SF2729 Groups and Rings
Make-up exam: solutions

Tuesday, June 4, 2013, 08:00–13:00

Problem 1

Let G be a group. An *automorphism* $\phi : G \to G$ is simply an isomorphism from G to itself. A subgroup $H \leq G$ is a *characteristic subgroup* if for any automorphism $\phi : G \to G$, then $\phi(H) = H$. Show that the center, $Z(G)$, of G is a characteristic subgroup.

Solution:

It suffices to show $\phi(Z(G)) \subseteq Z(G)$; for the other inclusion one can take ϕ^{-1}. We thus need to show that if $z \in Z(G)$ then $\phi(z) \in Z(G)$. Let $a \in G$. Then

$$[\phi(z), a] = [\phi(z), \phi(\phi^{-1}(a))] = \phi([z, \phi^{-1}(a)]) = \phi(1) = 1$$

since $z \in \mathbf{Z}(G)$.

Problem 2

Show that a group of order 1001 cannot be simple i.e., it must have a non-trivial proper normal subgroup.

Solution:

We have $1001 = 7 \cdot 11 \cdot 13$. Let n_k $(k = 7,\ 11,\ 13)$ be the number of k-Sylow subgroups of the group. By the Sylow theorems, we have

$$n_7 \mid 143, \quad n_7 \equiv 1 \pmod 7$$

The only divisor of $143 = 11 \cdot 13$ which is 1 modulo 7 is 1 itself, hence $n_7 = 1$ and the 7-Sylow subgroup is normal. Thus the group is not simple.

Problem 3

Let G be a group and let $x, y \in G$. Suppose that $[x, y] \in Z(G)$; show that $x^n y^n = (xy)^n [x, y]^{\frac{n(n-1)}{2}}$ for all integers $n \geq 0$.

Solution:

By induction, the case $n = 1$ being trivial. For the inductive step, we first show by nested induction:

$$[x^n, y] = [x, y]^n :$$

Again, this is clear for $n = 1$. For the inductive step, we compute, using that $[x, y]$ is in the center,

$$[x^{n+1}, y] = x^n xyx^{-1}y^{-1}yx^{-(n-1)}y^{-1} = x^n[x, y]yx^{-(n-1)}y^{-1} = [x, y][x^{n-1}, y] = [x, y]^n.$$

Using this, we have have

$$(xy)^{n+1}[x, y]^{\binom{n+1}{2}} = (xy)(xy)^n[x, y]^{\binom{n}{2}}[x, y]^n = (xy)x^n y^n[x, y]^n = x[x, y]^n yx^n y^n = xx^n yy^n.$$

Problem 4

Let X be a set and let $\mathcal{P}(X)$ denote the power set of X, i. e. the set of all subsets of X. For $S, T \in \mathcal{P}(X)$, define

$$S + T = (S \cup T) - (S \cap T) \quad \text{and} \quad S \cdot T = S \cap T.$$

1. Show that this defines a unital ring structure on $\mathcal{P}(X)$. State explicitly what the zero element, the unity, and the negative of an element is. **(3 points)**

2. Denote by $F(X, \mathbf{Z}/2\mathbf{Z})$ the ring of functions from X to $\mathbf{Z}/2\mathbf{Z}$, where addition and multiplication are defined by $(f + g)(x) = f(x) + g(x)$ and $(f \cdot g)(x) = f(x)g(x)$. Show that $\mathcal{P}(X)$ and $F(X, \mathbf{Z}/2\mathbf{Z})$ are isomorphic rings. **(3 points)**

Solution:

The zero element is $\emptyset$ (because $\emptyset + S = S$), the unity is X (because $X \cap S = S$), and both operations are commutative by definition. An additive inverse is given by $-X := X$ since

$$S + S = (S \cup S) - (S \cap S) = S - S = \emptyset.$$

Multiplication is clearly associative, but associativity for addition has to be checked. Note that $x \in S + T$ iff x is either in S or in T, but not in both. So $x \in (S + T) + U$ if x is either in U or in $S + T$, which means x is in either one or three of the sets S, T, U, which is therefore seen to be the same condition as for $S + (T + U)$.

For distributivity, an element x is in $S \cdot (T + U)$ iff it is in S and exactly one of T and U, which is the same as being in exactly one of $S \cap T$ and $S \cap U$.

An isomorphism $\phi \colon \mathcal{P}(X) \to F(X, \mathbf{Z}/2\mathbf{Z})$ is given by

$$\phi(S)(x) = \begin{cases} 1; & x \in S \\ 0; & x \notin S. \end{cases}.$$

An inverse map is given by

$$\psi(f) = \{x \in X \mid f(x) = 1\}.$$

The maps are clearly inverses of each other; we have to check that they are in fact ring maps. For this, we compute

$$\phi(S+T)(x) = \begin{cases} 1; & x \in S \text{ or } x \in T \text{ but not both} \\ 0; & \text{otherwise} \end{cases} = \phi(S)(x) + \phi(T)(x) \in \mathbf{Z}/2\mathbf{Z};$$

$$\phi(X)(x) = 1 \quad \text{for all } x\text{; and}$$

$$\phi(S \cdot T)(x) = \begin{cases} 1; & x \in S \text{ and } x \in T \\ 0; & \text{otherwise} \end{cases} = \phi(S)(x) \cdot \phi(T)(x) \in \mathbf{Z}/2\mathbf{Z};$$

Problem 5

Show that for every $n \in \mathbf{N}$ there exists an irreducible polynomial of degree n over $\mathbf{Q}$. When using a theorem from this class, write down its full statement. **(6 points)**

Solution:

We use Gauss's lemma and the Eisenstein criterion to see that $x^n + p$ is irreducible over $\mathbf{Z}$, and hence over $\mathbf{Q}$, for any n and any prime p. (For the statements, consult the textbook.)

Problem 6

Let A be a finitely generated abelian group. For every prime number p, the module A/pA is a vector space over $\mathbf{Z}/p\mathbf{Z}$; denote by n_p its dimension.

1. Show that if A is torsion then $n_p = 0$ for all but finitely many p. **(3 points)**
2. Show that if all n_p are the same then A is a free abelian group. **(3 points)**

Solution:

If A is torsion then by the structure theorem,

$$A \cong A_{p_1} \oplus \cdots \oplus A_{p_n}$$

where p_i are distinct primes and A_{p_i} are abelian p_i-groups. Thus $A/pA \cong A_{p_i}/p_iA_{p_i}$ if $p = p_i$ and zero otherwise. So there are only finitely many p such that $A/pA \neq 0$.

For the second part, we know, again by the structure theorem, that

$$A \cong \mathbf{Z}^n \oplus A_{p_1} \oplus \cdots \oplus A_{p_n},$$

where the A_{p_i} are as before. Assume all the n_p are the same. Then $n_p = n$ because we can choose p to be a prime outside $\{p_1, \ldots, p_m\}$. But then, choosing $p = p_i$, we see that $A_{p_i} = 0$ for all i. Thus $A \cong \mathbf{Z}^n$.