gradeup

Group Theory Part-2

Group Theory Part-2

Content:

1. **Field**
2. **Semi Group**
3. **Ring**
4. **R-module**
5. **Vector Space**
6. **Ideal**
7. **Prime Field**
8. **Linear Group**
9. **Summary of Group Theory**

Fields:

A glossary of algebraic systems

Semi-group: A semi-group is a set with an associative binary operation.

Ring: A ring is a set with two binary operations, addition and multiplication, linked by the distributive laws

$a(b + c) = ab + ac$

$(b + c)a = ba + ca$

Rings are abelian groups under addition and are semigroups under multiplication. We will assume our rings have the multiplicative identity 1 not equal to 0.

Commutative ring: A commutative ring is a ring in which the multiplication is commutative.

Domain: A domain (or integral domain) is a ring with no zero divisors, that is

$ab = 0 \Rightarrow a = 0$ or $b = 0$ for all a, b in the domain .

Field: A field is a commutative ring in which every nonzero element has a multiplicative inverse.

Skew field: A skew field (or division ring) is a ring (not necessarily commutative) in which the nonzero elements have a multiplicative inverse.

The quaternions

$Q = \{1 + ai + bj + ck : a, b, c \in R\}$

where $ij = k, jk = i, ki = j$, and $i^2 = j^2 = k^2 = -1$ is an example of a skew field.

R-module: If R is a commutative ring then an abelian group M is an R-module if scalar multiplication (r, m) 7→ rm is also defined such that for all $r, s \in R$ and $m, n \in M$:

$(r + s)m = rm + sm$

$(m + n)r = mr + nr$

$(rs)m = r(sm)$

$1_R \cdot m = m$

Vector Space: A vector space is an R-module where R is a field.

Euclidean Domain A domain D with a division algorithm is called a Euclidean Domain (ED).

By a division algorithm on a domain D we mean there is a function

$\deg : D\ 7\!\rightarrow \{0\} \cup N$

such that if $a, b \in D$ and b 6 not equal to 0 then there exists $q, r \in D$ such that $a = q^b + r$ where either $r = 0$ or $\deg(r) < \deg(b)$.

Ideals

A subset I of a ring R is an ideal if 1. if $a, b \in I$, then $a + b \in I$,

2. if $r \in R$ and $a \in I$, then $ra \in I$ and $ar \in I$

We write I C R and say I is an ideal of R.

A function $f : R \rightarrow S$ is a homomorphism of the rings R, S if for all a, b, $\in$ R

$f(a + b) = f(a) + f(b)$

$f(ab) = f(a)f(b)$

If f is a homomorphism, then the $\text{kernel}(f) = \{x \in R : f(x) = 0\}$.

Proposition: The kernel of a ring homomorphism is an ideal.

An ideal I that is singularly generated, i.e. I = (a), is called a principle ideal.

A ring with only principle ideals is called a principle ideal ring (PIR).

And similarly a domain with only principle ideals is a principle ideal domain (PID).

Theorem: If R is a Euclidean Domain, then R is a principle ideal domain.

An ideal P is a prime ideal, if whenever $ab \in P$, then either $a \in P$ or $b \in P$.

For example the prime ideals of Z are (p) = pZ = {xp : x ∈ Z}, where p is prime integer

The prime field:

A prime field is a field with no proper subfields.

Theorem: Every prime field Π is isomorphic to Z_p or Q.

Theorem: Every field F contains a unique prime field Π.

Theorem: Every finite field F has p n elements for some prime p and natural number n.

Theorem: The commutative ring R is a field if and only if R contains no proper ideals

An ideal M of R is a maximal ideal if M 6= R and there is no proper ideal of R that contains M

Theorem: M is a maximal ideal of the commutative ring R if and only if R/M is a field.

Theorem: Every prime ideal of a PID is a maximal ideal.

