

# Final Practice

Trustin Nguyen

May 10, 2023

## Final Practice

**Exercise 1:** Suppose  $G$  is a group and  $H = \{g^2 : g \in G\}$ . For each of the following statements, give a proof or a counter-example:

1. If  $G$  is abelian,  $H$  is a subgroup of  $G$ .

*Proof.* Suppose  $G$  is abelian. Then we have that for  $g_1, g_2 \in G$ ,  $g_1 g_2 = g_2 g_1$ . Clearly,  $H$  contains  $e$  since  $e \in G$ . Now to prove that  $H$  is closed under the operation, take two arbitrary elements of  $H$  called  $g_1^2, g_2^2$ :

$$\begin{aligned} g_1^2 g_2^2 &= g_1 g_2 g_1 g_2 \\ &= (g_1 g_2)^2 \end{aligned}$$

which is in  $G$  as  $g_1 g_2 \in G$ . Now associative property is inherited from  $G$ . So  $H$  is a subgroup and a subset of  $G$ . Therefore,  $H \leq G$ .  $\square$

2. If  $G$  is finite and its order is odd, then  $H = G$ .

*Proof.* We can look at what happens in the mapping

$$\begin{aligned} \varphi : G &\rightarrow G \\ \varphi : g &\mapsto g^2 \end{aligned}$$

We can either try to prove injectivity or surjectivity. Injectivity might be harder because we cannot simply say that  $\ker \varphi = \{e\}$  as  $H$  might not be a subgroup of  $G$  and this therefore might not be a group homomorphism. So we try surjectivity. Take an arbitrary  $g \in G$  and observe that we can write it as an element of greater order:

$$\begin{aligned} g^{|G|+1} &= g \\ (g^{(|G|+1)/2})^2 &= g \end{aligned}$$

which is a construction of  $g$  as an element of  $k \in G$  such that  $k^2 = g$ .  $\square$

3. If  $n \geq 4$  and  $G = S_n$ , then  $H = G$ .

*Proof.* This is not true. We observe that if we take the mapping

$$\begin{aligned} \varphi : G &\rightarrow G \\ \varphi &:= g \mapsto g^2 \end{aligned}$$

Then this mapping is not injective, as we have elements of order 2 in  $S_n$ . This tells us that the image cannot be all of  $G$ .  $\square$

4. If  $G = D_{2n}$ , then  $H$  is a subgroup of  $G$ .

*Proof.* This is true. We use the definition of  $D_{2n}$ :

$$D_{2n} = \{s^k r^j : s^2 = e, r^n = e, sr^i s^{-1} = r^{-i}\}$$

and we check what elements are in  $H$ . We have that the elements of the form  $sr^j$  gets mapped to the identity as

$$sr^j \mapsto sr^j sr^j = r^{-j} r^j = e$$

Now for elements of the form  $r^j$ . Since these form a cyclic group which is abelian, the action forms a subgroup of  $G$  by part (1). So the elements of the group are just the image of the homomorphism

$$\varphi : \langle r \rangle \rightarrow G$$

$$\varphi := r \mapsto r^2$$

and the image is a subgroup of  $G$ . □

**Exercise 2:** Let  $f(x) = x^3 + x^2 + x + 1 \in \mathbb{Z}/2\mathbb{Z}[x]$  and  $R = \mathbb{Z}/2\mathbb{Z}[x]/(f)$ .

1. Is  $f$  irreducible? Give a proof or factorize  $f$  into irreducibles.

*Proof.* This is not irreducible because we can rewrite  $f$  as

$$f(x) = x^3 - x^2 + x - 1$$

which factors as

$$f(x) = x^2(x - 1) + 1(x - 1) = (x^2 + 1)(x - 1)$$

□

2. How many elements are there in  $R$ ?

*Proof.* We know that the elements of  $R$  must have degree less than or equal to 3 so

$$p(x) = a_0 + a_1x + a_2x^2$$

Where  $a_i = 0, 1$ . Therefore,  $|R| = 2^3 = 8$ . □

3. Are there any nilpotent elements in  $R$ ? If so, write them all down.

*Proof.* By the previous idea, we get all elements that have the factor  $(x - 1), (x + 1)$ :

$$\text{nil}(R) = (f), (f) + (x + 1), (f) + (x + 1)^2 = (f) + x^2 + 1, (f) + x(x + 1)$$

□

**Exercise 3:** What are the cycle shapes of elements of order 3 in  $S_9$ ? How many elements of order 3 are there in  $S_9$ ? What is the greatest order of an element of  $A_9$ ?

*Proof.* We can write the elements of  $S_9$  as a product of disjoint cycles. The order of these elements is the least common multiple of the sizes of these cycles. So we must have that the lcm is 3. Therefore, we have the cycle shapes as  $(3, 3, 3), (3, 3)$ , or  $(3)$ . Now we count the number of

such elements with those cycles types:

	$(3, 3, 3)$	$(3, 3)$	$(3)$
Count	$\binom{9}{3} \binom{6}{3} \binom{3}{3} (2)^3$	$\binom{9}{3} \binom{6}{3} (2)^2$	$\binom{9}{3} (2)^1$

The process:

- We choose three elements to go in the first cycle:  $\binom{9}{3}$
- We choose three elements to go in the second cycle:  $\binom{6}{3}$
- We choose three elements to go in the third cycle:  $\binom{3}{3}$
- We permute the elements in each cycle:  $2^3$
- The cycles are disjoint, so now we divide by the number of ways to permute the cycles:  $3!$

To check the element of greatest order in  $A_9$ , we go by cases:

- We have a cycle of order 9 in disjoint cycle notation. The order is 9, certainly not the greatest.
- We have a cycle of order 8. Then the element must have order 8.
- We have a cycle of order 7. Then we can have a cycle of order 2. So the cycle order is max of 14.
- We have a cycle of order 6. Then we can have a cycle of not order 3, not 2, and not 1. The max order is 6.
- We have a cycle of order 5. Then the element can also have a cycle of order 4, 3 and 1, or 2 and 2. the largest order is 20.

