Recap: Groups, generators, subgroup, normal subgroup, factor group, homomorphism, isomorphism, hom. theorem

Rings

$\boxed{\text{Definition:}}$ A set with two operations, $(R,+,\cdot)$, is called a "ring" if

a.) $(R,+)$ a commutative group, (e is usually written as 0

b.) $a(bc) = (ab)c$ for $a,b,c \in R$ (associative law)

c.) $a(b+c) = ab + ac$, $(b+c)a = ba + ca$, for $a,b,c \in R$ (distributivity law)

R is called "commutative" if

d.) $ab = ba$ for $a,b \in R$

R is called "ring with identity" if a neutral element "1" for "$\cdot$" exists:

e.) $a \cdot 1 = 1 \cdot a = a$ for $a \in R$

Definition: A ring $(R,+,\cdot)$ is called a "field" if $(R\setminus\{0\},\cdot)$ is a commutative group, i.e. R is commutative and all $a \neq 0$ have a multiplicative inverse.

Examples:

		comm	identity	field
- $(\mathbb{Z},+,\cdot)$	$\checkmark$	$\checkmark$	$\checkmark$	$\lightning$
- $(\mathbb{Q},+,\cdot)$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$
- $(\mathbb{C}[x],+,\cdot)$	$\checkmark$	$\checkmark$	$\checkmark$	$\lightning$
- $(\mathbb{R}^{n\times n},+,\cdot)$	$\checkmark$	$\lightning$	$\checkmark$	$\lightning$
- $(GL_n(\mathbb{C}),+,\cdot)$	$\lightning$			
- $(\mathbb{C}(x),+,\cdot)$	$\checkmark$	$\checkmark$	$\checkmark$	$\checkmark$

$\mathbb{C}(x) = \{ \frac{p(x)}{q(x)} \mid p,q \in \mathbb{C}[x] \}$

$\boxed{\text{Generators}}$

- $\langle 1 \rangle_{ring} = \langle 1 \rangle_{group} = \mathbb{Z}$

- $\langle x \rangle_{ring} = \mathbb{Z}[x] \neq \langle x \rangle_{group}$

Ideals

- $(R,+,\cdot)$ a ring. $S \subseteq R$ is a "subring" if $(S,+,\cdot)$ is a ring.
- R/S a ring? $\quad [x]+[y]=[x+y] \quad$ (or: $x+S+y+S = x+y+S$)

$(x \sim y \Leftrightarrow x-y \in S) \quad [x][y]=[xy] \quad$ (or: $(x+S)(y+S) = xy+S$)

"+" is well-defined since $(S,+) \trianglelefteq (R,+)$

"$\cdot$" ? assume $a \sim x$, $b \sim y$

$$\Rightarrow a = x+s,\ b = y+t,\quad s,t \in S$$

$$\Rightarrow ab = (x+s)(y+t) = xy + \underbrace{sy}_{\in SR} + \underbrace{xt}_{\in RS} + \underbrace{st}_{\in S} \overset{?}{\in} xy+S$$

<u>Definition:</u> $I \subseteq R$ is called a "left ideal" if

a.) $(I,+) \leq (R,+)$ (necessarily normal)

b.) $RI \subseteq I$ (means: for all $r \in R$, $x \in I$: $rx \in I$)

