M 380 D 55630 Final Exam

Name:

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

1. Let F be a field and R be the ring $F[x]/(x^3)$. Explain why the classification of modules over PID's implies that every finitely generated R module is a direct sum of cyclic R modules. Describe all possible isomorphism classes of cyclic R modules. Suppose that $F = \mathbf{Z}/(2)$, the field of two elements, describe all possible isomorphism classes of R modules with 8 elements.

The ring R is a quotient of the ring $F[x]$, so any R-module M can be considered as an $F[x]$-module by $am = \pi(a)m$, where $a \in F[x], m \in M, \pi : F[x] \to R$ is the natural map. Moreover, such an R-module M will be annihilated by (x^3) as an $F[x]$-module since $\pi(a) = 0, a \in (x^3)$. Assume now that M is a finitely generated R module. Then it is finitely generated as an $F[x]$-module and the classification of modules over PID's, applied to the PID $F[x]$, (NOTE: R is not a PID since it isn't a domain) gives that M is a direct sum of cyclic $F[x]$-modules and since M is annihilated by (x^3) we get that the cyclic factors also have to be annihilated by (x^3) and therefore are themselves cyclic R-modules. So, M is a direct sum of cyclic R modules.

A cyclic R module is isomorphic to R/I for some ideal I of R. The ideals of R are in $1-1$ correspondence with the ideals of $F[x]$ containing (x^3) and those are $(1), (x), (x^2), (x^3) = (0)$ so the cyclic R modules are isomorphic to $0, R/(x), R/(x^2), R$.

If $F = \mathbf{Z}/(2)$ then the R modules $R/(x), R/(x^2), R$ have, respectively $2, 4$ and 8 elements, so the isomorphism classes of R modules with 8 elements are

$$R, R/(x) \oplus R/(x^2), R/(x) \oplus R/(x) \oplus R/(x).$$

2. Let F be a field and K/F be a purely inseparable extension. Let $f(x)$ be a separable irreducible polynomial in $F[x]$. Prove that $f(x)$ is irreducible in $K[x]$. Give an example where the hypothesis that $f(x)$ be separable is dropped and the conclusion no longer holds. Give an example where the hypothesis that K/F be purely inseparable is dropped and the conclusion no longer holds.

Let E be the splitting field of $f(x)$ over F and $\alpha_1, \ldots, \alpha_n$ the roots of $f(x)$ in E. Since $f(x)$ be separable we have that E/F is separable. A monic factor of $f(x)$ will be of the form $(x - \alpha_{i_1}) \cdots (x - \alpha_{i_k})$ for some $i_1, \ldots, i_k$ so will have coefficients in E. Hence if f has a factor in K, this factor will have coefficients in $E \cap K$. Now, an element of K is purely inseparable over F so has minimal polynomial having only one root. On the other hand an element of E is separable over F so has minimal polynomial having distinct roots. It follows that an element of $E \cap K$ has minimal polynomial over F of degree one, so $E \cap K = F$. Hence any factor of f with coefficients in K has coefficients in F, but $f(x)$ is irreducible over F, hence it must be irreducible over K.

For the first example, take $F = \mathbf{F}_p(t)$ for a variable t and $f(x) = x^p - t$. Then $f(x)$ is irreducible over F but factors over the purely inseparable extension $K = \mathbf{F}_p(t^{1/p})$ as $(x - t^{1/p})^p$.

For the second example, take $F = \mathbf{Q}$, $f(x) = x^2 + 1$, $K = \mathbf{Q}(i)$. Then $f(x)$ is a separable irreducible polynomial in $F[x]$, but factors over K. (Of course there are many other such examples).

3. Let $K/\mathbf{Q}$ be an extension of degree n, where $\mathbf{Q}$ is the field of rational numbers. Show that the number of subfields of K is at most $2^{n!}$. Suppose that $K = \mathbf{Q}(\alpha, \beta)$ and prove that there exists $m, 0 \leq m \leq 2^{n!}$ such that $K = \mathbf{Q}(\alpha + m\beta)$.

By the primitive element theorem $K = \mathbf{Q}(\alpha)$ for some α of degree n over $\mathbf{Q}$. Let L be the splitting field of the minimal polynomial of α over $\mathbf{Q}$ and G its Galois group. Then, $|G| = [L : \mathbf{Q}] \leq n!$. The subfields of K are among the subfields of L. The subfields of L are in $1-1$ correspondence with the subgroups of G by the fundamental theorem of Galois theory. Now, G has at most $2^{|G|}$ subsets, so at most $2^{|G|}$ subgroups and, by above, $2^{|G|} \leq 2^{n!}$. Hence K has at most $2^{n!}$ subfields. (Another solution is to look at the monic factors of the minimal polynomial of α over $\mathbf{Q}$, of which there are only 2^n and show that subfields F of K are characterized by minimal polynomial of α over F, which are among those 2^n factors, this leads to a much sharper bound of 2^n for the number of subfields of K).

Among the $2^{n!} + 1$ fields $\mathbf{Q}(\alpha + m\beta), 0 \leq m \leq 2^{n!}$, two of them have to coincide by the first part. If $F = \mathbf{Q}(\alpha + m\beta) = \mathbf{Q}(\alpha + n\beta), m \neq n$, then there exists $\gamma, \delta \in F, \alpha + m\beta = \gamma, \alpha + n\beta = \delta$, so $\beta = (\gamma - \delta)/(m - n), \alpha = \gamma - m\beta$ are both in F so $F = K$ and $K = \mathbf{Q}(\alpha + m\beta)$.

4. State and prove from first principles the Nullstellensatz for polynomials in **one** variable.

Let F be an algebraically closed field. To state the Nullstellensatz, define for $X \subset F$ the ideal $\mathcal{I}(X) = \{f \in F[x] \mid f(a) = 0, \forall a \in X\}$, and for an ideal I of $F[x]$ define $Z(I) = \{a \in F \mid f(a) = 0, \forall f \in I\}$ and $\mathrm{rad}(I) = \{f \in F[x] \mid \exists m \geq 1, f^m \in I\}$. The Nullstellensatz states that $\mathcal{I}(Z(I)) = \mathrm{rad}(I)$.

First note that, if $f \in \mathrm{rad}(I), \exists m \geq 1, f^m \in I$ so $f^m(a) = 0$ if $a \in Z(I)$, but F is a domain so this implies $f(a) = 0$ if $a \in Z(I)$, thus $f \in \mathcal{I}(Z(I))$ that is $\mathrm{rad}(I) \subset \mathcal{I}(Z(I))$.

We now prove the reverse inclusion. Let I be an ideal of $F[x]$. If $I = (0)$ then $Z(I) = F$ and the result is clear. If $I = F[x]$, then $Z(I) = \emptyset$ and the result is also clear. Otherwise $I = (f(x))$ for some non-constant polynomial $f(x)$. Since F is algebraically closed, $f(x) = (x - a_1)^{n_1} \cdots (x - a_k)^{n_k}$ for distinct elements $a_1, \ldots, a_k \in F$. Moreover $Z(I) = \{a_1, \ldots, a_k\}$, clearly. So if $g(x) \in \mathcal{I}(Z(I))$ then $g(x)$ vanishes on all a_i so $g(x)$ is divisible by $(x - a_1) \cdots (x - a_k)$. If $m \geq n_1, \ldots, n_k$, then $g(x)^m$ is divisible by $f(x)$, so $g(x)^m \in I$ and finally $g(x) \in \mathrm{rad}(I)$ as desired.