"Also problems 7.4 #1 & 4" (corrected in class from 7.3)

#1a show $f: \mathbb{R} \to \mathbb{R}$ (given it is a function) given by $f(x) = 3x$ is an isomorphism of additive groups

- Check that it is a homomorphism (additive)

$$f(x+y) = 3(x+y) = 3x+3y = f(x)+f(y)$$

- Check that it is onto:

Let $y \in \mathbb{R}$.

then $y/3 \in \mathbb{R}$ and $f(y/3) = 3(y/3) = y$

so f is onto.

- Check that it is 1-1:

Let $a, b \in \mathbb{R}$.

Suppose $f(a) = f(b)$

$\Rightarrow \quad 3a = 3b$

$\Rightarrow \quad \frac{3a}{3} = \frac{3b}{3}$

$\Rightarrow a = b$ so f is 1-1.

This f is an isomorphism.

7.4 16.

Show $f: \mathbb{R}^{**} \longrightarrow \mathbb{R}^{**}$ is <u>not</u> a homomorphism of the multiplicative group $\mathbb{R}^{**}$ (positive reals)

- $2, 3 \in \mathbb{R}^{**}$

  $f(2 \cdot 3) = f(6) = 3 \cdot 6 = 18$

  $f(2) \cdot f(3) = (3 \cdot 2) \cdot (3 \cdot 3) = 6 \cdot 9 = 54$

  f does not preserve multiplication so it is not an isomorphism (or even a homomorphism) on $\mathbb{R}^{**}$

7.4 #4

Prove $f: \mathbb{R}^* \to \mathbb{R}^*$ (the function (given)) defined by $f(x) = x^3$ is an isomorphism

$\mathbb{R}^*$ = non-zero reals with multiplication.

- show homomorphism:

  Let $a, b \in \mathbb{R}^*$

  $f(a \cdot b) = (ab)^3 = a^3 \cdot b^3 = f(a) f(b)$

- show onto:

  Let $y \in \mathbb{R}^*$. then $\sqrt[3]{y} \in \mathbb{R}$ and

  $f(\sqrt[3]{y}) = (\sqrt[3]{y})^3 = y$ so f is onto.

- show 1-1:

  Let $a, b \in \mathbb{R}^*$.

  Suppose $f(a) = f(b)$

  $\Rightarrow a^3 = b^3$

  $\Rightarrow (a^3)^{1/3} = (b^3)^{1/3}$

  $\Rightarrow a = b$ so f is 1-1

Some group theorems you should be able to prove:

Thm 7.1 Every ring is an abelian group under addition.

Let R be a ring:

then R is closed under addition.
It has an additive identity 0.
Every element (a) has an additive inverse $(-a)$
addition is associative

Therefore $R, +$ is a group

Addition in R is commutative
therefore $R, +$ is an abelian group.

7.2 The non-zero elements F^* of a field F form an abelian group under multiplication

F is a ring, ~~so it is closed under multiplicati~~
—: multiplication is associative

F also has a multiplicative identity, 1, and every non-zero element (a) has a multiplicative inverse, so every element in F^* has a multiplicative inverse.

Every element in F^* is a unit, and units are never zero-divisors, so if $a, b \in F^*$, then

$ab \in F$ (because F is closed under multiplicat)
and $ab \neq 0$ (because a, b are not zero divisors)
so $ab \in F^*$, so F^* is closed under multiplicat

F is a commutative ring, so F^* is an abelian group ($ab = ba$).

7.5. Let G be a group, and $a, b, c \in G$, then

(1.) G has a unique identity.

(2.) cancellation holds: if $ab = ac$ then $b = c$. and if $ba = ca$ then $b = c$.

(3.) Each element of G has a unique inverse

Proof of (1): by definition, G has an identity element e. ← tell why there is one

Suppose it also has an element e' such that ← Suppose there are two

$e'a = ae' = a$ for all $a \in G$.

then $e \cdot e' = e'$ because e is an identity

and $e \cdot e' = e$ because e' is an identity

Prove they are really the same → so $e = e'$, so the identity element is unique.

