=: Basics of Algebra. :=

In algebra.

a. Algeraic Structure : $(S, OP_1, OP_2, \ldots OP_k)$.

b. We deal with mathematical expressions defined on that Structure.

Example: 1. Boolean algebra: $(\{0,1\}$, AND, OR, NOT, XOR).

2. $(\mathbb{Z}, +, -, \times)$; $(\mathbb{Q}, +, -, \times, \div)$; $(\mathbb{R}, +, -, \times, \div)$; $(\mathbb{C}, +, -, \times)$.

3. $(\mathbb{Z}_n, +_n, \times_n)$, where $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

4. $(M_n$, matrix-addition, matrix-mul).

5. $(S_n$, composition), for any graph G, $(Aut(G)$, composition).

6. $(\mathbb{R}^n$, Coordinate-wise-addition). 7. $(\mathbb{R}[x]$; poly-add, poly mul).

.... There any many exotic algebraic structres in mathematics

Abstract algebra: Instead of study each algeraci structre separately, in abstract algebra we classify them in few number of "abstract" algebraic structres & study these structres:

1. Groups 2. Rings 3. Fields 4. Vector Spaces.

Groups: either +/−, or ×/÷ (only one operation).

Rings: +/−, × but may not division.

Fields: +/−, ×/÷

Vector space: abstruction of $\mathbb{R}^n$, i.e., vector-addition &

scalar multiplication.

Group: $(G, \cdot)$ with $\cdot : G \times G \to G$ with the following properties

1. Closure: $\forall a, b$, $a \cdot b \in S$
2. Associativity: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

$\Rightarrow a_1\ a_2\ a_3\ a_4 \to$ apply a process i.e. replace two consecutive element (a, b) by $a \cdot b$

3. Identity: $\exists\ e \in G$ s.t. $\forall\ a \in G$, $a \cdot e = e \cdot a = a$
4. Inverse: $\forall\ a\ \exists\ b \in G$ s.t. $a \cdot b = b \cdot a = 1$.

$\Rightarrow$ replacing substraction by addition.

Q2: How many identity elements: Unique. (Exercise)

Q3: How many inverse element? Unique (h^{-1}) (Exercise)

G is commutative if $\forall\ a, b \in G$, $a \cdot b = b \cdot a$.

✓ ✗ ✓ ✓ ✓ ✗ $(\mathbb{Z}_n^*)$

$(\mathbb{Z}, +)$, $(\mathbb{Z}, \times)$, $(\mathbb{Q}, +)$, $(\mathbb{Q}, \div)$, $(Z_n, +_n)$, $(Z_n, \times_n)$,

~ ✗ ~ ✓ ✓

$(M_n, +)$, $(M_n, \times)$, $(S_n$, Composition$)$, $(\mathrm{Aut}(h)$, composition$)$,

✓ ~ ✗

$(R^n$, cordinate-wise add$)$, $(R[x]$, poly-add$)$, $(R[x]$, poly. mul$)$

Subgroup: $S \subseteq G$, $(S, \cdot)$ subgroup if it is also a group

i.e. 1. $\forall\ a, b$, $a \cdot b \in S$

2. $\forall\ a$, $a^{-1} \in S$.

Associativity, identity. follows from these two.

Q4: Can we remove any one of them? No; $(\mathbb{Z}_{\geq 0}, +)$

But for finite G, we can remove 2.

Q4: Instead of two conditions, can we make one conditions which will imply the two?

Yes! $\forall\ a, b,\ \ a \circ b^{-1} \in S$.

Ring: $(R, +, \times)$ is ring if

a. $(R, +)$ is commutative group (addition)

b. $(R, \times)$ where $\times$ stasfies closure & associativity property. (multiplication).

c. **Distributive:** $a \times (b+c) = (a \times b) + (a \times c)$ &

$(b+c) \times a = (b \times a) + (c \times a)$.

Additive identive is denoted by 0,
if multiplicative identity exists, denoted by 1.
Commutative ring $\Rightarrow$ multiplication is commutative

Eg:
$(\mathbb{Z}_n, +_n, \times_n)$, $(M_n, \text{mat-add}, \text{mat-mul})$,
$(R[x], \text{poly-add}, \text{poly-mul})$.

Field: A ring $(F, +, \times)$ is field if
$(F \setminus \{0\}, \times)$ is a commutative group
(multiplicative group).

Eg: $(\mathbb{Q}, +, \times)$, $(\mathbb{R}, +, \times)$, $(\mathbb{C}, +, \times)$.

In this course, we are interested a special kind of field called "finite fields, when $|F|$ is finite.

Q5: Does finite field exists?

Yes! Let p a prime number.

$(Z_p, +_p, \times_p)$ is a field. To show it is a field, need to show that $\forall$ nonzero $a \in Z_p$ $\exists$ a nonzero b: s.t. $a \times_p b = 1$. (Denote it by F_p).

Q6: Are there exists any other kind of finite field?

Like $R[x]$, for every field F, we can define $F[x]$ be set of all univariate polynomials over F & it forms a ring under poly-add & poly-mul.

For a polynomial $f \in F[x]$, $\deg(f) := \max\{i \in \mathbb{Z}_{\geq 0} \mid \text{coeff}_{x^i}(f) \neq 0\}$.

$f(x) \in F[x]$ can have at most d root.

Irreducible polynomials: $f(x)$ is reducible if $f(x) = a(x) \cdot b(x)$ where $\deg(a), \deg(b) < \deg(f)$.

Otherwise, irreducible.

Eg: $\forall \alpha \in F$, $x - \alpha$ is irreducible polynomial.

$\forall f(x) \in F[x]$, can be written product of irreducible polynomials.

It is unique up to rearrangement & product by scalars from F.

Division theorem: for any two polynomials $f(x)$ & $g(x)$ $\exists$ a quotient $Q(x)$ [unique] & remainder $R(x)$.

s.t. $f(x) = Q(x)g(x) + R(x)$ s.t. $R(x) = 0$, or $\deg(R) < \deg(g)$.

for any $f(x)$, $\left(F[x]/\langle f(x)\rangle, \text{poly-add}_p, \text{poly-mul}_p\right)$ is a commutative ring, where $F[x]/\langle p(x)\rangle$ is the set of polynomials of degree less than $\deg(p)$.

Field extension: When $f(x)$ is a irreducible polynomial, $\left(F[x]/\langle f(x)\rangle, \text{poly-add}_p, \text{poly-mul}_p\right)$ forms a field.

For any prime p, an positive integer s, $\exists$ a irreducible polynomial $f(x)$ over the F_p.

$\Rightarrow$ $\forall$ prime p & positive integer s, we have a finite field p^s.

QC: Does there exists finite field of whose cardinality is not of the form p^s? No!

Theorem: $\forall$ prime p & positive integer s. $\exists$ a finite field of size p^s. Conversely, the size of any finite field is of form p^s for some prime p & positive integer s.

Q7: How many different finite fields of size p^s exists? Unique!

Theorem: For every prime p & positive integers s, $\exists$ a unique finite field of size p^s (up to isomorphism).

Exercise: For any finite field, its multiplicative group is cyclic.