/n_1\mathbb{Z}$$

Prop 57 finishes the proof. $\square$

<u>Remark</u>: In general for a group $(G,*)$ one defines the dual $G^\wedge := \mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Q}/\mathbb{Z})$.

<u>Ex</u>: $G := \bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$ $\quad$ G has exponent 2.

$$\mathrm{Hom}_{\mathbb{Z}}(G, \mathbb{Z}/2\mathbb{Z}) \simeq \prod_{i=1}^{\infty} \mathrm{Hom}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/2\mathbb{Z})$$

$$\simeq \prod_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}$$

$$\not\simeq$$

$$\bigoplus_{i=1}^{\infty} \mathbb{Z}/2\mathbb{Z}.$$

II. Rings

Def 59: A triple $(R,+,\cdot)$ consisting of an abelian group $(R,+)$ and a semigroup $(R,\cdot)$ is called <u>a ring</u> if it satisfies the distributivity laws

(left distributivity) $r(s+t) = rs + rt$

(right — " —) $(s+t)r = sr + tr$

for all $r,s,t \in R$.

A ring $(R,+,\cdot)$ is called v

Ex 1) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ ~~are~~ rings

$(\mathbb{Z},+,\cdot)$

2) $(M_n(\mathbb{Z}),+,\cdot)$ ← $A = (a_{ij})$ $A+B := (a_{ij}+b_{ij})_{ij}$

matrix multiplication

For $n \geq 2$ it is a non-commutative ring $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

Def 60: 1) A ring $(R,+,\cdot)$ is called

- Commutative, if $(R,\cdot)$ is so
- unital (unitary), if $(R,\cdot)$ is a monoid.

2) An element $r \in R$ is called a zero divisor if $\exists s \neq 0 : rs = 0$

3) A unitary ring is called an <u>integral domain</u>, if $(R, +, \cdot)$ is commutative and zero divisor free.

<u>Ex</u> 1) $(\mathbb{Z}, +, \cdot)$ is an integral domain

2) $(\mathbb{Z}/n\mathbb{Z}, +, \cdot) = (R, +, \cdot)$ is unitary ring.

It is an integral domain iff n is a prime number

<u>Proof</u>: "$\Rightarrow$" Suppose R is an integral domain. Assume n is not a prime

$\Rightarrow \exists\, l, m \in \mathbb{N} : l \cdot m = n$

$$\Rightarrow \quad (l 1_R)(m 1_R) \overset{\text{distributivity}}{=} \sum_{i=1}^{m} (l 1_R) 1_R$$

$$= \sum_{i=1}^{m} l 1_R = (ml) 1_R = ml [1]_n$$

$$= [n]_n = [0]_n \quad ↯$$

"$\Leftarrow$" exercise $\square$

<u>Def 61:</u> Let $(R, +, \cdot)$ be a ring and $S \subseteq R$.
$(S, +|_{S\times S}, \cdot|_{S\times S})$ is called a subring of R if $(S, +|_{S\times S}, \cdot|_{S\times S})$ is a ring.
If R is unitary then S is called a unitary subring of R if S is a subring and $1_R \in S$.

<u>Ex:</u> 1) $(C(\mathbb{R}^n, \mathbb{R}), +, \cdot)$ with $(f+g)(x) := f(x) + g(x)$
$(f \cdot g)(x) := f(x)\, g(x)$

is a unitary ring and
$(C^\infty(\mathbb{R}^n, \mathbb{R}), +, \cdot)$ is a subring in fact a unitary subring.

2) $(\mathrm{End}_{\mathbb{R}}(V), +, \circ)$ $\quad$ ($V/\mathbb{R}$ vector space

is a unitary ring.
<u>Proof:</u> · $(\mathrm{End}_{\mathbb{R}}(V), +)$ is a group ✓

- $(\mathrm{End}_R(V), \circ)$ is a monoid. ✓

- $h, f, g \in \mathrm{End}_R(V)$

$$((f+g)\circ h)(v) = (f+g)(h(v))$$
$$= f(h(v)) + g(h(v))$$
$$= (f\circ h)(v) + (g\circ h)(v) = (f\circ h + g\circ h)(v).$$

left-distributivity similar.

<u>Prop 62:</u> (Subring criterion)

Let $(R, +, \cdot)$ be a ring and $S \subseteq R$.

Then are equivalent:

1° $(S, +|_{S\times S}, \cdot|_{S\times S})$ is a subring of R

2° $S \neq \emptyset$, $\forall s_1, s_2 \in S$:

$s_1 - s_2 := s_1 + (-s_2)$, $s_1 \cdot s_2 \in S$.

<u>Proof:</u> <u>1° ⇒ 2°:</u> $(S, +) \leq (R, +)$ and $(S, \cdot)$ magma ⇒ 2°

<u>2° ⇒ 1°</u> 2° ⇒ $(S, +) \leq (R, +)$ and —"—

Associativity and left/right-distributivity is inherited by S.

$\Rightarrow (S, +, \cdot)$ is a ring $\square$

lecture 10 (Next lecture: mention left and right zero-divisors)

Remark: Let $(R, +, \cdot)$ be a ring. Then we have

1) $0_R \cdot x = 0_R \quad \forall x \in R$

2) $(-x)y = -xy = x(-y)$

Proof: 1) $0_R x = (0+0)x = 0x + 0x \quad | -0x$

$\Rightarrow \quad 0 = 0x$

2) $xy + (-x)y = (x + (-x))y = 0_R y = 0_R$ $\square$

Def 62: 1) Let R be a ring with unit element 1_R

$R^\times := \{x \in R \mid \exists y \in R : xy = yx = 1_R\}$

is called the group of units of R.

2) R is called a division ring if R unitary and $R^\times = R \setminus \{0_R\}$. ($\Rightarrow 1_R \neq 0_R$)

3) A commutative division ring is called a field.

Remark on zero-divisors:

<u>Def</u>: Let R be a ring. $x \in R$ is called a <u>right zero divisor</u> if $x \neq 0$ and $\exists\, y \in R \setminus \{0\}$: $yx = 0$.

$x \in R$ is called a <u>left zero divisor</u> if $x \neq 0$ and $\exists\, y \in R \setminus \{0\}$: $xy = 0$.

An element of R is called a <u>zero divisor</u> if it is a right or a left zero divisor. An element which is a right and a left zero divisor is called a two-sided zero divisor.

<u>Ex.:</u> 1) $(\mathbb{Q}, +, \cdot)$ are fields
$\mathbb{C}$
$\mathbb{R}$

2) Exercise: $(\mathbb{Z}/p\mathbb{Z}, +, \cdot)$ is a field.

3) quaternion division ring over $\mathbb{C}$
(Hamiltonian ring)

$$H(\mathbb{C}) := \left\{ \begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix} \;\middle|\; a, b \in \mathbb{C} \right\}$$

$$\subseteq M_2(\mathbb{C}) \quad \text{a subring.}$$

For $(a,b) \neq (0,0)$ $\quad \begin{pmatrix} a & -b \\ \bar{b} & \bar{a} \end{pmatrix}^{-1} = \dfrac{1}{|a|^2+|b|^2} \begin{pmatrix} \bar{a} & b \\ -\bar{b} & a \end{pmatrix} \in H(\mathbb{C})$

$$\begin{pmatrix} & -1 \\ 1 & \end{pmatrix} =: \underline{j}. \quad \underline{i} := \begin{pmatrix} i & \\ & -i \end{pmatrix}$$

$$\underline{k} := \begin{pmatrix} & -i \\ -i & \end{pmatrix}.$$

$$\underline{i}\underline{j} = \underline{k} = -\underline{j}\,\underline{i} \neq \underline{j}\,\underline{i}$$

$$H(\mathbb{C}) = \mathbb{C} \oplus \underline{j}\,\mathbb{C}.$$

4) group ring: let R be a commutative unitary ring and G be a group

$$R[G] := \{ f \in \mathrm{Map}(G,R) \mid \underbrace{\mathrm{supp}(f)}_{\{g \in G \mid f(g) \neq 0\}} \text{ is finite} \}$$

$$G \hookrightarrow R[G], \quad g \longmapsto f_g \quad (f_g(g') := \underbrace{\delta_{gg'}}_{\text{Kronecker symbol}})$$

$R[G]$ is a ring via the following structures

- $(f_1 + f_2)(g) := f_1(g) + f_2(g)$
- $(f_1 * f_2)(g) = \sum_{\substack{(g_1,g_2) \in G \\ g_1 g_2 = g}} f_1(g_1) f_2(g_2)$. ("convolution")
- f_{e_G} is the unit element and

The zero map is the neutral element.

We have $\cdot$ $(f_{g_1} * f_{g_2})(g) = \sum_{\substack{(h_1,h_2) \in G \\ h_1 h_2 = g}} f_{g_1}(h_1) f_{g_2}(h_2)$

$$= f_{g_1 g_2}(g)$$

i.e. $(G,*) \xrightarrow{g \mapsto f_g} (R[G],*)$ is a homomorphism.

$(f_g)_{g\in G}$ are R-linear independent, i.e.

$\lambda_g \in R, \lambda_g = 0_R$ a.a., $\sum_{g\in G} \lambda_g f_g = 0 \Rightarrow \lambda_g = 0_R$ for all $g \in G$

<u>Proof:</u> $\left(\sum_{g\in G} \lambda_g f_g\right)(h) = \lambda_h f_h(h) = \lambda_h$ $\square$

Thus, we can identify G with $\{f_g \mid g \in G\}$, i.e. the elements of $R[G]$ are of the form $\sum_{g\in G} \lambda_g g$, $\lambda_g = 0_R$ a.a.

5) $(S(\mathbb{R}), +, *)$ <u>Schwartz space</u>

$S(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{C}\ C^\infty \mid$ all derivatives $f^{(i)}$ are <u>rapidly decreasing</u>$\}$

$\left(\sup_{x\in\mathbb{R}} |x^k f^{(i)}(x)| < \infty \quad \forall (i,k) \in \mathbb{N}_0^2.\right)$

$$(f*g)(x) := \int_{-\infty}^{\infty} f(y)\, g(x-y)\, dy$$

MA II $\Rightarrow$ $* : S(\mathbb{R}) \times S(\mathbb{R}) \to S(\mathbb{R})$

is well-defined, i.e.

$f*g$ is rapidly decreasing and

$f*g \in C^\infty(\mathbb{R}, \mathbb{C})$.

(Fourier Analysis, Elias M. Stein
Rami Shakarchi)

There is another multiplication on

$S(\mathbb{R})$. $(f \cdot g)(x) := \underbrace{f(x) \cdot g(x)}_{\text{in } \mathbb{C}}$

<u>Def. 63:</u> A map $f : (R, +, \cdot) \longrightarrow (S, +, \cdot)$
between two rings is called ring
homomorphism if f is
a homomorphism from $(R, +)$ to
$(S, +)$ and

· a homomorphism from $(R,\cdot)$ to $(S,\cdot)$.

Write $\mathrm{Hom}_{rings}(R,S)$.

Example:

1) $\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ $\quad f(z) := [z]_n$

2) $(\mathcal{P}(X), \triangle, \cap)$ is a ring (commutative and unitary)

$\emptyset \neq S \subseteq X$.

$$(\mathcal{P}(X), \triangle, \cap) \xrightarrow{\phi} (\mathcal{P}(X), \triangle, \cap)$$

$$\phi(A) := A \cup S$$

is not a ring homomorphism

$$\phi(\emptyset \triangle \emptyset) = S$$

$$\phi(\emptyset) \triangle \phi(\emptyset) = S \triangle S = \emptyset \neq S.$$

$\phi(A) = A \cap S$ defines a ring homomorphism.

Def 64: $f \in \mathrm{Hom}_{rings}(R,S)$. $\ker(f) = \{x \in R \mid f(x) = 0\}$

Ex: There is no multiplicative structure on $\mathbb{Q}/\mathbb{Z}$ different from 0, s.t.

$(\mathbb{Q}/\mathbb{Z}, +, *)$ is a ring.

$$\ulcorner [q_1]_{\mathbb{Z}} * [q_2]_{\mathbb{Z}} \underset{\substack{q_2 = \frac{a}{b} \\ (a,b)=1}}{=} (b[\tfrac{1}{b} q_1]) * [q_2]$$

$$\underset{\text{distributivity (left)}}{=} \sum_{i=1}^{b} \left([\tfrac{1}{b} q_1]_{\mathbb{Z}} * [q_2]_{\mathbb{Z}} \right)$$

$$\underset{\text{right-distributivity}}{=} [\tfrac{1}{b} q_1] * (b[q_2]_{\mathbb{Z}}) =$$

$$= [\tfrac{1}{b} q_1]_{\mathbb{Z}} * [0]_{\mathbb{Z}} = [0]_{\mathbb{Z}} \ \lrcorner$$

<u>Ex:</u> 1) $S(\mathbb{R}) \longrightarrow S(\mathbb{R})$ Laplace transform

$f \longmapsto \hat{f}$ is a ring homomorphism

from $(S(\mathbb{R}), +, *)$ to $(S(\mathbb{R}), +, \cdot)$.