Proof of (2). Let $ab = ac$

by defn. of group, there is an element $d \in G$ such that $ad = da = e$.

$ab = ac$

$\Rightarrow d(ab) = d(ac)$

$\Rightarrow (da)b = (da)c$

$\Rightarrow eb = ec$

$\Rightarrow b = c$

Similarly, if

$ba = ca$

$\Rightarrow (ba)d = (ca)d$

$\Rightarrow b(ad) = c(ad)$

$\Rightarrow be = ce$

$\Rightarrow b = c$.

7.5 proof of (3).

tell why there's one

Let $a \in G$, (inverse)

by def. of group, there is an element $d \in G$ such that

$ad = da = e$.

Suppose there is also $f \in G$ such that

Suppose there are two

$af = fa = e$

Then $(fa)d = f(ad) = fe = f$

and $(fa)d = ed = d$

So $f = d$ ← prove they are really the same

So a has a unique inverse

Hence every element of G has a unique inverse

Cor. 7.6

If G is a group and $a, b \in G$ then

(1) $(ab)^{-1} = b^{-1}a^{-1}$

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

---

proof of (1)

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$$

$$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$$

so $b^{-1}a^{-1}$ is an inverse of ab, and by thm 7.5, it is unique, so $(b^{-1}a^{-1}) = (ab)^{-1}$

proof of (2)

$(a^{-1})^{-1} \cdot a^{-1} = e$ and $a^{-1}(a^{-1})^{-1} = e$ by defn. of $(a^{-1})^{-1}$

also $a \cdot a^{-1} = e$ and $a^{-1} \cdot a = e$ by defn of a^{-1}.

start with the definition

end with one of these

- so a is an inverse of a^{-1} and $(a^{-1})^{-1}$ is an inverse of a^{-1}, so by thm 7.5 (uniqueness) $a = (a^{-1})^{-1}$

or

- so $(a^{-1})^{-1} \cdot a^{-1} = a \cdot a^{-1}$ and by cancellation (thm. 7.5)

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

7.14. If G is a group, and $a \in G$, then $\langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.

Note these definitions:

if $n > 0$ then $a^n = \underbrace{a \cdot a \cdot a \cdots a}_{n \text{ times}}$

if $n = 0$ then $a^n = a^0 = e$ ← or 1 or whatever you're calling the identity

if $n < 0$ then $a^n = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{|n| \text{ times}}$

Proof: Let $a^i, a^j \in \langle a \rangle$

then $a^i \cdot a^j = a^{i+j}$ ⟶

so $\langle a \rangle$ is closed.

If $i \in \mathbb{Z}$, then $-i \in \mathbb{Z}$, so $a^{-i} \in \langle a \rangle$

and $a^i \cdot a^{-i} = a^{-i} \cdot a^i = e$

so inverses are in $\langle a \rangle$

$a^0 = e \in \langle a \rangle$

so $\langle a \rangle$ is a group

(and since $\langle a \rangle \leq G$

$\langle a \rangle$ is a subgroup of G)

To do this justice, we should do a bunch of cases, like $i, j > 0$; $i = 0$; $i, j < 0$; $i < 0, j > 0$, $|i| > |j|$ etc.

I might conceivably ask you to do one. For instance

$i < 0, j > 0, |i| > |j|$

then $a^i \cdot a^j = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{|i| \text{ times}} \cdot \underbrace{a \cdot a \cdots a}_{j \text{ times}}$

$= \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{|i|-j \text{ times}} \left(\underbrace{a^{-1} a^{-1} \cdots a^{-1}}_{j \text{ times}} \cdot \underbrace{a \cdot a \cdots a}_{j \text{ time}} \right)$

$= \underbrace{a^{-1} \cdots a^{-1}}_{|i|-j \text{ times}} \cdot e = a^{i+j}$

$|i| - j = i + j$