Survey HW 6

Sankalpa Banjade nxr8dq

October 2023

1 Introduction

1.1 Problems: 13.3.1, 13.3.4, 14.2.1, 14.2.2, 14.2.5, 15.4.1, 15.4.4.

13.3.1 **Proof**: Let R be a ring. We consider the set $R^\times$ which consists of all invertible elements of R under multiplication.

Definition: An element a in R is called *invertible* if there exists an element b in R such that

$$a \cdot b = b \cdot a = e,$$

where e is the multiplicative identity in R.

To prove that $R^\times$ forms a group under multiplication, we need to verify the four group axioms:

1. **Closure**: Let a, b be elements in $R^\times$. Then there exist a^{-1} and b^{-1} in R such such that

$$a \cdot a^{-1} = e$$

and

$$b \cdot b^{-1} = e.$$

Considering the product $(a \cdot b) \cdot (b^{-1} \cdot a^{-1})$, we have:

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e.$$

Hence, $b^{-1} \cdot a^{-1}$ is the inverse of $a \cdot b$, which means $a \cdot b$ is in $R^\times$. Therefore, $R^\times$ is closed under multiplication.

2. **Identity**: The multiplicative identity e of R is also in $R^\times$, because $e \cdot e = e$. In this case, e will be 1, and 1 is in $R^\times$ because the inverse of 1 is 1.

3. **Invertibility**: By the definition of $R^\times$, for every a in $R^\times$, there exists a^{-1} in $R^\times$ such that

$$a \cdot a^{-1} = e.$$

4. **Associativity**: This property is inherited from the ring R. For any a, b, c in $R^\times$, we have:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Hence, the set $R^\times$ with multiplication forms a group.

13.3.4 **Proof**:

Let $G = \mathbb{R} \setminus \{1\}$ be the set of real numbers different from 1, and define a binary operation $*$ on G by

$$x * y = x + y - xy.$$

Prove that $(G, *)$ is a group. Consider two numbers x and y in $\mathbb{R}$, the set of real numbers. We define a binary operation $*$ on $\mathbb{R}$ by

$$x * y = x + y - xy.$$

To ascertain that this operation equips $\mathbb{R}$ with a group structure, we must verify the following group axioms:

To show that the operation $*$ defined by

$$x * y = x + y - xy$$

on a set G forms a group, we need to verify the group axioms:

1. **Closure:** If G is the set of real numbers different from 1, then $x * y = x + y - xy$ always yields another real number different from 1. Therefore, the operation is closed on G. We proceed by contradiction. Assume that the operation can result in 1 even when neither of its arguments are 1, where both x and y are real numbers different from 1.

   Starting with the equation:

   $$x + y - xy = 1$$

   Add the additive inverse of x to both sides:

   $$(-x) + x + y - xy = 1 + (-x)$$

   By the property of additive inverses, this becomes:

   $$y - xy = 1 - x$$

   Using the distributive property, we can factor out y:

   $$y(1 - x) = 1 - x$$

   Since $x \in G$, it follows that $x \neq 1$. Thus, we may cancel, giving

   $$y = 1.$$

   But as $y \in G$, y cannot be 1, giving a contradiction. So, it must be the case that $x * y \neq 1$, and thus, $x * y \in G$.

2. **Associativity:** For $x, y, z \in G$, we need to show that $(x*y)*z = x*(y*z)$:

$$\begin{aligned}(x * y) * z &= (x + y - xy) * z \\ &= x + y + z - xy - xz - yz + xyz \\ x * (y * z) &= x * (y + z - yz) \\ &= x + y + z - yz - xy - xz + xyz\end{aligned}$$

   Both expressions are equal, thus the operation is associative.

3. **Identity:** For an identity element $e \in G$, we need:

$$x * e = x$$

   Substituting the operation we get:

$$x + e - xe = x$$

   From which we infer:

$$e = 0$$

   Thus, 0 is the identity element for G.

