KTH Teknikvetenskap

SF2729 Groups and Rings
Suggested solutions to the final exam
Friday, May 27, 2011

PART I - GROUPS

(1) (a) The axioms of a group only state the existence of an identity element e such that $a * e = e * a = a$ for all a in the group. Show that this element is unique. **(2)**

(b) The dihedral group D_{2n} can be defined as the symmetries of a regular n-gon. Show that the center of D_{2n} is trivial if and only if n is odd. **(2)**

(c) Determine the highest order of an element in the symmetric group S_{10}. **(2)**

SOLUTION

a). Suppose that e' was another identity element. This means that we have that

$$e' = e * e' = e$$

where the first equality comes from e' being an identity element and the second from e being an identity element.

b). The dihedral group consists of n reflections in the n symmetry axes and n rotations, r^i, where r is the basic rotation by $2\pi/n$. For any reflection s, we have that $sr = r^{-1}s$, which means that no reflection is in the center, unless $r = r^{-1}$ which happens only if $n = 2$, where D_4 is abelian.

For any rotation r^i, and any reflection s, we have that $sr^i = r^{-i}s$. This means that r^i cannot be in the center unless $r^i = r^{-i}$. This happens exactly when $r^{2i} = e$. If n is odd this is impossible, and the center is therefore trivial. If n is even, we have that $r^{n/2}$ commutes with all reflections and with all rotations. Hence the center is non-trivial if n is even.

c). The order of a permutation is the least common multiple of the length of its cycles. In order to get a large order, we need cycle with no common factors between the cycle lenths. With one cycle, the order is 10, with two cycles, the order is maximal for the partition $3 + 7$, where we get order 21. With three cycles, and no common factor, we get the highest order for $5 + 3 + 2$, where we get order 30. When there are more than three cycles, we cannot avoid common factors, and the order will be smaller. Of course, we can run through all the partitions 42 partitions of 10.

(2) (a) The First Isomorphism Theorem says that there is an isomorphism $G/\ker\Phi \cong \operatorname{im}\Phi$ for any group homomorphism $\Phi : G \longrightarrow H$. Prove this theorem. **(2)**

(b) Use the First Isomorphism Theorem to show that $\mathbb{Z}^2/K \cong \mathbb{Z}_2 \times \mathbb{Z}$, where $K \leq \mathbb{Z}^2$ is the subgroup generated by $(4, 6)$. (*Hint*: Find a surjective group homomorphism $\mathbb{Z}^2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}$ with kernel K.) **(4)**

SOLUTION

a). Let $K = \ker\Phi$ and define a homorphism

$$\Psi : G/K \longrightarrow H$$

by $\Psi(aK) = \Phi(a)$, for $a \in G$. This is well-defined since if $aK = bK$, we have $ab^{-1} \in K$ and $\Phi(ab^{-1}) = e_H$. Hence $\Phi(a) = \Phi(b)$. It is a homomorphism since $\Psi(aK * bK) = \Psi(abK) = \Phi(ab) = \Psi(aK)\Psi(bK)$, for all cosets $aK, bK \in G/H$.

The homomorphism Ψ is injective since the kernel of Ψ is given by

$$\ker\Psi = \{aK \in G/K | aK = K\} = \{K\}.$$

Thus Ψ gives an isomorphism of G/K onto the image $\operatorname{im}\Psi = \operatorname{im}\Phi$.

b). In order to define a homomorphism $\Phi : \mathbb{Z}^2 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}$, it is sufficient to define $\Phi(1, 0) = (a, b)$ and $\Phi(0, 1) = (c, d)$, since $\mathbb{Z}^2$ is a free abelian group. The kernel is given by the elements $(x, y) \in \mathbb{Z}^2$ such that $ax + cy = 0$ in $\mathbb{Z}_2$ and $bx + dy = 0$ in $\mathbb{Z}$. We need that $\ker\Phi = H$. In order for $(4, 6)$ to be in the kernel, we need that $4b + 6d = 0$ in $\mathbb{Z}$, which is true if $b = 3$ and $d = -2$. The solutions to the equation $3x - 2y = 0$ is given by the multiples of $(x, y) = t(2, 3)$. In order for the kernel to be generated by $(4, 6)$ rather than by $(2, 3)$, we need that the first equation excludes $(2, 3)$ as a solution. This means that $2a + 3c \neq 0$ in $\mathbb{Z}_2$, i.e. that $c = 1$. The homomorphism $\Phi(x, y) = (\bar{y}, 3x - 2y)$ has kernel generated by $(4, 6)$ and therefore, by the isomorphism theorem, we have that $\mathbb{Z}^2/K \cong \mathbb{Z}_2 \times \mathbb{Z}$.

