

## Qualifying Examination

(January 2008 Solutions)

### Abstract Algebra

Each part (a), (b) or (c) below is worth 3 points, and the total points are 30.

1. (a) Let  $G_1$  and  $G_2$  be two normal subgroups of a group  $G$  with  $G_1 \cap G_2 = \{1\}$ . Prove that  $a_1a_2 = a_2a_1$  for all  $a_1 \in G_1$  and  $a_2 \in G_2$ .

Consider the element  $g = a_1a_2a_1^{-1}a_2^{-1}$ . Since  $G_2$  is normal,  $a_1a_2a_1^{-1} \in G_2$ , so  $g \in G_2$ . Since  $G_1$  is normal,  $a_2a_1^{-1}a_2^{-1} \in G_1$ , so  $g \in G_1$ . Hence  $a_1a_2a_1^{-1}a_2^{-1} \in G_1 \cap G_2 = \{1\}$ , i.e.,  $g = 1$ . Thus  $a_1a_2 = a_2a_1$ .

- (b) The center  $Z(G)$  of a group  $G$  is defined to be

$$Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

Prove that if  $G$  is a non-abelian simple group, then  $Z(G) = \{1\}$ .

$Z(G)$  is normal in  $G$  since for  $g \in Z(G)$  and  $x \in G$ ,  $x^{-1}gx = gx^{-1}x = g1 = g \in Z(G)$ . If  $Z(G) = G$  then  $G$  is abelian, so  $Z(G) \neq G$ . Since the group is simple the only other normal subgroup is  $\{1\}$ .

2. (a) Let  $n \geq 3$ . State the definition of the alternating group  $A_n$ .

$A_n$  is the subgroup of the symmetric group  $S_n$  consisting of permutations that can be written as the product of an even number of 2-cycles.

- (b) Prove that  $A_n$  is generated by all the 3-cycles in the symmetric group  $S_n$ .

We first note that  $(abc) = (cb)(ac)$  (in this notation permutations act of the left), so that every 3-cycle is in  $A_n$ . Suppose to the contrary, that  $A_n$  has an element which can not be written as the product of 3-cycles. Choose  $\pi \in A_n$  an element that cannot be written as a product of 3-cycles and such that  $\pi$  can be written as a product of 2-cycles in the shortest possible way. Clearly  $\pi \neq 1$ , since 1 is the empty product of 3 cycles. Say  $\pi = (ab)(cd)\pi'$ . If  $(ab) = (cd)$  then  $\pi = \pi'$ , a contradiction. If  $(ab)$  and  $(cd)$  are disjoint then  $(ab)(cd) = [(ab)(bc)][(bc)(cd)] = (abc)(bcd)$ , so  $\pi'$  is a shorter choice, a contradiction. The only other possibility is that, after renaming,  $a, b = c$ , and  $d$  are distinct numbers, and then  $(ab)(cd) = (ab)(bd) = (abd)$ , so again,  $\pi'$  is a shorter counterexample. Hence  $A_n$  is generated by the 3-cycles.

3. (a) Let  $R$  be an integral domain (with multiplicative identity  $1 \neq 0$ ). State the definition of the characteristic of  $R$ . Can the characteristic of  $R$  be equal to 6?

Let  $\phi : \mathbb{Z} \rightarrow R$  be the ring homomorphism sending  $n \mapsto n \cdot 1_R$ . Since  $\mathbb{Z}$  is a PID,  $\ker(\phi)$  is  $t\mathbb{Z}$  where we can chose  $t \geq 0$ . Then  $t$  is the characteristic of  $R$ . If  $R$  is a domain, then it has no zero-divisors. If the characteristic of  $R$  is 6, then  $(2 \cdot 1_R)(3 \cdot 1_R) = 0$  in  $R$ . Neither of the factors is zero, contradicting the hypothesis that  $R$  is a domain, i.e., the answer is no.

(b) Let  $F$  be a field of characteristic zero. What is the smallest subfield, up to isomorphism, contained in  $F$ ? Justify your answer.

If the characteristic of  $F$  is zero then  $F$  contains  $\mathbb{Z}$  as a subring (i.e., the map  $\phi$  above is injective). Moreover, every subring of  $F$  must contain a copy of  $\mathbb{Z}$  as well. Thus, every subfield of  $F$  must contain the field of fractions of this copy of  $\mathbb{Z}$ , which is  $\mathbb{Q}$ .

