



4. (a) Prove *Wilson's Theorem*: If  $p$  is a prime, then  $(p - 1)! = -1 \pmod{p}$ .  
 (b) If  $p$  is not a prime, is it possible for  $(p - 1)! = -1 \pmod{p}$ ?  
 (c) If  $G$  is an abelian group with elements  $a_1, a_2, \dots, a_n$ , and  $n$  is odd, show that  $a_1 a_2 \cdots a_n = e$ , where  $e$  denotes the identity.  
 (d) If  $G$  is abelian, and has exactly one element  $z$  of order 2 (that is,  $z^2 = e, z \neq e$ ), show that  $a_1 a_2 \cdots a_n = z$ .  
 (e) (\*) If  $G$  is abelian, and has more than one element of order 2, show that  $a_1 a_2 \cdots a_n = e$ .
5. Let  $G$  be a group generated by two elements  $a$  and  $b$ , satisfying the relations

$$a^4 = e, \quad b^4 = e, \quad a^2 = b^2, \quad b a b^{-1} = a^{-1}$$

Here  $e$  denotes the identity element of  $G$ .

- (a) Show that  $G$  is a group with eight elements.  
 (b) Describe all groups with eight elements.  
 (c) Which one of these groups is  $G$ ?
6. (a) Define what it means for a matrix to be (i) orthogonal, (ii) symmetric, and (iii) positive definite. (*Three separate questions.*)  
 (b) Prove that the only real matrix which is orthogonal, symmetric, and positive definite is the identity matrix.  
 (c) Prove that, if  $A$  is real, positive definite, and symmetric matrix, then  $A = P^t P$  for some nonsingular real matrix  $P$ .
7. Define rings  $R_1, R_2, R_3, R_4$  as follows:

$$R_1 = \mathbb{Z}, \quad R_2 = \mathbb{Z}[i], \quad R_3 = \mathbb{Z}[x], \quad R_4 = \mathbb{Z}[x, y]$$

Considering each  $R_i$  in turn, determine whether the following statements are true or false. Give reasons and/or examples to justify your conclusions.

- (a) The ideal  $\langle 2 \rangle$  is a prime ideal in  $R_i$ .  
 (b) The ideal  $\langle 2 \rangle$  is a maximal ideal in  $R_i$ .  
 (c) Every prime ideal in  $R_i$  is maximal.  
 (d) Every maximal ideal in  $R_i$  is prime.  
 (e) The quotient ring  $R_i / \langle 2 \rangle$  is a field.  
 (f) Every ideal in  $R_i$  is a principal ideal.

Recall that an ideal  $J$  in a commutative ring  $R$  is *prime* if, whenever  $ab \in J$ , either  $a \in J$  or  $b \in J$ .

(*Notation: if  $R$  is a ring and  $\alpha \in R$ , then  $\langle \alpha \rangle$  denotes the ideal generated by  $\alpha$ , i.e., the smallest ideal in  $R$  containing  $\alpha$ . The rings  $\mathbb{Z}[x]$  and  $\mathbb{Z}[x, y]$  are polynomial rings, and  $\mathbb{Z}[i]$  denotes the set of complex numbers of the form  $a + bi$ , where  $a, b \in \mathbb{Z}$ .)*

8. Determine whether the following statements are true or false. Give reasons to justify your conclusions.

- (a)  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$  is a field.
- (b)  $\mathbb{R}[x]/\langle x^2 + 1 \rangle$  is isomorphic to  $\mathbb{C}$  (the field of complex numbers).
- (c)  $\mathbb{R}[x]/\langle x^2 + x + 1 \rangle$  is a field.
- (d)  $\mathbb{R}[x]/\langle x^2 + x + 1 \rangle$  is isomorphic to  $\mathbb{C}$ .
- (e)  $\mathbb{R}[x]/\langle x^2 - 1 \rangle$  is not a field.
- (f)  $\mathbb{R}[x]/\langle x^2 - 1 \rangle$  is isomorphic to the ring  $\mathbb{R} \times \mathbb{R}$ .
- (g)  $\mathbb{R}[x]/\langle x^2 \rangle$  is not a field.
- (h)  $\mathbb{R}[x]/\langle x^2 \rangle$  is isomorphic to the ring  $\mathbb{R} \times \mathbb{R}$ .

In each case where you assert that there is an isomorphism, please describe it explicitly.

9. Consider the following statement:

*If  $G$  is a finite group with more than two elements, then  $G$  has a nontrivial automorphism.*

Is this statement true? If so, give a proof. If not, find a counterexample.

10. An  $n \times n$  matrix  $A$  is *nilpotent* if  $A^k = 0$  for some  $k > 0$ .

- (a) Give examples of two nonzero  $3 \times 3$  nilpotent matrices  $A$  and  $B$  that are not similar to each other. (*Two matrices  $A$  and  $B$  are similar if there exists an invertible  $C$  such that  $B = C^{-1}AC$ .*)
- (b) Prove that every nonzero  $3 \times 3$  nilpotent matrix is similar to either  $A$  or  $B$ .
- (c) Prove that, if an  $n \times n$  matrix is nilpotent, then  $A^n = 0$ .

11. Let  $K$  denote the splitting field of the polynomial  $p(x) = x^4 - 4$  over  $\mathbb{Q}$ , and let  $G$  denote the Galois group of  $K$  over  $\mathbb{Q}$ . Let  $L$  denote the splitting field of  $q(x) = x^4 - 1$  over  $\mathbb{Q}$ , and let  $H$  denote the Galois group of  $L$  over  $\mathbb{Q}$ .

- (a) Is  $L$  a subfield of  $K$ ? Is  $H$  a subgroup of  $G$ ? Explain these relationships exactly.
- (b) Compute  $|G|$  and  $|H|$ , and describe the elements of  $G$  and  $H$  explicitly.
- (c) Find all fields  $F$  such that  $\mathbb{Q} \subseteq F \subseteq K$ , and describe exactly how each one corresponds to a subgroup of  $G$ .
- (d) Show that  $G$  is abelian.
- (e) Show that each subfield  $F$  with  $\mathbb{Q} \subseteq F \subseteq K$  is a splitting field.
- (f) Consider the last two properties in general. Does (d) always imply (e)? Does (e) always imply (d)? Are the two properties equivalent? State any general results you are using here.

12. Would any of the answers to problem 10 be different if we had taken  $K$  instead to be the splitting field of the polynomial  $r(x) = x^4 - 3$ ? Explain.