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

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

Algebraic constructions: Constructing an algebraic structure 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: The Cartesian product of sets $A$ and $B$ is

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

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

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

Extension to $A_1 \times A_2 \times \ldots \times A_n$ is straightforward, $A^n = A \times A \times \ldots \times A$ (n factors).
Definition: Let $G, H$ be groups (rings, vector spaces,...).
Then $G \times H$ is again a group (ring, vector space,...)
by the pointwise operation:

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

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

$\dim V = n \Rightarrow V \cong \mathbb{F} \oplus \cdots \oplus \mathbb{F} = \mathbb{F}^n$

"inner" vs. "outer" direct sum:
$U, V \subseteq W$ s.t. $W = U \oplus V$ (inner)

$\Rightarrow$ for $x \in W$ exists unique $u \in U, v \in V$: $x = u + v$

by identifying $u + v$ with $(u, v)$ we can identify
the inner and outer direct sum, or

Let $W = U \oplus V \Rightarrow U \oplus V$

$U + V \rightarrow(U, V)$

is a VS isomorphism.

example: $W = \mathbb{R}^2$, $U = \langle (0) \rangle$, $V = \langle (1) \rangle$
$W = U \oplus V$ (inner)

$(\frac{a}{b}) = (\frac{a}{b}) + (\frac{0}{1})$

$U \oplus V$ (outer) = \{ $(\frac{a}{b}), (\frac{0}{b})$ \}
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

\[
\Phi: i \mapsto (i \mod p, i \mod q).
\]

Can be extended to \( n = p_1 \ldots p_k, p_i, p_j \) mutually coprime.

proof:

a) well-defined?

\( i \sim j \Rightarrow n | (i - j) \Rightarrow p, q | (i - j) \Rightarrow i \mod p = j \mod p \) \( \mod q = j \mod q \)

b) hom. bijective omitted.

example:

\[
\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}
\]

\[
2 \mapsto (2, 2)
\]

\[
\cdot \quad \quad 3 \mapsto (1, 2)
\]

\[
14 \leftrightarrow (2, 4)
\]

Origin of CRT: - Sun Tzu (China, 3rd century)

- See problems of this sort already in the 5th century B.C.
  (Brahma gupta)

The CRT can be extended to principal ideal domains.

For us most important is its version for polynomial algebras

\[
\mathbb{C}[x]/\langle p(x) \rangle \cong \mathbb{C}[x]/\langle p(x) \rangle
\]

shorter notation
Theorem (CRT for polynomials)

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

\[
\mathbb{F}[x]/p(x) \cong \mathbb{F}[x]/q(x) \oplus \mathbb{F}[x]/r(x)
\]

as algebras

\( \Phi : s(x) \mapsto (s(x) \mod q(x), s(x) \mod r(x)) \)

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

In particular: assume \( p(x) = (x - x_0) \cdots (x - x_{n-1}) \) (deg\(p\) = \( n \)) is "separable" (\( x_i \neq x_j \) for \( i \neq j \)), then

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

\( \Phi : s(x) \mapsto (s(x) \mod (x-x_0), \ldots, s(x) \mod (x-x_{n-1})) = (s(x_0), \ldots, s(x_{n-1})) \)

One viewpoint:

\( \Phi : \text{evaluation of a polynomial } s \text{ of degree } \leq n \)

at \( n \) points

\( \Phi' : \text{interpolation, i.e., finding the unique polynomial } s \text{ of degree } \leq n \) with given values \( s(x_i), 0 \leq i < n \).

Example:

\[
\Phi : \mathbb{C}[x]/x^2 - 1 \rightarrow \mathbb{C}[x]/x - 1 \oplus \mathbb{C}[x]/x + 1
\]

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

is the DFT on 2 points (more later)

Proof: (*) only

a) well-defined: as for integers

b) ring hom:

\[
+: s(x) + s'(x) \mapsto (s(x_0) + s'(x_0), \ldots, s(x_{n-1}) + s'(x_{n-1})) = (s(x_0), \ldots, s(x_{n-1}) + (s'(x_0), \ldots, s'(x_{n-1}))
\]

e) lin. mapping:

+: see above

scalar mult: similar
d.) Bijective:

since \( \dim(\mathbb{F}^n / \rho(x)) = n = \dim(\mathbb{F}^n / (x-a_i)) \)

injective \(\iff\) surjective

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

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

Case 1: \(\beta_i = 1\), \(\beta_j = 0\), \(j \neq i\)

solution: \(s_i(x) = \frac{\prod_{j \neq i} (x-a_j)}{\prod_{j \neq i} (a_i-a_j)}\), \(\deg s_i < n\)

Case 2: general case

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

This is called "Lagrange interpolation."

There about \(s_i(x)\):

\[
\begin{align*}
\Psi: & \quad s_0(x) \mapsto (1, 0, \ldots, 0) \\
& \quad s_1(x) \mapsto (0, 1, 0, \ldots, 0) \\
& \quad \vdots \\
& \quad s_{n-1}(x) \mapsto (0, \ldots, 0, 1) \\
\Sigma: & \quad \sum s_i(x) \mapsto (1, \ldots, 1)
\end{align*}
\]

Properties of \(s_i(x)\)

1. \(\{s_0(x), \ldots, s_{n-1}(x)\}\) is a basis of \(\mathbb{F}^n / \rho(x)\) since

\[
s(x) = \sum s(a_i) s_i(x)
\]

2. \(\sum_{i=0}^{n-1} s_i(x) = 1\), \(s_i(x) s_j(x) = \delta_{i,j}\)

3. \(\Psi(s_i(x)) = e_i\), \(0 \leq i < n\).