2) Given a ring homomorphism

$R \xrightarrow{\varphi} S$ we get

a ring homomorphism $M_n(R) \longrightarrow M_n(S)$

<u>Def 65:</u> (ideals) Let R be a unitary ring. $\mathfrak{a} \subseteq R$ is called a left-ideal, if $(\mathfrak{a},+) \leq R$ and $\forall r \in R, a \in \mathfrak{a}: ra \in \mathfrak{a}$, and a right ideal if —"— $ar \in \mathfrak{a}$.
$\mathfrak{a}$ is called two-sided ideal if it is a left- and a right ideal. We call two-sided ideals also just ideals.

<u>Ex:</u> 1) The ideals of $(\mathbb{Z},+,\cdot)$ are $m\mathbb{Z}$, $m \in \mathbb{Z}$. $(m\mathbb{Z},+) \leq (\mathbb{Z},+)$ and $\forall z,z' \in \mathbb{Z}$: $z(mz') = mzz' \in m\mathbb{Z}$.

2) A field has only two ideals the zero ideal and the full ring.

<u>Pf:</u> F a field ($\Rightarrow |F| \geq 2$ because $1_F \neq 0_F$)
$\mathfrak{a} \subseteq F$. Suppose $\mathfrak{a} \neq (0)$
$\Rightarrow \exists a \in \mathfrak{a} \setminus \{0\}$ and thus
$1_F = a^{-1}a \in \mathfrak{a}$.
$\Rightarrow F \subseteq \mathfrak{a}$. $\square$

We will see later that the converse is also true.

3) We look for all left-ideals of $M_2(\mathbb{R})$.

Take $\mathfrak{a} \overset{\neq (0)}{\subseteq} M_2(\mathbb{R})$ a left-ideal.

Multiply $\mathfrak{a}$ with $\begin{pmatrix} 1 & \\ & 0 \end{pmatrix}$.

$W := \begin{pmatrix} 1 & \\ & 0 \end{pmatrix} \mathfrak{a}$ is an $\mathbb{R}$-vector space.

<u>Case 1:</u> $\dim_{\mathbb{R}} W = 2$: Then $\mathfrak{a} = M_2(\mathbb{R})$.

<u>Case 2:</u> $\dim_{\mathbb{R}} W = 1$: $W = \begin{cases} \mathbb{R}\begin{pmatrix} 1 & a \\ 0 & 0 \end{pmatrix} \\ \mathbb{R}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}. \end{cases}$

4) Ideals for $M_2(\mathbb{R})$: $\mathcal{J} \subseteq M_2(\mathbb{R})$ an ideal and $\mathcal{J} \neq \{0\}$.

$A \in \mathcal{J} \setminus \{0\}$, $A = (a_{ij})$, $\exists_{(i,j)}$: $a_{ij} \neq 0$

$$E_{ii} A E_{jj} = \begin{array}{c} \\ i \\ \\ \end{array}\!\!\begin{array}{c} \begin{array}{ccc} & j & \end{array} \\ \begin{pmatrix} & & \\ & a_{ij} & \\ & & \end{pmatrix} \\ \neq 0 \end{array} \Rightarrow (*) \subseteq \mathcal{J}$$

multiply with $\begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \Rightarrow M_2(\mathbb{R}) \subseteq \mathcal{J}$.

II.1. Zorn's Lemma and maximal left-ideals

<u>Lemma</u> (Zorn) Let $\mathcal{M}$ be a set and $\leq$ an order on $\mathcal{M}$ s.t. $(\mathcal{M}, \leq)$ is inductively ordered,

i.e. $\forall\, \mathcal{N} \subseteq \mathcal{M}$ totally ordered w.r.t. "$\leq$" $\exists\, M \in \mathcal{M} : \forall_{N \in \mathcal{N}} : N \leq M$.

(M is called an upper bound for $\mathcal{N}$ in $\mathcal{M}$.),

then $\exists\, \hat{M} \in \mathcal{M} : \hat{M}$ is a maximal element of $\mathcal{M}$ w.r.t. "$\leq$".

Zorn's Lemma is equivalent to the axiom of choice.

<u>Axiom of choice</u> Let X be a set and $f : I \to \mathcal{P}(X)$ be a map s.t. $f(i) \neq \emptyset$ for all $i \in I$.

Then $\exists\ g : I \longrightarrow X$ s.t. $g(i) \in f(i)$ for all $i \in I$.

Lecture 11:

<u>Proof</u> (of equivalence):

<u>Zorn's Lemma $\Rightarrow$ Ax of choice:</u>

$$\mathcal{M} := \Big\{ (J, g) \mid J \subseteq I \text{ and } g : J \to X \text{ s.t. } \forall j \in J : g(j) \in f(j) \Big\}$$

<u>Def:</u> $(J, g) \leq (J', g')$ if $J \subseteq J'$ and $g'|_J = g$.

$\mathcal{M}$ is inductively ordered.

$\Rightarrow$ $\mathcal{M}$ has a maximal element $(\hat{J}, \hat{g})$.

<u>Claim:</u> $\hat{J} = I$. If not, take $i \in I \setminus \hat{J}$.

and define $\tilde{g} : \tilde{J} := \hat{J} \cup \{i\} \to X$

via $\tilde{g}(j) = \begin{cases} \hat{g}(j), & j \in \hat{J} \\ b, & j = i \end{cases}$

for some $b \in f(i) \setminus \hat{g}(\hat{J})$. $\Rightarrow (\tilde{J}, \tilde{g}) \geq$

Ax of choice $\Rightarrow$ Zorn's Lemma:

(Serge Lang "Algebra" Appendix 2 Corollary 2.5.) $\square$

Def. 67 Let R be a unitary ring. A left-ideal $\mathfrak{m} \subsetneq R$ is called <u>maximal</u> if for every ideal $\mathfrak{a}$ containing $\mathfrak{m}$ we have $\mathfrak{a} = \mathfrak{m}$ or $\mathfrak{a} = R$.

Prop 68: Every unitary ring has a maximal left-ideal.

Proof: Consider $S := \{\mathfrak{a} \subsetneq R \mid \mathfrak{a} \text{ left-ideal}\}$. Then $(0) \in S$, so $S \neq \emptyset$.

Let $T \subseteq S$ be totally ordered w.r.t. "$\subseteq$".

Then $\bigcup T = \bigcup_{\mathfrak{b} \in T} \mathfrak{b} =: \mathfrak{t}$ is a left-ideal.

$a, b \in \mathfrak{t} \Rightarrow \exists\, \mathfrak{b}_1, \mathfrak{b}_2 \in T$: $a \in \mathfrak{b}_1$, $b \in \mathfrak{b}_2$.

T totally ordered $\Rightarrow$ $\mathfrak{b}_1 \overset{I}{\subseteq} \mathfrak{b}_2$ or $\mathfrak{b}_2 \subseteq \mathfrak{b}_1$. $\Rightarrow$ W.l.o.g. (I).

$\Rightarrow$ $a, b \in \mathfrak{b}_2 \Rightarrow a - b \in \mathfrak{b}_2 \subseteq \mathfrak{t}$

For $\lambda \in R$ and $a \in \mathfrak{t} \Rightarrow \exists\, \mathfrak{b} \in T : a \in \mathfrak{b}$

$\overset{\mathfrak{b} \text{ ideal}}{\Rightarrow}$ $\lambda a \in \mathfrak{b} \Rightarrow \lambda a \in \mathfrak{t}$. So $\mathfrak{t}$ is an ideal. Assume $1_R \in \mathfrak{t}$ then $\exists\, \mathfrak{b} \in T$: $1_R \in \mathfrak{b}$. $\Rightarrow$ $R = \mathfrak{b}$ ↯

So $\mathfrak{t} \in S$ and $\forall \mathfrak{b} \in T : \mathfrak{b} \subseteq \mathfrak{t}$.

So $(S, \text{"}\subseteq\text{"})$ is inductively ordered

Zorn's Lemma $\Rightarrow$ $\exists\, \mathfrak{a} \in S : \hat{\mathfrak{a}}$ is a "$\subseteq$" maximal element of S.

$\Rightarrow$ $\hat{\mathfrak{a}}$ is a maximal ideal of R $\square$

<u>Prop 69:</u> Let R be a ring and $\mathfrak{a}$ be an ideal of R. Then the factor group $(R/\mathfrak{a}, +)$ together with the multi-

plication: $[r_1]_{\mathfrak{a}} \cdot [r_2]_{\mathfrak{a}} := [r_1 r_2]_{\mathfrak{a}}$ is a ring. (factor ring of R by $\mathfrak{a}$.)

<u>Proof:</u> We have to show that $\cdot$ is well-defined. The distributivity is inherited by $R/\mathfrak{a}$ from R.

$[r_1]_{\mathfrak{a}} = [r_1']_{\mathfrak{a}}$ and $[r_2]_{\mathfrak{a}} = [r_2']_{\mathfrak{a}}$

$\Rightarrow r_1 - r_1' \in \mathfrak{a}$ and $r_2 - r_2' \in \mathfrak{a}$

$\Rightarrow r_1 r_2 - r_1' r_2' = (r_1 - r_1') r_2 + r_1'(r_2 - r_2')$

$\in \mathfrak{a}$, because $\mathfrak{a}$ is a left and a right-ideal. $\square$

<u>Prop 70:</u> Let R be a commutative unitary ring. Then are equivalent for an ideal $\mathfrak{m}$ of R

1° ~~R~~ $\mathfrak{m}$ is a maximal ideal

2° $R/\mathfrak{m}$ is a field.

<u>Proof:</u> 1° $\Rightarrow$ 2° Take $[a]_{\mathfrak{m}} \in R/\mathfrak{m} \setminus \{[0]_{\mathfrak{m}}\}$.

$\Rightarrow R \cdot a + \mathfrak{m} = R \Rightarrow \exists\, b \in R$:

$ba + \mathfrak{m} \ni 1_R. \Rightarrow [b]_{\mathfrak{m}} [a]_{\mathfrak{m}} = [1]_{\mathfrak{m}}$.

$2^\circ \Rightarrow 1^\circ$ Take $\mathfrak{n} \subseteq R$ an ideal of R s.t. $\mathfrak{m} \subseteq \mathfrak{n}$. If $\mathfrak{n} \neq \mathfrak{m}$ then $\exists\, a \in \mathfrak{n} \setminus \mathfrak{m}$

$\Rightarrow \exists\, b \in R : [b]_{\mathfrak{m}} [a]_{\mathfrak{m}} = [1_R]_{\mathfrak{m}}$

$\Rightarrow 1_R \in ba + \mathfrak{m} \subseteq \mathfrak{n} \Rightarrow \mathfrak{n} = R$ $\square$

<u>Def. 71:</u> Let R be a commutative unitary ring and $\mathfrak{a} \subsetneq R$ be an ideal. $\mathfrak{a}$ is called a prime ideal if $\forall\, a, b \in R : (ab \in \mathfrak{a} \Rightarrow a \in \mathfrak{a}$ or $b \in \mathfrak{a})$

(Recall: R integral domain $\overset{\text{def.}}{\Leftrightarrow}$ R commutative with $1_R \neq 0_R$ and no zero divisors)

<u>Prop 72:</u> Let R be a commutative ring with $1_R \neq 0_R$ and let $\mathfrak{a}$ be an ideal of R. Then are equivalent:

1° $\mathfrak{a}$ is a prime ideal

2° $R/\mathfrak{a}$ is an integral domain.

<u>Proof:</u> <u>$1^\circ \Rightarrow 2^\circ$:</u> $\mathfrak{a} \neq R$, so $1_R \notin \mathfrak{a} \ni 0_R$ and so $[1_R]_{\mathfrak{a}} \neq [0_R]_{\mathfrak{a}}$.

Take $a, b \in R$ s.t. $[ab]_{\mathfrak{a}} = [0]_{\mathfrak{a}}$

$\Rightarrow ab \in \mathfrak{a} \Rightarrow a \in \mathfrak{a}$ or $b \in \mathfrak{a}$, because $\mathfrak{a}$ is a prime ideal. $\Rightarrow [a]_{\mathfrak{a}} = [0]_{\mathfrak{a}}$ or $[b]_{\mathfrak{a}} = [0]_{\mathfrak{a}}$

Thus $R/\mathfrak{a}$ is an integral domain.

