Final (In Class Part)

M552 – Abstract Algebra

May 16th, 2008

1. Let R be the ring of real continuous functions $f(x)$ such that $f(x+\pi) = f(x)$, and M be the R-module of real continuous functions $g(x)$ such that $g(x+\pi) = -g(x)$. Let c and s be the usual cosine and sine functions [in M].

(a) Show that $R \not\cong M$ [as R-modules]. [**Hint:** Use calculus.]

(b) Show that $(f, g) \mapsto (fc + gs, -fs + gc)$ is an isomorphism between $R \oplus R$ and $M \oplus M$ [even though $M \not\cong R$].

(c) Show that $f \mapsto fs \otimes s + fc \otimes c$ is an isomorphism between R and $M \otimes_R M$ [even though $M \not\cong R$]. [**Hint:** Find an inverse.]

Proof. Suppose that $\phi : R \to M$ is an isomorphism. Then, $M = R \cdot \phi(1)$. If $f = \phi(1) \in M$, then $f(0) = -f(\pi)$, and hence f has a root in $[0, \pi]$, say at x_0. Since $M = R \cdot f$, all $g \in M$ also have a zero at x_0. But $g(x) \stackrel{\text{def}}{=} \cos(x - x_0) \in M$, while $g(x_0) = 1$. So, (a) is proved.

The map in (b) is clearly a homomorphism. If $fc + gs = 0 = -fs + gc$, then we can multiply the first equality by s and the second by c. Adding, we get $g(c^2 + s^2) = 0$, i.e., $g = 0$. If we now multiply the first equality by c and the second by s and subtract them, we get that $f(c^2 + s^2) = 0$. Hence, the map is injective.

Now, let $u, v \in M$. Taking $f = cu - sv$ and $g = su + cv$, we get that $(f, g) \mapsto (u, v)$ and hence the map is also onto.

The map given in (c), say Φ is clearly a homomorphism. Consider the map $\Psi : u \otimes v \to uv$ [extended linearly to $M \otimes M$]. Note that $uv \in R$ and the map is well-defined [since the map is $(u, v) \mapsto uv$ is bilinear].

We have that $\Psi \circ \Phi(f) = \Psi(fs \otimes s + fc \otimes c) = f(s^2 + c^2) = f$. Also, $\Phi \circ \Psi(u \otimes v) = uvs \otimes s + uvc \otimes v = u \otimes vs^2 + u \otimes vc^2 = u \otimes v(s^2 + c^2) = u \otimes v$. [Note that $cv, sv \in R$.] $\square$

2. Let R be a commutative with $1 \neq 0$ and M an R-module. Show that $\mathrm{Hom}_R(R \oplus R, M)$ is projective if, and only if, M is a projective R-module.

Proof. We have that $\mathrm{Hom}_R(N_1 \oplus N_2, M) \cong \mathrm{Hom}_R(N_1) \oplus \mathrm{Hom}_R(N_2, M)$. Indeed Let $\Phi : \mathrm{Hom}_R(N_1 \oplus N_2, M) \to \mathrm{Hom}_R(N_1, M) \oplus \mathrm{Hom}_R(N_2, M)$, defined by $\Phi(\phi) \stackrel{\text{def}}{=} (\phi|_{N_1}, \phi|_{N_2})$. Then, it clearly is an isomorphism.

We also claim that $\mathrm{Hom}_R(R, M) \cong M$. Indeed, let $\Psi : \mathrm{Hom}_R(R, M) \to M$ be defined by $\Psi(\phi) \stackrel{\text{def}}{=} \phi(1)$. Then, it's clearly an isomorphism.

So, $\mathrm{Hom}_R(R \oplus R, M) \cong M \oplus M$. Now, if M is projective, then there exists an R-module N such that $M \oplus N = F$, with F free. Then $(M \oplus M) \oplus (N \oplus N) = F \oplus F$ is free. Hence, $M \oplus M \cong \mathrm{Hom}_R(R \oplus R, M)$ is projective. [So, we use the fact that a module is projective if, and only if, it is a direct summand of a free module.]

Conversely, if $M \oplus M$ is projective, then there is N such that $(M \oplus M) \oplus N = M \oplus (M \oplus N)$ is free. Hence M is projective.

$\square$

3. Let $f(x) \in F[x]$ be irreducible, with $F \subseteq \mathbb{R}$. Suppose that there is $\alpha_0 \in \mathbb{C} - \mathbb{R}$ such that $f(\alpha_0) = 0$ and $|\alpha_0| = 1$. Show that if α is a root of $f(x)$, then so is $1/\alpha$.

Proof. Since $\alpha \notin \mathbb{R}$, but $F \subseteq \mathbb{R}$, we have that $\bar{\alpha}_0$ is also a root of f [and $\alpha_0 \neq \bar{\alpha}_0$]. But, since $|\alpha_0| = 1$, we have that $\bar{\alpha}_0 = \alpha_0^{-1}$.

Let K be the splitting field of f and $\alpha \in K$ be a root of f. Then, there exists $\sigma \in \mathrm{Gal}(K/F)$ [note it's separable, since we are in characteristic 0] such that $\sigma(\alpha_0) = \alpha$. But, since σ fixes F, it must take roots of f to roots of f. Hence, $\sigma(\alpha_0^{-1}) = (\sigma(\alpha_0))^{-1} = \alpha^{-1}$ is also a root of f [since $\bar{\alpha}_0 = \alpha_0^{-1}$ is a root of f].

$\square$

4. Let ζ_n be a primitive n-th root of unity, and $\alpha \in \mathbb{Q}[\zeta_n] \cap \mathbb{R}$, such that $\alpha^m \in \mathbb{Q}$ for some $m \geq 2$. Show that $\alpha^2 \in \mathbb{Q}$.

Proof. We have that $\mathbb{Q}[\zeta_n]/\mathbb{Q}$ is *Abelian*, and hence $K \stackrel{\text{def}}{=} \mathbb{Q}[\zeta_n] \cap \mathbb{R}$ is Galois over $\mathbb{Q}$. Now, $f(x) \stackrel{\text{def}}{=} \min_{\alpha,\mathbb{Q}}(x) \mid (x^m - \alpha^m)$, so its roots are of the form $\alpha\zeta_m^r$, for some integer r, where ζ_m is a primitive m-th root of unity. But, since $K/\mathbb{Q}$ is Galois, and $\alpha \in K$ is a root of f, all roots of f are in K. But since $\alpha \in K \subseteq \mathbb{R}$, we have that $\alpha\zeta_m^r \in K$ implies that $\zeta_m^r \in \mathbb{R}$. Thus, $\zeta_m^r = \pm 1$.

Thus, $f(x) = (x - \alpha)(x + \alpha)$ or $f(x) = (x - \alpha)$ [since these are all possible roots of f]. In either case, $\alpha^2 \in \mathbb{Q}$.

$\square$