Recap: rings, ideals, homs, hom. theorem

Some additions

Lemma: A group (ring) hom. φ is injective if and only if $\ker\varphi$ is trivial, i.e., $\ker\varphi = \{e\}$ ($\ker\varphi = \{0\}$).

proof: „$\Rightarrow$"
φ injective and let $x \in \ker\varphi \Rightarrow \varphi(x) = \varphi(0) \Rightarrow x = 0$

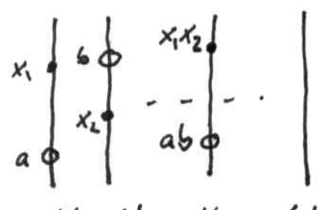
„$\Leftarrow$" $\ker\varphi = \{0\}$. Let $x \neq y \Rightarrow x-y \neq 0 \Rightarrow x-y \notin \ker\varphi$
$\Rightarrow \varphi(x-y) \neq 0 \Rightarrow \varphi(x) \neq \varphi(y)$

Visualization of Factor Structures

$(G,\cdot)$ group, $H \leq G$, equ. rel. $x \sim y \Leftrightarrow x^{-1}y \in H \Leftrightarrow y \in xH$

equ. classes: xH

partition: $G = x_1H \cup \dots \cup x_nH$, $|G/H| = n$

G: 

$\underbrace{x_1H \; x_2H \cdots x_iH \cdots x_nH}_{G/H}$

- all the same size $|H|$
- partitions G
- arranges elements into an $|H| \times |G/H|$ array

well-defined: $x_1x_2 \in x_iH \Rightarrow ab \in x_iH$ for all $a \in x_1H$, $b \in x_2H$

$$\boxed{\begin{array}{l} \text{Operations on Sets (shorthands)} \\ A \circ B = \{a \circ b \mid a \in A, b \in B\}, \quad \circ = +, \cdot, \dots \\ x \circ A = \{x \circ a \mid a \in A\}, \quad \circ = +, \cdot, \dots \end{array}}$$

Example: $(G,\cdot) = (\mathbb{Z},+)$, $H = 3\mathbb{Z}$, equ. classes: $x + 3\mathbb{Z}$, $x \in \{0,1,2\}$

$$\mathbb{Z}: \quad \underbrace{\begin{array}{ccc} 0 & 1 & 2 \\ 3 & 4 & 5 \\ 6 & 7 & 8 \\ 9 & 10 & 11 \\ \vdots & \vdots & \vdots \\ [0] & [1] & [2] \\ \shortparallel & \shortparallel & \shortparallel \\ 0+3\mathbb{Z} & 1+3\mathbb{Z} & 2+3\mathbb{Z} \end{array}}_{\mathbb{Z}/3\mathbb{Z} = \{[0],[1],[2]\} = \{0,1,2\} \text{ with op. mod } 3}$$

Types of Rings $(R, +, \cdot)$ a ring with 1

About division

	$\mathbb{Z}$	$\mathbb{Z}/8\mathbb{Z}$
- if $c = ab$ we say $a \mid c$	$2 \mid 4$	$2 \mid 4$, $3 \mid 1$
- a^{-1} exists $\Leftrightarrow a \mid 1$	$1 \mid 1$, $-1 \mid 1$	$1,3,5,7 \mid 1$
- the set $R^\times = \{a \in R \mid a \mid 1\}$ is a multiplicative group (group of units)	$\mathbb{Z}^\times = \{1, -1\}$	$(\mathbb{Z}/8\mathbb{Z})^\times = \{1,3,5,7\}$

- we say $g = \gcd(a, b)$ if
  a.) $g \mid a$, $g \mid b$; b.) $h \mid a$, $h \mid b \Rightarrow h \mid g$.
  $g = 1$: a, b are "coprime"

  $\gcd(6, 9) = 3$
- g, g' gcds of a and b
  $\Rightarrow g = x g'$, $x \in R^\times$
  (and vice versa)