$2^\circ \Rightarrow 1^\circ$ $R/\mathfrak{a}$ is an integral domain $\Rightarrow$

$[1_R]_{\mathfrak{a}} \neq [0_R]_{\mathfrak{a}} \Rightarrow 1_R \notin \mathfrak{a} \Rightarrow \mathfrak{a} \subsetneq R$.

Take $a, b \in R$ s.t. $ab \in \mathfrak{a}$.

$\Rightarrow [a]_{\mathfrak{a}} [b]_{\mathfrak{a}} = [0_R]_{\mathfrak{a}}$

$\Rightarrow [a]_{\mathfrak{a}} = [0_R]_{\mathfrak{a}}$ or $[b]_{\mathfrak{a}} = [0_R]_{\mathfrak{a}}$

$\Rightarrow a \in \mathfrak{a}$ or $b \in \mathfrak{a}$.

Thus $\mathfrak{a}$ is a prime ideal.

Lecture 12

Ex: 1) $\mathbb{Z}$ $2m\mathbb{Z}$, $m \in \mathbb{N}^{\geq 2} \cup \{0\}$,

$m\mathbb{Z}$ is a prime ideal $\Leftrightarrow$ m is a prime number or $m=0$.

proof: "$\Rightarrow$": let $t \in \mathbb{N}^{\geq 2, < m}$ be a divisor of $m \neq 0$

Then $\exists s \in \mathbb{N}^{\geq 2, < m}$: $ts = m$.

$\Rightarrow ts \in m\mathbb{Z} \underset{m\mathbb{Z} \text{ prime ideal}}{\Rightarrow} t \in m\mathbb{Z}$ or $s \in m\mathbb{Z}$

$\Rightarrow m \mid t$ or $m \mid s$.

W.l.o.g. $m \mid t$, i.e. $\exists \ell \in \mathbb{N}$: $m\ell = t$

$m\ell s = m \Rightarrow m(\ell s - 1) = 0$

$\Rightarrow$ no zero divisor $\ell s = 1$. $\Rightarrow 1 \leq s \leq \ell s \leq 1 \Rightarrow t = m$ ↯

~~"$\Leftarrow$": $ab \in m\mathbb{Z} \Rightarrow \exists s \in \mathbb{Z}: ms = ab$.~~

~~$a = q_a m + r_a \quad 0 \le r_a < m$~~

~~$b = q_b m + r_b \quad 0 \le r_b < m$~~

~~$\Rightarrow ms = q_a q_b m^2 + q_a r_b m + q_b r_a m + r_a r_b$.~~

```
dbegin=temp(1);
dend=temp(end);
r=max(dend-max_index,max_index-dbegin);
res=sum(abs(T(max_index-r:max_index)-T(max_index+r:-1:max_index)))
res=res/5;
end

function res=costbound(res,min)
    if(abs(res-min)/min>0.05)
        res=1;
    else
        res=0;
en
d
en
d
```

"$\Leftarrow$" $ab \in m\mathbb{Z}$, i.e. $m \mid ab$.

Assume $m \nmid a$. $\Rightarrow \gcd(m,a) = 1$, because m has exactly two divisors in $\mathbb{N}$ (namely 1 and m)

Bezout $\Rightarrow \exists \lambda, \mu \in \mathbb{Z}: \lambda m + \mu a = 1$

$\Rightarrow b = b\lambda m + \mu ab \Rightarrow m \mid b$. $\square$

To get more examples we introduce polynomial rings:

II.2. polynomial rings

<u>Construction:</u> Let R be a commutative ring with $1_R \neq 0_R$.

Consider $\{(a_n)_{n \in \mathbb{N}_0} \mid a_n \in R, \ a_n = 0 \text{ for a } n \in \mathbb{N}_0\} =: R[X]$

We consider the following structures on $R[X]$.

$+$: $(a_n)_{n\in\mathbb{N}_0} + (b_n)_{n\in\mathbb{N}_0} := (a_n + b_n)_{n\in\mathbb{N}_0}$

$\cdot$: $(a_n)_{n\in\mathbb{N}_0} \cdot (b_n)_{n\in\mathbb{N}_0} := (c_n)_{n\in\mathbb{N}_0}$ $\quad c_n = \sum_{m=0}^{n} a_m b_{n-m}$.

$(R[X], +, \cdot)$ is a ~~unitary~~ commutative ring with unit el. $1_{R[X]} := (1, 0, \dots)$ and neutral element

$0_{R[X]} = (0, 0, \dots)$.

We can embed R into $R[X]$ via

$R \xhookrightarrow{\varphi} R[X]$, $\quad a \longmapsto (a, 0, 0, \dots)$ (identify them)

Also we write $X := (0, 1, 0, \dots)$, so we have

$X^n = (\underbrace{0, \dots, 0}_{n \text{ zeros}}, 1, 0, \dots,)$

So for $(a_n)_{n\in\mathbb{N}_0} \in R[X] \setminus \{0\}$ we have the following

$\exists\, m \in \mathbb{N}_0 : a_m \neq 0$ and $a_{m+1} = a_{m+2} = \dots = 0$

and

$(a_n)_{n\in\mathbb{N}_0} = a_0 X^0 + a_1 X^1 + \dots + a_m X^m$.

(a is identified with $(a, 0, \dots)$)

<u>Def 73:</u> Let $P \in R[X]$. The <u>degree of P</u> is the following

$$\deg(P) := \begin{cases} -\infty, & \text{if } P = 0 \\ \max\{n \mid a_n \neq 0\}, & \text{if } P = (a_n)_{n\in\mathbb{N}_0} \neq 0 \end{cases}$$

~~Prop 74:~~

<u>Def 74:</u> Let R be a non-zero unitary ring.

A polynomial function on R in one variable is a map $f: R \to R$ for which $\exists$ $P \in R[X]$, s.t. $f(r) = P(r)$ for all $r \in R$.

<u>Remark 75:</u> Two different polynomials can give the same polynomial function, e.g.

$R = \mathbb{Z}/p\mathbb{Z} =: \mathbb{F}_p$ the field of p elements (p a prime)

$$P(X) := (X - \bar{1})(X - \bar{2}) \cdots (X - \bar{p})$$

$$Q(X) = 0$$

Then $P(x) = Q(x) = \bar{0}$ for all $x \in \mathbb{F}_p$.

<u>Proposition 76:</u> Let R be a non-zero unitary ring. Then we have:

(i) $\forall\, P(X) = \sum_{m=0}^{n} a_m X^m$, $Q(X) = \sum_{m=0}^{n} b_m X^m$:

If $P = Q$ then $a_0 = b_0, a_1 = b_1, \dots, a_m = b_m$.

(2) If R is an infinite field then for all $P, Q \in R[X]$:

$$\underline{P = Q} \iff P(x) = Q(x) \ \forall x \in R.$$

(3) (euclidean property)

Suppose $P, Q \in R[X]$ and Q is <u>monic</u>, i.e. the leading ~~coef~~ coefficient is 1_R: $Q(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$,

then $\exists!\ S, T \in R[X]$ with $\deg(T) < \deg(Q)$:

$$P = SQ + T.$$

(4) Let R be an ~~monic~~ ~~field~~ integral domain and $P \in R[X]$, then P has at most $\deg(P)$ zeros in R.

(A zero (or root) of P is an element $x \in R$, s.t. $P(x) = 0$)

(5) Let R be a field then every ideal of $R[X]$ is generated by one element.

<u>Proof:</u> (1) Given $P(X) = \sum_{m=0}^{n} a_m X^m = Q(X) = \sum_{m=0}^{n} b_m X^m$

we get $(a_0, \dots, a_n, 0, 0, \dots)$
$\quad = (b_0, \dots, b_n, 0, 0, \dots)$

$\Rightarrow \forall_{i=0,\dots,n} \; a_i = b_i$.

(2) <u>Uniqueness:</u> $P = S_1 Q + T_1 = S_2 Q + T_2$

$\Rightarrow (S_1 - S_2) Q = T_2 - T_1$

Assume $S_1 \neq S_2$. Then $\deg(S_1 - S_2) \geq 0$ (not $-\infty$)

Q monic $\Rightarrow \deg(S_1 - S_2) Q = \deg(S_1 - S_2) + \deg(Q) \geq \deg(Q)$

$\gneq \deg(T_2 - T_1)$ ↯

Thus $S_1 = S_2$, so $T_1 = T_2$.

<u>Existence:</u> (induction on $\deg P$).

<u>$\deg P < \deg Q$:</u> Take $S = 0$ and $T = P$.

<u>$\deg P \geq \deg Q$:</u> $P = b_\ell X^\ell + P_1$

$\deg P_1 < \ell$,

Then $P = b_\ell X^{\ell - \deg(Q)} \cdot Q$

$+ b_\ell X^{\ell - \deg(Q)} (X^{\deg(Q)} - Q)$

$+ P_1$

$= b_\ell X^{\ell - \deg(Q)} Q + P_2$

with $\deg P_2 < \deg P$.

Apply (IH) $\Rightarrow$ assertion.

(4) By induction on $\deg P$, $P \neq 0$.

$\mathrm{zeros}_R(P) := \{ x \in R \mid P(x) = 0 \}$

Assertion: $|\mathrm{zero}_R(P)| \leq \deg(P)$ if $P \neq 0$.

<u>$\deg(P) = 0$:</u> ✓, because $\mathrm{zero}_R(P) = \emptyset$.

<u>$\deg(P) > 0$:</u> Let $x \in \mathrm{zero}_R(P)$.

(if $\mathrm{zero}_R(P) = \emptyset$, then we are done.)

(3) $\Rightarrow \exists\, S, T \in R[X] : \deg T \leq 0$:

$P = S(X - x) + T$.

$\deg T \leq 0 \Rightarrow T \in R$.

~~We get~~ $\cancel{0 = P(x) = S(x)(x-x) + T(x)}$

$$= \underbrace{T}_{\in R}$$

$$\Rightarrow \quad P(X) = S(X) \cdot (X - x).$$

R is zero divisor free $\Rightarrow$ Every root $\tilde{x}$ of P different from x must be a root of S, because

$$0 = P(\tilde{x}) = S(\tilde{x}) \underbrace{(\tilde{x} - x)}_{\neq 0}.$$

$$(IH) \Rightarrow \quad |\mathrm{zeros}_R(S)| \leq \deg(S) = \deg(P) - 1$$

$$\Rightarrow \quad |\mathrm{zeros}_R(P)| \leq \deg(P)$$

(2) If R is an infinite field and $P, Q \in R[X]$ satisfy $P(X) = Q(x)$ $\forall x \in R$, then $P - Q$ has infinitely many zeros, i.e. $P - Q = 0$ by (4).

(5) Let $\mathfrak{a}$ be a non-zero proper ideal of $R[X]$ and R be a field.

Let $P \in \mathfrak{a}$ be a non-zero polynomial of minimal degree.

Then we can assume w.l.o.g. that P is monic.

Take $Q \in \mathfrak{a} \setminus \{0\}$.

(3) $\Rightarrow$ $\exists S, T \in R[X]$ $\deg(T) < \deg(P)$:

$$Q = SP + T. \Rightarrow T = Q - SP \in \mathfrak{a}.$$

$0 \leq \deg(P)$ minimal $\Rightarrow$ $T = 0$. $\Rightarrow$ $Q = SP$

$\square$

So $\mathfrak{a} = (P)_{R[X]}$

<u>Ex:</u> 1) $X^4 + X^3 + 2X^2 + 1 = P(X) \in \mathbb{R}[X]$

$Q = X^2 + X \in \mathbb{R}[X]$.

$$P(X) = X^2 Q + 2Q - 2X + 1$$

$$= \underbrace{(X^2+2)}_{S} Q(X) + \underbrace{(-2X+1)}_{T}$$

<u>Def 77:</u> 1) Let $R_1 \subseteq R_2$ be two ~~[illegible]~~ rings (we call R_2/R_1 a ring extension) and $S \subseteq R_2$. We write $R_1[S]$ for the ring generated by R_1 and S, i.e. for

$$R_1 \cup S \subseteq \underset{\text{ring}}{R} \subseteq R_1 \quad R$$

2) Let $F_1 \subseteq F_2$ be fields (we call $F_2 | F_1$ a field extension) and $S \subseteq F_2$.

We write $F_1(S)$ for the sub-field of F_2 generated by F_1 and S, i.e. for

$$\bigcap_{\substack{F_1 \cup S \subseteq F \subseteq F_2 \\ F \text{ field}}} F .$$

Convention: $S = \{s_\lambda \mid \lambda \in \Lambda\}$ We also write $R_1[s_\lambda \mid \lambda \in \Lambda]$ for $R[S]$ etc.

