Modern Algebra II: Problem Set 8

Nilay Kumar

Last updated: March 24, 2013

Problem 1

Let F be a field of characteristic p and p be a positive integer that divides n, i.e. $n = pq$ for some positive integer q. Take the polynomial $f(x) = x^n - 1$. The derivative is $nx^{n-1} = 0$, i.e. every root will be a multiple root in some extension field of F. One, for example, is a multiple root of f.

If, on the other hand, F has characteristic 0, the derivative of f, $Df = nx^{n-1} \neq 0$ in general, and thus only zero can possibly be a multiple root of f. Zero, however, is not a root of f, so f has no multiple roots in any extension field E. Precisely the same reasoning holds if F has characteristic p but p does not divide n.

Problem 2

Let F be a field.

(i) By polynomial long division, we see that $(y^n - x^n)/(y - x)$ is given by $y^{n-1} + xy^{n-2} + \ldots + x^{n-2}y + x^{n-1}$, which is an element of $F[x, y]$.

(ii) If we now let $f(x) = \sum_i a_i x^i \in F[x]$, we can write

$$\frac{f(y) - f(x)}{y - x} = \frac{\sum_i a_i(y^n - x^n)}{y - x} = \sum_i a_i \left(y^{n-1} + xy^{n-2} + \ldots + x^{n-2}y + x^{n-1}\right),$$

which is again a polynomial, call it $Q_f(x, y)$ in x and y.

(iii) Given any $c \in F$, and $f, g \in F[x]$,

$$Q_{cf}(x, y) = \frac{cf(y) - cf(x)}{y - x} = c\frac{f(y) - f(x)}{y - x} = cQ_f.$$

Furthermore, we can write

$$\begin{aligned} Q_{f+g}(x,y) &= \frac{f(y)+g(y)-f(x)-g(x)}{y-x} \\ &= \frac{f(y)-f(x)}{y-x} + \frac{g(y)-g(x)}{y-x} \\ &= Q_f(x,y) + Q_g(x,y) \end{aligned}$$

Additionally, the product behaves as

$$\begin{aligned} Q_{fg}(x,y) &= \frac{f(y)g(y)-f(x)g(x)}{y-x} \\ &= \frac{f(y)g(y)-f(x)g(x)-f(y)g(x)+f(y)g(x)}{y-x} \\ &= \frac{f(y)g(y)-f(y)g(x)}{y-x} + \frac{f(y)g(x)-f(x)g(x)}{y-x} \\ &= f(y)Q_g(x,y) + Q_f(x,y)g(x) \end{aligned}$$

(iv) If we let $f_n(x) = x^n$, we can compute

$$Q_{f_n}(x,y) = \frac{y^n - x^n}{y-n} = y^{n-1} + xy^{n-2} + \ldots + x^{n-2}y + x^{n-1}.$$

If we now evaluate $Q_{f_n}(x,x)$, we simply insert x for y into the above expression. Since each of the n terms has products of x's and y's totalling to powers of $n-1$, when we perform the substitution we are simply left with nx^{n-1}. Using this result, given any polynomial $f(x) = \sum_i a_i x^i$, and its formal derivative $Df(x) = \sum_i i a_i x^{i-1}$, we can write

$$Df(x) = \sum_{i=1}^{n} i a_i x^{i-1} = \sum_{i=1}^{n} a_i Q_{x^i}(x,x) = Q_f(x,x),$$

where in the last equality we have used the definition of $f(x)$ and the linear property of the difference quotient.

Problem 3

Let F be a field, and suppose that F is a subring of a ring R. Let $r \in R$ and let $M_r : R \to R$ be multiplication by r, i.e. $M_r(s) = rs$. Note that if $s, t \in R$ and $a, b \in F$,

$$M_r(as+bt) = (as+bt)r = asr + btr = M_r(as) + M_r(bt)$$

and so M_r is an F-linear map.

Furthermore, $\ker M_r$ is the set of all elements of R that do not vanish when multiplied by r. Consequently, M_r is injective if r is not a zero divisor. Conversely, if r is not a zero divisor, $M_r(s) \neq 0$ for all $s \neq 0$, i.e. $\ker M_r = 0$ so M_r is injective.

If r happens to be a unit, one can always find an $s' \in R$ such that $M_r(s') = s$ for any $s \in R$:

$$M_r(s') = s'r = s$$
$$s' = s/r$$

and so M_r will be surjective. Conversely, if we know that M_r is surjective, it means that for each s, we can find an s' such that $s = s'r = M_r(s)$. Since this holds for every non-zero $s \in R$, and the associated s' obviously cannot be zero, this implies that r cannot a zero divisor (if it were, $s'r$ would be zero, not s). Consequently, by the above observations, M_r is injective as well, and thus an isomorphism from R to R (as F-vector spaces). Conversely, if we know that M_r is an isomorphism, it must be a surjection, and as above, r must be a unit.

Problem 4

Consider the field $\mathbb{Q}(\sqrt{2})$, viewed as a vector space of dimension 2 over $\mathbb{Q}$. Let $r + s\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. We now define the multiplication map $M_{r+s\sqrt{2}} : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ as above: $M_{r+s\sqrt{2}}(\alpha) = (r + s\sqrt{2})\alpha$.