(c) Construct a finite field of order 27. Justify your construction.

If  $F$  is a field, then the polynomial ring  $F[X]$  is a PID. Hence being a prime element of  $F[X]$  is equivalent to being irreducible, and if  $g(x)$  is prime then  $F[X]/(g(X))$  is a field extension of  $F$ , which as an  $F$ -vector space is of dimension  $\deg(g)$ .

To construct a field of order  $27 = 3^3$  we need to give an irreducible polynomial of degree three in  $\mathbb{Z}_3[X]$ . Since the degree of the product of two polynomials is the sum of the degrees (this only requires that the base be an integral domain), if a degree three polynomial factors in a non-trivial way then it has a linear factor, i.e., a root in  $\mathbb{Z}_3$ . Consider  $g(X) = X^3 - X + 1$ . A simple check shows that  $g(0) = g(1) = g(2) = 1$ . So  $\mathbb{Z}_3[X]/(X^3 - X + 1)$  is a field of order 27.

4. Let  $I$  be an ideal of a commutative ring  $R$ . Define

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some positive integer } n\}.$$

It is known that  $\sqrt{I}$  is an ideal of  $R$ .

(a) Let  $I = (x^{2008}, y^{2009})$  be the ideal of the polynomial ring  $\mathbb{C}[x, y]$  generated by  $x^{2008}$  and  $y^{2009}$ . Prove that  $\sqrt{I} \supset (x, y)$ , the ideal generated by  $x$  and  $y$ .

Since  $x^{2008} \in I$ ,  $x \in \sqrt{I}$ . Since  $y^{2009} \in I$ ,  $y \in \sqrt{I}$ . Given that  $\sqrt{I}$  is an ideal then it must contain the ideal generated by  $x$  and  $y$ , i.e.,  $\sqrt{I} \supset (x, y)$ .

(b) Prove that  $\sqrt{I} = (x, y)$ .

If  $\sqrt{I}$  is bigger than  $(x, y)$ , then it is all of  $\mathbb{C}[x, y]$ , since the ideal  $(x, y)$  is maximal in  $\mathbb{C}[x, y]$  (because  $\mathbb{C}[x, y]/(x, y) \cong \mathbb{C}$  is a field). Thus we would have  $1 \in (x, y)$ . But all powers of 1 give 1, which is not in  $(x, y)$ .

(c) If  $J = (x^{2008} + y^{2007}, y^{2009})$ , what is  $\sqrt{J}$ ? Justify your answer.

Since  $y^{2009} \in J$ , we have  $y \in \sqrt{J}$ . Then  $y^{2007} \in \sqrt{J}$  too. Note that  $J \subset \sqrt{J}$ . So  $x^{2008} = (x^{2008} + y^{2007}) - y^{2007} \in \sqrt{J}$ . Hence  $x \in \sqrt{J}$  as well. Thus  $\sqrt{J} \supseteq (x, y)$ . As in (a), if it is larger then  $1 \in J$ , and this is not the case. So  $\sqrt{J} = (x, y)$ .

## Linear Algebra

A. (a) (1 pt) What is the dimension of the vector space  $V_n$  of real polynomials in one variable of degree at most  $n$ ? (No justification required).

*Solution:*  $\dim(V_n) = n + 1$  (the set  $\{1, x, x^2, \dots, x^n\}$  is a basis for  $V_n$ )

(b) (2 pts) Let  $D: V_n \rightarrow V_n$  be the derivative map,  $f \mapsto f'$ . Is  $D$  a diagonalizable linear operator? Explain.

*Solution:*  $D$  is *not* diagonalizable if  $n \geq 1$ . To see this, let  $M$  be the matrix representation of  $D$  corresponding to some fixed basis of  $V_n$ , and suppose on the contrary that  $M = A\Delta A^{-1}$  for some diagonal matrix  $\Delta$  and invertible matrix  $A$ . Since  $D^{n+1}$  is the zero map on  $V_n$ , we have

$$\begin{aligned} A\Delta^{n+1}A^{-1} &= (A\Delta A^{-1})^{n+1} = M^{n+1} = O \\ \implies \Delta^{n+1} &= O \\ \implies \Delta &= O \\ \implies M &= A\Delta A^{-1} = O, \end{aligned}$$

hence  $D$  is the zero map on  $V_n$ . But  $D(x) = 1 \neq 0$ , which is a contradiction.

