KTH Teknikvetenskap

SF2729 Groups and Rings
Suggested solutions to the final exam
Thursday, August 19, 2010

PART I - GROUPS

(1) (a) Give an example of a binary operation on $S = \{1, 2, 3\}$ which is commutative with a unit, but which fails to be associative. **(2)**
(b) Show that any finite cyclic group has exactly one subgroup of any order dividing the order of the group. **(2)**
(c) For all integers $n \geq 2$, compute the center of the dihedral group, D_{2n}, i.e. the group of symmetries of a regular n-gon. **(2)**

SOLUTION

a). Assume that 1 is the unit element. If we have that $a * b = 1$ and $b * c = 1$, we get that $(a * b) * c = 1 * c = c$, while $a * (b * c) = a * 1 = a$, so if $a \neq c$, the operation is not associative. We can acheive this if $a * b = 1$ whenever $a \neq 1$ and $b \neq 1$. In order for the operation to be commutative, we need that the table is symmetric. Hence the following operation satisfies the criteria:

$*$	1	2	3
1	1	2	3
2	2	1	1
3	3	1	1

since for example $(2 * 2) * 3 = 1 * 3 = 3$, while $2 * (2 * 3) = 2 * 1 = 2$.

b). We can assume that our cyclic group is of order n and equals $\mathbb{Z}_n$ under addition since all cyclic groups of the same order are isomorphic.

Let d be any divisor of n. We can define a subgroup of order d as

$$\langle [n/d]_n \rangle = \{[n/d]_n, [2n/d]_n, 3[n/d]_n, \ldots, d[n/d]_n = 0\}.$$

Let H be any subgroup of $\mathbb{Z}_n$ of order d and let a be the least positive integer such that $[a]_d \in H$. Then H consists of all multiples of $[a]_n$. In fact, if $[b]_n$ is in H we can divide b by a and get $b = qa + r$, where $0 \leq r < a$. Since H is a subgroup we have that $[r]_n = [b]_n - q[a]_n$ is also in H and by the minimality of a we get that $r = 0$ and hence $[b]_n = q[a]_n$.

Now H has order n/a and we deduce that H is exactly the subgroup of order d given before. Hence there is exactly one subgroup of order d for any d dividing n.

c). The symmetries of a regular n-gon consists of n rotations, including the trivial rotation which is the unit element, together with n reflections. Let r be a rotation generating the rotation subgroup and let s be any of the reflections. Then D_{2n} is generated by r and s. In order to find the center, it is sufficient to find all the elements which commute with both generators.

We can write any of the rotations as r^i for some $i = 0, 1, \ldots, n-1$. In trivially commutes with r, but in order to commute with s, we have to have

$$r^i s = sr^i.$$

We have the relation $sr = r^{-1}s$, which comes from that when we conjugate a rotation by a reflection, we get the reverse rotation. Hence we have that $r^i s = sr^{-i}$ and in order for r^i to commute with s, we need $sr^i = sr^{-i}$, which is equivalent to $r^{2i} = 1$. Thus we conclude that the only rotations that are in the center are $r^0 = 1$ and $r^{n/2}$ if n is even.

The reflections can be written as sr^i and for this to commute with s we need

$$ssr^i = sr^i s \Longleftrightarrow r^i = r^{-i}$$

but in order to commute with r we need

$$rsr^i = sr^i r \Longleftrightarrow r^{i-1} = r^{i+1} \Longleftrightarrow r^2 = 1.$$

Hence a reflection is in the center if and only if $n = 2$, in which case the group is of order 4 and abelian. Hence for $n \geq 2$ we have that the center is trivial for odd n and equal to $\{1, r^{n/2}\}$ for even n.

