Q9. $G = \mathbb{R} \setminus \{-1\}$.

Define operation $*$ on G by

$$a * b = a + b + ab$$

Is $a * b \in G$?

what if $a * b = a + b + ab = -1$?

$$\iff a(1+b) = -b-1.$$

$$\iff a = \frac{-(b+1)}{b+1}, \text{ since } b \neq -1$$

$$\iff a = -1.$$

So for $a, b \in G$, $a * b \in G$

So $*$ is a closed binary operation on G.

Is $*$ associative on G.

$$\begin{aligned} a * (b * c) &= a * (b + c + bc). \\ &= a + b + c + bc + a(b + c + bc) \\ &= a + b + c + bc + ab + ac + abc. \\ &= \underbrace{a + b + ab} + c + c(\underbrace{a + b + ab}) \\ &= (\underbrace{a + b + ab}) * c \\ &= (a * b) * c. \end{aligned}$$

So $*$ is associative on G.

The identity element for $*$ on G.

$e = 0$ since

$$a * 0 = a + 0 + a \cdot 0 = a$$

And given $a \in G = \mathbb{R} \setminus \{-1\}$, a^{-1} should be element satisfying

$$a * a^{-1} = e.$$

$$\Leftrightarrow \quad a + a^{-1} + a a^{-1} = 0$$

$$\Leftrightarrow \quad a^{-1}(1 + a) = -a.$$

$$\Leftrightarrow \quad \boxed{a^{-1} = \frac{-a}{1+a}}$$

since $a \neq -1$

and note $\dfrac{-a}{1+a} \in G$

So $(G, *)$ is a group.

Claim $G \cong \mathbb{R}^*$, the group of nonzero reals under regular multiplication.

Proof:

We need to define an isomorphism.

$$\phi : G = \mathbb{R} \setminus \{-1\} \to \mathbb{R}^* = \mathbb{R} \setminus \{0\}.$$

defined by

$$\phi(a) = \frac{a+1}{} ?$$

and then prove that

$$\phi(a * b) = \phi(a)\phi(b)$$

Note that this ϕ does map $0 \to 1$

which is $e_G \to e_{\mathbb{R}^*}$ ✓

Prove the homomorphism property for ϕ.

$$\phi(a*b) = \phi(a + b + ab)$$

$$= a + b + ab + 1$$

$$\Downarrow$$

$$= (a+1)(b+1) \quad ✓$$

$$= \phi(a)\phi(b)$$

So ϕ is indeed an isomorphism

and so $G \cong \mathbb{R}^*$

Q34 Automorphisms are isomorphisms of a group to itself.

Clearly $id : G \to G$
$g \mapsto g$
is an automorphism, but it's known as the trivial one.

What is interesting is whether or not there are non-trivial automorphisms

$$G \to G.$$

"i.e. symmetries of G"

Complex conjugation is a map

$\phi : \mathbb{C} \to \mathbb{C}$. $\quad (\mathbb{C}, +)$

$\phi(a+ib) = a - ib$

Claim ϕ is an automorphism $\mathbb{C} \to \mathbb{C}$

Q35 Claim " " " $\mathbb{C}^* \to \mathbb{C}^*$

$\mathbb{C}^* =$ gp of non-zero complex numbers under mult.

Proof: Firstly $\phi : \mathbb{C} \longrightarrow \mathbb{C}$,

or $\phi : \mathbb{C}^* \longrightarrow \mathbb{C}^*$

these are both bijections.

Hom. prop for $+$.

$$\boxed{\phi\big((a+ib)+(c+id)\big)}$$

$$= \phi\big((a+c)+i(b+d)\big)$$

$$= (a+c) - i(b+d)$$

$$= (a-ib)+(c-id)$$

$$= \boxed{\phi(a+ib)+\phi(c+id)}$$

Similarly, for mult.

$$\boxed{\phi\big((a+ib)(c+id)\big)}$$

$$= \phi\big((ac-bd)+i(ad+bc)\big)$$

$= (ac - bd) - i(ad + bc)$

$\Updownarrow$ ✓

$= (a - ib)(c - id)$.

$\boxed{= \phi(a + ib)\phi(c + id).}$

So ϕ is an automorphism of $\mathbb{C}$ and $\mathbb{C}^*$

"Special Linear group"

$\boxed{\text{Q36}}$ Consider $SL_2(\mathbb{R}) =$ gp of 2×2 real matrices with determinant 1.

Claim conjugation by B is an automorphism of $SL_2(\mathbb{R})$.

i.e. let B be a fixed matrix from $GL_2(\mathbb{R}) =$ gp of 2×2 matrices with non-zero determinant under mat. mult.

Claim $\phi(A) = B^{-1}AB$ is an automorphism of $SL_2(\mathbb{R})$.

Proof: So we need to show two things.

① Given $A \in SL_2(\mathbb{R})$, $\phi(A) = B^{-1}AB \in SL_2(\mathbb{R})$

② For $A_1, A_2 \in SL_2(\mathbb{R})$

$$\phi(A_1 A_2) = \phi(A_1)\phi(A_2).$$

①. Assume $A \in SL_2(\mathbb{R})$, i.e. $\det(A) = 1$.
and $B \in GL_2(\mathbb{R})$, $\det(B) \neq 0$.

