

## **Final Exam**

ALECK ZHAO

December 10, 2016

1. (20 points) Let  $G$  be a group of order 6.

(a) (5 points) How many 3-Sylow subgroups are there in  $G$ ?

*Solution.* We have  $|G| = 3^1 \cdot 2$ . By Sylow's Third Theorem, we have

$$\begin{aligned} n_3 &\equiv 1 \pmod{3} \\ n_3 &\mid 2 \end{aligned}$$

From the second condition, we must have either  $n_3 = 1$  or  $n_3 = 2$ . Only  $n_3 = 1$  satisfies the first condition, so there is exactly  $\boxed{1}$  3-Sylow subgroup in  $G$ .  $\square$

(b) (5 points) Show that  $G$  contains at least one subgroup of order 2.

*Proof.* Since  $|G| = 2^1 \cdot 3$ , by Sylow's First Theorem,  $G$  contains a subgroup of order  $2^1 = 2$ , as desired.  $\square$

Assume, for the remaining part of the exercise, that  $G$  is not cyclic.

(c) (5 points) Let  $H$  be a subgroup of  $G$  of order 2. Consider the set  $\Omega = \{aH \mid a \in G\}$  of left cosets of  $H$  in  $G$ .  $G$  acts on  $\Omega$  as follows:

$$G \times \Omega \rightarrow \Omega, \quad (g, aH) \mapsto gaH, \quad \forall g \in G, \forall a \in G$$

Determine the cardinality  $|\Omega|$  of  $\Omega$ .

*Solution.* We have

$$|G : H| = \frac{|G|}{|H|} = \frac{6}{2} = 3$$

and  $|G : H|$  counts the number of cosets of  $H$  in  $G$ , which is exactly  $|\Omega|$ .  $\square$

(d) (5 points) Let

$$\varphi : G \rightarrow S_{|\Omega|}, \quad \varphi(g)(aH) = gaH$$

be the group homomorphism of  $G$  into the group of permutations of  $\Omega$ . Determine  $\ker(\varphi)$ .

*Solution.* Since  $|G| = 2^1 \cdot 3$  and  $H$  is a Sylow 2-subgroup, by Sylow's Third Theorem, we have the following:

$$\begin{aligned} n_2 &\equiv 1 \pmod{2} \\ n_2 &\mid 3 \\ n_2 &= |G : N(H)| \end{aligned}$$

Since  $G$  is not commutative, it follows that  $N(H) \neq G$ , so  $n_2 \neq 1$ . Thus, it must be that  $n_2 = 3$  to satisfy the first 2 equations, so there are 3 unique Sylow 2-subgroups.

If  $g \in \ker(\varphi)$ , then

$$\varphi(g)(aH) = aH \implies (ga)H = aH, \quad \forall a \in G$$

Since these are cosets, we must have

$$a^{-1}ga \in H \implies g \in aHa^{-1}, \quad \forall a \in G$$

Since there are three unique Sylow 2-subgroups that are all conjugates of  $H$ , the only element contained in all conjugates of  $H$  is the identity element. Thus,  $g = 1$ , so  $\ker(\varphi) = \{1\}$ .  $\square$

2. (20 points) Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 10 & 9 & 8 & 11 & 7 & 3 & 2 & 6 & 12 & 5 & 4 & 1 \end{pmatrix}$$

be a permutation of the set  $X_{12} = \{1, 2, 3, \dots, 12\}$ . Compute  $\sigma^{2000}$ .

*Solution.* We may decompose  $\sigma$  into disjoint cycles:

$$\sigma = (1, 10, 5, 7, 2, 9, 12)(3, 8, 6)(4, 11)$$

Since disjoint cycles commute with each other, we have

$$\sigma^{2000} = (1, 10, 5, 7, 2, 9, 12)^{2000}(3, 8, 6)^{2000}(4, 11)^{2000}$$

The first cycle has 7 elements, so it has order 7. Similarly, the second cycle has order 3, and the third cycle has order 2. Thus, we have

$$\begin{aligned} \sigma^{2000} &= (1, 10, 5, 7, 2, 9, 12)^{2000}(3, 8, 6)^{2000}(4, 11)^{2000} \\ &= (1, 10, 5, 7, 2, 9, 12)^{7 \cdot 285 + 5}(3, 8, 6)^{3 \cdot 666 + 2}(4, 11)^{2 \cdot 1000} \\ &= (1, 10, 5, 7, 2, 9, 12)^5(3, 8, 6)^2 \end{aligned}$$