"right ideal" if

b.) $IR \subseteq I$

"two-sided ideal" if

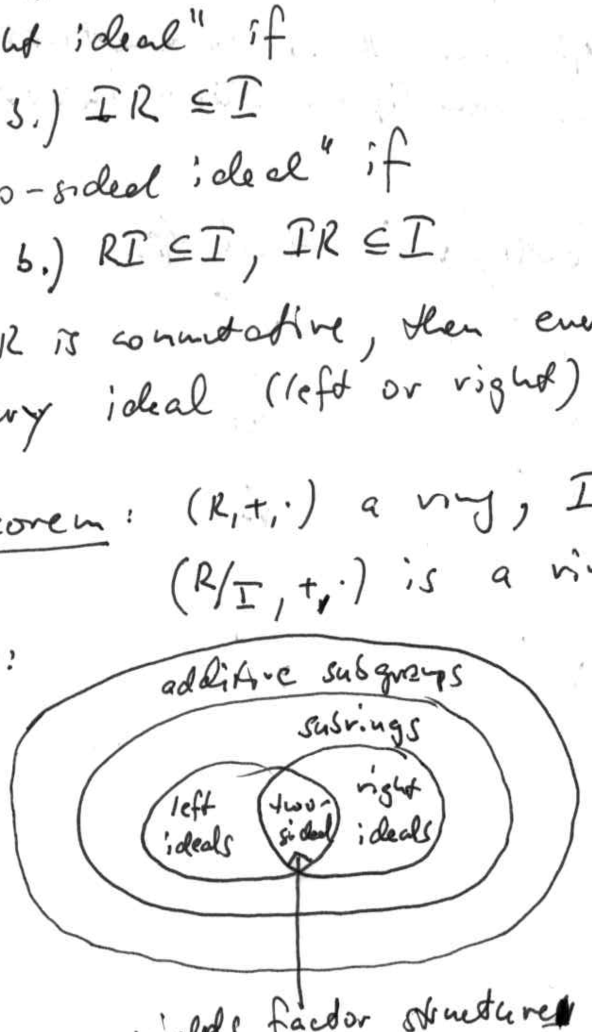
b.) $RI \subseteq I$, $IR \subseteq I$ $\quad$ we write $I \trianglelefteq R$

If R is commutative, then every ideal is two-sided.

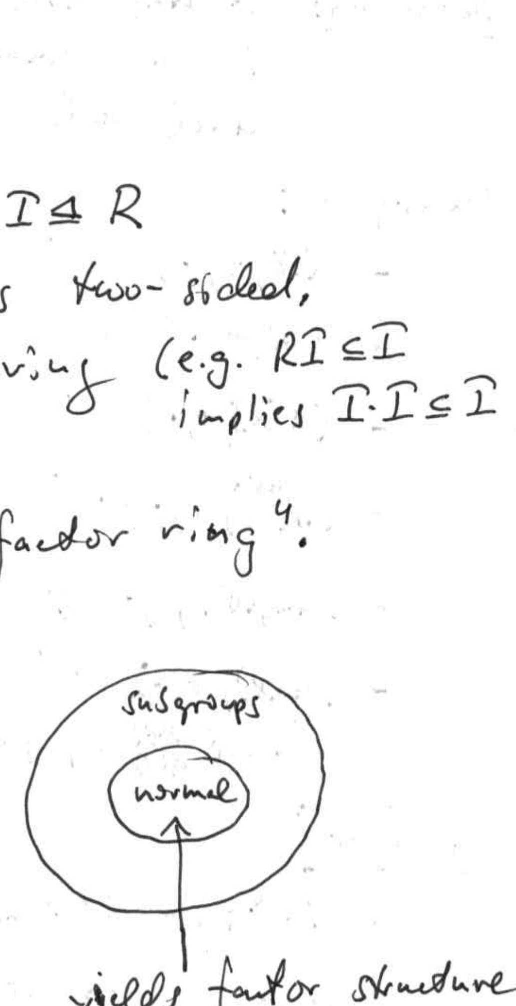
Every ideal (left or right) is a subring (e.g. $RI \subseteq I$ implies $I \cdot I \subseteq I$).

