	group G	ring R	vector space V
generators $\langle \dots \rangle$	group generators	ring generators	generating set (basis if lin. ind.)
substructures	subgroup	ideal	subspace
homomorphisms	group hom.	ring hom.	linear mapping
Kernels of hom.'s = yields factor structures	normal subgroups	two-sided ideals ↳ generators	any subspace
hom. theorem	—— $X/_{\ker\varphi} \cong \varphi(X)$, $X \in \{G, R, V\}$ —		
classification	infinite/finite, abelian/non-abelian	commutative, integral domain, principal ideal domain, Euclidean ring, field	$\dim V = n \Rightarrow V \cong \mathbb{F}^n$

Definition: An algebra A is a ring $(A, +, \cdot)$ that is also a vectorspace $(A, +)$ such that the "+" in both coincides.

Examples: $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{C}[x,y]$, $\mathbb{R}$, $\mathbb{C}$

Algebraic constructions: Constructing an algebraic structures from another algebraic structure (often of the same type).

Examples:

a.) Forming substructures (e.g. subgroup from a group)

b.) Forming factor structures

c.) Group of units $R^\times$ from a ring R.

d.) Cartesian product

Definition: ~~Let G, H be groups (rings, vector spaces).~~

For two sets A, B,

$$A \times B = \{(a,b) \mid a \in A, b \in B\}$$

is called the "Cartesian product" of A and B.

Obviously $|A \times B| = |A||B|$.

Extension to $A_1 \times A_2 \times \dots \times A_n$ is straightforward.

$A^n = A \times \dots \times A$ (n factors)

<u>Definition:</u> Let G, H be groups (rings, vector spaces, ...).
Then $G \times H$ is again a group (ring, vector space, ...)
w.r.t. pointwise operation:

group $(G, \cdot)$: $(g,h)\cdot(g',h') = (gg', hh')$
ring $(R,+,\cdot)$: as above for "$\cdot$" and "$+$"
VS $(V,+)$: as above for "$+$" and $\alpha(u,v) = (\alpha u, \alpha v)$, $\alpha \in \mathbb{F}$

groups: $G \times H$ "direct product", $|G \times H| = |G||H|$
not every group is a direct product
rings: $R \times S$ "direct product", $|R \times S| = |R||S|$
not every ring is a direct product
vector spaces: $U \oplus V$ "(outer) direct sum", $\dim(U \oplus V) = \dim U + \dim V$

$$\dim V = n \Rightarrow V \cong \underbrace{\mathbb{F}}_{\dim = 1} \oplus \ldots \oplus \mathbb{F} = \mathbb{F}^n$$

<u>"inner" vs. "outer" direct sum:</u>
$U, V \leq W$ s.t. $W = U \oplus V$ (inner)
$\Rightarrow$ for $x \in W$ exists unique $u \in U, v \in W$: $x = u + v$
by identifying $u+v$ with (u,v) we can identify the inner and outer direct sum, or

$$\varphi: W = \overset{\text{inner}}{U \oplus V} \to \overset{\text{outer}}{U \oplus V}$$
$$u + v \to (u,v)$$

is a VS isomorphism.
example: $W = \mathbb{R}^2$, $U = \langle \binom{1}{0} \rangle$, $V = \langle \binom{0}{1} \rangle$ $\quad W = U \oplus V$ (inner)
$\binom{\alpha}{\beta} = \binom{\alpha}{0} + \binom{0}{\beta}$

$$U \oplus V \text{ (outer)} = \{ (\binom{\alpha}{0}, \binom{0}{\beta}) \}$$

Chinese remainder theorem (CRT)

Theorem (CRT for integers):

Let $n = pq$, p, q coprime ($\gcd(p,q) = 1$). Then

$$\mathbb{Z}/_{n\mathbb{Z}} \cong \mathbb{Z}/_{p\mathbb{Z}} \times \mathbb{Z}/_{q\mathbb{Z}}$$

The isomorphism is given by

$$\varphi: \; i \mapsto (i \bmod p \, , \; i \bmod q).$$

Can be extended to $n = p_1 \cdots p_k$, p_i, p_j mutually coprime.

proof:

a.) well-defined?

$$i \sim j \Rightarrow n \mid (i-j) \Rightarrow p, q \mid (i-j) \Rightarrow \begin{array}{l} i \bmod p = j \bmod p \\ i \bmod q = j \bmod q \end{array}$$

b.) hom., bijective omitted.

example: $\mathbb{Z}/_{15\mathbb{Z}} \cong \mathbb{Z}/_{3\mathbb{Z}} \times \mathbb{Z}/_{5\mathbb{Z}}$

$$\begin{array}{rcl} 2 & \mapsto & (2, 2) \\ \cdot \; 7 & \mapsto & (1, 2) \\ \hline 14 & \leftarrow\!\shortmid & (2, 4) \end{array}$$