Let  $\tau = (1, 10, 5, 7, 2, 9, 12)$  and  $\lambda = (3, 8, 6)$ . We have

$$\tau = \begin{cases} 1 \mapsto 10 \\ 10 \mapsto 5 \\ 5 \mapsto 7 \\ 7 \mapsto 2 \\ 2 \mapsto 9 \\ 9 \mapsto 12 \\ 12 \mapsto 1 \end{cases} \implies \tau^5 = \begin{cases} 1 \mapsto 9 \\ 9 \mapsto 7 \\ 7 \mapsto 10 \\ 10 \mapsto 12 \\ 12 \mapsto 2 \\ 2 \mapsto 5 \\ 5 \mapsto 1 \end{cases}$$

and

$$\lambda = \begin{cases} 3 \mapsto 8 \\ 8 \mapsto 6 \\ 6 \mapsto 3 \end{cases} \implies \lambda^2 = \begin{cases} 3 \mapsto 6 \\ 6 \mapsto 8 \\ 8 \mapsto 3 \end{cases}$$

Thus, we conclude that

$$\sigma^{2000} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 9 & 5 & 6 & 4 & 1 & 8 & 10 & 3 & 7 & 12 & 11 & 2 \end{pmatrix}$$

□

3. (20 points) Let  $A = C([0, 1], \mathbb{R})$  be the ring of continuous (for the Euclidean topology) functions  $f : [0, 1] \rightarrow \mathbb{R}$  and let  $I \subset A$  be the subset of functions  $f \in A$  such that  $f(1/2) = 0$ .

- (a) (5 points) Show that  $I$  is an ideal of  $A$ .

*Proof.* We first show that  $I$  is an additive subgroup of  $A$ . The additive identity in  $A$  is  $f_0(x) \equiv 0$  which is in  $I$  because  $f_0(1/2) = 0$ . Next, for two functions  $f, g \in I$ , we have

$$(f + g)(1/2) = f(1/2) + g(1/2) = 0$$

so  $f + g \in I$ . Finally, if  $h \in I$ , then  $h(1/2) = 0$ . The additive inverse of  $h$  is  $-h$ , and

$$(-h)(1/2) = -h(1/2) = 0$$

so  $-h \in I$  as well. Thus,  $I$  is an additive subgroup of  $A$ .

Let  $f \in A$ . We know that  $A$  is a commutative ring, so it suffices to consider a single direction of multiplication. Let  $g \in I$ , so for the product  $fg$ , we have

$$(fg)(1/2) = f(1/2) \cdot g(1/2) = f(1/2) \cdot 0 = 0.$$

Thus,  $fg \in I$  as well, so  $fI \subset I$  thus  $I$  is an ideal, as desired.  $\square$

- (b) (5 points) Is  $I$  a prime ideal? Prove or disprove it.

*Proof.* Since  $A$  is a commutative ring,  $I$  being a prime ideal is equivalent to  $A/I$  being an integral domain. Let  $f + I, g + I \in A/I$  where  $f, g \in A$ . Then the product is

$$(f + I)(g + I) = fg + I$$

If this product is equal to 0 coset, then it is equal to  $I$ . Thus,  $fg \in I$ , so,

$$(fg)(1/2) = f(1/2) \cdot g(1/2) = 0$$

Since  $f(1/2), g(1/2) \in \mathbb{R}$  it must be that either  $f(1/2) = 0$  or  $g(1/2) = 0$ . Thus,  $f \in I$  or  $g \in I$ , which means either  $f + I = I$  or  $g + I = I$ , so  $A/I$  is an integral domain. Thus,  $I$  is indeed a prime ideal.  $\square$

- (c) (10 points) Is  $I$  a maximal ideal? Prove or disprove it.

*Proof.* Since  $A$  is a commutative ring,  $I$  being a maximal ideal is equivalent to  $A/I$  being a field. We already know that  $A/I$  is a ring, so we must show that every element except the 0 coset has an inverse. Let  $f + I, g + I \in A/I$  be inverses of each other, where  $f, g \notin I$ . The identity element is  $f_1 + I$  where  $f_1(x) \equiv 1$ . Then

$$(f + I)(g + I) = fg + I = f_1 + I \implies fg - f_1 \in I$$

Thus,

$$\begin{aligned} (fg - f_1)(1/2) &= f(1/2) \cdot g(1/2) - f_1(1/2) = 0 \implies f(1/2) \cdot g(1/2) = 1 \\ &\implies f(1/2) = \frac{1}{g(1/2)} \end{aligned}$$

Let

$$g(x) := \frac{1}{f(1/2)}$$

which is a continuous function because we assumed that  $f \notin I$  so  $f(1/2) \neq 0$ . Thus, any  $f + I \in A/I$  has the inverse  $g + I$  where  $g$  is as prescribed above, so  $A/I$  is a field. Thus,  $I$  is indeed a maximal ideal.  $\square$

4. (20 points) Consider the polynomial  $f(x) = x^2 + 2x + 3$  in  $\mathbb{Z}_5[x]$ .

