SF2729 Groups and Rings
Final exam solutions

Monday, March 11, 2013

Problem 1

Let G be a group. A subgroup H of a group G is a *fully invariant subgroup* if for any homomorphism $\phi : G \to G$ we have $\phi(H) \leq H$. Show that the commutator subgroup $[G, G]$ of G is a fully invariant subgroup.

Solution

We have to show that $\phi([G, G]) \subseteq [G, G]$. It suffices to show that the image of a commutator under a homomorphism is a commutator. Indeed,

$$\phi([g, h]) = \phi(ghg^{-1}h^{-1}) = \phi(g)\phi(h)\phi(g)^{-1}\phi(h)^{-1} = [\phi(g), \phi(h)].$$

Problem 2

Show that a group of order 495 cannot be simple i.e., it must have a non-trivial proper normal subgroup.

Solution

The prime decomposition of 495 is $5 \cdot 3^2 \cdot 11$. By Sylow's theorem, the number of p-Sylow subgroups if congruent to 1 modulo p and divides the order of the group. We can thus have 1 or 45 different 11-Sylow subgroups, and 1 or 55 different 3-Sylows (or order 9). If there is only one p-Sylow subgroup, it has to be normal. Thus assume that the number of 11-Sylows is 45 and the number of 3-Sylows is 55. Since their pairwise intersect is only the identity, this would mean that the group has at least $1 + (11 - 1) \cdot 45 + (3 - 1) \cdot 55 = 561$ elements, which is a contradiction. Hence either an 11-Sylow or a 3-Sylow has to be normal.

Problem 3

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

Solution

We use induction, the cases $n = 0$ and $n = 1$ being trivial. Then

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

where the last equality uses the inductive assumption.

Problem 4

Let A be an abelian group and define a multiplication on the abelian group $R = \mathbf{Z} \times A$ by

$$(n,a) \cdot (m,b) = (nm, nb + ma).$$

1. Show that this defines a unital ring structure on $R = \mathbf{Z} \times A$ by verifying the axioms. State explicitly what the zero and unity elements are. **(3 points)**
2. Show that the group of units $R^\times$ is isomorphic to $\mathbf{Z}/2 \times A$. **(3 points)**

Solution

The multiplication is symmetric in the factors and hence commutative. The zero element is $(0,0)$ (given by the product groups structure on $\mathbf{Z} \times A$) and the unity is $(1,0)$. Check:

$$(1,0) \cdot (n,a) = (1 \cdot n, 1 \cdot a + n \cdot 0) = (n,a).$$

For distributivity, we compute

$$\begin{aligned}(n_1 + n_2, a_1 + a_2) \cdot (m,b) &= ((n_1 + n_2)m, (n_1 + n_2)b + m(a_1 + a_2)) \\ &= (n_1 m, n_1 b + m a_1) + (n_2 m, n_2 b + m a_2) = (n_1, a_1) \cdot (m,b) + (n_2, a_2) \cdot (m,b).\end{aligned}$$

For associativity, we have

$$\begin{aligned}((n,a) \cdot (m,b)) \cdot (k,c) &= (nm, nb + ma) \cdot (k,c) = (nmk, knb + kma + nmc) \\ &= (n,a) \cdot (km, kb + mc) = (n,a) \cdot ((m,b) \cdot (k,c))\end{aligned}$$

An element (n,a) is invertible iff there exist (m,b) such that $(nm, nb + ma) = (1,0)$, i. e. if $n = \pm 1$. In this case,

$$(n,a)^{-1} = (n, -a).$$

Thus $R^\times = \{(n,a) \mid n = \pm 1\}$. An isomorphism $\phi \colon \mathbf{Z}/2 \times A \to R^\times$ is given by

$$\phi(\epsilon, a) = ((-1)^\epsilon, (-1)^\epsilon a).$$

This is obviously bijective; to verify it is a homomorphism, we compute

$$\phi((\epsilon,a)(\delta,b)) = \phi(\epsilon + \delta, a + b) = ((-1)^{\epsilon+\delta}, (-1)^{\epsilon+\delta}(a+b))$$

and

$$\phi(\epsilon,a) \cdot \phi(\epsilon,b) = ((-1)^\epsilon), (-1)^\epsilon a) \cdot ((-1)^\delta, (-1)^\delta b) = ((-1)^{\epsilon+\delta}, (-1)^{\epsilon+\delta}(a+b))$$

Problem 5

Let R be a commutative ring possessing exactly three ideals $(0) \subsetneq I \subsetneq R$.

1. Show that $I = R - R^\times$, i. e. that I consists precisely of the nonunits of R. **(4 points)**
2. Give a concrete example of such a ring. **(2 points)**

Solution

If I contained a unit, it would be all of R, hence $I \subseteq R - R^\times$. For the other inclusion, let $x \neq 0$ be a nonunit. Then the principal ideal (x) is neither 0 nor R because it contains x and if 1 were an element of (x) then x would have an inverse. Thus $(x) = I$, in particular, $x \in I$.

An example of such a ring is $\mathbf{Z}/4\mathbf{Z}$ with the ideals $(0) \subsetneq (2) \subsetneq \mathbf{Z}/4\mathbf{Z}$.

Problem 6

Let $R = \mathbf{Z}[i]$ be the ring of Gaussian integers and consider the submodule $M < R^2$ generated by the single element $(2, 1+i)$. According to the structure theorem of finitely generated modules over PIDs, the quotient module R^2/M is isomorphic to a sum of a free module and modules of the form $R/(p^n)$, where p is a prime element. Find this decomposition and the corresponding isomorphism.

Solution

I claim that $R^2/M \cong \mathbf{Z}[i] \oplus \mathbf{Z}[i]/(1+i) \cong \mathbf{Z}[i] \oplus \mathbf{Z}/2\mathbf{Z}$ by the following isomorphism:

$$\phi\colon \mathbf{Z}[i] \oplus \mathbf{Z}[i]/(1+i) \to R^2/M, \quad \phi(x, [y]) = [(x + (1-i)y, y)].$$

First for well-definedness: if $y' = y + r(1+i)$ for some $r \in \mathbf{Z}[i]$ then

$$\phi(x, [y']) - \phi(x, [y]) = [(r(1+i)(1-i), r(1+i))] = [r \cdot (2, 1+i)] = 0 \in R^2/M.$$

By definition, ϕ is a homomorphism. For injectivity, Assume $\phi(x, [y]) = 0$, thus

$$(x + (1-i)y, y) = r \cdot (2, 1+i) = r(1+i) \cdot (1-i, 1) \quad \text{for some } r \in \mathbf{Z}[i].$$

Then $y = r(1+i)$ and hence $x + (1-i)y = x + 2r = 2r$, hence $x = 0$ and $[y] = 0 \in \mathbf{Z}[i]/(1+i)$. For surjectivity, let $[(x, y)] \in R^2/M$. Then

$$\phi(x - (1-i)y, y) = [(x - (1-i)y + (1-i)y, y)] = [(x, y)].$$