Origin of CRT:
- Sun Tzu (China, 3rd century)
- but problems of this sort already in the 5th century B.C. (Brahmagupta)

The CRT can be extended to principal ideal domains. For us most important is its version for polynomial algebras

$$\mathbb{C}[x]/_{p(x)\,\mathbb{C}[x]} = \underbrace{\mathbb{C}[x]/_{p(x)}}_{\text{shorter notation}}$$

Theorem (CRT for polynomials)

Let $p(x) = q(x)\, r(x)$, q, r coprime. Then

$$\mathbb{F}[x]/p(x) \cong \mathbb{F}[x]/q(x) \oplus \mathbb{F}[x]/r(x) \quad \text{as } \underline{\text{algebras}}$$

$$\varphi,\quad s(x) \mapsto (s(x) \bmod q(x),\ s(x) \bmod r(x))$$

An extension to $p(x) = q_1(x) \cdots q_k(x)$, q_i mutually coprime is straightforward.

In particular: assume $p(x) = (x-\alpha_0)\cdots(x-\alpha_{n-1})$ $(\deg(p)=n)$ is "separable" ($\alpha_i \neq \alpha_j$ for $i \neq j$); then

$$(*) \qquad \mathbb{F}[x]/p(x) \cong \bigoplus_{k=0}^{n-1} \mathbb{F}[x]/(x-\alpha_k)$$

$$\varphi:\quad s(x) \mapsto (s(x) \bmod (x-\alpha_0), \ldots, s(x) \bmod (x-\alpha_{n-1}))$$
$$= (s(\alpha_0), \ldots, s(\alpha_{n-1}))$$

One view point:

φ: <u>evaluation</u> of a polynomial s of degree $< n$ at n points

φ^{-1}: <u>interpolation</u>, i.e., finding the unique polynomial s of degree $< n$ with given values $s(\alpha_i)$, $0 \le i < n$.

example: $\varphi: \mathbb{C}[x]/x^2-1 \to \mathbb{C}[x]/x-1 \oplus \mathbb{C}[x]/x+1$

$$s(x) = ax+b \mapsto (a+b,\ a-b)$$

is the DFT on 2 points (more later)

proof: $(*)$ only

a.) well-defined: as for integers

b.) ring hom.:

$+$: $s(x) + s'(x) \mapsto (s(\alpha_0)+s'(\alpha_0), \ldots, s(\alpha_{n-1}) + s'(\alpha_{n-1}))$
$= (s(\alpha_0), \ldots, s(\alpha_{n-1})) + (s'(\alpha_0), \ldots, s'(\alpha_{n-1}))$

$\cdot$: similar

c.) lin. mapping:

$+$: see above

scalar mult: similar

d.) Bijective:

since $\dim\left(\mathbb{F}[x]/p(x)\right) = n = \dim\left(\bigoplus \mathbb{F}[x]/(x-\alpha_i)\right)$

injective $\Leftrightarrow$ surjective

show surjective: given $(\beta_0, \dots, \beta_{n-1})$

find $s(x)$, $\deg(s) < n$ s.t. $s(\alpha_i) = \beta_i$.

<u>Case 1:</u> $\beta_i = 1$, $\beta_j = 0$, $j \neq i$

solution: $$s_i(x) = \frac{\prod_{j\neq i}(x-\alpha_j)}{\prod_{j \neq i}(\alpha_i - \alpha_j)}, \quad \deg s_i < n$$

<u>Case 2:</u> general case

solution: $$s(x) = \sum_{i=0}^{n-1} \beta_i s_i(x), \quad \text{where } \beta_i = s(\alpha_i)$$

This is called "Lagrange interpolation."

More about $s_i(x)$:

$$\begin{aligned} \varphi: \quad & s_0(x) \longmapsto (1, 0, \dots 0) \\ & s_1(x) \longmapsto (0, 1, 0 \dots 0) \\ & \quad \vdots \\ & s_{n-1}(x) \longmapsto (0, \dots, 0, 1) \\ \hline \Sigma: \quad & \sum s_i(x) \longmapsto (1, \dots, 1) \end{aligned}$$

<u>Properties of $s_i(x)$</u>

a.) $\{s_0(x), \dots, s_{n-1}(x)\}$ is a basis of $\mathbb{F}[x]/p(x)$ since

$$s(x) = \sum s(\alpha_i)\, s_i(x)$$

b.) $\sum_{i=0}^{n-1} s_i(x) = 1$, $\quad s_i(x)\, s_j(x) = \begin{cases} 1 & i = j \\ 0 & \text{else} \end{cases}$

c.) $\varphi(s_i(x)) = e_i$, $0 \leq i < n$.