Ex: 1) $\mathbb{Z} \subseteq \mathbb{C}$ $\quad S = \{i\}$.

$$\mathbb{Z}[S] = \mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z} i + \mathbb{Z} i^2 + \dots$$
$$= \mathbb{Z} + \mathbb{Z} i .$$

just notation. ring of Gaussian integers.

2) (i) $\mathbb{Q} \subseteq \mathbb{C}$,

$\mathbb{Q}(i) =$ (w.r.t. $\subseteq$) smallest field in $\mathbb{C}$ containing $\mathbb{Q}$ and i.

Claim: $\mathbb{Q}(i) \overset{\mathrm{I}}{=} \mathbb{Q}[i] \overset{\mathrm{II}}{=} \mathbb{Q} + \mathbb{Q} i$

Proof: II ✓ (exercise)

I $\supseteq$ ✓ a field is a ring.

$\subseteq$ $\mathbb{Q}[i]$ is a field, because $a + ib \neq 0$ has inverse

$\frac{1}{a^2+b^2}(a-ib)$. $\square$

(ii) $\mathbb{Q}(\pi) \supsetneq \mathbb{Q}[\pi]$. ($\frac{1}{\pi} = a_0 + a_1\pi + \dots + a_n\pi^n \Rightarrow a_n\pi^{n+1} + \dots + a_0\pi - 1 = 0$ ↯)

3) The ideals (X, p), p a prime are maximal ideals in $\mathbb{Z}[X]$.

<u>Proof:</u> $\mathbb{Z}[X] \xrightarrow{\varphi} \mathbb{Z}/p\mathbb{Z}$

$$\varphi(P) = [P(0)]_p = \overline{P(0)}$$

φ is a ring homomorphism.

$\Rightarrow$ $\ker\varphi$ is an ideal.

$X, p \in \ker\varphi. \Rightarrow (X, p) \subseteq \ker(\varphi)$

Take $Q \in \ker(\varphi)$ $Q(X) = a_0 X^0 + a_1 X + \dots + a_n X^n$.

$\bar{0} = \varphi(Q) = \overline{a_0} \Rightarrow a_0 \in p\mathbb{Z} \subseteq p\mathbb{Z}[X] \subseteq (X, p)$

Thus $Q \in (X, p)$.

So $\mathbb{Z}[X]/(X,p) \simeq \mathbb{Z}/p\mathbb{Z}$ a field

$\square$

Def 78: We write for a non-zero unitary commutative ring R:

$$R[X_1,\dots,X_n] := ((R[X_1])[X_2])\cdots[X_n]$$

and we use the ~~Canon~~ canonical maps

$$R \subseteq R[X_1] \subseteq R[X_1,X_2] \subseteq \dots \subseteq R[X_1,\dots,X_n]$$

to consider $X_1,\dots,X_n$ as elements of $R[X_1,\dots,X_n]$.

II.3. Chinese remainder theorem.

Theorem 79: Suppose R is a non-zero commutative unitary ring and $\mathfrak{a}_1,\dots,\mathfrak{a}_\ell$ are proper ideals of R s.t. $\forall_{i\neq j}: \mathfrak{a}_i + \mathfrak{a}_j = R$.

Then ① $\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_\ell = \mathfrak{a}_1 \cdots \mathfrak{a}_\ell$

$$\left(\mathfrak{a}_1 \cdots \mathfrak{a}_\ell := (\{a_1 \cdots a_\ell \mid a_i \in \mathfrak{a}_i\})_R\right)$$

② $$R/\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_\ell \xrightarrow[\sim]{\varphi} R/\mathfrak{a}_1 \times \dots \times R/\mathfrak{a}_\ell$$

$$[a] \longmapsto ([a]_{\mathfrak{a}_1},\dots,[a]_{\mathfrak{a}_\ell})$$

<u>Ex:</u> (for product of ideals):

In $\mathbb{Z}[X,Y]$:

$$(X,Y)\cdot(X^2,p) \qquad p \text{ prime.}$$

$$= (\{X^3, YX^2, Xp, Yp\})_{\mathbb{Z}[X,Y]}$$

$$= \{ Q_1(X,Y)X^3 + Q_2(X,Y)YX^2 + Q_3(X,Y)Xp + Q_4(X,Y)Yp \mid Q_1,\dots,Q_4 \in \mathbb{Z}[X,Y] \}$$

<u>Proof:</u> (Theorem 79)

① "$\supseteq$" $\mathfrak{a}_1 \cdots \mathfrak{a}_\ell$ is generated by $a_1 \cdots a_\ell$, $a_i \in \mathfrak{a}_i$, and $a_1 \cdots a_\ell \in \mathfrak{a}_i \ \forall i = 1,\dots,\ell$.

"$\subseteq$" Induction ℓ. <u>$\ell = 1$</u> ✓

<u>$\ell = 2$</u>: Take $a \in \mathfrak{a}_1 \cap \mathfrak{a}_2$

$\mathfrak{a}_1 + \mathfrak{a}_2 = R \Rightarrow \exists\, e_i \in \mathfrak{a}_i$:

$e_1 + e_2 = 1$.

~~$\Rightarrow a = a e_1 + a e_2 \in \mathfrak{a}_1 \cdot \mathfrak{a}_2$~~

$\underline{\ell > 2}$: (IH) $\Rightarrow$ $\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_{\ell-1} = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_{\ell-1}$. (*)

Further, for each $j \in \{1, \dots, \ell-1\}$

$\exists\, e_j \in \mathfrak{a}_j,\ f_j \in \mathfrak{a}_\ell$: $e_j + f_j = 1_R$.

$$\Rightarrow 1_R = 1_R \cdot \ldots \cdot 1_R = (e_1 + f_1) \cdot \ldots \cdot (e_{\ell-1} + f_{\ell-1})$$

$$= \underbrace{f}_{\mathfrak{a}_\ell} + e_1 \cdot \ldots \cdot e_{\ell-1}$$

$$\Rightarrow \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_{\ell-1} + \mathfrak{a}_\ell = R$$

$\ell = 2$ case $\Rightarrow$ $(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_{\ell-1}) \cap \mathfrak{a}_\ell = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_{\ell-1} \cdot \mathfrak{a}_\ell$

$\overset{\text{(IH)}}{=}$

$\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_\ell$

② Induction on ℓ: $\ell = 1$ ✓

$\underline{\ell = 2}$: Take $e_i \in \mathfrak{a}_i$: $e_1 + e_2 = 1_R$.

$\Rightarrow$ For $a_i \in R, i = 1, 2$. $a := a_2 e_1 + a_1 e_2$.

~~Then~~ $\cancel{[a]_{\mathfrak{a}_1} = [a_1 e_1]_{\mathfrak{a}_1} = [a_1 e_2 + a_1 e_1]_{\mathfrak{a}_1}}$

$$= [a_1 1_R]_{\mathfrak{a}_1} = [a_1]_{\mathfrak{a}_1}.$$

and $[a]_{\mathfrak{a}_2} = [a_2]_{\mathfrak{a}_2}$.

φ is injective: (exercise).
homomorphism.

<u>$\ell > 2$:</u> $$R/\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_\ell \simeq R/\mathfrak{a}_1 \cap \dots \cap \mathfrak{a}_{\ell-1} \times R/\mathfrak{a}_\ell$$

$$\underset{\text{IH}}{\simeq} \left(R/\mathfrak{a}_1 \times \dots \times R/\mathfrak{a}_{\ell-1} \right) \times R/\mathfrak{a}_\ell.$$

$\square$

<u>Ex:</u> 1) $$\mathbb{Z}/12\mathbb{Z} \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

$(4\mathbb{Z} + 3\mathbb{Z} = \mathbb{Z}.)$

Find $z \in \mathbb{Z}$: $z \equiv_4 3$
$z \equiv_3 2$

$\cdot\ 4 \in 4\mathbb{Z}$ $(-3) \in 3\mathbb{Z}$ $4 + (-3) = 1.$

$\cdot\ z_0 := 2 \cdot 4 + 3 \cdot (-3) = 8 - 9 = -1$

$[-1]_4 = [3]_4$, $[-1]_3 = [2]_3$.

$Sol^{us} = \{ 12k - 1 \mid k \in \mathbb{Z} \}.$

<u>lecture 14</u>

An extra example for the CRT.

<u>Example:</u> 1) Solve

$$P(X,Y) \equiv_{(Y^2,\, XY)} X+Y$$

$$P(X,Y) \equiv_{(1-Y,\, X^2)} 1-X$$

$$P(X,Y) \equiv_{((1-X)Y,\, 1+Y)} XY$$

in $\mathbb{Q}[X,Y]$.

$$\mathfrak{a}_1 := (Y^2, XY)_{\mathbb{Q}[X,Y]}$$

$$\mathfrak{a}_2 := (1-Y, X^2)_{\mathbb{Q}[X,Y]}$$

$$\mathfrak{a}_3 := ((1-X)Y, 1+Y)_{\mathbb{Q}[X,Y]}.$$

Note: They are all proper ideals.

$$\mathfrak{a}_1 \subseteq \{ P \in \mathbb{Q}[X,Y] \mid P(0,0)=0 \}$$

$$\mathfrak{a}_2 \subseteq \{ \qquad \mid P(0,1)=0 \} \quad \subsetneq \mathbb{Q}[X,Y]$$

$$\mathfrak{a}_3 \subseteq \{ \qquad \mid P(1,-1)=0 \}$$

I $\mathfrak{a}_1 + \mathfrak{a}_2 = \mathbb{Q}[X,Y]$ $\qquad Y^2 + (1-Y)(Y+1) = 1$

II $\mathfrak{a}_1 + \mathfrak{a}_3 = \;''\;$ $\qquad (-XY) + (Y(X-1) + (1+Y)) = 1$

III $\mathfrak{a}_2 + \mathfrak{a}_3 = \;''\;$ $\qquad \frac{1}{2}(1-Y) + \frac{1}{2}(1+Y) = 1$

CRT $\underline{\mathrm{I}_1\mathrm{II}}$: $\underbrace{Y^2}_{f}(1-X) + \underbrace{(1-Y^2)}_{f}(X+Y)$

$$= X + Y + Y^2 - 2XY^2 - Y^3$$

$\mathfrak{a}_1\mathfrak{a}_2 + \mathfrak{a}_3 = \mathbb{Q}[X,Y]$:

$$\underbrace{X^2Y^2}_{\in \mathfrak{a}_1\mathfrak{a}_2} + \underbrace{(1-X^2Y^2)}_{\in \mathfrak{a}_3} = 1$$

Sol^n by CRT: It is the $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3$ residual class of

$$X^2Y^2\cdot(X+Y) + (1-X^2Y^2)(X+Y+Y^2 - 2XY^2 - Y^3)$$

$$= X^3Y^3 + X + Y + Y^2 - 2XY^2 - Y^3 - X^3Y^2 - X^2Y^3 - X^2Y^4 + 2X^3Y^4 + X^2Y^5$$

$$= X^2Y^5 + 2X^3Y^4 + X^3Y^3 - X^2Y^4 - X^2Y^3 - X^3Y^2 - Y^3 - 2XY^2 + Y^2 + X + Y. \quad =: P_0(X,Y)$$

$P_0(X,Y) \equiv_{\mathfrak{a}_1} X+Y$; $\equiv_{\mathfrak{a}_2} -1-2X+1+X+1 \equiv 1-X$

$$\equiv_{\mathcal{O}_3} -1+2-1-1+1-1+1$$

$$-2+1+X+(-1) = X-2$$

$$\equiv_{\mathcal{O}_3} -XY+2Y \equiv_{\mathcal{O}_3} -XY+2XY \equiv_{\mathcal{O}_3} XY.$$

---

2) $z \equiv_3 1 \wedge z \equiv_{11} 7 \wedge z \equiv_7 3$

$\underline{\mathrm{I} \wedge \mathrm{II}}$: $\underbrace{3\cdot 4}_{e} + \underbrace{(-11)}_{f} = 1$: Sol $\wedge$ $\vee$ $-11 + 7\cdot 12 \mod 33$ dan of

$= 73 \equiv_{33} 7$.

$\underline{(\mathrm{I} \wedge \mathrm{II}) \wedge \mathrm{III}}$: Find $e+f=1$:

Euclidean algorithm to find Bézout + decomposition of $\gcd(33,7)=1$.