(c) (3 pts) A function of one real variable is *real analytic* if it can be represented by a power series  $\sum_{i=0}^{\infty} a_i x^i$  which converges for all  $x \in \mathbb{R}$ . Let  $\mathcal{A}$  be the vector space of real analytic functions. Determine the eigenvalues and eigenfunctions of the derivative  $D: \mathcal{A} \rightarrow \mathcal{A}$ ,  $f \mapsto f'$ .

*Solution:* Let  $f = \sum_{i=0}^{\infty} a_i x^i$  be an eigenfunction of  $D$  with eigenvalue  $\lambda$ . Then

$$\sum_{i=0}^{\infty} \lambda a_i x^i = \lambda \sum_{i=0}^{\infty} a_i x^i = \lambda f = D(f) = \sum_{i=1}^{\infty} i a_i x^{i-1} = \sum_{i=0}^{\infty} (i+1) a_{i+1} x^i,$$

and thus  $(i+1)a_{i+1} = \lambda a_i$  for  $i = 0, 1, 2, \dots$ . Using induction on  $i$ , it is easy to see that  $a_i = \lambda^i a_0 / i!$  for each  $i$ ; consequently,

$$f = \sum_{i=0}^{\infty} \left( \frac{\lambda^i a_0}{i!} \right) x^i = a_0 \sum_{i=0}^{\infty} \frac{(\lambda x)^i}{i!} = a_0 e^{\lambda x}.$$

On the other hand, every function of the form  $f = a_0 e^{\lambda x}$  satisfies  $D(f) = \lambda f$ , hence it is an eigenfunction with eigenvalue  $\lambda$ . To summarize, every real number  $\lambda$  is an eigenvalue of  $D$ , and the eigenfunctions corresponding to  $\lambda$  are those functions of the form  $f = a_0 e^{\lambda x}$ , where  $a_0$  is a nonzero real number.

**B.** (a) (2 pts) Let  $V$  be a vector space over a field  $k$ . Define what it means for a function  $\langle, \rangle: V \times V \rightarrow k$  to be *bilinear*.

*Solution:* A function  $\langle, \rangle: V \times V \rightarrow k$  is bilinear if the following properties hold:

- $\langle a_1 + a_2, b \rangle = \langle a_1, b \rangle + \langle a_2, b \rangle$  for all  $a_1, a_2, b \in V$ ;
- $\langle a, b_1 + b_2 \rangle = \langle a, b_1 \rangle + \langle a, b_2 \rangle$  for all  $a, b_1, b_2 \in V$ ;
- $\langle xa, b \rangle = \langle a, xb \rangle = x\langle a, b \rangle$  for all  $x \in k$  and  $a, b \in V$ .

(b) (2 pts) What does it mean for a bilinear form to be *non-degenerate*?

*Solution:* The bilinear form  $\langle, \rangle: V \times V \rightarrow k$  is non-degenerate if the following properties hold:

- $\langle a, b \rangle = 0$  for all  $a \in V$  implies  $b = 0$ ;
- $\langle a, b \rangle = 0$  for all  $b \in V$  implies  $a = 0$ .

(c) (3 pts) Prove or give a counter-example. If  $\langle, \rangle$  is a bilinear form such that  $\langle a, a \rangle = 0$  for all  $a \in V$ , then  $\langle, \rangle$  is degenerate.

*Solution:* The statement is false. Let  $V$  be the two-dimensional space of column vectors:

$$V = \left\{ \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} : x_1, x_2 \in k \right\}.$$

Let  $\langle, \rangle: V \times V \rightarrow k$  be the function given by

$$\langle a, b \rangle = \det \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \end{pmatrix} = x_1y_2 - x_2y_1 \quad \text{for all } a = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, b = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \in V. \quad (1)$$

To show that  $\langle, \rangle$  is bilinear, one verifies the three properties listed in part (a). For instance, if

$$a_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \quad a_2 = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix},$$

then

$$\begin{aligned} \langle a_1 + a_2, b \rangle &= (x_1 + y_1)z_2 - (x_2 + y_2)z_1 \\ &= (x_1z_2 - x_2z_1) + (y_1z_2 - y_2z_1) \\ &= \langle a_1, b \rangle + \langle a_2, b \rangle. \end{aligned}$$

The other properties are proved similarly.