---

(2) (a) Show that the center of any group is a normal subgroup and deduce that any simple group has a trivial center. **(2)**

(b) Let $\Phi : G \longrightarrow H$ be a group homomorphism and let K be a normal subgroup of H. Show that $\Phi^{-1}(K) = \{a \in G | \Phi(a) \in K\}$ is a normal subgroup of G. **(2)**

(c) Show that in the situation described in (2b) we get an induced homomorphism

$$\tilde{\Phi} : G/\Phi^{-1}(K) \longrightarrow H/K.$$

(2)

SOLUTION

a). Let $Z = Z(G)$ be the center of a group G and let z be any element of Z. Then we have that

$$aza^{-1} = zaa^{-1} = z$$

for any element $a \in G$. Hence $aZa^{-1} = Z$ and Z is normal. A simple group has no non-trivial normal subgroups and hence its center has to be trivial since it is normal.

b). Let a be any element of G and let b be any element of $\Phi^{-1}(K)$. Then we have that $\Phi(b) \in K$ and we get that

$$\Phi(aba^{-1}) = \Phi(a)\Phi(b)\Phi(a^{-1}) = \Phi(a)\Phi(b)\Phi(a)^{-1} \in K$$

since $\Phi(b) \in K$ and K is normal. We thus have that aba^{-1} is in $\Phi^{-1}(K)$ and hence $\Phi^{-1}(K)$ is normal.

c). We define the homomorphism $\tilde{\Phi} : G/\Phi^{-1}(K) \longrightarrow H/K$ by $\tilde{\Phi}(a\Phi^{-1}(K)) = \Phi(a)K$, for $a \in G$. We have to check that this is well-defined. If $a\Phi^{-1}(K) = b\Phi^{-1}(K)$ we have that $a^{-1}b \in \Phi^{-1}(K)$ and hence $\Phi(a^{-1}b) \in K$ and $\Phi(a)K = \Phi(b)K$, which shows that the result doesn't depend on which representative we choose for the cosets of $\Phi^{-1}(K)$.

Furthermore, $\tilde{\Phi}$ is a homomorphism since

$$\begin{aligned}\tilde{\Phi}(a\Phi^{-1}(K)b\Phi^{-1}(K)) &= \tilde{\Phi}(ab\Phi^{-1}(K)) = \Phi(ab)K = \Phi(a)K\Phi(b)K \\ &= \tilde{\Phi}(a\Phi^{-1}(K))\tilde{\Phi}(b\Phi^{-1}(K)).\end{aligned}$$

---

(3) A group G which acts on a set X is said to act *freely* if all stabilizers are trivial.
- (a) Show that any group acts freely on itself by left multiplication. **(1)**
- (b) Show that if a finite group G acts freely on a non-empty set X, then $|X| \geq |G|$. **(2)**
- (c) Show that any free action of a group G can be identified with the action of the group on a union of copies G where G acts by left multiplication on each copy of G. **(3)**

SOLUTION

a). A group acts on itself by left multiplication as we have that

$$e.a = e * a = a, \qquad \forall a \in G,$$

and

$$a.(b.c) = a * (b * c) = (a * b) * c = (a * b).c.$$

This action is free since $a.b = b \iff a * b = b \iff a = e$. Hence the stabilizer G_b is trivial for any element b in G.

b). If G is a finite group acting on a set X we have that $|G| = |Gx||G_x|$ for any element x in X. If the action is free we have that all orbits have size $|G|$. Since X is a disjoint union of the orbits under the action X contains at least one subset of size $|G|$.

c). Let G be a group that acts freely on a set X and let B be a subset of X consisting of exactly one element from each orbit. Then we can identify X with $B \times G$ under the map

$$\begin{aligned} G \times B &\longrightarrow X \\ (a, b) &\longmapsto a.b \end{aligned}$$

The map is surjective since X is the union of the orbits and each orbit is mapped onto by $G \times \{b\}$, where b is the element in B corresponding to the orbit. It is injective since $a.b = c.d$ implies that $b = d$ since B has only one element from each orbit, and hence $a.b = c.b$ which implies that $a^{-1}c$ is in G_b. Since the action is free, we deduce that $a = c$ and the map is injective.

When identifying $G \times B$ with X in this way, we get that the action of G on X corresponds to an action of G on $G \times B$ given by

$$c.(a, b) = c.(a.b) = (ca).b$$

Thus the action is equivalent to left muliplication on each orbit.

