Some practice problems for midterm 2

Kiumars Kaveh

November 14, 2011

Problem: Let $Z = \{a \in G \mid ax = xa, \ \forall x \in G\}$ be the center of a group G. Prove that Z is a normal subgroup of G.

Solution: First we prove Z is a subgroup. Let $a, b \in Z$, we need to show that $ab \in Z$. Take $x \in G$ then $(ab)x = a(bx) = a(xb) = (ax)b = x(ab)$, which shows that $ab \in Z$. Also $ex = xe$ for every $x \in G$ thus $e \in Z$. Finally to show that Z contains inverses of its elements, take $a \in Z$, then $ax = xa$ for all x, multiplying by a^{-1} from left and right we get $xa^{-1} = a^{-1}x$ which proves that $a^{-1} \in Z$. Next let us show that Z is a normal subgroup. We need to show that for any $x \in G$ and $a \in Z$, $x^{-1}ax$ lies in Z. But $x^{-1}ax = ax^{-1}x = a \in Z$. Thus Z is a normal subgroup.

Problem: Let $G = \mathbb{Z}_4 \times \mathbb{Z}_4$, $H = \{(0,0), (2,0), (0,2), (2,2)\}$ and $K = \langle (1,2) \rangle$. Is G/H isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$? How about G/K?

Solution: G/H has 4 elements consisting of H, $(1,0)+H$, $(0,1)+H$ and $(1,1)+H$. The last three cosets have order 2, and hence G/H is isomorphic to the Klein group $\mathbb{Z}_2 \times \mathbb{Z}_2$. As for the group G/K, note that $(1,2)$ has order 4 and K consists of $\{(0,0), (1,2), (2,0), (3,2)\}$. Since K does not contain any element of the form (x,x) except for $(0,0)$ we see that the order of the element $(1,1)+K$ in G/K is equal to 4. It follows that G/K is cyclic isomorphic to $\mathbb{Z}_4$.

Problem: Let G be a finite group and let H be a normal subgroup. Prove that, for any $g \in G$, the order of the element gH in G/H must divide the order of g in G.

Solution: Consider the natural homomorphism $\phi : G \to G/H$, given by $x \mapsto xH$. Let K be the subgroup of G generated by g and K' the subgroup of $G' = G/H$ generated by $g + H$. One easily sees that $\phi : K \to K'$ is an onto homomorphism. It follows that $|K|$ is divisible by $|K'|$ (recall that for any homomorphism the number of elements in the image is the index of the kernel subgroup). But $|K'|$ (respectively $|K|$) is the order of $g + H$ in G/H (respectively g in G).

Problem: Suppose that $\phi : G \to G'$ is a homomorphism between the groups G and G'. Let N' be a normal subgroup of G'. Prove that the inverse image of N', namely $N = \phi^{-1}(N') = \{x \mid \phi(x) \in N'\}$ is a normal subgroup of G.

Solution: One can prove this directly from definition of normal subgroup and homomorphism. We give another shorter proof. Consider the natural homomorphism $\psi : G' \to G'/N'$. Then N' is the kernel of ψ. Consider the composition of the homomorphisms ϕ and ψ. It is a homomorphism $\psi \circ \phi : G \to G'/N'$. Also from definition the inverse image N is the kernel of $\psi \circ \phi$. This shows that N is a normal subgroup because it is kernel of the homomorphism $\psi \circ \phi$.

Problem: Determine the number of ways, up to rotation of the square, in which four corners of a square can be colored with two colors. (it is permissible to use a single color on all four corners.)

Solution: Consider the set X of all the colorings or the corners of square with two colors. Clearly X has $2^4 = 16$ elements. The group $G \cong \mathbb{Z}_4$ of rotations generated by $90°$ rotation acts on X. The question asks to compute the number of orbits in this action. We use Burnside's theorem. Recall that it states that number of orbits is equal to:

$$\frac{1}{|G|} \sum_{g \in G} |X_g|.$$

For each rotation g we compute the number of fixed points (colorings which remain the same after the rotation):
The number of colorings fixed by $0°$ degree rotation $= 16$.
The number of colorings fixed by $90°$ degree rotation $= 2$.
The number of colorings fixed by $180°$ degree rotation $= 4$.
The number of colorings fixed by $270°$ degree rotation $= 2$.

Applying Burnside's theorem, the number of different colorings is: $(1/4)(16 + 2 + 4 + 2) = 24/4 = 6$.

Problem: Wooden cubes of the same size are to be painted a different color on each face to make children's blocks. How many distinguishable blocks can be made if 8 colors of paint are used?

Solution: Consider the group G of rotations of a cube (Section 9, Ex. 45). It has 24 elements. This group acts on the set X of all possible colorings of a cube by 8 colors. One computes that the number of elements in X, i.e the number of colorings, is $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3$. We also observe that, since each coloring consists of different colors, each rotation (except identity rotation) sends a coloring to a different coloring. In other words, for any $g \in G$, the fixed point set $X_g = \emptyset$, unless $g = e$ where $X_e = X$. Thus the number of orbits is equal to $(1/24)(8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) = 840$. One can also see this without Burnside's theorem: since no rotation fixes a coloring, all orbits have $|G| = 24$ elements. Thus the number of orbits is $|X|/|G| = 840$.

Problem: Give examples of the following:

(i) A finite noncommutative ring.

Solution: Consider 2×2 matrices with entires in some field $\mathbb{Z}_p$.

(ii) Give an example of a subset of a ring which is a subgroup under addition but not a subring.

Solution: In the field of complex numbers $\mathbb{C}$, consider the line consisting of all the imaginary numbers $I = \{0 + yi \mid y \in \mathbb{R}\}$. Clearly it is a subgroup with addition but it is not a subring because $i \cdot i = -1$ which is not in I.