- (a) (5 points) Is  $f(x)$  irreducible in  $\mathbb{Z}_5[x]$ ? If yes, prove it, if not determine a proper factorization of  $f(x)$  in  $\mathbb{Z}_5[x]$ .

*Proof.* If  $f$  is reducible in  $\mathbb{Z}_5[x]$ , then  $f$  factors as  $(x - a)(x - b)$ . However, we have

$$\begin{aligned} f(0) &= 3 \\ f(1) &= 1 + 2 + 3 \equiv 1 \\ f(2) &= 4 + 4 + 3 \equiv 1 \\ f(3) &= 9 + 6 + 3 \equiv 3 \\ f(4) &= 16 + 8 + 3 \equiv 2 \end{aligned}$$

so there does not exist a value  $a \in \mathbb{Z}_5$  such that  $f(a) = 0$  since  $\mathbb{Z}_5$  is an integral domain. Thus,  $f$  does not factor as a product of linear terms, so it is irreducible.  $\square$

- (b) (10 points) Let  $I = (f(x))$  be the principal ideal in  $\mathbb{Z}_5[x]$  generated by  $f(x)$ . Consider the factor ring  $F = \mathbb{Z}_5[x]/I$ .

Prove that the coset  $\bar{x} := x + I$  is invertible in  $F$  (i.e. find its multiplicative inverse) and determine the order of  $\bar{x}$  in the multiplicative group  $F^\times$  of units of  $F$ .

*Proof.* The multiplicative identity in  $F$  is  $1 + I$ , since for any coset  $f + I$ , we have

$$(f + I)(1 + I) = f + I$$

Thus, we must find an element  $g + I \in F$  such that

$$(g + I)(x + I) = gx + I = 1 + I$$

which means that  $gx - 1 \in I$  where  $g \in \mathbb{Z}_5[x]$ . Thus, we must have

$$gx - 1 = h(x^2 + 2x + 3)$$

for some  $h \in \mathbb{Z}_5[x]$  with degree at most 1. For simplicity, let  $h = 3$ , so

$$\begin{aligned} gx - 1 &= 3(x^2 + 2x + 3) = 3x^2 + 6x + 9 \\ &\equiv 3x^2 + x - 1 \\ \implies gx &= 3x^2 + x \\ \implies g &= 3x + 1 \end{aligned}$$

Thus, the multiplicative inverse of  $\bar{x}$  is given by  $3x + 1 + I$ .

Let  $o(\bar{x}) = n$ , so that

$$\begin{aligned} (x + I)^n &= x^n + I = 1 + I \\ \implies x^n - 1 &\in I \end{aligned}$$

Note that  $x^5 \equiv x \pmod{5}$  by Fermat's Little Theorem, so  $x^4 = 1$  in  $\mathbb{Z}_5$ . If  $n = 4q + r$  where  $1 \leq r \leq 4$ , then

$$x^n - 1 = x^{4q+r} - 1 = x^r - 1$$

in  $\mathbb{Z}_5$ . However, since we assumed  $n$  was the smallest integer that satisfied  $x^n - 1 \in I$ , it must be that  $r = n$ , so  $1 \leq n \leq 4$ .

If  $n = 1$ , then

$$x - 1 \in I \implies x - 1 = h(x^2 + 2x + 3)$$

for some  $h \in \mathbb{Z}_5[x]$ . This is impossible, because  $\mathbb{Z}_5$  is an integral domain, so the degree of the RHS is greater than 1. Thus,  $n \neq 1$ .

If  $n = 2$ , then

$$x^2 - 1 \in I \implies x^2 - 1 = h(x^2 + 2x + 3)$$

Here, we must have  $\deg h = 0$  and  $h$  monic, so  $h = 1$ , but this does not satisfy the equality. Thus,  $n \neq 2$ .

If  $n = 3$ , then

$$x^3 - 1 \in I \implies x^3 - 1 = h(x^2 + 2x + 3)$$

Here, we must have  $\deg h = 1$  and  $h$  monic, so  $h = x + a$  and  $a \in \mathbb{Z}_5$ , and

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

We must have  $2 + a = 0 \implies a = 3$ , but then  $3 + 2a = 3 + 2(3) = 9 \neq 0$ , so there is no solution for  $a$ . Thus,  $n \neq 3$ .

Thus,  $n = 4$  is the smallest integer that satisfies  $x^n - 1 \in I$ , and we know this is true because  $x^4 - 1 \equiv 1 - 1 = 0$  in  $\mathbb{Z}_5$ . Thus, the order of  $\bar{x}$  is  $\boxed{4}$ .  $\square$

(c) (5 points) Find, if exists, a coset of order 3 in  $F^\times$ .