PART II - RINGS

(1) Consider the function $\phi : \mathbb{Z}[x] \to \mathbb{Z}_8$ defined by $f(x) \mapsto [f(3)]_8$.

  (a) Show that ϕ is a ring homomorphism. **(1)**

  (b) Show that $ker(\phi)$ is not a prime ideal. **(2)**

  (c) Show that $ker(\phi)$ is finitely generated and find a finite set of generators. **(3)**

SOLUTION

a). $\phi((f+g)(x)) = [(f+g)(3)]_8 = [f(3)]_8 + [g(3)]_8 = \phi(f) + \phi(g)$, $\phi((f \cdot g)(x)) = [(f \cdot g)(3)]_8 = [f(3)]_8 \cdot [g(3)]_8 = \phi(f) \cdot \phi(g)$

b). ϕ is surjective since for every $[k]_8 \in \mathbb{Z}_8$ we have that $\phi([k]_8) = [k]_8$. The fundametal theorem of ring homomorphisms implies that

$$\mathbb{Z}[x]/Ker(\phi) \cong \mathbb{Z}_8.$$

Because $\mathbb{Z}[x]$ is a commutative ring with unity and because $\mathbb{Z}_8$ is not an integral domain (for ex. $[2]_8 \cdot [4]_8 = 0$) the ideal $ker(\phi)$ cannot be prime.

c). We see that $ker(\phi) = \{f(x) \| [f(3)]_8 = 0\}$. Clearly $x - 3$ and 8 belong to $ker(\phi)$ so that $< x-3, 8 > \subseteq ker(\phi)$. Let $f(x) \in ker(\phi)$. Because $x - 3$ is monic the division theorem implies that

$$f(x) = (x-3)q(x) + r(x)$$

with $r(x) = 0$ or $\deg(r(x)) = 0$. Assume $r(x) = r \in \mathbb{Z}$. Because $[f(3)]_8 = 0$ it follows that $[r]_8 = 0$ and thus $r \in 8\mathbb{Z}$. This shows that $f(x)$ can be written as a combination of $(x-3)$ and 8 which implies that $ker(\phi) \subseteq < x-3, 8 >$ and thus

$$ker(\phi) = < x-3, 8 > .$$

---

(2) Consider the field with q elements, $\mathbb{F}_q$, and the polynomial $f(x) = x^2 + 1 \in \mathbb{F}_q[x]$. Let $K = \mathbb{F}_q[x]/(f(x))$.

  (a) Compute the number of elements in K. **(2)**

  (b) Determine all integers q for which K is a field. **(4)**

SOLUTION

a). Observe that K is a vector field over $\mathbb{F}_q$ of dimension 2. In fact it is

$$K = \{a_0 + a_1 x, a_0, a_1 \in \mathbb{F}_q\}.$$

Moreover the elements $1, x$ are linearly independet so that $\{1, x\}$ is a basis of K as a vector space over $\mathbb{F}_q$ and thus $|K| = q^2$.

b). Because $\mathbb{F}_q$ is a field the integer q must be a power of a prime. Moreover $\mathbb{F}_q[x]$ is an Eucledian Domain and thus a PID. This implies that the ideal generated by the polynomial $f(x)$ is maximal if and only if $f(x)$ is irreducible and thus K is a field if and only if $f(x)$ is irreducible. Because $\mathrm{char}(\mathbb{F}_q) = 2$ for all even q the polynomial is reducible for all such q. In fact we have that