4. **Invertibility:** For each $x \in G$, we need to find an inverse x^{-1} such that:

$$x * x^{-1} = 0$$

   This gives:

$$x + x^{-1} - xx^{-1} = 0$$

   From which we deduce:

$$x^{-1} = \frac{x}{x - 1}$$

   Therefore, every element x in G has an inverse in G.

Based on the above, the set of real numbers different from 1 with the operation $x*y = x+y-xy$ forms a group. The proof for invertibility would commence by finding the inverse of an element with respect to the defined operation.

14.2.1 Show that the following are equivalent:

1. $(x * y)^n = x^n * y^n$ for all $x, y \in G$ and $n \in \mathbb{Z}$;
2. $(x * y)^{-1} = x^{-1} * y^{-1}$ for all $x, y \in G$;
3. G is an abelian group, i.e., $x * y = y * x$ for all $x, y \in G$.

Proof:

To show that the statements are equivalent, we will demonstrate the implications: (1) implies (2), (2) implies (3), and (3) implies (1).

1. **(1 implies 2):** Given (1)

$$(x * y)^n = x^n * y^n,$$

if we let $n = -1$, we get

$$(x * y)^{-1} = x^{-1} * y^{-1},$$

proving statement (2).

2. **(2 implies 3):** Assuming (2)

$$(x * y)^{-1} = x^{-1} * y^{-1},$$

to show G is abelian, we want $x * y = y * x$. Using the inverse property and the given:

$$\begin{aligned} e &= (x * y) * (x^{-1} * y^{-1}) \\ &= x * (y * x^{-1}) * y^{-1}, \end{aligned}$$

which implies that

$$x * y = y * x.$$

Thus, G is abelian, proving statement (3).

3. **(3 implies 1):** Given (3) that G is abelian, for positive n:

$$(x * y)^n = x^n * y^n.$$

Given that G is abelian, and let $x, y \in G$. We wish to show $(xy)^n = x^n y^n$ for all $n \in \mathbb{Z}$. We will split into two cases: when $n \geq 0$ and when $n < 0$.

First, consider when $n \geq 0$. We proceed by induction.

For $n = 0$, observe that

$$(xy)^0 = e = e \cdot e = x^0 y^0$$

as desired.

Now, suppose for some $n \in \mathbb{Z}$ with $n \geq 0$, $(xy)^n = x^n y^n$. Observe that

$$\begin{aligned} (xy)^{n+1} &= (xy) \cdot (xy)^n \\ &= (xy) \cdot (x^n y^n) \text{ by the inductive hypothesis} \\ &= (yx) \cdot (x^n y^n) \text{ as } G \text{ is abelian} \\ &= y(x \cdot x^n) y^n \\ &= y x^{n+1} y^n \\ &= x^{n+1} (y \cdot y^n) \\ &= x^{n+1} y^{n+1} \end{aligned}$$

as desired. For the case in which n is negative, we can induct in the negative direction, i.e., for $1 - n$, and the proof for when n is less than 0 becomes analogous to this proof.

Having shown each implication, it follows that the three statements are equivalent.

14.2.2

Let G be a group, and suppose that $x^{-1} = x$ for all $x \in G$. Prove that G is abelian. **Proof:**

Let G be a group, and assume that for all $x \in G$, $x^{-1} = x$. We aim to show that G is abelian.

For any two elements $x, y \in G$, we will evaluate their product in two different orders:

1. The product xy
2. The product yx

To show that G is abelian, we need to prove $xy = yx$.

Given the property $x^{-1} = x$ and $y^{-1} = y$, we can manipulate the product xy:

$$\begin{aligned} x(xy)y &= x^2yy \\ &= x^2y^2 \\ &= e \end{aligned}$$

Similarly, for yx:

$$\begin{aligned} y(yx)x &= y^2xx \\ &= y^2x^2 \\ &= e \end{aligned}$$

Since the identity element in a group is unique, it implies $xy = yx$.

Thus, G is abelian.

