Question:	1	2	3	4	Total
Points:	2	18	8	12	40
Score:					

## Question 1 (2 points)

Prove that a group G of order 72 cannot be simple. (Hint: Consider the Sylow 3 subgroups of G. )

Question 2 (18 points)

Let k be an arbitrary field.

(a) (2 points) Let p and q be non-negative integers. Show that the groups  $\mathbf{Z}/n\mathbf{Z}$  and  $\mathbf{Z}/p\mathbf{Z} \times \mathbf{Z}/q\mathbf{Z}$  are isomorphic if and only if n = pq and p and q are relatively prime.

(b) (2 points) Deduce that if  $m = d_1 \cdot \ldots \cdot d_l$  with integers  $d_1, \ldots, d_l$  being pairwise relatively prime, then we have  $\mathbf{Z}/m\mathbf{Z} \cong \mathbf{Z}/d_1\mathbf{Z} \times \ldots \times \mathbf{Z}/d_l\mathbf{Z}$ . (Hint: Use part (a) and induction.)

(c) (2 points) Show that a non-zero polynomial  $f(X) \in k[X]$  can have at most deg(f)-many zeros in k.

(d) (2 points) Show that if G is a finite subgroup of the multiplicative group  $k^{\times}$  then G is cyclic. (Hint: Say G is of order m. Find a polynomial which admits every element of G as a root. Use the classification theorem of finite abelian groups and parts (b) and (c) to conclude. )

(e) (2 points) Deduce that the multiplicative group of a finite field is cyclic.

(f) (2 points) Show that the group  $\mathbf{Z} \times \mathbf{Z}$  is not cyclic.

(g) (2 points) Show that  $\mathbf{Q}$  and  $\mathbf{Q} \times \mathbf{Q}$  cannot be isomorphic as additive groups using parts (d) and (f).

(h) (2 points) Construct a field of size 8, say K.

(i) (2 points) Find a generator of the multiplicative group  $K^{\times}$ , say  $\alpha$ . Write the elements  $\alpha^2, \alpha^4, \alpha^6$  in terms of polynomials. What can you say about the multiplication table of the group  $K^{\times}$ .

## Question 3 (8 points)

Let R be any commutative ring with identity.

(a) (2 points) Show that if R is a PID and I is an ideal of R, then R/I is also a PID.

(b) (2 points) Show that every prime ideal of R is maximal if R is a PID.

(c) (2 points) Let R = k[X]; where k is a field (so that it is a PID). Show that there is a one to one correspondence between maximal ideals of R and monic irreducible polynomials in R.

(d) (2 points) True/False : if  $r \in R$  is irreducible (R is just a commutative ring with identity), then  $\langle r \rangle$  is maximal.

## Question 4 (12 points)

Decide whether the following statements are true or false and circle your claim. If true give a proof, if false give a counter-example

(a) (2 points) Let G be a group and  $g_1, g_2$  be two elements of orders n and m in G. Then the order of the product  $g_1g_2$  divides nm. True / False :

(b) (2 points) The groups  $(\mathbf{Q}, +)$  and  $(\mathbf{Q} \setminus \{0\}, \cdot)$  are not isomorphic. True / False :

(c) (2 points) If  $\varphi \colon G \to G'$  is an isomorphism of groups, then its inverse (as a bijection from G' to G) is a group homomorphism. True / False : (d) (2 points) If R is an integral domain and I is an ideal of R, then R/I is an integral domain, too.
True / False :

(e) (2 points) The extension  $\mathbf{Q}(\sqrt[3]{\pi})/\mathbf{Q}$  is algebraic. True / False :

(f) (2 points) The extension  $\mathbf{Q}(\sqrt[3]{\pi})/\mathbf{Q}(\pi)$  is algebraic. True / False :