(i) We can write a basis for $\mathbb{Q}(\sqrt{2})$ is $\{1, \sqrt{2}\}$. Take any $a+b\sqrt{2}$ in $\mathbb{Q}(\sqrt{2})$. Then

$$M_{r+s\sqrt{2}}(a + b\sqrt{2}) = ra + 2sb + (rb + sa)\sqrt{2}.$$

In matrix notation, we can write

$$M \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} ra + 2sb \\ rb + sa \end{pmatrix}$$

and so we can represent

$$M = \begin{pmatrix} r & 2s \\ s & r \end{pmatrix}.$$

(ii) Given any matrix $A \in M_2(\mathbb{Q})$, in order for $A = M_{r+s\sqrt{2}}$ for some r, s, it must be of the form above for some r, s.

(iii) It should be clear the determinant of $M_{r+s\sqrt{2}}$ is given by $r^2 - 2s^2$. Furthermore, if the determinant is zero and the number we are multiplying is non-zero, the map is not full-rank, i.e. the kernel forms a linear subspace of non-zero dimension (by the rank-nullity theorem). However, this contradicts that $\mathbb{Q}(\sqrt{2})$ is a field and that it has no zero divisors, and thus the number we are multiplying by must be zero. Conversely, if the number we are multiplying by is zero, the matrix is the zero matrix, and thus the determinant must be zero.

(iv) We may compute the inverse matrix using the usual technique for 2-by-2 matrices,

$$M^{-1}_{r+s\sqrt{2}} = \frac{1}{r^2 - 2s^2} \begin{pmatrix} r & -2s \\ -s & r \end{pmatrix}.$$

This shows that the inverse map is of the form $M_{t+u\sqrt{2}}$, where $t = r/(r^2 - 2s^2)$ and $u = -s/(r^2 - 2s^2)$. We can thus explicitly construct a multiplicative inverse for $r + s\sqrt{2}$ as

$$(r + s\sqrt{2})^{-1} = \frac{r}{r^2 - 2s^2} - \frac{s\sqrt{2}}{r^2 - 2s^2}$$

Problem 5

Consider the field $\mathbb{Q}(\sqrt{2})$ as a $\mathbb{Q}$-vector space of dimension 3. Take $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \in \mathbb{Q}(\sqrt{2})$. Similar to above, we define the multiplication map (with subscripts supressed),

$$M(\alpha) = \left(a + b\sqrt[3]{2} + c\sqrt[3]{2}^2\right)\alpha$$

(i) Let us choose the basis $\{1, \sqrt[3]{2}, \sqrt[3]{2}^2\}$ for $\mathbb{Q}(\sqrt[3]{2})$. Then we have

$$\begin{aligned} M(r + s\sqrt[3]{2} + t\sqrt[3]{2}^2) = {} & ra + rb\sqrt[3]{2} + rc\sqrt[3]{2}^2 \\ & + sa\sqrt[3]{2} + sb\sqrt[3]{2}^2 + 2sc \\ & + ta\sqrt[3]{2}^2 + 2tb + 2tc\sqrt[3]{2} \end{aligned}$$

This is written in matrix form as

$$M \begin{pmatrix} r \\ s \\ t \end{pmatrix} = \begin{pmatrix} ra + 2sc + 2tb \\ rb + sa + 2tc \\ rc + sb + ta \end{pmatrix}$$

and so we can represent

$$M = \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}$$

(ii) Given any matrix $A \in M_3(\mathbb{Q})$, in order for $A = M_{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2}$, it must be of the form above for some a, b, c.

(iii) We can compute

$$\det M_{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2} = a^3 + 4c^3 + 2b^3 - 6abc.$$

Just as above, the determinant must be non-zero as long as a, b, c are all non-zero. If the determinant is zero and the number we are multiplying is non-zero, the map is not full-rank, i.e. the kernel forms a linear subspace of non-zero dimension (by the rank-nullity theorem). However, this contradicts that $\mathbb{Q}(\sqrt[3]{2})$ is a field and that it has no zero divisors, and thus the number we are multiplying by must be zero. Conversely, if the number we are multiplying by is zero, the matrix is the zero matrix, and thus the determinant must be zero.

(iv) The inverse of M can be written

$$M^{-1}_{a+b\sqrt[3]{2}+c\sqrt[3]{2}^2} = \frac{1}{a^3 + 4c^3 + 2b^3} \begin{pmatrix} a^2 - 2bc & 2b^2 - 2ac & 4c^2 - 2ab \\ 2c^2 - ab & a^2 - 2bc & 2b^2 - 2ac \\ b^2 - ac & 2c^2 - ab & a^2 - 2bc \end{pmatrix}$$

Note that if we take $d = (a^2 - 2bc)/(a^3 + 4c^3 + 2b^3)$, $e = (2c^2 - ab)/(a^3 + 4c^3 + 2b^3)$, $f = (b^2 - ac)/(a^3 + 4c^3 + 2b^3)$, this matrix is of the form of a multiplication map $M_{d+e\sqrt[3]{2}+f\sqrt[3]{2}^2}$. In fact, we can use this to explicitly construct a multiplicative inverse for $a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$ as

$$(a+b\sqrt[3]{2}+c\sqrt[3]{2}^2)^{-1} = \frac{a^2 - 2bc}{a^3 + 4c^3 + 2b^3} + \frac{2c^2 - ab}{a^3 + 4c^3 + 2b^3}\sqrt[3]{2} + \frac{b^2 - ac}{a^3 + 4c^3 + 2b^3}\sqrt[3]{2}^2.$$