Groups $\quad G \times G \to G$

unit el't $\quad 1 \in G \quad 1g = g1 = g \quad \forall g \in G$

$(fg)h = f(gh)$, $\quad g^{-1}g = gg^{-1} = 1$

Conceptually, a group is all <u>symmetries</u> of an object X

$X = $ set $\{1, \dots, n\}$ $\quad Sym(X) = S_n$

$\mathbb{R}^n$ vect. space $\quad \mathbb{R}^n \xrightarrow{\sim} \mathbb{R}^n$ invertible linear maps

$GL(n)$ or $GL(n, \mathbb{R})$ $\quad$ noncommutative $n \geq 2$

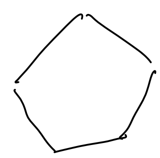
V - vect space $\quad V \xrightarrow{\sim} V$

$GL(V) \simeq GL(n)$ $\quad$ to set up an isomorphism, pick a basis of V

$V \simeq \mathbb{R}^n$

n-gon, regular

$Sym(\;) \simeq D_n \qquad D_{2n}$



$|D_n| = 2n$

$|G| = p$ prime $\quad G \simeq C_p$

<u>abelian groups</u>

$\forall$ fin. ab group $\quad C_{n_1} \times C_{n_2} \times \dots \times C_{n_k}$

<u>Principle</u> Abelian structures are relatively easy to classify.

ab. group, vector spaces,

fin. generated ab. group

$\mathbb{Z} \times \dots \times \mathbb{Z} \times$ fin. ab group

goods
services $\Big\} \to \mathbb{N} = \{0, 1, 2 \dots\}$

$\mathbb{Q}_+ = \left\{\frac{n}{m} \geqslant 0\right\}$

ab. group

$\frac{\mathbb{Z}}{100}$

$\mathbb{N} = \{0, 1, 2 \dots\}$ $\qquad +, \cdot$

$\mathbb{Z}$, $\mathbb{Q}$.

$Mat_n(\mathbb{R}) \qquad M_n(\mathbb{R})$

$n \times n$ matrices

$A, B \rightsquigarrow A+B, \; AB$.

Def A ring $R = (R, +, \cdot)$ is a set R with 2 binary operations $+, \cdot$ such that

(1) $(R, +)$ is an abelian group

(2) (2a) $\cdot$ is associative

(2b) $\exists$ an identity (unit element) 1

$1 \cdot a = a \cdot 1 = a \quad \forall a \in R$

occasionally 2b is dropped
rung

(3) Distributivity

$(a+b)c = ac + bc, \qquad c(a+b) = ca + cb.$

$a+b=b+a, \quad (a+b)+c=a+(b+c)$

$(+,0) \qquad 0+a=a+0=a \quad \forall a\in R$

$$\boxed{\begin{array}{l} 0 : \text{identity for } + \\ 1 : \text{identity for } \cdot \end{array}}$$

$-a$: additive inverse $\quad a+(-a)=0$

$(ab)c=a(bc)$.

multiplicative inverse of a, if exists, is denoted a^{-1}. $\quad a^{-1}a=aa^{-1}=1$.

$0=0+0 \qquad 0\cdot\cancel{a}=(0+0)a=\cancel{0a}+0a$

$\Rightarrow 0a=0 \quad \forall a \qquad a0=0$

$(-a)b=-(ab)=a(-b)$.

$a+a=2a \qquad \underbrace{-a-a\ldots-a}_{n}=-na$

$\underbrace{a+\ldots+a}_{n}=na \quad n\geq 0$

map

$0, 1, 1+1, 1+1+1, \ldots, -1, \ldots$

$$\begin{aligned} \mathbb{Z} &\longrightarrow R \\ 0 &\longmapsto 0 \\ 1 &\longmapsto 1 \\ -1 &\longmapsto -1 \end{aligned}$$

homomorphism $\longrightarrow$ respects the ring structure

sometimes R contains a copy of $\mathbb{Z}$ (as a subring)

$\mathbb{Z} \longrightarrow \mathbb{Z}/n$ cosets of $n\mathbb{Z}$ in $\mathbb{Z}$

$0, 1, 2, \ldots, n-1$

na

$\cancel{\mathbb{N}}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(\mathbb{R}), M_n(\mathbb{C})$

$(+, \cdot)$

$\{1, -1\}$

$(-1)^{-1} = -1$

$R^* = \{a \in R \mid \exists b \quad ab = ba = 1\}$

multiplicative inverse of a.

<u>Exercise</u> R^* is a group under multiplication

$M_n(R)^* = GL(n, \mathbb{R}) \qquad GL_n(\mathbb{R})$

$a^2 = a \cdot a \qquad a^n = \underbrace{a \cdots a}_{n \text{ times}} \qquad a^0 = 1$

$na = \underbrace{a + a + a \ldots + a}_{n} \qquad (-1)a = -a \qquad 0a = 0$

$\varphi(n)$

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\varphi} & R \\ \in & & \in \\ n & & n \end{array}$$

<u>Def</u> Ring R is called <u>commutative</u> if $ab = ba \quad \forall a, b \in R$.

