KTH Teknikvetenskap

SF2729 Groups and Rings
Suggested solutions to the final exam
Wednesday, May 26, 2010

PART I - GROUPS

(1) (a) Show directly from the axioms that there is a unique group with three elements up to isomorphism. **(2)**
(b) Show that the group $\mathrm{Gl}_2(\mathbb{F}_2)$ of invertible 2×2-matrices over the field $\mathbb{F}_2 = \{0, 1\}$ is isomorphic to the symmetric group S_3 by giving an explicit isomorphism. **(2)**
(c) Compute the center of the general linear group $\mathrm{Gl}_n(\mathbb{C})$, i.e., the group of invertible complex $n \times n$-matrices. **(2)**

SOLUTION

a). Denote the three elements by e, a and b, where e is the unit element. We then have that $e * e = e$, $a * e = e * a = a$ and $e * b = b * e = b$. Thus the group table is given by

$*$	e	a	b
e	e	a	b
a	a	?	?
b	b	?	?

Suppose that $a*a = a$. Since we have an inverse to a, say a^{-1}, we get by multiplication to the left that

$$a^{-1} * (a * a) = a^{-1} * a = e$$

but by the associativity, we get $A^{-1} * (a * a) = (a^{-1} * a) * a = e * a = a$, which is a contradiction since a and e are supposed to be distinct elements. In the same way, we get that $b * b \neq b$.

If $a * b = a$, we get

$$e = a^{-1} * a = a^{-1} * (a * b) = (a^{-1} * a) * b = e * b = b$$

and if $a * b = b$, we get

$$e = b * b^{-1} = (a * b) * b^{-1} = a * (b * b^{-1}) = a * e = a.$$

Thus we conclude that $a * b = e$ and by symmetry in the argument, we also get $b * a = e$.

If $a * a = e$, we get that

$$b = e * b = (a * a) * b = a * (a * b) = a * e = a,$$

contradicting $a \neq b$. By symmety, we get $b * b \neq e$.

We have already seen that $a*a \neq a$ and thus we must have $a*a = b$. By the symmetry we also get $b * b = a$.

We have concluded that the group table has to be

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

b). There are six invertible matrices in $\mathrm{Gl}_2(\mathbb{F}_2)$, since the first row can be chosen as any of the three non-zero rows and the second as anything but the two multiples of the first.

Thus we have the six matrices

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$
$$C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, D = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, E = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

We have that I is the unity and A, C and E are their own inverses, since $A^2 = C^2 = E^2 = I$. The remaining elements B and D have order three since $B^2 = D$, $D^2 = B$ and $B^3 = B(B^2) = BD = I = D^2D = D^3$.

We can find an explicit isomorphism to S_3 by sending the generators A and C to $s_1 = (1\,2)$ and $s_2 = (2\,3)$, respectively. Thus we get

$$\Phi(I) = Id,\ \Phi(A) = (1\,2),\ \Phi(C) = (2\,3),$$
$$\Phi(B) = \Phi(AC) = (1\,2)(2\,3) = (1\,2\,3),$$
$$\Phi(D) = \Phi(CBC) = (2\,3)(1\,2\,3)(2\,3) = (1\,3\,2)$$
$$\Phi(E) = \Phi(CAC) = (2\,3)(1\,2)(2\,3) = (1\,3).$$

We can check that the group tables are the same:

$\cdot$	I	A	B	C	D	E
I	I	A	B	C	D	E
A	A	I	C	B	E	D
B	B	E	D	A	I	C
C	C	D	E	I	A	B
D	D	C	I	E	B	A
E	E	C	A	D	C	I

c). An element in the center commutes with every element in the group and in particular, we have that it commutes with all the elementary matrices E_{ij}, corresponding to interschanging row i and row j, when multiplying to the left. However, when multiplying to the right it corresponds to interchanging columns i and j.

