SF2729 Groups and Rings
Final exam

Monday, March 19, 2013

Examiner Tilman Bauer

Allowed aids none

Time 14:00–19:00

Present your solutions in such a way that the arguments and calculations are easy to follow. Provide detailed arguments to your answers. An answer without explanation will give few or no points.

Each problem is worth 6 points, for a total of 36 points. Your end score will be the better of the exam score and the weighted average

$$0.75\ (\text{exam score}) + 0.25\ (\text{homework score}).$$

It is thus important that you do **all problems** even if you scored high on the homework. Good luck!

Problem 1

Show for each integer a that $35 \mid a^{13} - a$.

Solution

It suffices to show that $a^{13} - a$ is divisible by 5 and by 7. Equivalently, we want to show that $a^{13} \equiv a \pmod{5, 7}$. Using Fermat's little theorem ($a^p \equiv a \pmod{p}$) repeatedly, we get

$$a^{13} = a^7 a^6 \equiv a a^6 = a^7 \equiv a \pmod{7}$$

and

$$a^{13} = a^5 a^8 \equiv a a^8 = a^5 a^4 \equiv a a^4 = a^5 \equiv a \pmod{5}.$$

Problem 2

Let G be a group of order $340 = 2^2 \cdot 5 \cdot 17$.

1. Show that G has normal cyclic subgroups of orders 5 and 17. (2p)
2. Show that G has a cyclic subgroup N of order $85 = 5 \cdot 17$. (3p)
3. Show that N is normal. (1p)

Solution

By the Sylow theorems, we have $n_5 \equiv 1 \pmod 5$ and $n_5 \mid 2^2 \cdot 17$. The only possibility is $n_5 = 1$, so we have a normal Sylow 5-subgroup S_5 of order 5, which therefore is cyclic. Similarly, $n_{17} \equiv 1 \pmod{17}$ and $n_{17} \mid 2^2 \cdot 5$ gives $n_{17} = 1$, thus a unique normal Sylow 17-subgroup S_{17}.

Now let x be a generator of the Sylow 5-subgroup and y a generator of the Sylow 17-subgroup. Then

$$[x, y] = xyx^{-1}y^{-1} = y'y^{-1} \in S_{17} \quad \text{because } S_5 \text{ is normal, and}$$
$$[x, y] = xyx^{-1}y^{-1} = xx' \in S_5 \quad \text{because } S_{17} \text{ is normal.}$$

Hence $[x, y] \in S_5 \cap S_{17} = \{e\}$, so x and y commute. This shows that $g = xy$ has order $5 \cdot 17$ and generates a cyclic subgroup $S_5 S_{17}$ of order 85. This subgroup is also normal because

$$gS_5S_{17} = S_5gS_{17} = S_5S_{17}g$$

by normality of both S_5 and S_{17}.

Problem 3

Let G be a group such that all non-identity elements are conjugate. Show that the order of G is 1, 2, or infinite.

Solution

Assume G has finite order $n > 1$. Then G acts on $X = G - \{e\}$ by conjugation, and by assumption, $Gx = X$ for all $x \in X$. By the orbit formula, the cardinality of the orbit is the index of the stabilizer G_x and thus divides the group order. Thus $n - 1 \mid n$, which is only possible if $n = 2$.

Problem 4

Let R be a commutative, unital ring and $I \trianglelefteq R$ an ideal. Define

$$\sqrt{I} = \{r \in R \mid r^n \in I \text{ for some } n \geq 1\}.$$

Show that $\sqrt{I}$ is an ideal.

Solution

First we show that it is an abelian subgroup. If $x, y \in \sqrt{I}$, say $x^m \in I$ and $x^n \in I$, then by the commutativity of R,

$$(x + y)^{m+n} = \sum_{i+j=m+n} \binom{m+n}{i} x^i y^j.$$

In this sum, either $i \geq m$ or $j \geq n$, so $x^i y^j \in I$ for all summands.

Next we show that I is closed under multiplication with elements of R. But if $x^m \in I$ then $(rx)^m = r^m x^m \in I$, again using that R is commutative.

Problem 5

Factor the polynomial $p(x) = x^4 + x + 1$ into indecomposable factors in the following rings:

1. $\mathbf{F}_2[x]$,
2. $\mathbf{F}_3[x]$,
3. $\mathbf{Q}[x]$.

In each case, argue carefully why the factors you give are indeed indecomposable.

Solution

Over $\mathbf{F}_2[x]$, $p(0) = p(1) = 1$, so there is no linear factor, and any decomposition would have to have the form $p(x) = (x^2 + ax + 1)(x^2 + bx + 1) = x^4 + (a + b)x^3 + abx^2 + (a + b)x + 1$, which is impossible. Hence p is indecomposable.

Over $\mathbf{F}_3[x]$, $p(1) = 0$, and we get $p(x) = (x - 1)(x^3 + x^2 + x + 2)$. Since the degree-3 factor has no further zero in $\mathbf{F}_3$, it is indecomposable.

Since p is indecomposable over $\mathbf{F}_2$, it is also indecomposable over $\mathbf{Z}$. Since it is primitive, it is also indecomposable over $\mathbf{Q}[x]$ by Gauss's lemma.

Problem 6

Let M be a finitely generated module over an integral domain R and let $\{x_1, \ldots, x_n\} \subseteq M$ be a maximal set of linearly independent elements and $N = \langle x_1, \ldots, x_n \rangle$ the submodule of M generated by this set. Show that M/N is a torsion module.

Solution

We need to see that for every $\overline{x} \in M/N$ there is an element $r \in R - \{0\}$ such that $r\overline{x} = 0 \in M/N$, or equivalently, that for every $x \in M$ there is an $r \in R - \{0\}$ such that $rx \in N$.

Since $\{x_1, \ldots, x_n, x\}$ is linearly dependent in M by assumption, there is a relation

$$\alpha_1 x_1 + \cdots + \alpha_n x_n + rx = 0$$

with not all α_i and r zero. Since the x_i are linearly independent, we must have $r \neq 0$. Thus

$$rx = -(\alpha_1 x_1 + \cdots + \alpha_n x_n) \in N.$$