$33 = 4\cdot 7 + 5$

$7 = 1\cdot 5 + 2$

$5 = 2\cdot 2 + 1$

$2 = 2\cdot 1 + \underline{0}$ $\Rightarrow \gcd(33,7)=1$

Backwards: $1 = 5 - 2\cdot 2$

$= 5 - 2(7 - 1\cdot 5)$

$= (-2)7 + 3\cdot 5$

$= 3\cdot 33 - 14\cdot 7.$

$= 99 - 98.$

$$\text{CRT Def}^n = [99 \cdot 3 - 98 \cdot 7]_{231}$$
$$= [297 - 686]_{231}$$
$$= [66 + 7]_{231}$$
$$= [73]_{231}$$

II.4. Field of fractions

Let R be an integral domain. We want to divide by elements of R. Consider the following equivalence relation on $R \times R \setminus \{0\}$

$(r_1, s_1) \sim (r_2, s_2)$

$\Longleftrightarrow_{\text{Def}} \quad r_1 s_2 = r_2 s_1$

enumerator
denominator

<u>Proof</u> (that this is an equivalence relation).

① $(r_1, s_1) \sim (r_1, s_1)$, $r_1 s_1 = r_1 s_1$, reflexivity ✓

② symmetry ✓

③ $(r_1, s_1) \sim (r_2, s_2) \sim (r_3, s_3)$

$\Rightarrow r_1 s_2 = r_2 s_1 \wedge r_2 s_3 = r_3 s_2$

$$\Rightarrow \quad r_1 s_2 s_3 = r_2 s_1 s_3 = r_3 s_2 s_1$$

$$\Rightarrow \quad (r_1 s_3 - r_3 s_1) s_2 = 0$$

$$\Rightarrow \quad r_1 s_3 - r_3 s_1 = 0$$

zero divisor free, $s_2 \neq 0$

$$\Rightarrow \quad (r_1, s_1) \sim (r_3, s_3). \quad \checkmark \quad \square$$

transitivity ✓

<u>Prop 80:</u> $Q(R) := R \times (R \setminus \{0\}) / \sim$ is a field w.r.t.

$$+ : [(r_1, s_1)]_\sim + [(r_2, s_2)]_\sim := [(r_1 s_2 + r_2 s_1, s_1 s_2)]_\sim$$

$$\cdot : [(r_1, s_1)]_\sim \cdot [(r_2, s_2)]_\sim = [(r_1 r_2, s_1 s_2)]_\sim$$

We call $Q(R)$ the field of fractions of R and we write $\frac{r}{s}$ for $[(r,s)]_\sim$.

<u>Proof:</u> (exercise) $\square$

<u>Ex:</u> 1) $Q(\mathbb{Z}) \simeq \mathbb{Q}$

$$[(z_1, z_2)]_\sim \longmapsto \frac{z_1}{z_2} \in \mathbb{Q}$$

2) $R = S[X]$ S an integral domain (e.g. $\mathbb{Z}$)

$$Q(R) \overset{\text{Def}}{:=} \left\{ \frac{P(X)}{Q(X)} \;\middle|\; \begin{array}{l} P \in S[X] \\ Q \in \\ Q \neq 0 \end{array} \right\}$$

3) If R is a field then $Q(R) \simeq R$ via $[(r,s)]_\sim \longmapsto r \cdot s^{-1}$

4) R ~~a ring~~ integral domain and F a field $\Rightarrow$ $\mathbb{Q}(R) \simeq \bigcap_{\substack{R \subseteq F' \subseteq F \\ \text{field}}} F'$

(homework)

We have the following universal property.

<u>Prop 81</u>: Let R be an integral domain.

1) Then, for every field F and every injective ring homomorphism

$$q : R \hookrightarrow F$$

$\exists$ field homomorphism $\psi : Q(R) \to F$:

$$\begin{tikzcd} R \arrow[r, hook, "q"] \arrow[d, hook, "a"] & F \\ Q(R) \arrow[ur, hook, "\psi"'] & \end{tikzcd}$$

$r \mapsto [(r,1)]$

2) If a field Q with injective ring homom. $R \xhookrightarrow{a} Q$ satisfies 1) in replacing $Q(R)$ by Q then $Q \simeq Q(R)$ (as fields).

<u>Remark!</u> ψ is automatically injective, because every non-zero ring homomorphism from a field to a ring is injective. (Pf: $a \neq 0$: $\psi(a)\psi(a^{-1}) = \psi(1) \neq 0$ (because $\psi \neq 0$))

$\Rightarrow \ker(\psi) = \{0\}$)

<u>Proof</u>: (of Prop 81)

1) • Define $\psi([(r,s)]_\sim) := \varphi(r)\varphi(s)^{-1}$

well-defined: $(r,s) \sim (r',s')$

$\Rightarrow rs' = r's \Rightarrow \varphi(r)\varphi(s') = \varphi(r')\varphi(s)$

$\Rightarrow \varphi(r)\varphi(s)^{-1} = \varphi(r')\varphi(s')^{-1}$ ✓

• $\psi([(1,0)]_\sim) = \varphi(1) = 1.$

ψ is a ring homomorphism.

$\psi([(r,s)]_\sim \cdot [(r',s')]_\sim) = \psi([(rr',ss')]_\sim)$

$= \varphi(rr')\varphi(ss')^{-1}$

$= \varphi(r)\varphi(s)^{-1}\varphi(r')\varphi(s')^{-1}$

$= \psi([(r,s)]_\sim) \cdot \psi([(r',s')]_\sim)$

For "+" (exercise).

$(\psi \circ L)(r) = \psi([(r,1)]_\sim)$

$= \varphi(r) \cdot \varphi(1)^{-1} = \varphi(r)$

($\varphi(1) = 1$ because $\varphi \neq 0$ and Fin a field $\varphi(1)^2 = \varphi(1)$)

2) By 1) we get

$$\psi_Q : Q(R) \hookrightarrow Q$$

and $\psi_{Q(R)} : Q \hookrightarrow Q(R)$,

more precisely

$$\begin{tikzcd}
Q(R) \arrow[r, hook, "\psi_Q"] & Q \arrow[dr, hook, bend left, "\psi_{Q(R)}"] & \\
 & & Q(R) \arrow[d, hook, "\psi_Q"] \\
R \arrow[uul, "\iota"] \arrow[uu, "\iota_Q"] \arrow[urr, "\iota"] \arrow[rr, "\iota_Q"'] & & Q
\end{tikzcd}$$

$$\Rightarrow \quad \psi_{Q(R)} \circ \psi_Q \circ \iota = \iota$$

$$\Rightarrow \quad \forall r \in R : (\psi_{Q(R)} \circ \psi_Q)([(r,1)]_\sim) = [(r,1)]_\sim$$

$\{[(r,1)]_\sim \mid r \in R\}$ generates $Q(R)$

$$\Rightarrow \quad \psi_{Q(R)} \circ \psi_Q = id_{Q(R)}$$

Thus $\psi_{Q(R)}$ is bijective

$$\Rightarrow \quad Q(R) \simeq Q \qquad \square$$

Ex: $\underbrace{\mathbb{Q}[X]}_{=R} \hookrightarrow \mathbb{R}[X,Y]$

$\varphi(P(X)) = P(X+Y)$

$$\begin{tikzcd}
P(X) \arrow[dr, mapsto] \arrow[rr, bend left] & & \mathbb{Q}(X) \arrow[ur, dashed] & \frac{P(X+Y)}{Q(X+Y)} \\
& \frac{P(X)}{1} & & \frac{P(X)}{Q(X)} \arrow[u, mapsto]
\end{tikzcd}$$

lecture 15

II.5 Noetherian rings

Let R be a non-zero unitary ring

Def 82: We call R left noetherian if all left ideals of R are finitely generated. R is called noetherian if R is left and right noetherian.

Ex: $F[X]$, F a field; $\mathbb{Z}$; any field are noetherian.

<u>Prop 87</u>: The following conditions are equivalent:

1° R is left noetherian

2° $\forall$ "∞" ascending chain of left ideals

$$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \dots$$

$$\exists_{k \in \mathbb{N}} \forall_{i \geq k}: \mathfrak{a}_k = \mathfrak{a}_{k+1}.$$

3° Every set of ideals of R has a maximal element w.r.t. "$\subseteq$".

<u>Proof</u>: <u>$1° \Rightarrow 2°$</u>: $\mathfrak{b} := \bigcup_{i=1}^{\infty} \mathfrak{a}_i$ is an ideal $1° \Rightarrow \mathfrak{b}$ is finitely generated $\mathfrak{b} = (f_1, \dots, f_\ell)_R$

$\Rightarrow \exists_{b \in \mathbb{N}} \; b_1, \dots, b_1 \in \mathfrak{a}_k$

$\Rightarrow \quad \mathfrak{b} \subseteq \mathfrak{a}_k \subseteq \mathfrak{a}_{k+1} \subseteq \dots \subseteq \mathfrak{b}$

$2^\circ \Rightarrow 3^\circ$ If a set $\mathfrak{M}$ of ideals of R does not contain a "$\subseteq$" maximal element then we can construct an ascending chain which doesn't stabilize.

Take $\mathfrak{a}_1 \in \mathfrak{M}$, $\mathfrak{a}_1$ not maximal in $\mathfrak{M}$

" $\mathfrak{a}_2 \in \mathfrak{M}$ with $\mathfrak{a}_2 \supsetneq \mathfrak{a}_1$,

and so on.

<u>$3^\circ \Rightarrow 1^\circ$</u>: Assume $\mathfrak{a}$ is not finitely generated. Take $a_1 \in \mathfrak{a} \setminus \{0\}$

$a_i \in \mathfrak{a} \setminus (Ra_1 + \dots + Ra_{i-1})$

Then $\{Ra_1 + \dots + Ra_i \mid i \in \mathbb{N}\}$

has no maximal element $\square$

<u>Ex:</u> 1) $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ is noetherian.

2) $M_n(R)$ is left noetherian,

because every left ideal is a left R vector space of dimension $\leq n^2$, so an ascending chain of ideals has to stabilize.

3) $R := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b \in \mathbb{R},\ c \in \mathbb{Q} \right\}$

is left noetherian, but not right noetherian

left noetherian: Every left ideal $\mathfrak{a}$ of R satisfies: (a) $\left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \cap \mathfrak{a}$ is a finite dim $\mathbb{R}$-vector space

(a) is left

(b) $\left\{ \begin{pmatrix} 0 & 0 \\ 0 & c \end{pmatrix} \middle| \, c \in \mathbb{Q} \right\} \cap \mathfrak{A}$

is a ~~fa~~ 0 or 1-dim $\mathbb{Q}$ vector space.

(a), (b) $\Rightarrow$ The ascending chain condition is satisfied.

<u>not right noetherian:</u> $\dim_{\mathbb{Q}} \mathbb{R} = \infty$, because $\mathbb{R}$ is not countable. Take a $\mathbb{Q}$-basis of $\mathbb{R}$ $(q_\lambda \mid \lambda \in \Lambda)$ and a countable subset $\Gamma \subseteq \Lambda$. $\Gamma = \{\lambda_1, \lambda_2, \lambda_3, \dots\}$

$$W_i := \mathbb{Q} q_{\lambda_1} + \mathbb{Q} q_{\lambda_2} + \dots + \mathbb{Q} q_{\lambda_i}$$

$$\Rightarrow \mathfrak{A}_i := \left\{ \begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix} \middle| \, b \in W_i \right\} \text{ (right ideals)}$$

satisfy $\mathfrak{A}_1 \subsetneq \mathfrak{A}_2 \subsetneq \mathfrak{A}_3 \subsetneq \dots$

So, R does not satisfy the ascending chain condition for right ideals.

4) Let $R \overset{\varphi}{\twoheadrightarrow} S$ be a surjective homomorphism of non-zero unitary rings.

Then S is left noetherian if R is left noetherian.

$$\mathfrak{A}_1 \subsetneq \mathfrak{A}_2 \subseteq \mathfrak{A}_3 \subseteq$$

$$\Rightarrow \quad \varphi^{-1}(\mathfrak{a}_1) \subseteq \varphi^{-1}(\mathfrak{a}_2) \subseteq \varphi^{-1}(\mathfrak{a}_3) \subseteq \dots$$

is an ascending chain of left ideals, so stabilizes, because R is noetherian, say

$$\varphi^{-1}(\mathfrak{a}_k) = \varphi^{-1}(\mathfrak{a}_{k+1}) = \varphi^{-1}(\mathfrak{a}_{k+2}) = \dots$$

Apply φ $\Rightarrow$ $\mathfrak{a}_k = \mathfrak{a}_{k+1} = \mathfrak{a}_{k+1} = \dots$

$\Rightarrow$ S satisfies the ACC.

