Algebras.

Definition. Let A be a ring. An A-**algebra** is a pair (B, ϕ), where B is a ring and $\phi\colon A \to B$ is a ring homomorphism.

If (B, ϕ) and (C, ψ) are A-algebras, then a ring homomorphism (resp. isomorphism) $\chi\colon B \to C$ is a **homomorphism (resp. isomorphism) of A-algebras** if $\chi \circ \phi = \psi$.

Remark. We usually omit the homomorphism $\phi\colon A \to B$ from the notation, and so say "B is an A-algebra" rather than "(B, ϕ) is an A-algebra". We also omit writing ϕ in relating elements of A to B, and will write things like "let $a \in A$ and $b \in B$, and consider $ab \in B$" instead of the formally correct "... consider $\phi(a)b \in B$".

Example. For any ring A, the polynomial ring $A[x_1, \ldots, x_n]$ is an A-algebra via the natural inclusion $\phi\colon A \to A[x_1, \ldots, x_n]$. All quotients $A[x_1, \ldots, x_n]/I$ are A-algebras, with A-algebra structure given by composing $A \to A[x_i] \to A[x_i]/I$.

Example. For any ring B, there is a unique ring homomorphism $\phi\colon \mathbb{Z} \to B$ given by $\phi(n) = n1_A$. Thus every ring is a $\mathbb{Z}$-algebra in precisely one way. Every homomorphism of rings is a homomorphism of $\mathbb{Z}$-algebras.

Definition. Let B be an A-algebra. We say B is a

- **finite** A-algebra if B is finitely generated as an A-module, i.e. if there exist finitely many elements $b_1, \ldots, b_n \in B$ such that every element of B can be written as
$$\sum_{i=1}^{n} a_i b_i \qquad a_i \in A, b_i \in B$$
- **finite type** A-algebra if there exist a finite set of elements $b_1, \ldots, b_n \in B$ such that every element in B can be written as a finite sum of the form
$$\sum_{i_j \geq 0} a_{i_1,\ldots,i_n} b_1^{i_1} \cdots b_n^{i_n}$$

Proposition. *Let B be an A-algebra. The following are equivalent*

(1) *B is of finite type.*
(2) *There exists a surjective A-algebra homomorphism $\phi\colon A[x_1, \ldots, x_n] \to B$*
(3) *There exists an A-algebra isomorphism $\psi\colon A[x_1, \ldots, x_n]/I \cong B$*

Proof. (1) $\implies$ (2): If B is generated by $b_1, \ldots, b_n$, then there is a surjective A-algebra homomorphism $\phi\colon A[x_1, \ldots, x_n] \to B$ given by
$$\phi\left(\sum_{i_j \geq 0} a_{i_1,\ldots,i_n} x_1^{i_1} \cdots x_n^{i_n}\right) = \sum_{i_j \geq 0} a_{i_1,\ldots,i_n} b_1^{i_1} \cdots b_n^{i_n}.$$

(2) $\implies$ (3): The fundamental homomorphism theorem gives a ring isomorphism
$$B \cong A[x_1, \ldots, x_n]/\ker\phi,$$
and it is easy to see that this is also an isomorphism of A-algebras if ϕ is an A-algebra homomorphism.

(3) $\implies$ (1): Let $\bar{x}_i = x_i + I$. Every element of $A[x_1, \ldots, x_n]/I$ can be written as a finite sum
$$\sum_{i_j \geq 0} a_{i_1,\ldots,i_n} \bar{x}_1^{i_1} \ldots \bar{x}_n^{i_n},$$

so every element of B can be written as a finite sum

$$\psi(\sum_{i_j \geq 0} a_{i_1,\ldots,i_n} \bar{x}_1^{i_1} \ldots \bar{x}_n^{i_n}) = \sum_{i_j \geq 0} a_{i_1,\ldots,i_n} \psi(\bar{x}_1))^{i_1} \ldots \psi(\bar{x}_n)^{i_n}.$$

□

Remark. A finite A-algebra is always of finite type, but not vice versa: The polynomial rings $A[x_1, \ldots, x_n]$ are of finite type, but not finite.