Is $\phi(A) = B^{-1}AB \in SL_2(\mathbb{R})$?

$$\det(\phi(A)) = \det(B^{-1}AB)$$
$$= \det(B^{-1})\det(A)\det(B)$$

(since det is multiplicative i.e.
$\det(XY) = \det(X)\det(Y)$.)

$$= \frac{1}{\cancel{\det(B)}} \underline{\underline{\det(A)}} \cancel{\det(B)}.$$

$$= \det(A) = 1$$

$\Rightarrow \phi(A) \in SL_2(\mathbb{R})$.

So ϕ is a map $SL_2(\mathbb{R}) \rightarrow SL_2(\mathbb{R})$.

Is ϕ ~~is~~ a bijection? 1-1? onto?

Assuming $\phi(A_1) = \phi(A_2)$.

$$\Rightarrow B^{-1}A_1B = B^{-1}A_2B$$

$$\Rightarrow \cancel{B}(\cancel{B^{-1}}A_1\cancel{B})\cancel{B^{-1}} = \cancel{B}(\cancel{B^{-1}}A_2\cancel{B})\cancel{B^{-1}}$$

$$\Rightarrow A_1 = A_2.$$

So ϕ is 1-1 ✓.

To prove onto. Let $Y \in SL_2(\mathbb{R})$.

$$\phi(\overbrace{\underbrace{BYB^{-1}}_{\det = \cancel{Y}\ \det(Y) = 1.}}^{\in SL_2(\mathbb{R})}) = B^{-1}BYB^{-1}B = Y$$

So ϕ is onto ✓.

So $\phi : SL_2(\mathbb{R}) \to SL_2(\mathbb{R})$

is a bijection.

Finally to show ϕ satisfies the hom. prop.

$$\phi(A_1 A_2) = B^{-1} A_1 A_2 B$$

$$= B^{-1} A_1 \underbrace{B B^{-1}}_{= I} A_2 B$$

$$= \phi(A_1) \phi(A_2)$$

So ϕ does satisfy the hom. prop.

<u>Q37</u> $\operatorname{Aut}(G) = \{ \phi : G \to G : \phi \text{ is an automorphism} \}$

is a group under the operation of composition.

<u>Pf</u>: Composition of maps is always associative.

and if $\phi_1 : G \to G$, $\phi_2 : G \to G$ are isomorphisms. In lecture we proved $\phi_2 \circ \phi_1 : G \to G$

is an isomorphism too.

So $\mathrm{Aut}(G)$ is closed under op. of composition

The identity element of $\mathrm{Aut}(G)$ is

the automorphism given by the identity

map $id : G \to G$.

(see above).

and $\phi \circ id = id \circ \phi = \phi$.

We've already proved the result about

inverses ie. given an isomorphism

$\phi : G \to G$

the inverse map $\phi^{-1} : G \to G$

is also an isomorphism, ie. an

automorphism. and

$\phi \circ \phi^{-1} = id$.

So $\mathrm{Aut}(G)$ is a group (gp operation

is composition).

Aut(G) is the "symmetry group of G"

$\boxed{Q38}$ Find Aut$(\mathbb{Z}_6)$.

We should be able to list the automorphisms in Aut$(\mathbb{Z}_6)$.

$\mathbb{Z}_6$ = int. under addition modulo 6.

Clearly there is the identity automorphism.

$$id : \mathbb{Z}_6 \longrightarrow \mathbb{Z}_6$$

$$n \longmapsto n.$$

What other automorphisms might there be?

Note $\mathbb{Z}_6$ is a cyclic group, generated by 1. $\mathbb{Z}_6 = \langle 1 \rangle$.

From what we've proved about isos already we know that if $\phi : \mathbb{Z}_6 \to \mathbb{Z}_6$ is an iso then $\phi(1)$ must also be a generator.

So what are the options for $\phi(1)$?

What other generators does $\mathbb{Z}_6$ have?

$$\mathbb{Z}_6 = \langle 1 \rangle = \langle 5 \rangle$$

But $2, 3, 4$ are not generators of $\mathbb{Z}_6$

$\langle 2 \rangle = \{0, 2, 4\} = \langle 4 \rangle$, $\langle 3 \rangle = \{0, 3\}$

See theorem 4.13

for $m \in \mathbb{Z}_6$ $|m| = \frac{6}{d}$, $d = \gcd(m, 6)$.

$$\{0, 5, 4, 3, 2, 1\} = \langle 5 \rangle = \mathbb{Z}_6.$$

So there is only other automorphism of $\mathbb{Z}_6$, which is the map ϕ

satisfying

$$\begin{cases} \phi(1) = 5. \\ \phi(2) = 4 \\ \phi(3) = 3 \\ \phi(4) = 2 \\ \phi(5) = 1 \end{cases}$$

$5 \equiv -1 \mod 6$

$4 \equiv -2 \mod 6$

$3 \equiv -3 \mod 6$

So actually this ϕ is an

inverse of the general automorphism that every group G has.

$$G \longrightarrow G$$
$$x \longmapsto x^{-1}$$

So in conclusion $|Aut(\mathbb{Z}_6)| = 2$.