*Solution.* Let  $f \in \mathbb{Z}_5[x]$  such that  $\deg f \leq 1$ . Then suppose the coset  $f + I$  has order 3, then

$$(f + I)^3 = f^3 + I = 1 + I \implies f^3 - 1 \in I$$

We can simplify by assuming  $\deg f \leq 1$ , so  $f = ax + b$ , and

$$(ax + b)^3 - 1 = (ax + b - 1) [(ax + b)^2 + (ax + b) + 1] \in I$$

If this is in  $I$ , then  $x^2 + 2x + 3$  divides this product, and since  $x^2 + 2x + 3$  is irreducible in  $\mathbb{Z}_5[x]$ , it must divide the quadratic part:

$$q(x^2 + 2x + 3) = (ax + b)^2 + (ax + b) + 1 = a^2x^2 + (2ab + a)x + (b^2 + b + 1)$$

The only possibility is  $q = a^2$ , so

$$a^2(x^2 + 2x + 3) = a^2 + 2a^2x + 3a^2 = a^2x^2 + (2ab + a)x + (b^2 + b + 1)$$

and equating coefficients, we have

$$\begin{aligned} 2a^2 &= 2ab + a \\ 3a^2 &= b^2 + b + 1 \end{aligned}$$

Since  $\mathbb{Z}_5$  is an integral domain, the first equation implies that  $2a = 2b + 1$ , which is impossible. Thus, there are no solutions for  $a$  and  $b$ , so no such  $f$  exists, and there is no coset of order 3 in  $F^\times$ .  $\square$

5. (20 points) **Answer this question OR 6**

A *local ring*  $A$  is a commutative, unital ring with a unique maximal ideal. Which of the following rings is local? For each ring, show or provide a counterexample to the statement: "the ring is local."

(a) (10 points)  $A = \mathbb{Z}/p^r\mathbb{Z}$

(b) (10 points)  $A_1 = \mathbb{Z}_p[x]$  ring of polynomials in  $x$  with coefficients in  $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ .

6. (20 points) **Answer this question OR 5.**

- (a) (10 points) Let  $p$  be a prime number. Consider the polynomial  $f(x) = x^p - px - 1$ . Prove or disprove the following statement:

$$f(x) \text{ is irreducible in } \mathbb{Q}[x].$$

*Proof.* If  $p = 2$ , then  $f(x) = x^2 - 2x - 1$  whose roots are  $1 \pm \sqrt{2} \notin \mathbb{Q}$ , so  $f$  is irreducible when  $p = 2$ .

If  $p > 2$ , then  $\deg f$  is odd. Thus, if  $f$  is reducible, then it must contain at least a single linear term, since polynomials in  $\mathbb{Z}[x]$  factor as a product of linear terms and irreducible quadratic terms. By the Rational Root Theorem, the only possible roots of  $f$  are  $\pm 1$ , where  $f(1) = -p \neq 0$  and  $f(-1) = p - 2 \neq 0$ . Thus, there are no rational roots, so the factorization of  $f$  cannot contain a linear term. Thus,  $f$  is irreducible.  $\square$

- (b) (10 points) Consider the polynomial  $g(x) = x^4 + 5x^2 + 3x + 2$ . Prove or disprove the following statement:

$$g(x) \text{ is irreducible in } \mathbb{Q}[x].$$

*Proof.* By the Rational Root Theorem, the only possible rational roots are  $\pm 1, \pm 2$ . We have

$$g(1) = 1 + 5 + 3 + 2 \neq 0$$

$$g(2) = 16 + 20 + 6 + 2 \neq 0$$

$$g(-1) = 1 + 5 - 3 + 2 \neq 0$$

$$g(-2) = 16 + 20 - 6 + 2 \neq 0$$

Thus,  $g$  has no rational roots. Suppose  $g$  factorizes as the product of two irreducible quadratics. Thus,

$$g(x) = x^4 + 5x^2 + 3x + 2 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a+c)x^3 + (b+d+ac)x^2 + (ad+bc)x + bd$$

Equating coefficients, we have

$$a + c = 0$$

$$b + d + ac = 5$$

$$ad + bc = 3$$

$$bd = 2$$

From the last condition, we can have either  $b = 1, d = 2$  or  $b = -1, d = -2$ . The other possibilities  $b = 2, d = 1$  and  $b = -2, d = -1$  are symmetric with the former 2.

If  $b = 1, d = 2$ , from the first equation we also have  $c = -a$ , so the system becomes

$$1 + 2 - a^2 = 5$$

$$2a - a = 3$$

From the second equation, we have  $a = 3$ , but this does not satisfy the first equation.

If  $b = -1, d = -2$ , the system becomes

$$-1 - 2 - a^2 = 5$$

$$-2a + a = 3$$

but there is no solution because the LHS in the first equation is negative.

Thus,  $g$  cannot factorize as a product of two irreducible quadratics, and cannot have any linear factors, so  $g$  is irreducible.  $\square$