---

(3) When a group acts on itself by conjugation, the orbits are called *conjugacy classes*.

(a) Show that in a finite group, the size of the conjugacy class containing an element a is related to the number of elements commuting with a, i.e., the size of the centralizer, $C_G(a)$. **(2)**

(b) Use the relation to compute the size of the conjugacy class containing the matrix

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

in the general linear group $\mathrm{Gl}_2(\mathbb{F}_3)$ of invertible 2×2-matrices over the field with three elements. (Hint: the number of elements in $\mathrm{Gl}_2(\mathbb{F}_3)$ is 48.) **(4)**

SOLUTION

a). For any group action of a finite group G on a set X we have that

$$|G| = |G_x| \cdot |Gx|$$

for any element $x \in X$. In the case where G acts on itself by conjugation, we have that the stabilizer, G_a, consists of the elements $b \in G$ such that $b.a = a$, i.e., $bab^{-1} = a$. This is exactly the set of elements commuting with a, i.e., the centralizer, $C_G(a)$. Thus we have that the size of the conjugacy class of a is given by $|G|/|C_G(a)|$.

b). We look at the condition to commute with A. For a given matrix

$$B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

to commute with A, we have the condition $AB - BA = 0$. We have that

$$\begin{aligned} AB - BA &= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} - \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix} - \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} = \begin{pmatrix} c & d-a \\ 0 & c \end{pmatrix} \end{aligned}.$$

This means $AB - BA = 0$ if and only if $a = d$ and $c = 0$. Thus the matrices commuting with A are exactly the matrices of the form

$$B = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}.$$

Now we look for the elements in $C_G(A)$, which means that we only count the invertible matrices commuting with A. The only condition for B to be invertible is that $a \neq 0$. Thus $|C_G(A)| = 2 \cdot 3 = 6$. The conclusion is therefore that the conjugacy class of A contains $|G|/|C_G(A)| = 48/6 = 8$ elements.

PART II - RINGS

(1) (a) Prove that a 2×2-matrix over a field is invertible if and only if the first column is a nonzero vector and the second column is not a multiple of the first column. **(2)**

(b) Let $\mathbb{F}_q$ be a finite field with q elements. Prove that the group $\mathrm{Gl}_2(\mathbb{F}_q)$ of invertible 2×2-matrices over $\mathbb{F}_q$ has $(q^2-1)(q^2-q)$ elements. **(2)**

(c) Determine the number of zero-divisors in the ring $M_2(\mathbb{F}_q)$ of 2×2-matrices over $\mathbb{F}_q$. **(2)**

SOLUTION

a). A 2×2-matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ over a field F is invertible if and only if its determinant $ad - bc$ is invertible in F, i.e., nonzero. (The usual formula for the inverse of a 2×2-matrix holds.) It is clear that the determinant is zero if the first column is zero or if the second column is a multiple of the first column. If $a \neq 0$, then $b = \lambda a$ for some $\lambda \in F$. Then $ad - bc = a(d - \lambda c)$, so the determinant is nonzero if the second column is not a multiple of the first column. Similarly when $c \neq 0$.

b). There are $q^2 - 1$ nonzero vectors in F^2 and each of them has q distinct multiples. So there are $q^2 - 1$ choices for the first column and for each of those choices, there are $q^2 - q$ possibilities for the second column.

c). A zero-divisor is certainly not invertible, so a 2×2-matrix that is a zero-divisor must have determinant zero. Conversely,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix},$$

so a nonzero matrix with zero determinant is a zero-divisor. There are $q^4 - q^3 - q^2 + q$ matrices with nonzero determinant among the q^4 elements of $M_2(\mathbb{F}_q)$, so there are $q^3 + q^2 - q - 1$ zero-divisors.