An element p ∈ R is an irreducible if and only if in every factorization p = ab either a or b is a unit. If p = uq where u is a unit then p and q are said to be associates.

Theorem: If R is a PID, then the non-zero prime ideals of R are the ideals (p), where p is irreducible.

Splitting fields

If the polynomial f(x) ∈ F[x] completely factors into linear factors

$f(x) = (x - \alpha_1)(x - \alpha_2) \cdot \cdot \cdot (x - \alpha_n)$

in the extension field K of F we say that f(x) splits over K. If f(x) splits over K and there is no subfield of K over which f(x) splits, then K is called the splitting field of f(x) over F.

Theorem: If F is a field and $f(x) \in F[x]$, then there exists a splitting field of f(x) over F.

Galois fields

Finite fields are also know as Galois fields. Recall that every finite field F is a vector space over its prime field Π. Thus if the characteristic of Π is the prime integer p, then $|F| = p^n$ where $n = [F : \Pi]$.

Theorem: For all primes p and positive integers n, all fields of order p^n are isomorphic.

Linear groups

The linear fractional group and PSL(2, q)

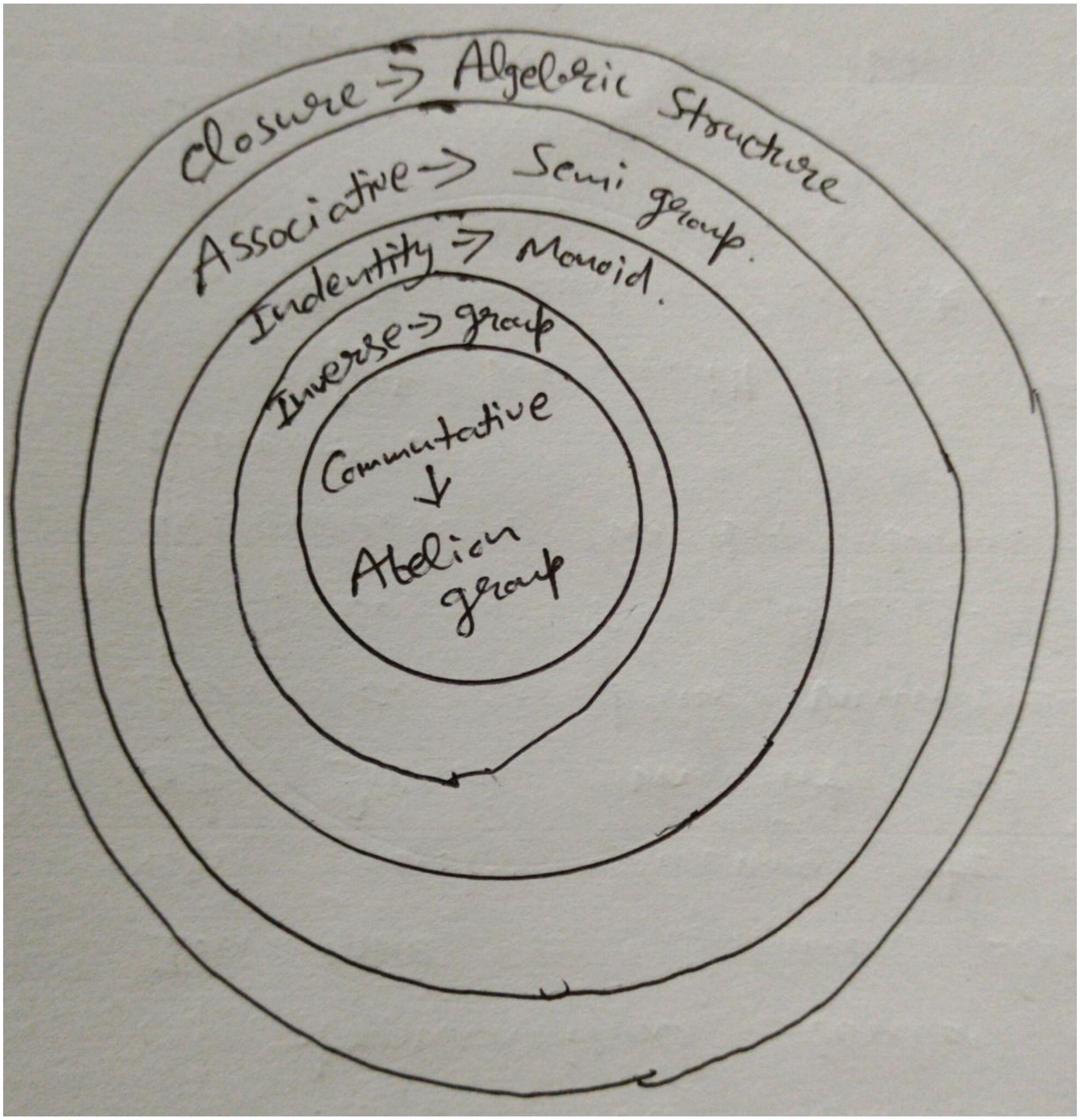
Let F_q be the finite field of order q and let $X = F_q \cup \{\infty\}$ (the so-called projective line). A mapping $f : X \to X$ of the form