Example. The natural inclusion $\mathbb{R} \to \mathbb{C}$ makes $\mathbb{C}$ into a finite $\mathbb{R}$-algebra, since every element of $\mathbb{C}$ can be written as $x \cdot 1 + y \cdot i$ with $x, y \in \mathbb{R}$.

Tensor product of algebras.

Definition. Let B and C be A-algebras. The A-module $B \otimes_A C$ is an A-algebra, with multiplication defined by

$$(b \otimes c)(b' \otimes c') = bb' \otimes cc',$$

and more generally by

$$(\sum_i b_i \otimes c_i)(\sum_j b'_j \otimes c'_j) = \sum_{i,j} b_i b'_j \otimes c_i c'_j.$$

Remark. The unit element in the ring $B \otimes_A C$ is $1 \otimes 1$.

Remark. It must be checked that this multiplication is well-defined. One way to see this is to observe that any time we rewrite the sums on the left hand side by using the relations

$$b \otimes (c + c') = b \otimes c + b \otimes c', \quad (b + b') \otimes c = b \otimes c + b' \otimes c$$

and

$$ab \otimes c = b \otimes ac,$$

the expression on the right hand side can also be rewritten using these relations. Alternatively one can use the defining property of the tensor product, see the textbook for details.

Example. Let A be a ring, consider $B = A[x]$ and $C = A[y]$. Then, as A-modules, we have isomorphisms

$$B = \bigoplus_{i \geq 0} Ax^i, \qquad C = \bigoplus_{i \geq 0} Ay^i,$$

or in words, B (resp. C) is the free A-module generated by $1, x, x^2 \ldots$ (resp. by $1, y, y^2, \ldots$). We then find a module isomorphism

$$B \otimes_A C \cong (\bigoplus_{i \geq 0} Ax^i) \otimes (\bigoplus_{j \geq 0} Ay^j) = \bigoplus_{i,j \geq 0} Ax^i \otimes y^j.$$

For the multiplication, we have

$$(x^{i_1} \otimes y^{j_1})(x^{i_2} \otimes y^{j_2}) = (x^{i_1} x^{i_2} \otimes y^{j_1} y^{j_2}) = x^{i_1 + i_2} \otimes y^{j_1 + j_2}.$$

From this we see that there is an isomorphism of A-algebras $B \otimes_A C \to A[x, y]$, given by $\sum a_{ij} x^i \otimes y^j \mapsto \sum a_{ij} x^i y^j$.

Example. For any A-algebra B, we have $A[x_1, \ldots, x_n] \otimes_A B \cong B[x_1, \ldots, x_n]$, via the map $ax_1^{i_1} \ldots x_n^{i_n} \otimes b \mapsto abx_1^{i_1} \ldots x_n^{i_n}$.

Example. Consider $\mathbb{C}$ as an $\mathbb{R}$-algebra. We have a natural basis $1, i \in \mathbb{C}$ as an $\mathbb{R}$-module, so $\mathbb{C} \cong \mathbb{R}1 \oplus \mathbb{R}i$. We have

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = (\mathbb{R}1 \oplus \mathbb{R}i) \otimes (\mathbb{R}1 \oplus \mathbb{R}i) = (\mathbb{R}1 \otimes 1 \oplus \mathbb{R}i \otimes 1 \oplus \mathbb{R}1 \otimes i \oplus \mathbb{R}i \otimes i).$$

In other words $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ is an $\mathbb{R}$-vector space with basis $1 \otimes 1, 1 \otimes i, i \otimes 1, i \otimes i$. The multiplication table is easy to write down in this basis, if $x = 1 \otimes i$, $y = i \otimes 1$, $z = i \otimes i$, then we have

$$x^2 = y^2 = -1, z^2 = 1$$

and

$$xy = z, yz = -x, zx = -y.$$

One can check that this ring is isomorphic to $\mathbb{C} \times \mathbb{C}$.