Since we have covered all possible cycle types or at least the ones that will yield the maximum order, the greatest order in  $A_9$  is 15.  $\square$

**Exercise 4:** Is 11 irreducible in  $\mathbb{Z}[\sqrt{-3}]$ ?

*Proof.* We use the norm function to find out:

$$N := a + b\sqrt{-3} \mapsto (a + b\sqrt{-3})(a - b\sqrt{-3})$$

So we have

$$N(11) = N(g_1)N(g_2)$$

for some  $a, b \in \mathbb{Z}[\sqrt{-3}]$ . So we require that for  $g_1 = a + b\sqrt{-3}$ ,  $g_2 = c + d\sqrt{-3}$ ,

$$121 = (a^2 + 3b^2)(c^2 + 3d^2) = a^2c^2 + 3(b^2c^2 + a^2d^2) + 9c^2d^2$$

$\square$

**Exercise 5:** Determine if  $f(x) = 2x^3 + 19x^2 - 54x + 3$  is irreducible over  $\mathbb{Q}$ .

*Proof.* We can make a change of variables:

$$p(x+1) = 2x^3 + 25x^2 - 10x - 30$$

and confirm that  $p = 5$  is prime in  $\mathbb{Z}$ . Using Eisenstein's criterion, we conclude that the polynomial is irreducible in  $\mathbb{Q}$ .  $\square$

**Exercise 6:** If every proper subgroup of a group  $G$  is cyclic, does it follow that  $G$  is abelian?

*Proof.* This is not true. Take the group  $D_8$  which has cyclic subgroups:

$$\begin{aligned} &\{e, r, r^2, r^3\} \\ &\{e, r^2\} \\ &\{e, sr\} \\ &\{e, sr^2\} \\ &\{e, sr^3\} \\ &\{e, s\} \end{aligned}$$

□

**Exercise 7:** If  $G$  has order 33, prove that  $G$  is cyclic.

*Proof.* Observe that since  $\gcd(3, 11) = 1$ , we have that

$$C_3 \times C_{11} \cong C_{33}$$

that is if  $G$  has proper subgroups, as they must divide the order of  $G$ . If  $G$  has no proper subgroups, then it is also cyclic. □

**Exercise 8:** Find the order and sign of  $(1\ 3)(2\ 4\ 5\ 7)(8\ 1\ 5) \in S_8$ .

*Proof.* The element written in disjoint cycle notation is

$$(1\ 7\ 2\ 4\ 5\ 8\ 3)$$

So we see that there are 7 elements that are changed in the cycle. The cycle shape is 7 so the order is 7. The sign is 1 since there is an even number of even cycles. □

**Exercise 9:** Show that  $\mathbb{Z}[\sqrt{-13}]$  is not a PID.

*Proof.* We can take the ideal:  $(2, 1 + \sqrt{-13})$ . Now we have that neither 2 nor  $1 + \sqrt{-13}$  are units and they are both irreducibles, since if

$$\begin{aligned} 4 &= (a^2 + 13b^2)(c^2 + 13d^2) \\ 14 &= (a^2 + 13b^2)(c^2 + 13d^2) \end{aligned}$$

Then we must have that  $b, d = 0$  for the first equation and either  $a, c$  to be 1. So 2 is irreducible. We see the same in 14 as if  $b, d \neq 1$ , then we must have that the two factors are 2 and 7, which is impossible as 7 is not a perfect square. So we also conclude that 2 does not divide  $1 + \sqrt{-13}$  nor the other way around as none of the factors of 2 divide that of  $1 + \sqrt{-13}$  and vice versa. Finally, we note that the whole ring is not generated, as 3 is not in the ideal. If it were, we would have

$$\begin{aligned} 3 &= 2(a + b\sqrt{-13}) + (1 + \sqrt{-13})(c + d\sqrt{-13}) \\ &= 2a + 2b\sqrt{-13} + c - 13d + (c + d)\sqrt{-13} \\ &= 2a + c - 13d + (2b + c + d)\sqrt{-13} \\ 9 &= (2a + c - 13d)^2 + 13(2b + c + d)^2 \end{aligned}$$

So we have a system of equations:

$$\begin{aligned} 2a + c - 13d &= \pm 3 & 2a + c - 13d &= \pm 3 \\ 2b + c + d &= 0 & d &= 2b - c \\ 2a + c - 13(2b - c) &= \pm 3 \\ 2a + 14c - 26b &= \pm 3 \end{aligned}$$

| Which is impossible as the left hand side is even and the right hand side is odd. □

**Exercise 10:** Find all integers  $x$  and  $y$  such that  $x^2 + 4 = y^3$ .

| *Proof.* □