$Aut(\mathbb{Z}_6) = \{ id, \phi \}$

$\boxed{Q40}$

Firstly. If $G \cong H$. then $Aut(G) \cong Aut(H)$.

But the converse doesn't hold.

i.e. $Aut(G) \cong Aut(H) \not\Rightarrow G \cong H$.

Can we find a counter-example for this.

i.e. a pair G, H of non-isomorphic groups, but whose $Aut(G) \cong Aut(H)$.

$|Aut(\mathbb{Z}_6)| = 2$.

Not all groups of order 2 are isomorphic.

	e	x
e	e	x
x	x	e

Can we produce another group H that also has $|Aut(H)| = 2$.

think of $\mathbb{Z}_4 = \langle 1 \rangle = \langle 3 \rangle \neq \langle 2 \rangle$

So the same analysis as before goes through for $\mathbb{Z}_4$. $\mathbb{Z}_4$ has only two automorphisms.

$id : \mathbb{Z}_4 \to \mathbb{Z}_4$

$\phi : \mathbb{Z}_4 \to \mathbb{Z}_4$

$1 \to 3$

$2 \to 2$

$3 \to 1.$

So $|Aut(\mathbb{Z}_4)| = 2$

so $Aut(\mathbb{Z}_4) \cong Aut(\mathbb{Z}_6)$

But $\mathbb{Z}_4 \not\cong \mathbb{Z}_6$.

$|\mathbb{Z}_4| = 4 \neq 6 = |\mathbb{Z}_6|$

Q47 If $\boxed{G \cong \overline{G} \text{ and } H \cong \overline{H}}$

then claim: $G \times H \cong \overline{G} \times \overline{H}$

Proof: What's the isomophism.

So there exist two isomorphisms

$\mu : G \to \overline{G}$, $\lambda : H \to \overline{H}$

$$\phi : G \times H \longrightarrow \overline{G} \times \overline{H}$$

defined by

$$\phi((g, h)) = (\mu(g), \lambda(h))$$

ϕ is a bijection since both μ and λ are. (details as an exercise).

Does ϕ satisfy the hom. prop?

$$\phi\big((g_1,h_1)(g_2,h_2)\big)$$

$$= \phi\big((g_1 g_2, h_1 h_2)\big)$$

$$= \big(\mu(g_1 g_2), \lambda(h_1 h_2)\big), \quad \text{def of } \phi.$$

$$= \big(\mu(g_1)\mu(g_2), \lambda(h_1)\lambda(h_2)\big), \quad \text{hom. prop for } \mu, \lambda.$$

$$= \big(\mu(g_1), \lambda(h_1)\big)\big(\mu(g_2), \lambda(h_2)\big).$$

$$= \phi\big((g_1,h_1)\big)\,\phi\big((g_2,h_2)\big)$$

So $G \times H \cong \overline{G} \times \overline{H}$

$\boxed{\text{Q48}}$ Claim: $G \times H \cong H \times G$.

Well define an isomorphism.

$$\phi : G \times H \to H \times G.$$

$$\phi\big((g,h)\big) = (h,g)$$

- ϕ is a bijection
- ϕ satisfies the hom. prop

$\boxed{Q50}$ Claim: $A \times B$ is abelian

$\iff$ A, B are abelian.

$\underline{\text{Proof}}$: $A \times B$ is abelian

$\iff \forall\ x, y \in A \times B$, $xy = yx$.

$\iff \forall\ (a_1, b_1), (a_2, b_2) \in A \times B$

$$(a_1, b_1)(a_2, b_2) = (a_2, b_2)(a_1, b_1).$$

$\iff \forall\ a_1, a_2 \in A\ \forall\ b_1, b_2 \in B.$

$$(\boxed{a_1 a_2}, \boxed{b_1 b_2}) = (\boxed{a_2 a_1}, \boxed{b_2 b_1})$$

$\iff \forall\ a_1, a_2 \in A\ \forall\ b_1, b_2 \in B$

$a_1 a_2 = a_2 a_1$ & $b_1 b_2 = b_2 b_1$

$\iff$ A is abelian & B is abelian.

Euler's theorem.

Remember if

$$\gcd(a, m) = 1$$

then.

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

$$a^0 \to a^1 \to a^2 \to a^3 \to \cdots \to a^0$$

So this means the cycle length of this divides m.

$$a^{\sim\sim\sim\sim} \equiv ?$$

$$\sim\sim\sim\sim = q \cdot \phi(m) + r.$$

$$a^{q\phi(m)+r}$$

$$= a^{q\phi(m)} \, a^{r}$$

$$= \left(a^{\phi(m)}\right)^{q} a^{r}$$

$$\|$$

$$1 \quad \equiv a^{r}.$$