<u>Theorem:</u> $(R,+,\cdot)$ a ring, $I \trianglelefteq R$. Then $(R/I,+,\cdot)$ is a ring called "factor ring".

rings:



groups:



$$\boxed{R/I \text{ a ring} \Leftrightarrow I \trianglelefteq R}$$

Examples:

- $R = (\mathbb{Z}, +, \cdot)$

  additive subgroups: $n\mathbb{Z}$, $n \in \mathbb{N}$

  ideal? $r \in \mathbb{Z}$, $nx \in n\mathbb{Z} \Rightarrow rnx = n \cdot rx \in n\mathbb{Z}$ ✓

  $\Rightarrow (\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ commutative ring

- $R = (\mathbb{C}[x], +, \cdot)$, find ideals I

  $p(x) \in I \Rightarrow p(x)\,\mathbb{C}[x] \subseteq I$ and $p(x)\,\mathbb{C}[x]$ is indeed an ideal

  - add. subgroup ✓
  - $r(x) \in \mathbb{C}[x] \Rightarrow r(x)\,p(x)\,\mathbb{C}[x] = p(x)\,r(x)\,\mathbb{C}[x] \subseteq p(x)\,\mathbb{C}[x]$ ✓

  factor ring:

  $$\mathbb{C}[x] / p(x)\,\mathbb{C}[x] = \mathbb{C}[x] / p(x) \quad \text{(simpler notation)}$$

- $R = (\mathbb{C}^{n \times n}, +, \cdot)$, $I = \{ n \times n \text{ diagonal matrices} \} \leq R$

  I subring but not an ideal.

<u>Lemma:</u> a.) the sum of finitely many ideals is an ideal

b.) the intersection of any number of ideals is an ideal

<u>ideal generators</u> R a ring (with identity), $d \in R$

$\Rightarrow \langle d \rangle_{\text{left ideal}} = Rd$ is called "principal ideal"

Similarly, $d_1, \dots, d_k \in R$

$\Rightarrow \langle d_1, \dots, d_k \rangle_{\text{left ideal}} = Rd_1 + \dots + Rd_k$

<u>note:</u> I an ideal of R, $1 \in I \Rightarrow I = R$

~~A ring in which every ideal is a principal ideal is called "principal ideal domain (PID)".~~

homomorphism

Definition: A ring homomorphism is a mapping $\varphi: R \to S$ (R, S are rings) such that

a.) $\varphi(a+b) = \varphi(a) + \varphi(b)$ for $a, b \in R$

b.) $\varphi(a \cdot b) = \varphi(a)\varphi(b)$ "

Further, $\ker\varphi = \{a \in R \mid \varphi(a) = 0\}$ is called the "Kernel of φ."

Lemma: a) $\ker\varphi \trianglelefteq R$. b.) Conversely, if $I \trianglelefteq R$, ~~then~~ and

$$\varphi: R \to R/I, \quad a \mapsto a + I$$

then $\ker\varphi = I$

$$\boxed{\text{two-sided ideals} \iff \text{kernels of ring homomorphisms}}$$

Proof: a) - $\ker\varphi$ subgroup ✓ (as kernel of a group hom.)

- $a \in R$, $x \in \ker\varphi \Rightarrow \varphi(ax) = \varphi(a)\varphi(x) = \varphi(a)\cdot 0 = 0$

$\Rightarrow ax \in \ker\varphi$ ✓

similarly $xa \in \ker\varphi$ ✓

b.) omitted

Theorem: $\varphi: R \to S$ ring hom. Then

$$R/\ker\varphi \cong \varphi(R)$$

proof: Define $\overline{\varphi}: R/\ker\varphi \to \varphi(S)$, $[a] \mapsto \varphi(a)$

- $\overline{\varphi}$ is hom. ✓ (check def.)
- $\overline{\varphi}$ surjective ✓ (from its definition obvious)
- $\overline{\varphi}$ injective:

$\overline{\varphi}(a + \ker\varphi) = \overline{\varphi}(b + \ker\varphi) \iff \varphi(a) = \varphi(b)$

$\iff \varphi(a-b) = 0 \iff a - b \in \ker\varphi \iff a + \ker\varphi = b + \ker\varphi$ ✓

groups G	rings R	
group generators	ring generators	
subgroups H	ideals I	– ideal generators
group hom's	ring hom's	
normal subgroups	two-sided ideals	← kernels of hom's
factor groups	factor rings	– yield factor structures
$G/\ker\varphi \cong \varphi(G)$	$R/\ker\varphi \cong \varphi(R)$	