5) If $S \hookrightarrow R$ is an injective homomorphism of unitary non-zero rings, then we cannot conclude noetherianity of S from R.

<u>Ex</u>: $R := \mathbb{Q}(X_1, X_2, X_3, \dots)$, the field of fractions of $\mathbb{Q}[X_1, X_2, X_3, \dots] =: S$

$S \hookrightarrow R$ (inclusion)

$p \mapsto \frac{p}{1}$

R is a field, so noetherian.

S is not ~~let~~ " , because

$$(X_1) \subsetneq (X_1, X_2) \subsetneq (X_1, X_2, X_3) \subsetneq \dots$$

does not stabilise.

Hilbert's basis theorem

<u>Theorem 84.</u> (Ü) Let R be a commutative noetherian ring. Then $A[X]$ is noetherian.

<u>Proof:</u> Let $\mathfrak{a}$ be an ideal. Assume $\mathfrak{a}$ is not finitely generated.

$\Rightarrow \mathfrak{a} \neq (0)$.

$\Rightarrow \exists\, Q_1 \in \mathfrak{a} \setminus (0)$. Choose Q_1 such that the degree is minimal. $d_1 := \deg Q_1 \geq 0$

$\mathfrak{a}$ is not finitely generated $\Rightarrow \exists\, Q_2 \in \mathfrak{a} \setminus (Q_1)_{A[X]}$ of minimal degree $d_2 \geq d_1$

$\vdots$

We obtain $Q_i \in \mathfrak{a} \setminus (Q_1, \dots, Q_{i-1})_{A[X]}$ of minimal degree $d_i \geq d_{i-1}$.

Write $Q_i = a_{d_i,i} X^{d_i} + a_{d_i-1,i} X^{d_i-1} + \dots + a_{1,i} X + a_{0,i}$

$$\Rightarrow (a_{d_1,1}) \subseteq (a_{d_1,1}, a_{d_2,2}) \subseteq (a_{d_1,1}, a_{d_2,2}, a_{d_3,3}) \subseteq \dots \subseteq (a_{d_1,1}, \dots, a_{d_i,i}) \subseteq \dots$$

stabilizes, because A is noetherian.

$\Rightarrow \exists_{k \in \mathbb{N}}: \quad a_{d_{k+1}, k+1} \in (a_{d_1,1}, \dots, a_{d_k,k})$

i.e. $$a_{d_{k+1},k+1} = \sum_{j=1}^{k} \lambda_j a_{d_j,j}$$

for certain $\lambda_j \in A$.

$$\deg\left(Q_{k+1} - \sum_{j=1}^{k} \lambda_j X^{d_{k+1}-d_j} Q_j\right) < \deg Q_{k+1}$$

Thus $\quad$ — " — $\quad \in (Q_1, \dots, Q_k)$,

thus $\quad Q_{k+1} \in (Q_1, \dots, Q_k)$ ↯ $\square$

<u>Ex:</u> Let $\alpha \in \mathbb{R}$. Then $\mathbb{Z}[\alpha] \subseteq \mathbb{R}$ is noetherian.

($\mathbb{Z}[\alpha]$ is the ring generated by $\mathbb{Z}$ and α:

$$\mathbb{Z}[\alpha] = \bigcap_{\substack{\mathbb{Z} \cup \{\alpha\} \subseteq S \subseteq \mathbb{R} \\ \text{ring}}} S = \mathbb{Z} + \mathbb{Z}\alpha + \mathbb{Z}\alpha^2 + \dots)$$

<u>Proof:</u> $$\mathbb{Z}[X] \twoheadrightarrow \mathbb{Z}[\alpha]$$
$$P(X) \longmapsto P(\alpha)$$ $\square$

<u>Theorem 85 (Cohen)</u> Let R be a non-zero commutative unitary ring. T.a.e.:

1° R is noetherian

2° Every prime ideal is finitely generated.

<u>Proof:</u> $2° \Rightarrow 1°$ Let $\mathfrak{a} \subsetneq R$ be an ideal. Assume that $\mathfrak{a}$ is not finitely generated

$$\mathfrak{M} := \{ \mathfrak{b} \mid \mathfrak{b} \subseteq R \text{ ideal which is not f.g.} \} \quad (\text{Note: } R = (1) \text{ f.g.})$$

$\mathfrak{a} \in \mathfrak{M}$.

Let $\emptyset \neq \mathfrak{N} \subseteq \mathfrak{M}$ be a chain $\mathfrak{p} := \bigcup_{\mathfrak{b} \in \mathfrak{N}} \mathfrak{b}$

is an ideal of R:

$1 \in R$, $a, b \in \mathfrak{p} \Rightarrow \exists\, \mathfrak{b}_1, \mathfrak{b}_2 \in \mathfrak{N} : a \in \mathfrak{b}_1 \wedge b \in \mathfrak{b}_2$

$\mathfrak{b}_1 \subseteq \mathfrak{b}_2$ or $\mathfrak{b}_2 \subseteq \mathfrak{b}_1$. W.l.o.g. $\mathfrak{b}_1 \subseteq \mathfrak{b}_2$

$\Rightarrow a, b \in \mathfrak{b}_2 \Rightarrow a+b, \lambda a \in \mathfrak{b}_2 \subseteq \mathfrak{p}$.

$\mathfrak{p}$ is not f.g. Otherwise $\mathfrak{p} = (a_1, \dots, a_\ell)$

Then $\exists\, \mathfrak{b}_i \in \mathfrak{p} : a_i \in \mathfrak{b}_i$. W.l.o.g.

$\mathfrak{b}_1 \supseteq \mathfrak{b}_2 \cup \mathfrak{b}_3 \cup \dots \cup \mathfrak{b}_\ell \Rightarrow a_1, \dots, a_\ell \in \mathfrak{b}_1$

$\Rightarrow \mathfrak{b}_1 = \mathfrak{p}$ $\mathfrak{p}$ is f.g. $\lightning$. $\Rightarrow \mathfrak{M}$ inductively ordered

Zorn's lemma $\Rightarrow \exists\, \hat{\mathfrak{a}}$ a maximal element in $\mathfrak{M}$. (w.r.t. "$\subseteq$")

<u>Claim</u>: $\hat{\mathfrak{a}}$ is prime. Let $x, y \in R$ s.t. $xy \in \hat{\mathfrak{a}}$. Assume $x, y \notin \hat{\mathfrak{a}}$.

$\Rightarrow Rx + \hat{\mathfrak{a}} \supsetneq \hat{\mathfrak{a}}$

$Ry + \hat{\mathfrak{a}} \supsetneq \hat{\mathfrak{a}}$.

$\Rightarrow$ $Rx + \hat{\mathfrak{a}}$ and $Ry + \hat{\mathfrak{a}}$ are f.g.

Say — " — $= \sum_{i=1}^{\ell} R(r_i x + a_i)$

Consider

$\mathcal{F}_x := \{ r \in R \mid r \cdot x \in \hat{\mathfrak{a}} \} \subseteq R$ ideal

$\hat{\mathfrak{a}} \subseteq \mathcal{F}_x$ and $y \in \mathcal{F}_x \setminus \hat{\mathfrak{a}}$.

$\Rightarrow$ $\mathcal{F}_x = (t_1, \dots, t_k)$ is ~~f.g.~~ finitely generated.

<u>Claim</u>: $(t_1 x, \dots, t_k x, a_1, \dots, a_\ell) = \hat{\mathfrak{a}}$.

"$\subseteq$" ✓

"$\supseteq$" $a \in \hat{\mathfrak{a}} \subseteq \hat{\mathfrak{a}} + Rx = (r_1 x + a_1, \dots, r_\ell x + a_\ell)$

$\Rightarrow \exists\, \lambda_1, \dots, \lambda_\ell \in R$: $a = \sum_{i=1}^{\ell} \lambda_i (r_i x + a_i)$

$= \sum_{i=1}^{\ell} \lambda_i a_i + x \left(\sum_{i=1}^{\ell} \lambda_i r_i \right)$

$\Rightarrow \sum_{i=1}^{\ell} \lambda_i r_i \in \mathcal{F}_x \Rightarrow \exists\, \mu_s : \sum_{s=1}^{k} \mu_s t_s = \sum_{i=1}^{\ell} \lambda_i r_i$.

$$\Rightarrow a = \sum \lambda_i a_i + \sum_{s=1}^{b} t_s \times \mu_s \quad \blacksquare$$

So $\mathfrak{A}$ is finitely generated $\lightning$

So $\hat{\mathfrak{A}}$ is prime $\lightning \Rightarrow \mathfrak{A}$ is finitely generated $\lightning$

$\square$

As an example we have the following corollary.

<u>Corollary 86:</u> Let A be an abelian group.

Consider $\mathbb{Z}_A := \mathbb{Z} \times A$ with

$$+ : \quad (z_1, a_1) + (z_2, a_2) := (z_1 + z_2, a_1 + a_2)$$

$$\cdot : \quad (z_1, a_1) \cdot (z_2, a_2) = (z_1 z_2, z_1 a_2 + z_2 a_1)$$

Then $(\mathbb{Z}_A, +, \cdot)$ is a non-zero commutative unitary ring. (exercise). T.f.a.e:

1° $\mathbb{Z}_A$ is noetherian

2° A is f.g. as a group.

où

<u>Proof:</u> $A^\circ \Rightarrow 2^\circ$ If A is not f.g. then

take $a_1 \in A$ and $a_2 \in A \setminus \mathbb{Z}a_1$

$a_i \in A \setminus (\mathbb{Z}a_1 + \mathbb{Z}a_2 + \dots + \mathbb{Z}a_{i-1})$

Then $\underbrace{\mathbb{Z}a_1}_{=:A_1} \subsetneq \underbrace{\mathbb{Z}a_1 + \mathbb{Z}a_2}_{=:A_2} \subsetneq \dots$

and $\{0\}\times A_1 \subsetneq \{0\}\times A_2 \subsetneq \{0\}\times A_3 \subsetneq \dots$

is an ascending chain of ideals of $\mathbb{Z}_A$.

Thus $\mathbb{Z}_A$ is not noetherian $\lightning$ to 1°

$2^\circ \Rightarrow 1^\circ$ (non-trivial)

Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}_A$.

$(0,a)(0,a) = (0, 0a + 0a) = (0, 0_A) \in \mathfrak{p}$

$\mathfrak{p}$ prime $\Rightarrow$ $(0,a) \in \mathfrak{p}$ $\forall a \in A$.

$\Rightarrow$ $\{0\} \times A \subseteq \mathfrak{p}$.

So if $(z,a) \in \mathcal{P}$ then $(z,0_A) = (z,a) - (0,a)$

$\in \mathcal{P}$. ~~Thus~~ Thus

$$\{ z \in \mathbb{Z} \mid \exists a \in A : (z,a) \in \mathcal{P} \}$$

$$= \{ z \in \mathbb{Z} \mid (z, 0_A) \in \mathcal{P} \}$$

and it is an ideal of $\mathbb{Z}$, so of form

$m\mathbb{Z}$. $m \in \mathbb{N}_0$.

So $\mathcal{P} = (m\mathbb{Z}) \times A$

Note: $m \neq 1$, because $(1,0) \notin \mathcal{P}$.

$$\mathbb{Z} \times A / m\mathbb{Z} \times A \xrightarrow{(z,a) \longmapsto z} \mathbb{Z}/m\mathbb{Z} \text{ is a ring}$$

isomorphism. $\mathcal{P}$ prime $\Rightarrow$ The factor rings

are integral domains. So $m\mathbb{Z}$ is prime

So $m = 0$ or m is a prime.

Take a finite generating set for A. $= (a_1, \dots, a_\ell)$

Then $\mathcal{P} = m\mathbb{Z} \times A = ((0,a_1), \dots, (0,a_\ell), (m,0))$

(infact already as a group.) $\mathbb{Z} \times A$

Cohen $\Rightarrow$ $\mathbb{Z}_A$ is noetherian. $\square$

II.6. UFD's 'unique factorization domains'

We want to generalize the concept of prime factorization to wider class of rings. Let R be an integral domain.

Def. 87: Let $c \in R \setminus R^\times$ ($R \setminus (R^\times \cup \{0\})$). We call c

(a) irreducible, if $\forall a, b \in R$:
$(ab = c \Rightarrow a \in R^\times$ or $b \in R^\times)$

(b) a prime element, if $\forall a, b \in R$
$(c \mid ab$; ~~i.e. if~~ $\Rightarrow c \mid a$ or $c \mid b)$

[Def: $c, d \in R$. We write $c \mid d$, say "c divides d", if $\exists\, b \in R$: $cb = d$.]

Remark 88: Prime elements are irreducible.