---

(2) (a) Define what it means for a group to act on a set and show that any group acts on itself by conjugation, i.e., by $a.b = aba^{-1}$, for $a, b \in G$. **(2)**

(b) Use 2a to prove the *class equation* for a finite group G, i.e.,

$$|G| = |Z(G)| + \sum_{i=1}^{r} \frac{|G|}{|C_G(a_i)|}$$

where $C_G(a) = \{b \in G | ab = ba\}$ and $a_1, a_2, \ldots, a_r$ are representatives of all the non-trivial conjugacy classes in G. **(2)**

(c) Use the class equation to show that any non-abelian group of order $2p$, where p is an odd prime, has p elements of order 2 and $p-1$ elements of order p. **(2)**

SOLUTION

a). The conjugation definines a function

$$G \times G \longrightarrow G$$

sending (a, b) to aba^{-1}. We have to check that it satisfies the conditions of a group action, i.e.,

(a) $e.x = x$, for all $x \in G$.

(b) $(ab).x = a.(b.x)$, for all $a, b \in G$ and for all $x \in G$.

We have 2a since $exe^{-1} = x$ for all $x \in G$ and we have 2b since

$$(ab).x = (ab)x(ab)^{-1} = abxb^{-1}a^{-1} = a(bxb^{-1})a^{-1} = a.(b.x)$$

for all $a, b \in G$ and all $x \in G$.

b). The conjugacy classes are the orbits of G under the action by conjugation. Thus they partition G into disjoint subsets. The stabilizor of an element a under this action is given by

$$G_a = \{b \in G | bab^{-1} = a\} = \{b \in G | ba = ab\} = C_G(a).$$

Hence we get that the size of the orbit of a is given by

$$[Ga| = \frac{|G|}{|G_a|} = \frac{|G|}{|C_G(a)|}.$$

The orbit is trivial, i.e., contains only a, if and only if $C_G(a) = G$, which is equivalent to that a commutes with all elements in G. Thus we can collect all trivial conjugacy classes and the union of them will be the center of G. Thus the class equation is the consequence of the partition of G into the center and the the non-trivial conjugacy classes.

c). If G has order $2p$ where p is an odd prime, the only possibilities for the order of a subgroup are 1, 2, p and $2p$ by Lagrange's theorem. Thus we have that the non-trivial conjugacy classes have 2 or p elements, since not all elements are in the same conjugacy class.

In the class equation, we have $2p$ on the left hand side and hence there cannot be two terms of size p in the sum, since the center contains at least one element. If there is no term of size p, we have that the center must be of size 2 or $2p$ since all other terms are even. In the latter case G would be abelian, which it is supposed not to be. Thus we

conclude that $|Z(G)| = 2$, but since the center is in all the centralizers $C_G(a)$, these have to have order 2 as well, which would give terms of size p in the sum.

Hence there must be exactly one term of size p in the sum. The center would then either have order 1 or p. Again, the center is contained in all the centralizers, which contradicts that one of the centralizers has order 2 if the center has order p. Hence the center must be trivial and there is one conjugacy class of size p and $(p-1)/2$ conjugacy classes of size 2.

The centralizer, $C_G(a)$ contains the subgroup generated by a. Hence the elements in the conjugacy classes of size 2 generates a subgroup of a group of order p, which means that they have to have order p. In the same way, the elements in the conjugacy class of size p generates subgroups of a group of order 2, which shows that they have order 2. We have concluded that there are exactly p elements of order 2 and $p-1$ elements of order p.

---

(3) (a) An *automorphism* of a group G is an isomorphism from G to itself. Show that the set $\mathrm{Aut}(G)$ of automorphisms of G forms a group under composition. **(2)**

(b) Show that the set $\mathrm{Inn}(G)$ of *inner automorphisms*, i.e., $a \mapsto bab^{-1}$, for some b in G, forms a subgroup of $\mathrm{Aut}(G)$. **(2)**

c) Determine the automorphism group of the non-cyclic group of order 4. **(2)**

SOLUTION

a). Composition of functions $X \to X$ satisfies associativity since there is a well define notion of composition of three maps $X \xrightarrow{\Phi} X \xrightarrow{\Psi} X \xrightarrow{\Xi} X$.

