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

**Definition:** A set with two operations, \((R, +, \cdot)\), is called a ring. If

1. \((R, +)\) a commutative group, \(e\) is usually written as 1.
2. \(a(bc) = (ab)c\) for \(a, b, c \in R\) (associative law).
3. \(a(b + c) = ab + ac\), \((b + c)a = ba + ca\), for \(a, b, c \in R\) (distributivity law).

\(R\) is called commutative if

4. \(ab = ba\) for \(a, b \in R\).

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

5. \(a \cdot 1 = 1 \cdot a = a\) 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:**

- \((\mathbb{Z}, +\cdot)\) ✓ comm ✓ identity ✓ field ✓
- \((\mathbb{Q}, +\cdot)\) ✓ ✓ ✓ ✓
- \((\mathbb{C}, +\cdot)\) ✓ ✓ ✓ ✓
- \((\mathbb{R}, +\cdot)\) ✓ ✓ ✓ ✓
- \((\mathbb{R}^*, +\cdot)\) ✓ ✓ ✓
- \((\mathbb{C}, +\cdot)\) ✓ ✓ ✓
- \((\mathbb{R}_x, +\cdot)\) ✓ ✓ ✓
- \((\mathbb{C}_x, +\cdot)\) ✓ ✓ ✓

\[\mathbb{Z} = \{n + \frac{a}{b(x)} | a, b \in \mathbb{C}, b(x) \neq 0\}\]

**Generators**

- \(<1>_{\mathbb{R}} = <1>_{\text{group}} = \mathbb{Z}
- \(<x>_{\mathbb{R}} = \mathbb{Z}[x] \neq <x>_{\text{group}}\)
ideals

- $(R, +)$ a ring. $S \subseteq R$ is a "subring" if $(S, +)$ is a ring.
- $R/S$ a ring: $[xS + yS] = [x + y]S$ (or: $x + S + y + S = x + y + S$)
- $(xy \in S) \Rightarrow xS \subseteq S$
- $[x] + [y] = [x + y]$ (or: $(x + S)(y + S) = xy + S$

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

2. Assume $a, b \in S$

$\Rightarrow a + S, b + S, a + b \in S$

$\Rightarrow a + S = (a + S)(b + S) = xy + S$

Definition: $I \subseteq R$ is called a "left ideal" if
1. $(I, +) \leq (R, +)$ (necessarily normal)
2. $RI \subseteq I$ (means: for all $r \in R, x \in I$: $rx \in I$)

Claim: "right ideal" if
3. $IR \subseteq I$

"two-sided ideal" if
4. $RI \subseteq I, IR \subseteq I$

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 $I : I \subseteq I$).

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

Rings:
- additive subgroup
- subrings
- left ideals
- right ideals

Groups:
- normal subgroup
- yields factor structure

$R/I \trianglelefteq R \iff I \trianglelefteq R$
Examples:
- \( \mathbb{Z}_2 \) (\( \mathbb{Z}/2\mathbb{Z} \))
  - additive subgroup: \( \mathbb{Z}_2 \), \( n \in \mathbb{N} \)
  - ideal: \( r \in \mathbb{Z}_2, x \in \mathbb{Z}_2 \Rightarrow rx = n - rx \in \mathbb{Z}_2 \)
  - \( (\mathbb{Z}/2\mathbb{Z}, +, \cdot) \) commutative ring
- \( \mathbb{R} \) (\( \mathbb{C} \times \mathbb{I} \)), find ideals \( I \)
  - \( p(x) \in \mathbb{C} \Rightarrow p(x) (\mathbb{C} \times \mathbb{I}) \subseteq I \) and \( p(x) (\mathbb{C} \times \mathbb{I}) \) is indeed an ideal
  - addl. subgroup \( \checkmark \)
  - \( r(x) \in (\mathbb{C} \times \mathbb{I}) \Rightarrow r(x) p(x) (\mathbb{C} \times \mathbb{I}) = p(x) r(x) (\mathbb{C} \times \mathbb{I}) \subseteq p(x) (\mathbb{C} \times \mathbb{I}) \)
- \( \mathbb{C} \times \mathbb{I} \), \( I = \{ x + iy \}_{x, y \in \mathbb{C}} \) ideal in \( \mathbb{C} \times \mathbb{I} \)
  - factor ring:
    \[ \mathbb{C} \times \mathbb{I} / p(x) (\mathbb{C} \times \mathbb{I}) = \mathbb{C} \times \mathbb{I} / p(x) \] (simple notation)
- \( \mathbb{R} \) (\( \mathbb{C} \times \mathbb{I} \)), \( I = \{ x + iy \}_{x, y \in \mathbb{C}} \) ideal in \( \mathbb{R} \)
  - \( I \) subsring but not an ideal.

Lemma:
1. The sum of finitely many ideals is an ideal.
2. The intersection of any number of ideals is an ideal.
3. Ideal generators: \( R \) a ring, \( d \in R \)
   - \( \langle d \rangle \) the ideal of \( \langle d \rangle \) is called a principal ideal.
4. Similarly, \( \langle d_1, \ldots, d_n \rangle \) \( d_i \in R \)
   - \( \langle d_1, \ldots, d_n \rangle \) the ideal of \( \langle d_1, \ldots, d_n \rangle \) is called a principal ideal.
5. Note: \( I \) an ideal of \( R \), \( 1 \in I \Rightarrow I = R \)

Any ring in which every ideal is a principal ideal is called a principal ideal domain (PID).
Definition: A ring homomorphism is a mapping $\phi: R \to S$ (R, S are rings) such that

\begin{enumerate}
\item $\phi(a + b) = \phi(a) + \phi(b)$ for $a, b \in R$
\item $\phi(ab) = \phi(a)\phi(b)$
\end{enumerate}

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

Lemma: a) $\ker \phi \subseteq R$. b) Conversely, if $I \trianglelefteq R$, and $\phi: R \to R/I$, $a \mapsto a + I$, then $\ker \phi = I$.

Proof: a) $\ker \phi$ is subgroup (as kernel of a group hom.)
- $a \in R, x \in \ker \phi \implies \phi(ax) = \phi(a)\phi(x) = \phi(a).0 = 0$
- $\implies ax \in \ker \phi$
- Similarly $xa \in \ker \phi$

b) omitted.

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

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

proof: Define $\bar{\phi}: R/\ker \phi \to \phi(S)$, $[a ] \mapsto \phi(a)$
- $\bar{\phi}$ is hom. (check def.)
- $\bar{\phi}$ surjective (from its definition obvious)
- $\bar{\phi}$ injective:
- $\bar{\phi}(a + \ker \phi) = \bar{\phi}(b + \ker \phi) \iff \phi(a) = \phi(b)$
- $\iff \phi(a-b) = 0 \iff a-b \in \ker \phi \iff a + \ker \phi = b + \ker \phi$
<table>
<thead>
<tr>
<th>Groups $G$</th>
<th>Rings $R$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group generators</td>
<td>Ring generators</td>
</tr>
<tr>
<td>Subgroups $H$</td>
<td>Ideals $I$ - ideal generators</td>
</tr>
<tr>
<td>Group homomorphisms</td>
<td>Ring homomorphisms</td>
</tr>
<tr>
<td>Normal subgroups</td>
<td>Two-sided ideals</td>
</tr>
<tr>
<td>Factor groups</td>
<td>Factor rings</td>
</tr>
<tr>
<td>$G/_{\ker\phi} \cong \mathbb{C}G$</td>
<td>$R/_{\ker\phi} \cong \mathbb{C}(R)$</td>
</tr>
</tbody>
</table>

$k$-Kernels of hom.'s - Yitel factor structures