Proof: Let $c \in R$ be a prime element, $a, b \in R$ s.t. $ab = c \Rightarrow c \mid ab \overset{c \text{ prime el}}{\Rightarrow} c \mid a$ or $c \mid b$

$\Rightarrow \exists\, d \in R$: w.l.o.g. $cd = a$

$\Rightarrow c(1 - db) = 0 \overset{c \neq 0,\ R \text{ integral domain}}{\Rightarrow} 1 - db = 0$ $\square$

$\Rightarrow b, d \in R^\times$

<u>Prop 89:</u> Suppose R is noetherian. Then every element of $R \setminus (\{0\} \cup R^\times)$ is a product of irreducible elements.

<u>Proof:</u> Take $a \in R \setminus (\{0\} \cup R^\times)$ a product of irreducible elts. Set $a_1 := a$

Assume that a is not irreducible.

$\Rightarrow \exists\, a_2, b_2 \in R \setminus R^\times$: $a_1 = a_2 b_2$ s.t. a_2 is not a product of irreducible elts.

$\Rightarrow$ ... We get $a_1, a_2, a_3, \ldots$ not prod. of irr. elts. and $b_2, b_3, b_4, \ldots$ all $\in R \setminus R^\times$

s.t. $a_i = a_{i+1} b_{i+1}$

Then we have for $\mathfrak{a}_i := (a_i)$

$\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \mathfrak{a}_3 \subseteq \ldots \qquad \mathfrak{a}_i \subseteq \mathfrak{a}_{i+1} \; \forall i \in \mathbb{N}.$

R is noetherian $\Rightarrow \exists_k \forall i \in \mathbb{N}$: $\mathfrak{a}_k = \mathfrak{a}_{k+i}$,

in particular $a_{k+1} \in (a_k)_R$, i.e. $\exists\, b \in R : a_{k+1} = b a_k$

$\Rightarrow a_{k+1} = b(a_{k+1} b_{k+1}) \underset{a_{k+1} \neq 0}{\Rightarrow} 1 = b\, b_{k+1}$

$\Rightarrow b_{k+1} \in R^\times$ ↯ $\square$

<u>Ex:</u> $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z} + \mathbb{Z}\sqrt{-5} + \mathbb{Z}\sqrt{-5}^2 + \dots$

$$= \mathbb{Z} + \mathbb{Z}\sqrt{5}$$

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

<u>Claim:</u> $2, 3, (1+\sqrt{-5}), (1-\sqrt{-5})$ are irreducible

<u>Proof:</u> Consider the norm map.

$$N : \mathbb{Z}[\sqrt{-5}] \longrightarrow \mathbb{Z}$$

$$N(a+b\sqrt{-5}) := a^2 + 5b^2 = (a+b\sqrt{-5})(a-b\sqrt{-5})$$

N is multiplicative:

$$N(\alpha\beta) = N(\alpha)N(\beta) \quad \forall \alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$$

$\alpha = a + b\sqrt{-5}$, $\beta = c + d\sqrt{-5}$.

$$N(\alpha\beta) = (ac - 5bd)^2 + 5(ad+bc)^2 = (*)$$

$$N(\alpha)N(\beta) = (a^2+5b^2)(c^2+5d^2)$$

$$= (ac)^2 + 25b^2d^2 + 5(a^2d^2 + (bc)^2) = (*)$$

<u>2 is irreducible:</u> $2 = \alpha\beta \implies 4 = N(\alpha)N(\beta)$

$$\implies N(\alpha), N(\beta) \in \{1, 2, 4\}$$

If $N(\alpha) = a^2 + 5b^2 = 2$ then $2 \equiv a^2 \mod 5$ ↯

So $N(\alpha) = 1$ or $N(\beta) = 1$.

So $\alpha \in \mathbb{Z}[\sqrt{5}]^\times$ or $\beta \in \mathbb{Z}[\sqrt{5}]^\times$.

<u>3 is irr.:</u> Similar

<u>$1 \pm \sqrt{5}$ is irr.:</u> exercise.

In particular the ~~decompos~~ expression as a product of irreducible elts is ind unique up to $R^\times$.

<u>Prop 90:</u> Suppose $\alpha \in R \setminus \{0\}$ has expressions

$$\varepsilon \alpha = c_1 \cdot \ldots \cdot c_\ell = d_1 \cdot \ldots \cdot d_s$$

into irreducible elements $c_1, \ldots, c_\ell, d_1, \ldots, d_s$, and $\varepsilon \in R^\times$, and suppose that $c_1, \ldots, c_\ell$ are prime.

Then $\ell = s = 0$ or ($\ell + s > 0$ and) $\exists\, \varphi \in \mathrm{Bij}(\mathbb{N}^{\leq \ell}, \mathbb{N}^{\leq k})$ s.t.

$$\exists\, \varepsilon_i \in R^\times \; i = 1, \ldots, \ell : \forall_{i \in \mathbb{N}^{\leq \ell}} : c_{\varphi(i)} = \varepsilon_i d_i)$$

<u>Proof:</u> (induction on $\ell + s$)

<u>$\ell + s = 0$:</u> The statement is empty.

<u>$\ell + s = 1$:</u> Say $\ell = 0$ and $s = 1$. Then

$$\varepsilon \alpha = 1 = d_1 \Rightarrow d_1 \in R^\times \lightning$$

$\underline{\ell + s > 1}$: $\ell = 0$ is not possible because then $d_1 \in R^\times$ ↯. Analogously $s > 0$.

$c_1 \mid d_1 \cdots d_s \Rightarrow \exists\, j \in \mathbb{N}^{\leq s}:\ c_1 \mid d_j$

$\Rightarrow a \in R:\ a c_1 = d_j$

$\underset{\substack{\uparrow \\ d_j \text{ irred.}}}{\Rightarrow}$ $a \in R^\times$, $c_1 \notin R^\times$

So we get for $\beta := d_1 \cdots \hat{d_j} \cdots d_s$

$a\beta = c_2 \cdots c_\ell = a d_1 \cdots \hat{d_j} \cdots d_s$

(IH) $\Rightarrow$ □

~~Def 91: R is called a factoriall factorial ring if R is noetherian and every irreducible element is a prime element.~~
(UFD)

~~Ex: 1) The ring $\mathbb{Z}[\sqrt{5}]$ is not factorial~~

~~2) $F[X]$, F a field is factorial~~

~~Theorem 92: The following assertions are equivalent:~~

~~1° R is factorial~~

~~2° $\forall a \in R \setminus R^\times\ \exists\, \ell \in \mathbb{N}\ \exists\, c_1, \dots, c_\ell \in R$ prime elements $a = c_1 \cdots c_\ell$~~

<u>Def 91:</u> R is called a factorial ring or a unique factorization domain (UFD) if every element of $R \setminus R^\times$ can be written as a product of prime elements.

<u>Ex:</u> 1) $\mathbb{Z}[\sqrt{5}]$ is not a UFD by Prop. 90.

2) F a field. Then $F[X]$ is a UFD.

<u>Proof:</u> $F[X]$ noetherian ~~So~~ by HBT

So we only need to show that all irr. elements are prime and apply Prop. 89.

$P(X) \in F[X] \setminus F^\times$ irreducible.

~~Say $P \mid QS$. If $P \mid Q$ and $P \nmid S$~~

~~then $\exists A, B, C, D \in F[X]$~~

~~$AP + BQ = 1 = CP + DS$.~~

~~(because we have the Euclidian algorithm here)~~

let $\mathfrak{m} \supseteq (P)$ be a maximal ideal.

$\mathfrak{m}$ is principal by Prop. 76 (5). Say

$\mathfrak{m} = (Q)$. $\Rightarrow$ $\mathfrak{m}$ is prime ideal

$\Rightarrow$ Q is a prime element, because $Q \neq 0$.

~~Now~~ Now $P \in (Q)_{F[X]} \Rightarrow \exists S \in F[X] : SQ = P$

$\Rightarrow$ $S \in R^\times$, because P is irreducible.

$\Rightarrow$ P is a prime element, as Q. $\square$

<u>Theorem 92:</u> T. f. a. a. e:

1° R is a UFD

2° (a) $\forall a \in R \setminus (R^\times \cup \{0\})$ a is a product of ired. elements

and

(b) All ired. elements are prime elts.

~~3° $\forall a \in R \setminus R^\times$ a is a product of prime elements.~~

<u>Proof:</u> 1° $\Rightarrow$ 2° (b) $a \in R \setminus (R^\times \cup \{0\})$ irr. $\Rightarrow a = p_1 \cdots p_l$

p_j prime element. If $l > 1$ then ~~$\exists$~~ $\exists j \leq l$:

$p_1 \in R^\times$ or $p_2 \cdots p_l \in R^\times$. $\Rightarrow \exists j \in \mathbb{N}^{\leq l}$: $p_j \in R^\times$. $\lightning$

~~By induction~~

$\square$

Ex: 1) We will see that $\mathbb{Z}[i]$ is a UFD.
(We postpone this to the next paragraph.)
So, in particular, irreducible elements are prime elements.
We want to find all prime elements of $\mathbb{Z}[i]$. As irred = prime here, we only have to consider the irreducibility property. Consider $N: \mathbb{Z}[i] \to \mathbb{Z}$ $N(\alpha) := \alpha\bar{\alpha}$.

Let $\alpha = a+ib \in \mathbb{Z}[i]$ be irreducible

~~Fact~~ Claim: α is irreducible $\Leftrightarrow$
($N(\alpha)$ is a prime number or
$N(\alpha) = p^2$, p a prime number $\equiv_4 3$)

Proof: "$\Leftarrow$" If $N(\alpha) = p$ a prime number then, if $\alpha = \beta\gamma$, we get $N(\beta)N(\gamma) = p$ so $N(\beta) = 1$ or $N(\gamma) = 1$, so $\beta \in \mathbb{Z}[i]^\times$ or $\gamma \in \mathbb{Z}[i]^\times$.

If $N(\alpha) = p^2$ for a prime number $\equiv_4 3$. Then from $\alpha = \beta\gamma$:
Assume $\beta, \gamma \notin \mathbb{Z}[i]^\times$.
$\Rightarrow N(\beta) = N(\gamma) = p$.
$\beta = c + id \Rightarrow N(\beta) = c^2 + d^2 = p \equiv_4 3$ ↯

"$\Rightarrow$" $N(\alpha) > 1$, because $\alpha \notin \mathbb{Z}[i]^\times \subset \{0\}$
Take $p \in \mathbb{N}^{>1}$ a prime number s.t.
$p \mid N(\alpha) = \alpha\bar{\alpha}$.

$$\text{"}\Leftarrow\text{"}$$

<u>Case 1:</u> $p \equiv_4 3 \Rightarrow p$ is a prime element. $\Rightarrow p \mid \alpha$ or $p \mid \bar{\alpha}$

$\Rightarrow p\varepsilon = \alpha$ or $p\varepsilon = \bar{\alpha}$ for some $\varepsilon \in \mathbb{Z}[i]^\times$, and so $N(\alpha) = p^2$.

<u>Case 2:</u> $p \equiv_4 1$.

<u>Fact:</u> (homework) $\exists c, d \in \mathbb{Z}: p = c^2 + d^2$

$\Rightarrow \beta = c + id$ satisfies:

$$\beta \mid \beta\bar{\beta} = p \mid N(\alpha) = \alpha\bar{\alpha}$$

β is a prime element $\Rightarrow \beta \mid \alpha$ or $\beta \mid \bar{\alpha}$.

$\Rightarrow N(\beta) = N(\alpha) = p$ because α and $\bar{\alpha}$ are irreducible.

$\square$

<u>Ex:</u> $\mathbb{Z}[i]^\times = \{a + ib \mid a^2 + b^2 = 1,\ a, b \in \mathbb{Z}\}$
$= \{\pm 1, \pm i\}$.

$\pm 7, \pm i7$ are the prime elements with Norm 49.

$\pm 1 \pm i4$; $\pm 4 \pm i$ are the prime elements with norm 17.

2) Consider $P(X) = X^4 - 2$ in $\mathbb{C}[X]$, $\mathbb{R}[X]$ and $\mathbb{Q}[X]$

	prim factorization	ring
I	X^4-2	$\mathbb{Q}[X]$
II	$(X^2+\sqrt{2})(X-\sqrt[4]{2})(X+\sqrt[4]{2})$	$\mathbb{R}[X]$
III	$(X+i\sqrt[4]{2})(X-i\sqrt[4]{2})(X-\sqrt[4]{2})\cdot(X+\sqrt[4]{2})$	$\mathbb{C}[X]$

Note $\mathbb{Q}[X]$, $\mathbb{R}[X]$ and $\mathbb{C}[X]$ are UFD's.

