A Group G is a set with a map $*: G \times G \to G$, Such that $\forall\, a,b,c \in G$:

1) $(ab)*c = a*(bc)$
2) $\exists\, e \in G$ s.t $a*e = e*a = a$
3) $\forall\, a \in G$, $\exists\, a^{-1}$ s.t $a*a^{-1} = a^{-1}*a = e$

$|G|$ is the order of G and is the cardinality of the set G. If $a \in G$, the order of a is $|a| = m$, where m is the smallest non-zero integer s.t $a^m = e$. If no such m exists, then a has infinite order.

EX) $GL(n, \mathbb{F}) = \{[A_{ij}] : A_{ij} \in \mathbb{F}$ and $\det[A_{ij}] \neq 0\}$

$SL(n, \mathbb{F}) = \{[B_{ij}] : B_{ij} \in \mathbb{F}$ and $\det[B_{ij}] = 1\}$

What is the order of $GL(n, \mathbb{F}_q)$ where $q = p^k$ for prime p?

* For $GL(n, \mathbb{F}_q)$:

r_1 has $q^n - 1$ choices

r_2 has $q^n - q$ choices

$\vdots$

r_n has $q^n - q^{n-1}$ choices

$$|GL(n, \mathbb{F}_q)| = \prod_{k=0}^{n-1} (q^n - q^k)$$

A set $H \subseteq G$ is called a subgroup if it is also a group under the operation of G.
If H is a subgroup we write $H \leq G$ instead of $\underline{H \subseteq G}$. It suffices to show that H is closed under inverse and product.

Ex) $SL(n, \mathbb{F}) \leq GL(n, \mathbb{F})$

- for $A, B \in SL(n, \mathbb{F})$

$\det(AB) = \underline{\det A \det B} = \underline{1 \cdot 1}$

- $\det(AA^{-1}) = \det(I)$

$= \underline{\det} A \underline{\det A^{-1}} \longrightarrow$

$\det A^{-1} = \underline{1}$

A map $\varphi : \underline{H} \to \underline{G}$, with H, G groups, is called a homomorphism if

$$\forall x, y \in H, \quad \underline{\varphi(xy)} = \underline{\varphi(x)\varphi(y)}$$

product in H product in G

If, in addition, φ is a bijection, then φ is an isomorphism of groups. If two groups are isomorphic we write $\boxed{H \simeq G}$.

$z^n = 1$

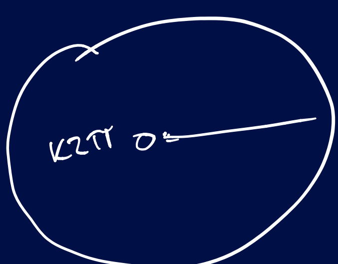
Ex) $\mu_n \simeq \mathbb{Z}_n$

μ_n are the n-th roots of unity and C_n is the cyclic group of order n.

for $z \in \mu_n$, $z = e^{\frac{2\pi i k}{n}}$ $\boxed{0 \le k \le n}$

- define $\varphi(z) = \boxed{\bar{k}}$
- for $x, y \in \mu_n$, $\varphi(xy) = \varphi\left(e^{\frac{2\pi i k}{n}} e^{\frac{2\pi i p}{n}}\right)$ $= \varphi\left(e^{\frac{2\pi i (k+p)}{n}}\right) = \bar{k} + \bar{p} = \varphi(x) + \varphi(y)$
- If $\varphi(z) = \bar{0}$, then $z = e^{\frac{2\pi i k}{n}}$, where $k = n \cdot l$, hence $z = e^{\frac{2\pi i (n l)}{n}} = e^{2\pi i l} = e^0$

hence $\ker \varphi = \{e^0\}$



- If $\bar{k} \in \mathbb{Z}_n$, then let m be the smallest non-negative member of $\bar{k}$ then $\varphi\left(e^{\frac{2\pi i m}{n}}\right) = \bar{k}$, so that

φ is surjective

If $H \leq G$, a left coset of H is defined to be $xH = \{xh : h \in H\}$ and $x \in G$. Right cosets are similarly defined.