From the definition (1), it is clear that  $\langle a, b \rangle \neq 0$  if and only if  $a$  and  $b$  are linearly independent over  $V$ . In particular,  $\langle a, a \rangle = 0$  for all  $a \in V$ . On the other hand, for every  $a \neq 0$  in  $V$  there is a vector  $b \in V$  such that  $a$  and  $b$  are linearly independent; thus,  $\langle a, b \rangle \neq 0$ . This proves the first property listed in part (b), and the other property is similar.

**C.** (a) (2 pts) Let  $V$  be a vector space. A linear operator  $P: V \rightarrow V$  is called a *projection* if  $P^2 = P$ . Prove that if  $P$  is projection, then the eigenvalues of  $P$  are either 0 or 1. (Do not assume that  $V$  is finite dimensional!)

*Solution:* If  $v \neq 0$  is an eigenvector with eigenvalue  $\lambda$ , then

$$(\lambda^2 - \lambda)v = \lambda(\lambda v) - (\lambda v) = \lambda P(v) - P(v) = P(\lambda v) - P(v) = P(P(v)) - P(v),$$

where we have used the linearity of  $P$  for the third equality. Since  $P^2(v) = P(v)$ , this shows that  $(\lambda^2 - \lambda)v = 0$ , and therefore  $\lambda^2 - \lambda = 0$ ; that is,  $\lambda = 0$  or 1.

(b) (3 pts) Let  $V$  be a vector space of dimension  $n$  and let  $P$  be a projection with  $\dim P(V) = k$ . Prove that there is an ordered basis for  $V$  such that the matrix representation of  $P$  with respect to this basis is a diagonal matrix with  $k$  1's and  $(n - k)$  0's on the diagonal.

*Solution:* For  $\lambda = 0$  or 1, let

$$V_\lambda = \{v \in V : P(v) = \lambda v\}.$$

Clearly,  $V_0 = \ker(P)$ , and it is easy to see that  $V_1 = P(V)$ . Indeed, the equality  $v = P(v)$  for each  $v \in V_1$  shows that  $V_1 \subseteq P(V)$ , whereas if  $v = P(w)$  is an arbitrary element of  $P(V)$ , then  $P(v) = P^2(w) = P(w) = v$ , hence  $v \in V_1$ ; this shows the opposite inclusion  $P(V) \subseteq V_1$ .

For every  $v \in V$ , we can write  $v = v_0 + v_1$ , where  $v_1 = P(v)$  lies in  $V_1$ , and  $v_0 = v - v_1 = v - P(v)$  lies in  $V_0$  since

$$P(v_0) = P(v - P(v)) = P(v) - P^2(v) = P(v) - P(v) = 0.$$

Therefore,  $V = V_0 + V_1$ . If  $v \in V_0 \cap V_1$ , then  $v = 1 \cdot v = P(v) = 0 \cdot v = 0$ ; thus,  $V_0 \cap V_1 = \{0\}$ , and we have shown that  $V = V_0 \oplus V_1$ .

Taking a basis  $\{u_1, \dots, u_h\}$  for  $V_0 = \ker(P)$ , where  $h = n - k$ , and a basis  $\{v_1, \dots, v_k\}$  for  $V_1 = P(V)$ , it is clear that  $\{u_1, \dots, u_h, v_1, \dots, v_k\}$  is a basis for  $V = V_0 \oplus V_1$  with the desired property.

**D.** (a) (3 pts) Prove or give a counter example: If  $A$  and  $B$  are  $n \times n$  matrices then the minimal polynomial of  $AB$  equals the minimal polynomial of  $BA$ .

*Solution:* This is false. Let  $A$  and  $B$  be the  $2 \times 2$  matrices over  $\mathbb{C}$  given by

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Both matrices

$$C = AB = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad D = BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

have the same characteristic polynomial  $x^2$ . However, the minimal polynomial of  $C$  is  $x^2$  whereas the minimal polynomial of  $D$  is  $x$ .