The identity map is a unity for composition and bijective maps are invertible with a bijective inverse. This shows that the set of bijective maps on a set X forms a group under composition. We now look at the subset of bijective homomorphisms of a group G. If Φ and Ψ are homomorphisms, we have that

$$\Psi \circ \Phi(ab) = \Psi(\Phi(ab)) = \Psi(\Phi(a)\Phi(b)) = \Psi(\Phi(a))\Psi(\Phi(b))$$

for any $a, b \in G$. Thus $\Phi \circ \Phi$ is also a homomorphism.

Furthermore, if Φ is bijective, it has an inverse Φ^{-1} and we get that

$$\Phi^{-1}(ab) = \Phi^{-1}(\Phi\Phi^{-1}(a)\Phi\Phi^{-1}(b)) = \Phi^{-1}(\Phi(\Phi^{-1}(a)\Phi^{-1}(b)) = \phi^{-1}(a)\Phi^{-1}(b)$$

which shows that Φ^{-1} is also a homomorphism. Thus the set of bijective homomorphisms form a subgroup of the symmetric group on G.

b). Let a be any element of a group G. Then the map Φ_a definied by

$$\Phi_a(b) = abbb^{-1}$$

defines a homomorphism of G since

$$\Phi_a(bc) = abca^{-1} \ = aba^{-1}aca^{-1} = \Phi_a(b)\Phi_a(c)$$

and it is bijective since

$$\Phi_a \circ \Phi_{a^{-1}}(b) = a(a^{-1}b(a^{-1})^{-1})a^{-1} = (aa^{-1})b(aa^{-1}) = b$$

for any element $b \in G$.

The composition of two inner automorphisms, Φ_a and Φ_b is given by Φ_{ab} since

$$\Phi_a \circ \Phi_b(c) = a(b(cb^{-1})a^{-1} = (ab)c(ab)^{-1} = \Phi_{ab}$$

for all elements $c \in G$. Furthermore, as we saw before, the inverse of en inner atuomoprphism Φ_a is $\Phi_{a^{-1}}$, which is also an inner arutomorphism. Hence $\mathrm{Inn}(G)$ is a subgroup of $\mathrm{Aut}(G)$.

c). The non-cyclic group G of order four has three elements of order 2. As we saw in part a) the automorphism group is a subgroup of the symmetric group on G. Since an automorphism has to send the unit element to the unit element, we have that the automorphism group is a subgroup of the stabilizer of the unit element, which means that it is isomorphic to a subgroup of S_3.

Now, write the group G as $G = \{e, a, b, c\}$, where a, b, c are the elements of order two.

The group G can be presented by the generators a and b with the relations $a^2 = b^2 = e$ and $ab = ba$. An automorphism is determined by the images of the generators, which in turn have to be a generating set of the group and have to satisfy the same relations.

There are six possiblilities of finding an ordered pairs of generators:

$$\{a, b\}, \{a, c\}, \{b, a\}, \{b, c\}, \{c, a\} \text{ and } \{c, b\}.$$

Each of these generator pairs satifsy the same relations, since

$$a^2 = b^2 = c^2 = e \text{ and } ab = ba,\ bc = cb,\ ac = ca.$$

Thus we have six different automorphism and hence the automorphism group is isomorphic to S_3.