Each coset is disjoint and has order $|H|$.

The number of cosets $= \frac{|G|}{|H|}$.

These cosets form a partition of G.

H is a normal subgroup of G, $H \trianglelefteq G$, if the left and right cosets are the same.

$\forall x \in G$: $xH = Hx$ or equivalently $xHx^{-1} = H$

If $H \trianglelefteq G$, we can form the quotient group G/H, where the elements of G/H are the cosets.

$$\forall\, xH, yH \in G/H, \quad (xH)(yH) = (xy)H$$

If $\varphi: G \to K$ is a homomorphism,
then $\ker\varphi \triangleleft G$.

- If $x \in \ker\varphi$ and $y \in G$

$\varphi(yxy^{-1}) = \varphi(y)\varphi(x)\varphi(y^{-1})$
$= \varphi(y)\varphi(y^{-1}) = \varphi(yy^{-1}) = \varphi(e)$

thus $yxy^{-1} \in \ker\varphi \quad \forall y \in G$

<u>First Iso.</u> Thm: $G/_{\ker\varphi} \simeq \mathrm{Im}(\varphi)$

Ex) $\det: GL(n, \mathbb{F}_q) \to \mathbb{F}_q^*$ is a homomorphism $\quad q-1$

- Consider $GL/_{\ker(\det)}$
- for any coset $A\ker(\det)$, if $B \in A\ker(\det)$, then $\det B = \det A$
- GL is partitioned into cosets with distinct det.
- order of $SL(n, \mathbb{F}_q)$
$= |GL(n, \mathbb{F}_q)| \to$

$q = p^k$ $\quad$ $\dfrac{\quad}{q-1}$

We say $x, y \in G$ are conjugate if $\exists g \in G$ s.t $\boxed{x = gyg^{-1}}$. The set of all elements conjugate to x, $Cl(x)$, is called the conjugacy class of x. Clearly, for an abelian group, the conjugacy classes are trivial.

$C_G(x) = \{g \in G : \boxed{gxg^{-1}} = x\} \leq G$ is the centraliser of x in G.

<u>Thm:</u> $\dfrac{|G|}{|C_G(x)|} = |Cl(x)|$

A Vector space V over the field $\mathbb{F}$ is a set such that:

- V is abelian under addition

- $\forall\, x, y \in V$ and $\forall\, a, b \in \mathbb{F}$
  - $a(x+y) = ax + ay$
  - $(a+b)x = ax + bx$
  - $(ab)x = a(bx)$
  - $1x = x$

A set of non-zero vectors $\{b_1 \dots b_n\}$ is a basis for V if:

- $\forall\, x \in V,\ \exists\, \{a_i\} \in \mathbb{F} : x = \sum_1^n a_i b_i$
- $\sum_1^n c_i b_i = 0 \rightarrow c_i = 0 \quad i \in \{1, \dots n\}$

Then number of elements in a basis is called the dimension of V.

A subset $U \subseteq V$ is called a subspace of V. if it is a vectorspace with respect to the addition and scalar multiplication of V.

If U is a subspace of V, then any basis of U can be extended to form a basis of V.

If $U_1 \dots U_n$ are subspaces of V, then

$$U_1 + U_2 \dots + U_n = \{u_1 + u_2 + \dots + u_n : u_i \in U_i\}$$

is also a subspace of V called the sum of the U_i. If every element of the sum can be written in a unique way, then the sum is called a direct sum, written

$$U_1 \oplus U_2 \dots \oplus U_n \qquad v \in V \quad v = \sum_1^n u_i$$

- For 2 subspaces $U + W$ is a direct sum iff $U \cap W = \{0\}$

- $U_1 + U_2 \dots + U_n$ is a direct sum iff $u_1 + u_2 \dots + u_n = 0 \longleftrightarrow u_i = 0$

If $U_1, \dots U_n$ are vector spaces over same field, the external direct sum is defined to be

$$V = \{ (u_1, u_2, \dots, u_n) : u_i \in U_i \}$$

and operations are done componentwise.