14.2.5 Review this Let G be a finite set with a binary operation $*$ such that it respects $(G1)$, $(G2)$, and the cancellation law. That is, if $a \cdot x = a \cdot y$ then $x = y$ for all $a, x, y \in G$. Prove that G satisfies $(G3)$ and is thus a group. Is this true without the assumption that G is finite?

Let $g \in G$ and consider the transformation f that maps G to G such that $f(h) = g * h$. Now, suppose $f(h) = f(j)$ for some $h, j \in G$. By the definition of the map, we have $g*h = g*j$. Since the transformation satisfies the cancellation law, it follows that $h = j$. Thus, f can be considered an injection on G. Since we consider G to be finite in this case and that the cardinality of G is equal to itself, it follows that f must also be surjective. Hence, there exists some $g_R \in G$ such that $f(g_R) = g * g_R = e$.

We can observe that

$$g_R = e * g_R = (g_L * g) * g_R = g_L * (g * g_R) = g_L * g = g_L,$$

and thus, for each $g \in G$, there exists some $g^{-1} \in G$ satisfying both $g^{-1} * g = e$ and $g * g^{-1} = e$. Namely, $g^{-1} = g_L = g_R$. Thus, G satisfies $(G3)$, and G is a group.

This does not necessarily hold without the assumption that G is finite, as an injection from an infinite set to another infinite set of the same cardinality is not required to be surjective. This can be observed by considering the natural numbers. Note that $\mathbb{N}$ satisfies $(G1)$, $(G2)$, and the cancellation law, but no $n \in \mathbb{N}$ has an inverse also in $\mathbb{N}$, and thus $\mathbb{N}$ is not a group.

15.4.1

Multiplication table for the group of symmetries of an equilateral triangle, D_3:

$\cdot$	e	r	r^2	f	rf	fr
e	e	r	r^2	f	rf	fr
r	r	r^2	e	rf	fr	f
r^2	r^2	e	r	fr	f	rf
f	f	fr	rf	e	r	r^2
rf	rf	f	fr	r^2	e	r
fr	fr	rf	f	r	r^2	e

15.4.4

For each of the following groups, write out its multiplication table, and determine whether it is cyclic. If it is cyclic, give a generator; if it is not, explain why not.

1. $(\mathbb{Z}/(7))^\times$ Multiplication table for $\mathbb{Z}/7\mathbb{Z}$:

$\times$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

This group is cyclic as 3 is the generator. The powers of 3 modulo 7 are:

$$3^1 = 3$$
$$3^2 = 2$$
$$3^3 = 6$$
$$3^4 = 4$$
$$3^5 = 5$$
$$3^6 = 1$$

2. $(\mathbb{Z}/(9))^\times$ Multiplication table for $\mathbb{Z}/9\mathbb{Z}$:

$\times$	[1]	[2]	[4]	[5]	[7]	[8]
[1]	[1]	[2]	[4]	[5]	[7]	[8]
[2]	[2]	[4]	[8]	[1]	[5]	[7]
[4]	[4]	[8]	[7]	[2]	[1]	[5]
[5]	[5]	[1]	[2]	[7]	[8]	[4]
[7]	[7]	[5]	[1]	[8]	[4]	[2]
[8]	[8]	[7]	[5]	[4]	[2]	[1]

This group is cyclic for 5 as the generator. The powers of 5 modulo 9 are:

$$5^1 = 5$$
$$5^2 = 7$$
$$5^3 = 8$$
$$5^4 = 4$$
$$5^5 = 2$$
$$5^6 = 1$$

$(\mathbb{Z}/(12))^\times$ Multiplication table $\mathbb{Z}/9\mathbb{Z}$:

$\times$	[1]	[5]	[7]	[11]
[1]	[1]	[5]	[7]	[11]
[5]	[5]	[1]	[11]	[7]
[7]	[7]	[11]	[1]	[5]
[11]	[11]	[7]	[5]	[1]

Not cyclic as every element has itself as an inverse, so when trying any number you would just get a loop with 1. Hence there is no generator ie 1's across the diagonal.