(b) (4 pts) What are the possible rational canonical forms of a real matrix whose characteristic polynomial is  $(x^4 - 1)(x - 1)$ ?

*Solution:* Since the characteristic polynomial  $p(x) = (x - 1)^2(x + 1)(x^2 + 1)$  and the minimal polynomial have the same irreducible factors, the minimal polynomial must be either

$$m_1(x) = (x - 1)(x + 1)(x^2 + 1) = x^4 - 1$$

or

$$m_2(x) = (x - 1)^2(x + 1)(x^2 + 1) = (x^4 - 1)(x - 1) = x^5 - x^4 - x + 1.$$

In the first case, the rational canonical form is the block matrix

$$\begin{pmatrix} C_{x-1} & O \\ O & C_{m_1(x)} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

and in the second case, the rational canonical form the companion matrix

$$C_{m_2(x)} = \begin{pmatrix} 0 & 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

**E.** Let  $V$  be the vector space of complex  $3 \times 3$  matrices. Define a Hermitian inner product  $\langle \cdot, \cdot \rangle: V \times V \rightarrow \mathbb{C}$ , by  $\langle A, B \rangle = \text{Tr}(AB^*)$  where  $B^* = \overline{B}^t$  is the adjoint of  $B$ . Let  $W \subset V$  be the subspace of  $3 \times 3$  matrices with trace 0.

(a) (2 pts) Find a linear basis of  $W$ .

*Solution:* For  $1 \leq i, j \leq 3$ , let  $E_{ij}$  be the matrix with an entry 1 in the  $i$ -th row and  $j$ -th column, and 0's elsewhere. Let  $S$  be the set consisting of the six matrices  $\{E_{ij} : i \neq j\}$  together with  $E_{11} - E_{33}$  and  $E_{22} - E_{33}$ . We claim that  $S$  is a basis for  $W$ . Indeed, if a matrix  $A = (a_{ij})$  lies in  $W$ , then  $a_{11} + a_{22} + a_{33} = \text{Tr}(A) = 0$ , so  $A$  has the form

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & -a_{11} - a_{22} \end{pmatrix} = \sum_{i \neq j} a_{ij} E_{ij} + a_{11}(E_{11} - E_{33}) + a_{22}(E_{22} - E_{33});$$

this shows that  $S$  spans  $W$ . From this equation, it also follows that  $S$  is a linearly independent set, for if

$$\sum_{i \neq j} a_{ij} E_{ij} + a_{11}(E_{11} - E_{33}) + a_{22}(E_{22} - E_{33}) = O,$$

then

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & -a_{11} - a_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

which implies  $a_{ij} = 0$  for  $1 \leq i, j \leq 3$ ,  $(i, j) \neq (3, 3)$ .

(b) (3 pts) Determine the orthogonal complement of  $W$  with respect to the inner product above.

*Solution:* Let  $U = \mathbb{C} \cdot I_3$  be the one-dimensional space of scalar matrices in  $V$ . For every  $A \in V$ , let  $\lambda = \frac{1}{3}\text{Tr}(A)$ ,  $B = \lambda I_3$ , and  $C = A - B$ . Since  $\text{Tr}(B) = 3\lambda = \text{Tr}(A)$ , we have  $\text{Tr}(C) = \text{Tr}(A - B) = \text{Tr}(A) - \text{Tr}(B) = 0$ ; thus,  $A = B + C$  with  $B \in U$  and  $C \in W$ , i.e.,  $V = U + W$ . The sum is clearly direct ( $V = U \oplus W$ ), for if  $\lambda I_3 \in U \cap W$ , then  $0 = \text{Tr}(\lambda I_3) = 3\lambda$ , and thus  $\lambda I_3 = O$ .

Now,  $U$  is an orthogonal complement of  $W$  with respect to the given inner product since for every  $\lambda I_3 \in U$  and  $A \in W$ , we have

$$\langle A, \lambda I_3 \rangle = \text{Tr}(A \cdot \bar{\lambda} I_3) = \bar{\lambda} \text{Tr}(A) = 0.$$