$u \in V$ $\quad \lambda u = (\lambda u_1, \lambda u_2 \dots)$

A linear transformation is a map $T: U \to V$ between vector spaces such that:

$T(x+y) = Tx + Ty \quad \forall x, y \in U.$

$\boxed{T(ax)} = aT(x), \quad a \in \mathbb{F}$

If $T: U \to U$, then it is called an endomorphism.

The set of all endomorphisms of U is denoted $\mathrm{End}(U)$ and is an algebra if multiplication is taken to be function composition.

An algebra is a vector space with a distributive product that respects scalar multiplication.

Given a basis in U, $\{b_1, b_2 \dots b_n\}$, if

$$T \in \mathrm{End}(U) \qquad \in U$$

$$\rightarrow T b_i = \sum c_{ij} b_j$$

$$\rightarrow [T] = [c_{ij}] = C$$

The set of invertable endomorphisms

space V is denoted

on a vector space V is denoted by $\underline{GL(V)} \simeq \underline{GL(n, \mathbb{F})}$.

If $T \in End(V)$, λ is said to be an eigenvalue of T if $\exists x \in V$ s.t. $x \neq 0$ and $\boxed{Tx = \lambda x}$

Projection

If $V = U_1 \oplus U_2 \oplus \dots \oplus U_n$,

define: $\pi_{U_i} : V \longrightarrow V$

by $\pi_{U_i} \underbrace{(u_1 + u_2 \dots + \overset{\overset{U_i}{\in}}{u_i} \dots + u_n)} = \underbrace{u_i}$

π_{U_i} is called the projection onto U_i.

$V = U_1 \oplus U_2$, $\operatorname{im} \pi_{U_1} = U_1$
$\ker \pi_{U_1} = U_2$

If $n = 2$, $\operatorname{im} \pi_{U_i} = U_i$ and $\ker \pi_{U_i} = U_j$ $j \neq i$

Any $T \in End(V)$ s.t. $T = T$ is also called a projection.

Thm: If π is a projection on V, then $V = \operatorname{im}\pi \oplus \ker\pi$.

$\to \quad v = \pi(v) + (v - \pi(v))$

$H \leq G \qquad [G : H] = 2$

H

$\operatorname{im}\pi_U = U \qquad V = U \oplus W$

$v \in V$

$v = u + w \qquad u \in U$

$w \in W$

$u \in U,$

$\pi(u+0) = u$

$u \in \pi(u)$

$v \in \operatorname{im} \pi_u \qquad s \notin U$

$v = s$

$\pi(u+w) = u$

$\pi(u) = u$

$\pi^2 = \pi$

$\operatorname{im} \pi_\mu = U$

$\ker \pi_\mu = W$

$v \in V \cancel{= U \oplus}$

$v = u + w$

$w \in W \qquad w = 0 + w$

$\pi(w) = 0$

$\in \ker \pi_\mu$

w

$v \in \ker \pi_u$

$v = 0 + \underbrace{w}$

$= w \in W$

$s, t \in V \Rightarrow s = u_1 + w_1$

$t = u_2 + w_2$

$\pi_u(s+t)$.

$= \pi(\underbrace{u_1 + u_2}_{u \in U} + \underbrace{w_1 + w_2}_{\to W})$

$= u = u_1 + u_2$

$= \pi(s) + \pi(t)$

$\pi(as) = \pi(au_1 + aw_1)$

$= au_1 = a\,\pi(s)$

$C_n = \mathbb{Z}_n$

$x \in \mathbb{Z}_n$

$Cl(x) = \{y \in \mathbb{Z}_n : \exists g \in \mathbb{Z}_n$

$\underbrace{y = gxg^{-1}}\}$

$y = \cancel{g}\cancel{g^{-1}}x$

ex

$y = x$

$Cl(x) = \{x\}$