For example: X^4-2 is irreducible in $\mathbb{Q}[X]$.

<u>Proof</u>: • If F is a field, $a \in F$, then

$X-a$ is irreducible in $F[X]$:

$X-a = Q\cdot R \qquad Q, R \in F[X]$

$\Rightarrow \quad 1 = \underbrace{\deg(Q)}_{\geq 0} + \underbrace{\deg(R)}_{\geq 0}$

$\Rightarrow \quad \deg(Q) = 0$ or $\deg(R) = 0$

$\Rightarrow \quad Q \in F[X]^\times$ or $R \in F[X]^\times$.

• The factors in III are prime elements in $\mathbb{C}[X]$.

So a monic divisor of X^4-2 of degree 1, 2 or 3 is a product of those factors.

$\Rightarrow$ It's absolute term satisfies

$|t| \in \{\sqrt{2}, \sqrt[4]{2}, \sqrt[4]{8}\}$

They are all not rational. $\lightning$

(If one of them is rational then $\sqrt[4]{2}$ or $\sqrt[4]{8} = \frac{2}{\sqrt[4]{2}} \in \mathbb{Q}$ then $\sqrt{2} \in \mathbb{Q}$ $\lightning$)

$$\Rightarrow \left(X^4-2 = SR \quad , S, R \in \mathbb{Q}[X] \right.$$

implies $\deg(S) = 0$ or $\deg(R) = 0$,

i.e. S or $R \in \mathbb{Q}^\times$ $\Big)$

$\Rightarrow$ X^4-2 is irreducible.

Analogously for the other polynomials.

<u>Theorem 93:</u> Let A be a UFD. Then $A[X]$ is a UFD.

~~Proof~~

Before we start the proof we need to introduce gcd and lcm.

<u>Def 94:</u> Let A be a UFD and $t \neq 0$, $a_1, \dots, a_\ell \in A$ (at least one $a_i \neq 0$)

1) We call t a g.c.d. of $a_1, \dots, a_\ell$, denoted by $t \in \gcd(a_1, \dots, a_\ell)$ if $\forall s \in A \setminus \{0\}$: $\left(s \mid a_1 \text{ and } s \mid a_2 \dots \text{ and } s \mid a_\ell \iff s \mid t \right)$.

2) We call t a lowest common multiple of $a_1, \dots, a_\ell$ (assuming all a_i non-zero) if $\forall s \in A \setminus \{0\}$: $\left(a_1 \mid s \wedge a_2 \mid s \wedge \dots \wedge a_\ell \mid s \iff t \mid s \right)$

We denote it by $t \in \operatorname{lcm}(a_1, \dots, a_\ell)$

3) $a, b \in A$ are called <u>associates</u> if $\exists\, u \in A^\times : \; a = ub$.

<u>Remark:</u> "Being associates" is an equivalence relation.

<u>Pf:</u> $\cdot \; a = 1 \cdot a$.
$\cdot \; a = {}_A u b \Rightarrow u^{-1} a = b$.
$\cdot \; a = ub \;\wedge\; b = vc \qquad u, v \in A^\times$
$\Rightarrow \; a = (uv)\, c \qquad uv \in A^\times$ $\square$

<u>Proposition 95:</u> Let A be a UFD, $a, b \in A \setminus \{0\}$, $p_1, \dots, p_\ell$ pairwise not associate prime elements, and let

$$a = \varepsilon\, p_1^{\nu_1} \cdots p_\ell^{\nu_\ell} \quad \text{and}$$
$$b = \varepsilon'\, p_1^{w_1} \cdots p_\ell^{w_\ell}$$

be prime factorizations of a and b.
$(\varepsilon, \varepsilon' \in A^\times, \nu_1, \dots, \nu_\ell, w_1, \dots, w_\ell \in \mathbb{N}_0)$

Then a) $c := p_1^{\min(\nu_1, w_1)} \cdots p_\ell^{\min(\nu_\ell, w_\ell)}$
is a gcd of a and b.

b) $d := p_1^{\max(\nu_1, w_1)} \cdots p_\ell^{\max(\nu_\ell, w_\ell)}$
is a lcm of a and b.

<u>Proof:</u> a) $\cdot \; c \mid a$ and $c \mid b$ ✓
$\cdot$ Let $s \in A \setminus \{0\}$ s.t. $s \mid a$ and $s \mid b$.
If $a \in A^\times$ or $b \in A^\times$ then $s \in A^\times$ so $s \mid c$.

<u>Else:</u> Suppose $a, b \in A \setminus (A^\times \cup \{0\})$ and $s \notin A^\times \cup \{0\}$.

Let $s = \varepsilon' q_1^{\alpha_1} \cdots q_k^{\alpha_k}$ be a prime factorization of s s.t. q_i not assoc. to q_j for $i \neq j$ and $\alpha_i > 0$ for all i.

$q_1 \mid a \Rightarrow \exists\, t \in \{1, \dots, \ell\}$: q_1 assoc. to p_t

So w.l.o.g. we have

$q_1 = p_1 \wedge \dots \wedge q_k = p_k \wedge k \leq \ell$.

Thus $p_1^{\alpha_1} \cdots p_k^{\alpha_k} \mid p_1^{\nu_1} \cdots p_\ell^{\nu_\ell}$

and $p_1^{\alpha_1} \cdots p_k^{\alpha_k} \mid p_1^{w_1} \cdots p_\ell^{w_\ell}$.

<u>Claim:</u> $\alpha_i \leq \min(\nu_i, w_i) \quad \forall i = 1, \dots, k$

<u>Pf:</u> If $\alpha_{i_0} > \min(\nu_{i_0}, w_{i_0}) = \nu_{i_0}$ then

$$p_{i_0} \mid p_1^{\nu_1} \cdots \widehat{p_{i_0}^{\nu_{i_0}}} \cdots p_\ell^{\nu_\ell},$$

So $p_{i_0} \mid p_j$ for some $j \neq i_0$ ↯

because p_{i_0} is not associate to p_j. ∎

Claim $\Rightarrow$ $s \mid c$.

b) Similar argument. □

<u>Lemma 96:</u> Let A be a UFD and p be a prime element of A. Then p is a — " — of $A[X]$.

<u>Proof:</u> $p \mid QR$ $\quad Q, R \in A[X]$.

Assume $p \nmid Q$ and $p \nmid R$

$$Q = \sum_{i=0}^{d_Q} a_i X^i \qquad R = \sum_{i=0}^{d_R} b_i X^i$$

$$i_0 := \max\{i \in \mathbb{N}_0^{d_Q} \mid p \nmid a_i\}$$

$$j_0 := \max\{j \in \mathbb{N}_0^{d_R} \mid p \nmid b_j\}$$

$\Rightarrow$ p does not divide the coefficient of QR for degree $i_0 + j_0$. $\lightning$ $\square$

<u>Lemma 97:</u> A a UFD. Every element of $A[X] \setminus (A^\times \cup \{0\})$ is a product of irreducible elements.

<u>Proof:</u> (induction on the degree)

Let $P \in A[X] \setminus (A^\times \cup \{0\})$.

A is a UFD, so lemma 96 implies the assertion if $\deg(P) = 0$.

<u>Base case:</u> $\deg(P) = 1$.

$$P = aX + b = c\,(eX + d) = c \cdot Q$$

with $c \in \gcd(a, b)$.

c has a prime factorization because A is a UFD and lemma 96.

<u>Claim:</u> Q is irreducible.

<u>Proof:</u> $Q = RS \Rightarrow \deg R = 0$ or $\deg S = 0$.

$R \in A^\times$ or $S \in A \setminus \{0\}$

~~The coefficients of R are coprime and~~

1_A is a gcd of the coefficients of R

and also a " " " " S.

So $R \in A^\times$ or $S \in A^\times = A[X]^\times$.

$\square$

<u>induction step $\deg(P) > 1$:</u>

Let c be a gcd of the coefficients of P. Then $P = c\,Q$

for $Q \in A[X]$ s.t. the coefficients of Q are coprime.

c has a prime factorization.

If Q is irreducible then ✓

Otherwise $Q = Q_1 Q_2$ with $Q_1, Q_2 \notin A^\times$.

In fact $Q_1, Q_2 \notin A$ because otherwise the coeff of Q wouldn't be coprime.

$\Rightarrow \deg(Q_i) \geq 1$ and

$\deg(Q_i) < \deg(Q)$

(IH) $\Rightarrow$ $\square$

<u>Lemma 98:</u> Let A be a UFD,

and $P \in A[X] \setminus (A^\times \cup \{0\})$. A

T.a.e.:

1° P is irreducible in $A[X]$

2° ~~The~~ 1_A is a g.c.d of the coeff. of P and

P is irreducible in $Q(A)[X]$.

<u>Proof:</u> $1° \Rightarrow 2°$ Note: $\deg(P) \geq 1$, because $P \notin A$.

1_A is ~~the~~ a g.c.d of the coeff of P, because otherwise an element of $A \setminus (A^\times \cup \{0\})$ would divide P.

<u>To show:</u> P is irreducible in $Q(A)[X]$.

$P = R \cdot S$, $R, S \in Q(A)[X]$.

$R = \frac{1}{d_R} \tilde{R}$ and $S = \frac{1}{d_S} \tilde{S}$ with

$\tilde{R}, \tilde{S} \in A[X]$.

Further $\tilde{R} = r_0 R_0$ and $\tilde{S} = s_0 S_0$, where r_0 is a g.c.d of the coeff of $\tilde{R}$, s_0 $\tilde{S}$.

$\Rightarrow d_R d_S P = r_0 R_0 s_0 S_0 = r_0 s_0 R_0 S_0$

$p \mid d_R$ a prime element of A $\Rightarrow p \mid r_0$ or $p \mid s_0$

because the coeff. of $R_0 S_0$ are coprime.

Taking a prime factorization of $d_R d_S$ and cancelling out all primes gives

$$P = r_1 s_1 R_0 S_0 \qquad r_1 | r_0 \,,\, s_1 | s_0$$

$$\Rightarrow \quad r_1 R_0 \in A^\times \quad \text{or} \quad s_1 S_0 \in A^\times.$$

$$\Rightarrow \quad R \in Q(A)^\times \quad \text{or} \quad S \in Q(A)^\times$$

<u>$2^\circ \Rightarrow 1^\circ$:</u> ~~Suppose~~

$$P = S R \quad \text{in} \quad A[X].$$

$$\overset{2^\circ}{\Rightarrow} \quad S \in Q(A)^\times \quad \text{or} \quad R \in Q(A)^\times$$

W.l.o.g. $S \in Q(A)^\times$

$$\Rightarrow \quad S \in Q(A)^\times \cap A[X] = A \setminus \{0\}$$

If $S \in A \setminus (A^\times \cup \{0\})$ then the coeff of P would not be coprime.

So $S \in A^\times$. $\square$

<u>Proof of Theorem 93:</u> By Lemma 97 we only need to show that every irreducible element of $A[X]$ is a prime element.

Take an irreducible element $P \in A[X]$.

If $\deg(P) = 0$ then $P \in A \setminus (A^\times \cup \{0\})$ and also P is an irreducible element of A.
(exercise)

Thus p_n is a prime element of A

$\overset{96}{\Longrightarrow}$ P is a prime element of $A[X]$.

Suppose $\deg(P) > 0$, i.e. $P \notin A$.

Let $R, S \in A[X]$ s.t. $P \mid RS$ in $A[X]$

$\Longrightarrow$ $P \mid RS$ in $Q(A)[X]$.

Lemma 98 $\Longrightarrow$ P is irreducible in $Q(A)[X]$

$\Longrightarrow$ P is a prime element in $Q(A)[X]$.

$Q(A)[X]$ is UFD

$\Longrightarrow$ $P \mid R$ or $P \mid S$, w.l.o.g. $P \mid R$ (in $Q(A)[X]$),

i.e. $\exists\, T \in Q(A)[X]$: $TP = R$

$T = \frac{t_0}{d_T} T_0$ s.t. 1_A is a gcd of the coeff of $T_0 \in A[X]$ and $t_0 \in A$ & $d_T \in A$.

$\Longrightarrow$ $d_T R = t_0 T_0 P$

Cancellation (1_R is g.c.d of coeff of R)

$\Longrightarrow$ $t_0 \mid d_T$ in A

Analogously $d_T \mid t_0$ in A

$\Longrightarrow$ $\exists\, \varepsilon \in A^\times$: $t_0 = \varepsilon d_T$

$\Longrightarrow$ $R = \underbrace{\varepsilon T_0}_{\in A[X]} P$ $\square$