Final (Solutions)

M552 – Modern Algebra II

May 2nd, 2012

We assume that R is a commutative ring with $1 \neq 0$.

1. Let R be a domain with field of fractions F and M be an R-module. Show that if $\operatorname{rank}(M) = r$, then $\dim_F(F \otimes_R M) = r$.

Proof. Remember first that if $1 \otimes m = 0$ in $F \otimes_R M$ if and only if there exists $c \in R \setminus \{0\}$ such that $cm = 0$.

Let $m_1, \ldots, m_r \in M$ be linearly independent elements. Suppose that $\sum_{i=1}^{r}(a_i/b_i)(1 \otimes m_i) = \sum_{i=1}^{r}(a_i/b_i) \otimes m_i = 0$. Let $b \overset{\text{def}}{=} b_1 \cdots b_r$. Then, $b/b_i \in R$ and

$$0 = b\left(\sum_{i=1}^{r}(a_i/b_i) \otimes m_i\right) = \sum_{i=1}^{r} a_i(b/b_i) \otimes m_i = \sum_{i=1}^{r} 1 \otimes (a_i(b/b_i)m_i) = 1 \otimes \left(\sum_{i=1}^{r} a_i(b/b_i)m_i\right).$$

Thus, we have then that there exists $c \in R \setminus \{0\}$ such that

$$0 = c\left(\sum_{i=1}^{r} a_i(b/b_i)m_i\right) = \left(\sum_{i=1}^{r} a_i(b/b_i)cm_i\right)$$

Since, $b_i, c, b \neq 0$ [remember that R is a domain] and $m_1, \ldots, m_r$ are linearly independent, we must have that $a_i = 0$ [and so $a_i/b_i = 0$] for all i, and hence $1 \otimes m_1, \ldots, 1 \otimes m_r$ are linearly independent in $F \otimes M$ and thus $\dim_F(F \otimes_R M) \geq r$.

Now, we observe that $F \otimes_R M = \{(1/d) \otimes m \;:\; d \in R \setminus \{0\}, m \in M\}$. Indeed, if $v \in F \otimes_R M$, then there are $a_i/b_i \in F$ and $m_i \in M$ such that

$$v = \sum_{i=1}^{k}(a_i/b_i) \otimes m_i = \sum_{i=1}^{k}(1/b_i) \otimes (a_i m_i).$$

Let $d = b_1 \cdots b_k$, and $d_i = d/b_i \in R$. Then,

$$v = \sum_{i=1}^{k}(d/b_i)/d \otimes (a_i m_i) = \sum_{i=1}^{k} 1/d \otimes (a_i d/b_i m_i) = 1/d \otimes \left(\sum_{i=1}^{k}(a_i d/b_i m_i)\right).$$

So, let $1/d_1 \otimes n_1, \dots, 1/d_k \otimes n_k$ be a basis of $F \otimes M$, and suppose that $\sum_{i=1}^k a_i n_i = 0$. Then,

$$0 = 1 \otimes \left(\sum_{i=1}^k a_i n_i \right) = \sum_{i=1}^k 1 \otimes (a_i n_i) = \sum_{i=1}^k a_i \otimes n_i = \sum_{i=1}^k a_i d_i ((1/d_i) \otimes n_i)$$

Thus, $a_i d_i = 0$ and since $d_i \neq 0$, we must have $a_i = 0$. Therefore, $n_1, \dots, n_k$ are linearly independent in M and thus $r = \mathrm{rank}(M) \geq k = \dim_F(F \otimes M)$.

With the two inequalities, we obtain the result. □

2. Let F be a field and M be a finitely generated $F[x]$-module. Show that M is projective if, and only if, M is isomorphic [as $F[x]$-module] to $F[x] \otimes V$ for some finite dimensional vector F-space V.

Proof. We first prove that a finitely generated $F[x]$-module M is projective if and only if it is free. We have that M is projective if and only if there exists an $F[x]$-module N such that $M \oplus N$ is free. [So, the "if" part is trivial.]

