

1. [6 points] Let  $R$  be a ring, and  $I$  an ideal in  $R$ . Prove that the quotient ring  $R/I$  is commutative if and only if  $xy - yx \in I$  for all  $x, y \in R$ .
2. (a) [4 points] List all the elements of the symmetric group  $S_3$ , using notation of your choice.  
 (b) [4 points] Which elements from part (a) are in the alternating group  $A_3$ ?  
 (c) [4 points] Let  $f = (1\ 2\ 3)$ . Determine the centralizer  $C_{S_3}(f)$  of  $f$  in  $S_3$ .

(Recall that the centralizer of  $f$  is the set of all elements of the group that commute with  $f$ .)

3. Let  $\phi : R \rightarrow S$  be a ring homomorphism.
  - (a) [4 points] Define the *kernel* of  $\phi$ , denoted  $\ker \phi$ , and prove that it is an ideal.
  - (b) [5 points] Assume that  $R$  is a commutative ring with unity, and  $S$  is an integral domain. Prove that either  $\ker \phi = R$  or  $\ker \phi$  is a *prime* ideal.

(Recall: An integral domain is a commutative ring with unity with at least two elements and no zero divisors. A prime ideal is an ideal  $I \neq R$  such that for all  $a, b \in R$ , if  $ab \in I$  then either  $a \in I$  or  $b \in I$ , or both.)

4. Suppose that  $G$  is a finite group, and  $g \in G$  is an element of order 9.
  - (a) [4 points] Prove that  $|G|$  is divisible by 9.
  - (b) [5 points] Prove that for all integers  $n$ ,  $g^n = e_G$  if and only if  $9 \mid n$ .

*Suggestion:* For the “only if” direction, use the division algorithm for  $\mathbb{Z}$ .

- (c) [3 points] Determine  $o(g^2)$  and  $o(g^3)$ .
5. Let  $R = \mathbb{Z} \times \mathbb{Z}$ , and let  $I = \{(2m, 3n) : m, n \in \mathbb{Z}\}$ .
  - (a) [4 points] Prove that  $I$  is an ideal in  $R$ .
  - (b) [2 points] Is  $I$  a principal ideal? Briefly justify your answer.
  - (c) [2 points] Is  $I$  a prime ideal? Briefly justify your answer.
  - (d) [2 points] Is  $I$  a maximal ideal? Briefly justify your answer.
6. Let  $G$  be a group,  $H$  a subgroup of  $G$ , and  $g$  an element of  $G$ . Define

$$K = gHg^{-1} = \{ghg^{-1} : h \in H\}.$$

- (a) [4 points] Prove that  $K \leq G$  ( $K$  is a subgroup of  $G$ ).
- (b) [4 points] Prove that  $K \cong H$ .
7. Let  $F$  be a field, and let  $F[X]$  denote the polynomial ring over  $F$ .
  - (a) [4 points] Prove that  $F[X]$  is an integral domain. You may assume that  $F[X]$  is a commutative ring with unity, as well as any basic facts about degrees of polynomials proved in class.
  - (b) [4 points] Let  $I = \langle X^2 + 1 \rangle$  denote the principal ideal generated by  $X^2 + 1$  in  $F[X]$ . Prove that every element in the quotient ring  $F[X]/I$  is equal to  $I + (a + bX)$  for some choice of elements  $a, b \in F$ .

- (c) [4 points] Let  $I$  be as in part (b). Prove that if  $a, b \in F$  satisfy  $a^2 + b^2 \neq 0$ , then the element  $I + a + bX \in F[X]/I$  is a unit in  $F[X]/I$ .

*Hint:* mimic the way that inverses are computed in  $\mathbb{C}$  or  $\mathbb{Q}[\sqrt{-1}]$ .

8. [6 points] Let  $R$  be an integral domain. Prove that if  $p \in R$  is a prime element, then  $p$  is also an irreducible element. In your argument, explicitly identify where you use the assumption that  $R$  is an integral domain.

(Recall: An element  $p \in R$  is *prime* if it is nonzero, it is not a unit, and for all  $a, b \in R$  such that  $p \mid ab$ , either  $p \mid a$  or  $p \mid b$ . An element  $p \in R$  is *irreducible* if it is nonzero, it is not a unit, and for all  $a, b \in R$  such that  $p = ab$ , either  $a$  is a unit or  $b$  is a unit.)

9. Suppose that  $G$  is a group, and  $H$  is a subgroup of  $Z(G)$ .

(a) [4 points] Prove that  $H$  is a normal subgroup of  $G$ .

(b) [6 points] Suppose that the quotient group  $G/H$  is cyclic, with generator  $Hg$ . Prove that  $G$  is abelian.

*Hint:* First show every element  $x \in G$  is equal to  $hg^n$  for some  $h \in H$  and integer  $n$ .

(c) (**Bonus**; up to 2 points of extra credit. I don't recommend spending time on this unless you've completed the rest of the exam!)

Prove that if  $G$  is a group of order  $p^3$ , for  $p$  a prime number, then  $g^p \in Z(G)$  for all  $g \in G$ .