

**Qualifying Exam in Algebra - Outline of Solutions.**

**August 17, 2001**

$\mathbb{Z}$  = integers.  $\mathbb{Q}$  = rational numbers.  $\mathbb{C}$  = complex numbers.

1. Find the set of integer solutions  $(x, y, z)$  of the equation

$$x + y + z = 0$$

and give its structure as a direct sum of cyclic groups.

The equation can be rewritten as  $z = -x - y$ , so the set of solutions is

$$\{(x, y, -x - y) \mid x, y \in \mathbb{Z}\}.$$

Since  $(x, y, -x - y) = x(1, 0, -1) + y(0, 1, -1)$ , the set of solutions is isomorphic to  $\mathbb{Z} \times \mathbb{Z}$ , with  $(1, 0, -1)$  and  $(0, 1, -1)$  forming a basis.

2. A group  $G$  has exponent  $e$  if  $g^e = 1$  for all  $g \in G$ . Let  $\mathbb{Z}_n^*$  denote the multiplicative group of integers prime to  $n$ , modulo  $n$ . Find all integers  $n$  such that  $\mathbb{Z}_n^*$  has exponent 2.

If  $n = p_1^{a_1} \dots p_k^{a_k}$  is written as a product of prime powers, then

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{a_1}}^* \times \dots \times \mathbb{Z}_{p_k^{a_k}}^*,$$

so the first step is to solve the problem for prime powers.

$$\mathbb{Z}_2^* \cong 1, \mathbb{Z}_4^* \cong \mathbb{Z}_2, \mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_{2^{n+2}}^* \cong \mathbb{Z}_2 \times \mathbb{Z}_{2^n}.$$

$$\text{For odd primes } p, \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}, \mathbb{Z}_{p^{n+1}}^* \cong \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^n}.$$

Thus the only prime powers for which  $\mathbb{Z}_{p^n}$  has exponent 2 are 2, 4, 8, 3. Hence  $\mathbb{Z}_n^*$  has exponent 2 if and only if  $n|24$ .

3. Let  $X$  be a  $3 \times 3$  matrix over  $\mathbb{C}$ , and let  $C(X)$  be the  $\mathbb{C}$ -vector space of  $3 \times 3$  matrices which commute with  $X$ . Show that the dimension of  $C(X)$  over  $\mathbb{C}$  is at least 3.

It is enough to prove the result for a matrix in Jordan canonical form. There are six different Jordan types to be considered. Three of these are diagonal matrices, so they centralize the three-dimensional space of diagonal matrices. For two of the remaining types,  $I, X$  and  $X^2$  are linearly independent, so they provide a three-dimensional subspace of matrices centralizing  $X$ . The remaining type has to be done by hand.

4. Let  $G$  be a group which has the following property: If  $a, b, c \in G$ , then at least two of  $a, b, c$  commute. Show that  $G$  is abelian.

Suppose that  $a, b \in G$ , and  $a$  and  $b$  do not commute. Then  $ab$  does not commute with either  $a$  or  $b$ , so  $\{a, b, ab\}$  is a set of three elements, no two of which commute.

5. Let  $X$  and  $Y$  be  $\mathbb{C}$ -linear transformations of an  $n$ -dimensional  $\mathbb{C}$ -vector space  $V$ , where  $n$  is a positive integer. Suppose that  $X$  and  $Y$  commute. Show that there exists a nonzero vector  $v \in V$ , and  $\alpha, \beta \in \mathbb{C}$ , such that  $X(v) = \alpha v$ ,  $Y(v) = \beta v$ .

(I.e. Show that  $X$  and  $Y$  have a common eigenvector. You may use the fact that a single linear transformation has an eigenvector.)

Let  $\alpha$  be an eigenvector for  $X$ . Then the subspace

$$W(\alpha) = \{w \in V \mid X(w) = \alpha w\}$$

is nonzero. The fact that  $X$  and  $Y$  commute implies that  $Y(W(\alpha)) \subseteq W(\alpha)$ . Thus  $Y|_{W(\alpha)}$  is a linear transformation of  $W(\alpha)$ , so there is a nonzero  $v \in W(\alpha)$  and some  $\beta \in \mathbb{C}$  (i.e.  $\beta$  is an eigenvalue of  $Y|_{W(\alpha)}$ ) such that  $Y(v) = \beta v$ .

6. Find all pairs of complex polynomials  $f(x), g(x) \in \mathbb{C}[x]$  such that  $f'(x)g(x) - f(x)g'(x) = 1$ . Hint:  $f'(x)f(x) - f(x)f'(x) = 0$ .