(iii) Give example of a noncommutative ring R and elements $a, b \in R$ with $ab = 0$ but $ba \neq 0$.

Solution: In the ring of 2×2 matrices with real entries consider:

$$a = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$b = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

Problem: Prove that a ring R is commutative if and only if $a^2 - b^2 = (a + b)(a - b)$ for all $a, b \in R$.

Solution: By distributivity, for all $a, b \in R$ we have $(a + b)(a - b) = a^2 + ba - ab - b^2$. Now $a^2 + ba - ab + b^2 = a^2 - b^2$ if and only if $ba - ab = 0$ which is equivalent to $ab = ba$.

Problem: Suppose R is a ring and that $x^2 = x$ for all $x \in R$. Show that R is a commutative ring.

Solution: First let us show that for any $x \in R$, $x = -x$. To prove this consider the element $x + x$. By assumption we have $x + x = (x + x)^2 = x^2 + x^2 + x^2 + x^2 = x + x + x + x$ which implies that $x + x = 0$, i.e. $x = -x$. Now let us show that R is commutative. Take $a, b \in R$. By distributivity we have $(a+b)^2 = a^2 + ab + ba + b^2$. By assumption $x^2 = x$ we have $a + b = a + ab + ba + b$. This implies that $ab + ba = 0$ and thus $ab = -ba$ which in turn is equal to ba.

Problem: Prove that any finite integral domain is a field.

Solution: see Theorem 19.11 (Section 19).

Problem: One can easily verify that $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a subring of $\mathbb{Q}$. Show that $1 + 2\sqrt{2}$ has an inverse in this ring. (in fact $\mathbb{Q}[\sqrt{2}]$ is a subfield, that is it contains the multiplicative inverses of all of its nonzero elements.)

Solution: One observes that $(1 + 2\sqrt{2})(1 - 2\sqrt{2}) = 1 - 4 \cdot 2 = -7$. Thus $(1 + 2\sqrt{2})\frac{(1-2\sqrt{2})}{-7} = 1$ which shows that $(1 + \sqrt{2})^{-1} = (-1/7) + (2/7)\sqrt{2}$.

Problem: Consider the ring $\mathbb{Z}_3[x]$ of polynomials with coefficients in the finite field $\mathbb{Z}_3$. Show that the polynomials x^2 and x^4 determine the same functions from $\mathbb{Z}_3$ to $\mathbb{Z}_3$.

Solution: Pluging in $x = 0, 1, 2$ in $x^4 - x^2$ we see that it gives 0 mod 3 which shows that x^2 and x^4 give the same function on $\mathbb{Z}_3$. Alternatively one can deduce the claim from Fermat's theorem that states that for any prime p and integer x not divisible by p, $x^{p-1} \equiv 1 \mod p$.

Problem: Let F be a field and let $f(x)$ be polynomial in the ring $F[x]$ (of polynomials with coefficients in F). Show that if f has r distinct roots then $\deg(f) \geq r$.

Solution: Let $\alpha_1, \ldots, \alpha_r \in F$ be distinct roots of f. Then $f(x)$ is divisible by $(x - \alpha_i)$, for $i = 1, \ldots, r$. Since the $(x - \alpha_i)$ are irreducible and the ring $F[x]$ is "unique factorization domain" (i.e. every element uniquely decomposes into product of irreducible elements) we conclude that $f(x)$ is divisible by the product $\prod_{i=1}^{r}(x - \alpha_i)$. The degree of this product is r and hence $\deg(f)$ is greater and equal to r.

Problem: Let p be a prime number. Show that in the ring of polynomials $\mathbb{Z}_p[x]$ we have the following:

$$x^p - x = x(x-1)\cdots(x-(p-1)).$$

Solution: By Fermat's theorem the polynomial $f(x) = x^p - x$ has $\alpha = 0, \ldots, p-1$ as roots. By Factor Theorem we conclude that $f(x)$ is divisible by all the $x - \alpha$, $\alpha = 0, \ldots, p-1$, and hence by their product $g(x) = x(x-1)\cdots(x-(p-1))$. Since both polynomials f and g have the same degree we conclude that $f = cg$ for some constant $c \in F$. But the coefficients of x^p in both f and g is equal to 1 and hence $c = 1$ which proves the claim.

Problem: We know that A_n is a normal subgroup of S_n. Also A_n is a simple group for $n \geq 5$. Prove that for $n \geq 5$, A_n is the only normal subgroup of S_n (except for trivial subgroups S_n and $\{e\}$).

Sketch of solution: By contradiction, suppose H is a normal subgroup of S_n different from $\{e\}$, A_n and S_n. Consider $K = A_n \cap H$. One proves that the intersection of two normal subgroups is always a normal subgroup. Thus K

should be a normal subgroup of S_n and hence a normal subgroup of A_n. But the only normal subgroups of A_n are $\{e\}$ and A_n itself. It follows that $K = A_n$ or $K = \{e\}$. If $K = A_n$ then $A_n \subset H$. This shows that $[S_n : H] < 2 = [S_n : A_n]$. Hence $[S_n : H] = 1$ i.e. $H = S_n$ which is a contradiction. Next consider the case $K = \{e\}$. This means that $H \cap A_n = \{e\}$. Thus $H \setminus \{e\}$ consists only of odd permutations. Now if $\sigma \in H$ is an odd permutation σ^2 is even which implies that $\sigma^2 = e$. Finally one verifies that there is $\tau \in S_n$ such that $\tau^{-1}\sigma\tau \neq \sigma$. Since H is normal we should have $\sigma' = \tau^{-1}\sigma\tau \in H$. But then $\sigma'\sigma \neq e$ is an even permutation and hence is in A_n. This contradicts that $A_n \cap H = \{e\}$.