PART II - RINGS

(1) Consider the ring $R = \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$.
   (a) Compute its characteristic, $\mathrm{char}(R)$. **(2)**
   (b) Show that $R \cong \mathbb{Z}_{60} \times \mathbb{Z}_3$ as rings. **(2)**
   (c) Let R be a commutative ring with unity and let I and J be two ideals in R satisfying $I + J = R$ and $I \cap J = (0)$. Show that $R \cong R/I \times R/J$. **(2)**

SOLUTION

a). For all $(n_1, n_2, n_3, n_4) \in \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$ and an integer k it is $k(n_1, n_2, n_3, n_4) = 0$ only if $3/k, 4/k, 5/k$, which implies that the minimum such k must be the $l.c.m(3, 5, 4) = 60$.

b). The ring homomorphism:

$$\phi : \mathbb{Z} \to \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3, n \mapsto ([n]_5, [n]_4, [n]_5)$$

is an a surjective ring homomorphism with $Ker(\phi) = 60\mathbb{Z}$ (because $3, 4, 5$ are relatively prime). The fundamental isomorphism theorem for rings then implies that

$$\mathbb{Z}/60\mathbb{Z} \cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3.$$

It follows that

$$(\phi, id) : \mathbb{Z}_{60} \times \mathbb{Z}_3 \to \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3$$

is also a ring isomorphism.

c). Consider the projection maps: $\phi_1 : R \to R/I, \phi_2 : R \to R/J$. Because ϕ_1, ϕ_2 are ring homomorphisms the product map:

$$\phi : R \to R/I \times R/J, \phi(r) = (\phi_1(r), \phi_2(r))$$

is a ring homomorphism, where the ring $R/I \times R/J$ has the coordinate-wise operations.
The kernel is

$$Ker(\phi) = \{r, r \in I \text{ and } r \in J\} = I \cap J = (0).$$

Moreover because $R = I + J$ for every $(a + I, b + J) \in R/I \times R/J$ we have that $a = a_1 + a_2$ where $a_1 \in I, a_2 \in J$ and $a + I = a_2 + I$. Similarly $b = b_1 + b_2$ where $b_1 \in I, b_2 \in J$ and $b + j = b_1 + j$. Which means that $\phi(a_2 + b_1) = (a + I, b + J)$. showing that $Im(\phi) = R/I \times R/J$. By the fundamental isomorphism theorem we have that

$$R/Ker(\phi) = R \cong Im(\phi) = R/I \times R/J.$$

(2) Consider the polynomial $p(x) = x^3 + 2x^2 - 5x - 3$ as a polynomial in the polynomial rings $\mathbb{Q}[x]$ and $\mathbb{Z}_5[x]$, and let $R = \mathbb{Q}[x]/(p(x))$ and $S = \mathbb{Z}_5[x]/(p(x))$.
   (a) Show that R is a vector space over $\mathbb{Q}$ and that S is a vector space over $\mathbb{Z}_5$. What are the dimensions of these vector spaces? **(2)**
   (b) Determine whether R and/or S are integral domains or even fields? **(2)**

(c) Show that R/P is a field whenever R is a PID and P is a prime ideal in R. **(2)**

SOLUTION

a). R and S are both abelian groups, therefore we have to show that they have a scalar multiplication satisfying the necessary properties. We do this for R, the prove for S is similar.

Define the scalar product as:

$$\mathbb{Q} \times \mathbb{Q}[x]/(p(x)) \to \mathbb{Q}[x]/(p(x))\,(a, f(x) + (p(x))) \mapsto af(x) + (p(x)).$$

It satisfies the properties:

- $(ab)(f(x) + (p(x))) = (ab)f(x) + (p(x)) = (a)(bf(x) + (p(x)))$.
- $(a+b)(f(x)+(p(x))) = (a+b)f(x)+(p(x)) = (a)f(x)+(p(x)))+a)f(x)+(p(x)))$.
- $a(f(x) + g(x) + (p(x))) = af(x) + ag(x) + (p(x))$.
- $1(f(x) + (p(x))) = f(x) + (p(x))$.

