M 380 C 54580 Second Midterm

Name:

Do three out of the four questions below and please indicate here which questions you chose:

1. Consider the ring $R = \mathbb{Z}/2\mathbb{Z}[x]/(x^2)$. Describe all isomorphism classes of $R$-modules with 16 elements.

   Let $M$ be an $R$-module. Then, since $R$ is a quotient of $\mathbb{Z}/2\mathbb{Z}[x]$, $M$ is also a $\mathbb{Z}/2\mathbb{Z}[x]$-module where $x^2$ acts as 0. If $M$ has 16 elements, then $M$ is finitely generated as a $\mathbb{Z}/2\mathbb{Z}[x]$-module and we can apply the classification theorem for modules over PID’s, since we know that $\mathbb{Z}/2\mathbb{Z}[x]$ is a PID. (Note that $R$ is not even a domain so we can’t apply the theorem directly to $R$-modules!) It tells us that $M$ is isomorphic to

   $$\mathbb{Z}/2\mathbb{Z}[x]/(x^r) \oplus \mathbb{Z}/2\mathbb{Z}[x]/(a_1) \oplus \cdots \oplus \mathbb{Z}/2\mathbb{Z}[x]/(a_m)$$

   where $a_1,a_2,\ldots,a_m$ are monic polynomials. Since $x^2$ acts as 0 on $M$ we must have $r = 0$ and $a_i|x^2, i = 1, \ldots, m$, so $a_i = x$ or $a_i = x^2, i = 1, \ldots, m$. Now, $R$ has 4 elements and $R/(x) = \mathbb{Z}/2\mathbb{Z}[x]/(x)$ has 2 elements, therefore the only possibilities when $M$ has 16 elements are $m = 2, a_1 = a_2 = x^2$, $m = 3, a_1 = a_2 = x, a_3 = x^2$ or $m = 4, a_i = x, i = 1,2,3,4$. 

2. Let $R$ be a PID. Prove that the intersection of two nonzero maximal ideals of $R$ cannot be zero. Assume that $R$ contains an infinite number of maximal ideals. Show that the intersection of all the nonzero maximal ideals of $R$ equals zero.

If $I, J$ are nonzero ideals of $R$, then there exists $a, b \in R$, $I = (a), J = (b)$, because $R$ is a PID and $a, b \neq 0$ since $I, J$ are non-zero. Since $I$ consists of the multiples of $a$, we have $ab \in I$ and likewise $ab \in J$ so $ab \in I \cap J$. As $R$ is a domain, $ab \neq 0$ so $I \cap J \neq (0)$.

Now, in a PID, maximal ideals are the same as prime ideals which are the ideals generated by irreducible elements. If $x \in R, x \neq 0$, then $x$ is a product of irreducible elements of $R$ in an essentially unique way, since PID’s are UFD’s, therefore $x$ is divisible by only finitely many irreducible elements, or equivalently, $x$ is contained in only finitely many maximal ideals. So $x$ cannot be contained in the intersection of all the nonzero maximal ideals of $R$ if there are infinitely many of them. Since $x \neq 0$ was arbitrary this completes the proof.
3. Let $G$ be a finite group and $R$ be the set of all functions $f : G \to \mathbb{Z}$. Define operations on $R$ as follows: Given $f, g \in R$, $(f+g)(x) = f(x)+g(x)$, $(fg)(x) = \sum_{y \in G} f(y)g(y^{-1}x), x \in G$. Prove the distributivity law on $R$. ($R$ is a ring with these operations, the integral group ring of $G$, you don’t need to prove this but we will assume it in the next part). Prove that $f$ is in the center of $R$ (that is, commutes with every element of $R$) if and only if $f$ is constant (as a function) on every conjugacy class of $G$.

$$(f+g)h(x) = \sum_{y \in G} (f+g)(y)h(y^{-1}x) = \sum_{y \in G} (f(y)+g(y))h(y^{-1}x) = \sum_{y \in G} f(y)h(y^{-1}x) + \sum_{y \in G} g(y)h(y^{-1}x) = fh + gh.$$

The other equality $h(f + g) = hf + hg$ is similar.

Let $f \in R$ be arbitrary and, for $z \in G$ define $g_z \in R, g_z(z) = 1, g_z(x) = 0, x \neq z$. Then, $fg_z(x) = \sum_{y \in G} f(y)g_z(y^{-1}x) = f(xz^{-1})$ and $g_zf(x) = \sum_{y \in G} g_z(y)f(y^{-1}x) = f(z^{-1}x)$. If $f$ is constant on every conjugacy class of $G$, then $f(z^{-1}x) = f(x(z^{-1}x)x^{-1}) = f(xz^{-1})$, so $f$ commutes with $g_z$. Now, given $g \in R, g = \sum_{z \in G} g(z)g_z$, so $f$ commutes with $g$. Conversely, if $f$ is in the center of $R$, then $f$ commutes with $g_z$, for all $z$, so $f(z^{-1}x) = f(xz^{-1})$ for all $x, z$ and, replacing $x$ by $xz$ we get $f(z^{-1}xz) = f(x)$ for all $x, z$, that is, $f$ is constant on every conjugacy class of $G$. 
4. Let $G$ be a finite abelian group. Prove that either $G$ has proper subgroups $H$ and $K$ such that $G$ is isomorphic to $H \times K$ or $G$ is cyclic of prime power order.

By the classification of finite abelian groups, $G$ is isomorphic to $\mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/(a_m)$, for integers $a_1, \ldots, a_m$. If $m > 1$ we can take $H = \mathbb{Z}/(a_1) \oplus \cdots \oplus \mathbb{Z}/0$, $K = 0 \oplus \cdots \oplus \mathbb{Z}/(a_m)$ and $G$ is isomorphic to $H \times K$. If $m = 1$ and $a_1$ is not a prime power, then we can write $a_1 = bc$ where $b, c > 1$ and $b, c$ are relatively prime integers. So, by the Chinese remainder theorem, $\mathbb{Z}/(a_1)$ is isomorphic to $\mathbb{Z}/(b) \times \mathbb{Z}/(c)$ and the two factors correspond to subgroups $H, K$ of $G$. The only remaining possibility is $m = 1$ and $a_1$ a prime power, in which case $G$ is cyclic of prime power order.