Assume  $\deg(f) \geq \deg(g)$ . There is a unique  $\alpha \in \mathbb{C}$  such that  $\deg(g - \alpha f) < \deg(f)$ . Set  $h = g - \alpha f$ . Then  $f'h - fh' = 1$ , but the degree of  $f'h - fh'$  is  $\deg(f) + \deg(h) - 1$ . This forces  $\deg(f) = 1, \deg(g) \leq 1$ , and it is easy to solve for all pairs of linear polynomials which satisfy the condition.

7. Define a binary operation  $*$  on the rational numbers  $\mathbb{Q}$  as follows:  $a*b = a+b+ab$ . Is  $\mathbb{Q}$  a group under this operation? (Explain your answer.)

It is not a group operation because  $a * (-1) = -1$  for all  $a \in \mathbb{Q}$ , which cannot happen in a group with more than one element. The identity  $(1+a)(1+b) = 1+a+b+ab$  shows that it is a group operation on  $\mathbb{Q} - \{-1\}$ . The point is that  $\mathbb{Q}$  is not a group under multiplication, although  $\mathbb{Q} - \{0\}$  is.

8. Let  $A \in M_2(\mathbb{C})$  be the  $2 \times 2$  matrix

$$A = \begin{pmatrix} 3 & 1 \\ 4 & 3 \end{pmatrix}$$

- (a) Find the eigenvalues of  $A$ .
- (b) For each eigenvalue, find a nonzero eigenvector.
- (c) Find an invertible matrix  $T$  such that  $T^{-1}AT$  is diagonal.

(a) The characteristic polynomial of  $A$  is  $\det(xI - A) = x^2 - 7x + 5$ . Its roots are 1, 5, so they are the eigenvalues of  $A$ .

(b) We assume the matrix acts from the left on column vectors, and write  $(a, b)^t$  for a column vector. Since  $A - I$  annihilates  $(1, -2)^t$  and  $A - 5I$  annihilates  $(1, 2)^t$ ,  $(1, -2)^t$  and  $(1, 2)^t$  are eigenvectors corresponding to the eigenvalues 1 and 5.

(c) Any matrix whose columns are eigenvectors for the distinct eigenvalues will work.

9. Let  $E$  be a splitting field of the polynomial  $x^5 - 2$  over  $\mathbb{Q}$ . Find the Galois group of  $E/\mathbb{Q}$ .

Let  $\alpha$  be a root of  $x^5 - 2$  and let  $\omega$  be a primitive fifth root of unity. Then  $E = \mathbb{Q}[\omega, \alpha]$  and the relevant tower of fields is  $\mathbb{Q} \subset \mathbb{Q}[\omega] \subset \mathbb{Q}[\omega, \alpha]$ , where  $\mathbb{Q}[\omega]$  is normal over  $\mathbb{Q}$  with Galois group  $\mathbb{Z}_4$ . The Galois group of  $\mathbb{Q}[\omega, \alpha]$  over  $\mathbb{Q}[\omega]$  is cyclic of order 5 with generator  $\sigma$ , where  $\sigma(\alpha) = \omega\alpha$ . The full Galois group has order 20, and is an extension of the above group by the automorphism  $\tau$ , where  $\tau(\omega) = \omega^2, \tau(\alpha) = \alpha$ . It has presentation  $\langle \sigma, \tau \mid \sigma^5 = 1, \tau^4 = 1, \tau\sigma\tau^{-1} = \sigma^2 \rangle$ .

10. Let  $A$  be a finite-dimensional associative algebra over a field  $F$ . Suppose that  $A$  has no zero divisors (i.e. If  $a, b \in A$ , and  $a, b \neq 0$ , then  $ab \neq 0$ .) Show that every nonzero element of  $A$  has a multiplicative inverse.

Let  $a$  be a nonzero element of  $A$ . Since  $A$  is finite-dimensional over  $F$ , the elements  $1, a, a^2, \dots$  are linearly dependent, so  $a$  has a minimal polynomial over  $F$ . I.e., there is a polynomial (which may be taken to be monic) of minimal degree satisfied by  $a$ , say  $f(t) = f_0 + f_1t + \dots + f_{n-1}t^{n-1} + t^n$ . If  $f_0 = 0$ , then  $a(f_1 + \dots + f_{n-1}a^{n-2} + a^{n-1}) = 0$ , so  $f_1 + \dots + f_{n-1}a^{n-2} + a^{n-1} = 0$  (since  $A$  has no zero divisors), which contradicts the minimal degree of  $f(t)$ . Dividing by  $f_0$  gives  $1 = a(f_1 + \dots + f_{n-1}a^{n-2} + a^{n-1})(-f_0^{-1})$ , which shows that  $a$  has a multiplicative inverse.