Notice that every element f in R (resp. in S) can be divided by p and can be written as $f = mp + r$ where $m \in \mathbb{Q}$ and $r \in R$ (resp. in S) is the class of a polynomial of degree at most 2. This shows that $S = span([1], [x], [x^2])$. Moreover $[1], [x], [x^2]$ are linearly independent over $\mathbb{Q}$ and thus

$$\dim_{\mathbb{Q}}(S) = \dim_{\mathbb{Q}}(R) = 3.$$

b). An ideal in R and S is maximal if and only if prime. Moreover an ideal is prime if and only if its generator (recall that R and S are PID) is irreducible.

One sees immediately that $p(x) = x^3 + 2x^2 - 5x - 3$ has the root 1 in $\mathbb{Z}_5$ and thus S is neither a field nor an integral domain.

The polynomial $p(x) = x^3 + 2x^2 - 5x - 3$ is going to be irreducible over $\mathbb{Q}$ if we prove that it is irreducible over $\mathbb{Z}$. If p is reducinble it would have at least one simple root α which should be an integer dividing -3. The only possibilities are $-3. -1, 1, 3$ which are not roots. It follows that R is a field.

c). Let $I = (a)$ be a prime ideal and assume $I \subset J \subset R$. Let $J = (b)$, then $a = bc$ for some element $c \in R$. Because I is prime then it is $b \in I$ which implies $I = J$ or $c \in I$, i.e. $c = ad$ and thus (because R is a domain) $bc = 1$ implying that $J = R$.

(3) Recall that a field extension L of a field F is called a splitting field of $f(x)$ over F if the following holds:
   (i) $f(x)$ splits as a product of linear factors in $L[x]$.
   (ii) If $L' \subseteq L$ is another extension such that $f(x)$ splits as a product of linear factors in $L'[x]$, then $L' = L$.
   (a) Show that $\mathbb{Q}(i)$ is a splitting field of $x^2 - 2x + 2$ over $\mathbb{Q}$. **(2)**
   (b) Let F be a field and let $f(x) \in F[x]$ be an irreducible polynomial of degree 2. Show that $F[x]/(f(x))$ is a splitting field of $f(x)$ over F of degree 2. **(2)**
   (c) Give an example of a field F and an irreducible polynomial $p(x) \in F[x]$ of degree 3 such that $F[x]/(p(x))$ is not a splitting field for $f(x)$ over F. **(2)**

SOLUTION

a). Because $x^2 - 2x + 2 = (x - 1 + i)(x - 1 - i)$ the extension $\mathbb{Q}(i)$ contains both roots. Any other algebraic extension, L, containing the two roots would have to contain the rational numbers and the complex number i giving $\mathbb{Q}(i) \subset L$.

b). Let $\alpha = x + (f(x)) \in F[x]/(f(x))$. It is $ev_\alpha(f(x)) = 0 \in F[x]/(f(x))$ and thus α is a root of f. It follows that $f(x) = (x-\alpha)(ax-\beta)$ for some $a, \beta \in F[x]/(f(x))$ and thus both roots must lie in $F[x]/(f(x))$. Moreover Let L be any other extension containing α. Because f is irreducible over F and $\alpha \notin F$ the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. Moreover because $\mathbb{Q}(\alpha) \subset F[x]/(f(x))$ and they are both of degree 2 it must be $\mathbb{Q}(\alpha) = F[x]/(f(x))$. But $\mathbb{Q}(\alpha) \subset L$ and thus $F[x]/(f(x)) \subset L$.

c). Consider $F = \mathbb{Q}$ and $p(x) = x^3 - 2$. The extension $\mathbb{Q}[x]/x^3 - 2 = \mathbb{Q}(\sqrt[3]{2})$, because $x^3 - 2$ is the minimal polynomial of $\sqrt[3]{2}$ over $\mathbb{Q}$. The other roots of p are $\xi\sqrt[3]{2}$ and $\xi^2\sqrt[3]{2}$ where $\xi \in \mathbb{C}$ is a third root of unity. It follows that the splitting field for $f(x)$ over F is $\mathbb{Q}(\sqrt[3]{2}, \xi) \neq \mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x]/x^3 - 2$.