  $\gcd(6,9) = \begin{matrix} 3 \\ -3 \end{matrix}$
- $a, b \neq 0$ with $ab = 0$ are called "zero divisors"
  A zero divisor cannot have an inverse (i.e., $\notin R^\times$)

  $\mathbb{Z}$: not possible

  $\mathbb{Z}/8\mathbb{Z}$: $2 \cdot 4 = 8 = 0 \pmod 8$

Euclidean algorithm in $\mathbb{Z}$

gcd of 7 and 5

$$7 = 1 \cdot 5 + 2$$
$$5 = 2 \cdot 2 + 1 \quad \leftarrow \text{gcd}$$
$$2 = 2 \cdot 1 + 0$$

↑ get smaller ↖ eventually 0

back substitution:

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 \\ &= 5 - 2(7 - 1 \cdot 5) \\ &= 3 \cdot \underline{5} - 2 \cdot \underline{7} \end{aligned}$$

<u>Theorem</u> $a, b \in \mathbb{Z}$, $g = \gcd(a, b)$. Then exist $x, y \in \mathbb{Z}$ s.t.

$$g = xa + yb$$

The converse is true for $g = 1$, i.e.,

$$1 = \gcd(a, b) \iff \text{there are } x, y \in \mathbb{Z}: \ 1 = xa + by$$

proof: "$\Rightarrow$" $g = xa + yb$ follows from Euclidean algorithm

"$\Leftarrow$" $1 = xa + yb$. Let $g \mid a$, $g \mid b \Rightarrow g \mid xa + yb = 1$

applications:

a.) $a \in (\mathbb{Z}/8\mathbb{Z})^\times \iff$ exists $x \in \mathbb{Z}/8\mathbb{Z}$: $ax = 1 \pmod 8$

$\iff ax = 1 + 8k$

$\iff 1 = ax - 8k$

$\iff \gcd(a, 8) = 1$

More general: $(\mathbb{Z}/n\mathbb{Z})^\times = \{ i \mid \gcd(i,n)=1,\ 0 \le i < n \}$

implies $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{0\} \iff n = p$ prime

$\Rightarrow \mathbb{Z}/p\mathbb{Z}$ is a field

b.) Consider $\langle a, b \rangle_{ideal} = \mathbb{Z}a + \mathbb{Z}b \trianglelefteq \mathbb{Z}$

Let $g = \gcd(a,b)$. Claim: $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}g$

proof: „$\supseteq$" write $g = xa + yb \Rightarrow g \in \mathbb{Z}a + \mathbb{Z}b$

$\Rightarrow \mathbb{Z}g \subseteq \mathbb{Z}a + \mathbb{Z}b$

„$\subseteq$" ~~let~~ $xa + yb \in \mathbb{Z}a + \mathbb{Z}b$. $g \mid (xa+yb) \Rightarrow xa + yb = z \cdot g \in \mathbb{Z}g$

So: - every ideal in $\mathbb{Z}$ is a principal ideal

- a consequence of having the Euclidean algorithm

<u>Definitions:</u> Let R be a commutative ring with 1.

a.) R is called an "integral domain" if it has no zero divisors.

b.) An integral domain is called "principal ideal domain" if every ideal is a principal ideal.

c.) An integral domain is called "Euclidean ring" if it has a proper division with rest (so the Euclidean algorithm can be used) formally: there is a function $\delta: R \to \mathbb{N}_0$ s.t.

a.) $a, b \neq 0 \Rightarrow \delta(ab) \geq \delta(a)$

b.) for $a, b \in R$, $b \neq 0$ there exists $x, r \in R$ s.t.

$$a = xb + r \quad \text{and} \quad \delta(r) < \delta(b)$$

examples: $R = \mathbb{Z}$, $\delta = |\cdot|$

$R = \mathbb{R}[x]$, $\delta = \deg$ $\quad \left(\deg\left(\sum_{i=0}^{n} a_i x^i\right) = n\right)$

[often one defines $\delta(0) = -\infty$]

Summary