4.11. **Rings of fractions.** Recall from a previous course (hopefully), that given any integral domain A, we can produce a field $K(A)$, whose elements are written a/b, with $a \in A, b \in A \setminus \{0\}$, the **fraction field** of A.

Example. We have $K(\mathbb{Z}) = \mathbb{Q}$ and, if k is a field, $K(k[x]) = k(x)$, the field of rational functions.

Formally, the field $K(A)$ is constructed as follows

(1) Consider all pairs $(a, b) \in A \times A$ with $b \neq 0$.
(2) Declare that $(a, b) \simeq (a', b')$ if

$$ab' - ba' = 0$$

(3) Check that this is an equivalence relation.
(4) Let $k(A)$ be the set of equivalence classes of pairs $(a, b) \in A \times A$.
(5) Define addition and multiplication, check all's well defined and gives a field.

Example. It is essential that A is an integral domain, otherwise $\sim$ is not an equivalence relation. E.g. in $\mathbb{Z}/(4)$, we find

$$(2, 2) \sim (1, 1) \qquad 2 \cdot 1 - 1 \cdot 2 = 0$$

and

$$(2, 2) \sim (0, 2) \qquad 2 \cdot 2 - 0 \cdot 2 = 0$$

but

$$(1, 1) \not\sim (0, 2) \qquad 2 \cdot 1 - 1 \cdot 0 = 2 \neq 0.$$

We may think of the construction as follows: Given an integral domain A, we build a "smallest" ring $K(A)$ from A such that every non-zero element in A has an inverse.

Generalised question: Given a ring A, and $S \subseteq A$, construct a new ring $S^{-1}A$ where elements of s have inverses.

Note that, if $s_1, s_2 \in S$, and s_1 and s_2 has inverses, then $s_1 s_2$ must also have an inverse. The element $1 \in A$ already has an inverse, so we can always add it in to S. It makes sense then to assume S is **multiplicatively closed**, meaning $1 \in S$ and $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$.

Definition. Given a ring A and a multiplicatively closed subset $S \subseteq A$, define the **ring of fractions of** A with respect to S as follows.

- The set $S^{-1}A$ consists of equivalence classes of pairs
$$(a, s) \qquad a \in A, s \in S,$$
under the equivalence relation that
$$(a, s) \sim (b, t)$$
if and only if there exists a $u \in S$ such that
$$(at - sb)u = 0.$$
- Addition and multiplication is defined by
$$(a, s) + (b, t) = (at + bs, st)$$
$$(a, s)(b, t) = (ab, st).$$

Remark. The proof that this is a ring is almost exactly the same as the construction of the fraction field of an integral domain.

Remark. We will always write a/s instead of (a, s). The formulas for addition and multiplication of these fractions are the same as the usual ones. The only thing that is harder is the new criterion for when two fractions are equal, i.e.
$$\frac{a}{s} = \frac{b}{t} \Leftrightarrow (at - bs)u = 0 \text{ for some } u \in S.$$

Remark. The unit element in $S^{-1}A$ is $1/1$, and the zero element is $0/1$.

Remark. There is a ring homomorphism $\phi\colon A \to S^{-1}A$ defined by $\phi(a) = \frac{a}{1}$.

Example. Let $S = \{2^n \mid n \geq 0\} \subset \mathbb{Z}$. Then $S^{-1}\mathbb{Z}$ consists of equivalence classes of pairs $(k, 2^n)$, with $k \in \mathbb{Z}$. The equivalence relation is such that $(k, 2^n) \sim (k', 2^{n'})$ if and only if $\frac{k}{2^n} = \frac{k'}{2^{n'}}$ in $\mathbb{Q}$. We can identify $S^{-1}\mathbb{Z}$ with the subring of $\mathbb{Q}$ consisting of elements of the form $\frac{k}{2^n}$.