R noncommutative if $ab \neq ba$ for some $a, b \in R$

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, M_n(\mathbb{R}), M_n(\mathbb{C})$

$M_1(\mathbb{R}) = \mathbb{R}$ not commutative $n \geq 2$

$M_n(R)$

any ring R

Mostly study commutative rings

$M_n(\mathbb{R})$, $M_n(\mathbb{C})$, $\mathbb{H}$.

trivial ring

$1 = 0$

$a = a \cdot 1 = a \cdot 0 = 0$

ring with 1 element

$(a+b)(c+d) = ac + ad + bc + bd$

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1, j=1}^{n, m} a_i b_j$$

$(a+b)^2 = (a+b)(a+b) = a^2 + ab + ba + b^2 \neq a^2 + 2ab + b^2$

if R is commutative $(a+b)^2 = a^2 + 2ab + b^2$

$(a+b)^3 =$ aab aba baa complicated

$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$ if a, b commute

$$\mathbb{Z} \ni \binom{n}{k} = \frac{n!}{k!(n-k)!} \qquad \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

$(ab)^2 = abab = a^2b^2$

if R commutative

0 1 0

0 1 1 0

0 1 2 1 0

0 1 3 3 1 0

1 4 6 4 1

1 5 10 10 5 1

$\mathbb{Z}/n$ ring of residues mod n.

$\mathbb{Z}$ $\quad n\mathbb{Z}$ – ab subgroup $\quad n\mathbb{Z}$

cosets $\quad a+n\mathbb{Z}$

$\mathbb{Z}, n\mathbb{Z} \qquad \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$

$+ \ , \quad (a+n\mathbb{Z})(b+n\mathbb{Z}) = ab+n\mathbb{Z}$

$\mathbb{Z}/n$ carries $\cdot$ as well

$\boxed{\mathbb{Z}/n \text{ is a commutative ring}}$

1 – mult. identity

0 – additive identity.

$R \subset S$

$\uparrow$

R is $\Leftarrow$ commutative

commutative

$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$

$\frac{1}{n} \qquad \frac{1}{n}\cdot\frac{1}{n} = \frac{1}{n^2} \ldots \qquad \frac{1}{n^k}$

$\mathbb{Z}[\frac{1}{n}] = \left\{ \frac{a}{n^k} \;\middle|\; a \in \mathbb{Z}, k \in \mathbb{N} \right\}$

$\mathbb{Z} \subset \mathbb{Z}[\frac{1}{n}] \subset \mathbb{Q} \qquad p \mid n$

$\not\Downarrow$

$\frac{1}{p}$

$\mathbb{Q} \subset \mathbb{R} \qquad \sqrt{2}\cdot\sqrt{2} = 2$

$\sqrt{2}$

$\mathbb{Q}[\sqrt{2}] = \{ a + b\sqrt{2} \mid a, b \in \mathbb{Q} \}.$

This is a ring

unique representation of an element of $\mathbb{Q}[\sqrt{2}]$

$(a_1+b_1\sqrt{2})+(a_2+b_2\sqrt{2}) = (a_1+a_2)+(b_1+b_2)\sqrt{2}$

$(-a)+(-b)\sqrt{2} = -a-b\sqrt{2}$

$(a_1+b_1\sqrt{2})(a_2+b_2\sqrt{2}) = (a_1a_2+2b_1b_2)+(a_1b_2+a_2b_1)\sqrt{2}$

$a_1+b_1\sqrt{2} = a_2+b_2\sqrt{2}$ $\qquad a_1-a_2 = (b_2-b_1)\sqrt{2}$

$\sqrt{2} = \dfrac{a_1-a_2}{b_2-b_1}$

$1+\frac{1}{n}+\left(\frac{1}{n}\right)^2+\dots$ makes sense in $\mathbb{R}$

$n \geq 2$

$1+1+1+1+\dots$

Need "topology" or "distance" on abelian group to form infinite sums.

$\mathbb{R}, \mathbb{C}.$ $\qquad e^a$

Polynomial rings

$R[x] =$ $\qquad ax^n$

$\{a_0+a_1x+\dots+a_nx^n \mid a_i \in R, n \in \mathbb{N}\}$

addition is term-wise

$(a_0+a_1x+\dots+a_nx^n)+(b_0+b_1x+\dots+b_mx^m) =$ $\qquad$ if $n<m$

$=(a_0+b_0)+(a_1+b_1)x+\dots (a_n+b_n)x^n+b_{n+1}x^{n+1}+\dots+b_mx^m$

$(a_0+\dots+a_nx^n)(b_0+\dots+b_mx^m) = \sum_{i=0,j=0}^{n,m} a_ib_jx^{i+j}$

$a_ix^ib_jx^j = a_ib_jx^{i+j}$

monomials
$$ax^n \cdot bx^m = ab\, x^n x^m =$$ x commutes with elements of R
$$= ab\, x^{n+m}$$

$$(a_0+a_1x)(b_0+b_1x) = a_0b_0 + a_0b_1x + a_1b_0x +$$
$$a_1b_1x^2 = a_0b_0 + (a_0b_1+a_1b_0)x + a_1b_1x^2$$

most of the time, R is commutative, $R[x]$ is commutative

$R \subset R[x]$ subring of constant polynomials

$x \quad ax \quad ax^k$

$$ax^k + bx^k = (a+b)x^k$$

$a_0 + a_1x + \ldots + a_nx^n$ $\qquad R[x]$

$$\begin{array}{l} (a_0, a_1, a_2 \ldots \; a_n, 0, 0, \ldots \quad) \\ +\, (b_0, b_1, b_2 \ldots \; b_m \ldots \quad) \\ \hline (a_0+b_0, a_1+b_1, \ldots \; a_m+b_m, a_{m+1} \ldots \; a_n, 0 \ldots 0) \end{array} \quad m<n$$

$$(\overset{0,1\ldots}{0\ldots}, \overset{k}{1}, 0 \ldots 0)(0 \ldots 0, \overset{n}{1}, \ldots 0) = (\overset{0}{0} \ldots, \overset{k+n}{1}, \ldots)$$
$a_0 \ldots a_k$

$$a+b = ab \qquad 0+b = 0b = 0$$