$x \to ax + b /cx + d$

The set of all linear fractional transformations whose determinant is a nonzero square is LF(2, q), the linear fractional group.

Theorem: LF(2, q) is a group.

Theorem: LF(2, q) ~= PSL(2, q)



Closure Property: A set 'A' w.r.t. operator ∗ is satisfy closure property if ∀ a,b ∈ A then a∗b ∈ A .

Algebraic Structure: if a set 'A' w.r.t. operator '∗' satisfy closure property then it is called Algebraic Structure(A,∗)

Associative Property: A set ‘A’ w.r.t. ‘∗’ is said to satisfy Associative property. If ∀ a,b,c ∈ A.

(a∗b) ∀ c = a ∗ (b∗c)

Semi group: if a Algebra structure satisfy associative property is it called Semi group.

Identity Property: A set ‘A’ w.r.t. operator ∗ is said to be satisfy identity property if ∀ a ∈ A there is an element ‘e’ such that a ∗ e = e∗a = a

Monoid: If a semi Group satisfy identity then it is called monoid.

a + 0 = a + → 0

a ∗ 1 = a ∗ → 1

Inverse Property: A set ‘A’ w.r.t. operator ‘∗’ is said to satisfy inverse property if ∀ a ∈ A there is an element a^{-1} such that $a * a^{-1} = a^{-1} * a = e$.

Group: if a monoid satisfy inverse property then it is called group .

Commutative Property: A set ‘A’ w.r.t. operator ∗ is said to satisfy commutative property if ∀ a, b ∈ A a∗b =b∗a .

Abelian Group: If a group satisfy commutative property then it is called Abelian Group.

	Algebric Structure	Semi group	Monoid	group	Abolien group
N, +	✓	✓	✗	✗	✗
N, −	✗	✗	✗	✗	✗
N, *	✓	✓	✓	✗	✗
N, ÷	✗	✗	✗	✗	✗
Z, +	✓	✓	✓	✓	✓
Z, −	✓	✗	✗	✗	✗
Z, *	✓	✓	✓	✗	✗
Z, ÷	✗	✗	✗	✗	✗
R, +	✓	✓	✓	✓	✓
R, −	✓	✗	✗	✗	✗
R, *	✓	✓	✓	✗	✗
R, ÷	✗	✗	✗	✗	✗
e +	✓	✓	✓	✓	✓
e *	✓	✗	✗	✗	✗
O +	✗	✗	✗	✗	✗
o *	✓	✓	✓	✓	✓
M +	✓	✓	✓	✗	✗
M *	✓	✓	✓	✗	✗
RE .	✓	✓	✓	✗	✗
RE ; +	✓	✓	✓		