Now, if M is not free, by the structure theorem of finitely generated modules over PIDs, we have that $F[x]/(f)$, for some $f \in F[X] \setminus F$, is a direct summand of M. So, there exists an element $m \in M \setminus \{0\}$ such that $fm = 0$. Hence, we have that $(m, 0) \in M \otimes N$ is such that $f(m, 0) = 0$, and therefore cannot be free.

So, M is projective if, and only if, $M \cong F[x]^r \cong F[x] \otimes F^r$. For this last isomorphism, remember that, as (S, R)-modules, we have that $N \otimes_R R \cong N$ for any (S, R)-modulo N, and $N \otimes_R (N' \oplus N") \cong (N \otimes_R N') \oplus (N \otimes_R N")$. So, $F[x] \otimes F^r \cong F[x]^r$. $\square$

3. Let $q = p^n$, where p is an odd prime, and consider $f = x^q - x - 1 \in \mathbb{F}_q[x]$. Show that every irreducible factor of f has degree p. [**Hint:** if α is a root, then show that $\alpha^{(q^p)} = \alpha$.]

Proof. If $f(\alpha) = 0$, then $\alpha^q = \alpha + 1$. So, $\alpha^{(q^i)} = \alpha + i$, and therefore $\alpha^{(q^p)} = \alpha$.

Let $g \stackrel{\text{def}}{=} \min_{\alpha,\mathbb{F}_q}$. [Clearly $g \mid f$ and is irreducible. We will show that $\deg g = p$.] Now, we have that $\mathbb{F}_q[\alpha]/\mathbb{F}_q$ is Galois [finite field extension], and its Galois group is generated by $\psi : a \to a^q$ [the n-th power of the Frobenius map]. Also, $\deg g = [\mathbb{F}_q[\alpha] : \mathbb{F}_q] = |\mathrm{Gal}(\mathbb{F}_q[\alpha]/\mathbb{F}_q)| = |\langle \psi \rangle|$. But $\psi^i = \mathrm{id}_{\mathbb{F}_q[\alpha]}$ if and only if $\alpha + i = \psi^i(\alpha) = \alpha$ [as ψ fixes $\mathbb{F}_q$], i.e., if and only if $i \mid p$. So, $\deg g = |\langle \psi \rangle| = p$.

Since all irreducible factors of f come from minimal polynomial of roots of f, we have that all irreducible factors of f have degree p. □

4. Let $F \subseteq K \subseteq L$ be fields, with K/F Galois, $\alpha \in L$ such that $F[\alpha]/F$ is also Galois. Assume also that $\mathrm{Gal}(K/F) \cong A_7$ and $\mathrm{Gal}(F[\alpha]/F) \cong Z_4 \times Z_7$. Find $\mathrm{Aut}(K[\alpha]/K)$.

Proof. We first prove that $K \cap F[\alpha] = F$. Indeed, if $E \stackrel{\text{def}}{=} K \cap F[\alpha]$, then since $F[\alpha]/F$ is abelian, we have that E/F is Galois. This implies that $\mathrm{Gal}(K/E) \triangleleft \mathrm{Gal}(K/F) \cong A_7$. Since A_7 is simple, we have $\mathrm{Gal}(K/E)$ is either trivial or the whole A_7. But the former cannot occur, since then $(7!)/2 = |A_7| = |\mathrm{Gal}(E/F)| \leq |\mathrm{Gal}(F[\alpha]/F)| = |Z_4 \times Z_7| = 28$.

Therefore, we have that $E = F$. Thus, since $F[\alpha] \cdot K = K[\alpha]$, by Natural Irrationalities, we obtain that $K[\alpha]/K$ is Galois with $\mathrm{Gal}(K[\alpha]/K) \cong \mathrm{Gal}(F[\alpha]/F) \cong Z_4 \times Z_7$. Since $K[\alpha]/K$ is Galois, we have $\mathrm{Aut}(K[\alpha]/K) = \mathrm{Gal}(K[\alpha]/K)$. □