(2) (a) Prove that $x^3 - x + 1$ is irreducible in $\mathbb{Z}_3[x]$. **(2)**

(b) Let F be the field $\mathbb{Z}_3[x]/(x^3 - x + 1)$. Write γ for the element $x + (x^3 - x + 1)$, so $F = \mathbb{Z}_3(\gamma)$. Determine the order of γ^2 in the multiplicative group F^*. **(2)**

(c) Let R be the ring $\mathbb{Z}[\sqrt{-3}]$. Is the ideal $(2, 1 + \sqrt{-3})$ a principal ideal in R? **(2)**

SOLUTION

a). A polynomial of degree 2 or 3 over a field is irreducible if and only if it has no zeroes. Every element of $\mathbb{Z}_3$ is a zero of $x^3 - x$, so $x^3 - x + 1$ has no zeroes.

b). F is indeed a field. As a vector space over $\mathbb{Z}_3$ it has dimension $n = 3$, so it has $3^n = 3^3 = 27$ elements. The multiplicative group F^* has 26 elements. The possible orders of elements of F^* are therefore 1, 2, 13 and 26; in fact, all orders occur, since F^* is well-known to be cyclic. The elements of F can uniquely be written in the form $a + b\gamma + c\gamma^2$, with a, b, and c arbitrary elements of $\mathbb{Z}_3$, so the order of γ^2 is not 1. Since $\gamma^3 = \gamma - 1$, we find that $\gamma^4 = \gamma^2 - \gamma$, so the order of γ^2 is not 2 either. Finally, since $\gamma^{26} = 1$, the order of γ^2 is at most 13 (in fact, it divides 13). So the order of γ^2 equals 13.

c). The ring $\mathbb{Z}[\sqrt{-3}]$ has a multiplicative norm given by

$$N(a + b\sqrt{-3}) = (a + b\sqrt{-3})(a - b\sqrt{-3}) = a^2 + 3b^2.$$

We see directly that the only units are ± 1. The elements 2 and $1 + \sqrt{-3}$ both have norm 4. If the ideal they generate is principal, then the norm of a generator must divide 4. The generator cannot have norm 4, since 2 and $1 + \sqrt{-3}$ don't differ by a unit. There is no element with norm 2, so the only possibility left is a generator with norm 1, in which case the ideal would equal R. However, one easily checks that every element $a + b\sqrt{-3}$ of the ideal $(2, 1 + \sqrt{-3})$ has the property that $a + b$ is even, so 1 is not in the ideal. The conclusion is that the ideal is not principal.

---

(3) (a) Prove that $f(x) = x^4 + 4x^2 + 2$ is irreducible in $\mathbb{Q}[x]$. **(2)**

(b) Let K be the field $\mathbb{Q}[x]/(f(x))$. Write α for the element $x + (f(x))$, so $K = \mathbb{Q}(\alpha)$. Put $\beta = \alpha^2$. Determine $[\mathbb{Q}(\beta) : \mathbb{Q}]$ and show that $f(x)$ factors as a product of two polynomials of positive degree in $\mathbb{Q}(\beta)[x]$. **(2)**

(c) Prove that $\alpha^3 + 3\alpha$ is a zero of $f(x)$ and conclude that $f(x)$ factors as a product of linear factors in $\mathbb{Q}(\alpha)[x]$. **(2)**

SOLUTION

a). This follows immediately from the Eisenstein criterion for $p = 2$.

b). The element $\beta = \alpha^2$ is a zero of the polynomial $g(x) = x^2 + 4x + 2$, which also is irreducible in $\mathbb{Q}[x]$ (for the same reason). So $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Clearly, $g(x) = (x - \beta)(x + 4 + \beta)$ in $\mathbb{Q}(\beta)[x]$. So $f(x) = g(x^2) = (x^2 - \beta)(x^2 + 4 + \beta)$ in $\mathbb{Q}(\beta)[x]$, which gives a factorisation as desired.

c). Clearly, α and $-\alpha$ are the zeroes of the factor $(x^2 - \beta)$ in $\mathbb{Q}(\alpha)$. So we should check that $\alpha^3 + 3\alpha$ is a zero of $x^2 + 4 + \beta$. A computation using that $\alpha^4 = -4\alpha^2 - 2$ and hence $\alpha^6 = -4\alpha^4 - 2\alpha^2$ shows that this is indeed the case:

$$(\alpha^3 + 3\alpha)^2 + 4 + \alpha^2 = \alpha^6 + 6\alpha^4 + 10\alpha^2 + 4 = 2\alpha^4 + 8\alpha^2 + 4 = 0.$$

Clearly, $-\alpha^3 - 3\alpha$ is then a zero of $f(x)$ as well. Having found four distinct zeroes of $f(x)$ in $\mathbb{Q}(\alpha)$, we conclude that $f(x)$ factors as a product of linear factors in $\mathbb{Q}(\alpha)[x]$. (We have shown that $\mathbb{Q}(\alpha)$ is a splitting field for $f(x)$ over $\mathbb{Q}$.)