$$(x^2 + 1) = (x + 1)^2.$$

Assume that q is odd. The polynomial $f(x)$ is irreducible if only if it has no root in $\mathbb{F}_q$, i.e. if there i no element $\alpha \in \mathbb{F}_q$ such that $\alpha^2 = -1$. Assume that $f(x)$ is reducible, then there is an element $\alpha \in \mathbb{F}_q$ such that $\alpha^2 = -1$. This means that α has order 4 in the group $(\mathbb{F}_q^*, \cdot)$. By Lagrange theorem the $4/|\mathbb{F}_q^*| = q - 1$, so that $q \equiv 1 \bmod 4$. Conversely if $q \equiv 1 \bmod 4$, then 4 divides $q - 1$ and since $\mathbb{F}_q^*$ is cyclic, there is an element $a \in \mathbb{F}_q^*$ of order 4, i.e. an element a such that $a^4 = 1$ and $a \neq \pm 1$. This implies that $\alpha^2 = -1$. We can conlude that K is a field if and only if q is odd and it is not congruent to 1 modulo 4. This is equivalent to $q \equiv 3 \pmod 4$, and since q is a prime power it is an odd power of a prime p satisfying $p \equiv 3 \pmod 4$.

---

(3) Let A be a commutative ring with unity. An element $a \in A$ is said to be *nilpotent* if $a^k = 0$ for some k. Let $N(A)$ be the set of all nilpotent elements of A.

(a) Show that $N(A)$ is an ideal. **(2)**

(b) Show that all $N(A)$ is contained in every prime ideal of A. **(1)**

(c) Show that $N(A)$ is the intersection of all prime ideals of A. **(3)**

SOLUTION

a). First we show that $N(A)$ is closed under addition. Let a and b be elements in $N(A)$. Then there are integers k and m such that $a^k = 0$ and $b^m = 0$ and since A is commutative we can use the binomial theorem to get that

$$(a + b)^{k+m} = \sum_{i=0}^{k+m} \binom{k+m}{i} a^i b^{k+m-i}$$

which is zero since $a^i = 0$ for $i \geq k$ and $b^{k+m-i} = 0$ for $i \leq k$. Hence $a + b \in N(A)$.

We now show that $N(A)$ is closed under multiplication by elements from A. Let $a \in A$ and $b \in N(A)$. There is k such that $b^k = 0$. Because A is commutative it is $(a \cdot b)^k = a^k \cdot b^k$ and thus $(a \cdot b)^k = a^k \cdot 0 = 0$ which implies that $a \cdot b \in N(A)$.

b). Let $x \in N(A)$. Then there is k such that $x^k = 0$. For every prime ideal P of A we have that $0 \in P$ and thus $x^k \in P$. From the definition of prime ideal it follows that $x \in P$.

c). We have shown in the previous part that:

$$N(A) \subseteq \bigcap_{P \text{ prime}} P.$$

Let now $x \notin N(A)$. We will show that there is a prime ideal P such that $x \notin P$, which will imply that $N(A) = \bigcap_{P \text{ prime}} P$. Let $S = \{x^n, n \in \mathbb{N}\}$ and consider

$$\mathcal{F} = \{I \subset A, I \text{ ideal }, I \cap S = \emptyset\}.$$

Because $x \notin N(A)$ it is $(0) \in \mathcal{F}$ and thus $\mathcal{F}$ is a non empty family of ideals. There is then a maximal element (by Zorn's Lemma) of $\mathcal{F}$ with respect to the inclusion order, $\subseteq$. Let P be the maximal element. By definition $x \notin P$. We are left to show that P is a prime ideal, i.e. that for all $a, b \in A$ such that $a \notin P$ and $b \notin P$ it is $ab \notin P$. Because $a \notin P$ and $b \notin P$ and because P is maximal in $\mathcal{F}$ the ideals $P + (a)$ and $P + (b)$ have to intersect S :

$$P + (a) \cap S \neq \emptyset, P + (b) \cap S \neq \emptyset.$$

It follows that there are $n, m \in \mathbb{N}, p_1, p_2 \in P, h_1, h_2 \in A$ such that $x^n = p_1 + ah_1, x^m = p_2 + bh_2$. This implies that:

$$x^{n+m} = p_1p_2 + p_1bh_2 + p_2ah_1 + abh_1h_2$$

and thus $x^{n+m} \in P + (ab)$. Because P does not intersect S it follows that $ab \notin P$.