

MATH 511B, SOLUTIONS 6

1.

- (a) The proof is by induction on n . This is clear if $n = 1$ ($f(x)$ is linear). Assume true for polynomials of degree up to $n - 1$. If $\deg f(x) = n$ and $f(x)$ has no roots at all, then we're done; otherwise $f(x)$ has a root r , and we may divide

$$f(x) = q(x)(x - r) + c$$

where c has degree less than 1, hence is a constant. Substituting $x = r$ in this equation gives $c = 0$ and $f(x) = q(x)(x - r)$. Every root of $f(x)$ is either a root of $q(x)$ or of $x - r$, but by induction $q(x)$ has at most $n - 1$ roots, so we're done.

- (b) We have $R[x] \subset K[x]$. Regarding $f(x)$ as an element of $K[x]$, we see that f has at most n roots in K , hence at most n roots in R (a subset of K).

2. Any divisor of x^n in R is also a divisor in $K[x]$, so is of the form cx^m with $c \in K$. Any equality in R is an equality in $K[x]$, so if cx^m divides x^n in R , it must be that $x^n = (cx^m)(c^{-1}x^{n-m})$ with $c^{-1}x^{n-m} \in R$. In particular neither m nor $n - m$ can be 1.

We deduce that the divisors of x^5 in R are the polynomials of the form c, cx^2, cx^3 . All of these are divisors of x^6 as well, so the common divisors of x^5 and x^6 are the polynomials of the form c, cx^2, cx^3 . Since x^2 does not divide cx^3 in R , none of these is a greatest common divisor.

3. Since $K(x)[y]$ is a polynomial ring in one variable over the field $K(x)$, it is a PID, and the ideal $(x^2 + y^3 + y^2 - p(x)y)$ is maximal if and only if its generator $f(y) = y^3 + y^2 - p(x)y + x^2$ is irreducible. But $f(y)$, a cubic in y , is reducible if and only if it has a root. Since $K(x)$ is the fraction field of the UFD $K[x]$ and $f(y)$ is monic, by Gauss's lemma $f(y)$ has a root if and only if it has a root in $K[x]$, which must then divide the constant term x^2 . The only possible roots are therefore polynomials of the form c, cx , or cx^2 with $c \in K^\times$.

We substitute each of these possibilities for y . We have $f(c) = 0$ if and only if

$$c^3 + c^2 - p(x)c + x^2 = 0,$$

i.e., if and only if $p(x) = c^2 + c + c^{-1}x^2$.

We have $f(cx) = 0$ if and only if $c^3x^3 + c^2x^2 - p(x)cx + x^2 = 0$, i.e., if and only if $p(x) = c^2x^2 + (c + c^{-1})x$.

Finally, we have $f(cx^2) = 0$ if and only if

$$c^3x^6 + c^2x^4 - p(x)cx^2 + x^2 = 0,$$

i.e., if and only if $p(x) = c^2x^4 + cx^2 + c^{-1}$.

These are the values of $p(x)$ for which $f(y)$ is reducible, i.e., for which $K(x)[y]/(f)$ is not a field.

4.

- (a) The polynomial $xw - yz \in K[x, y, z][w]$ is linear in w , hence is irreducible if and only if the GCD of its coefficients is 1. The GCD of x and yz in $K[x, y, z]$ is certainly 1.
- (b) Part (a) is the case $n = 2$. We proceed by induction on n .

Let M_i be the minor submatrix of M obtained by deleting the first row and i th column. The cofactor expansion of $\det(M)$ is

$$\det(M) = \sum_{i=1}^n (-1)^{i+1} x_{1i} \det(M_i),$$

and none of the polynomials $\det(M_i)$ involve any x_{1j} . Regarded as a polynomial in $K[x_{12}, \dots, x_{nn}][x_{11}]$, $\det(M)$ is a linear polynomial $\det(M_1)x_{11} + C$ with leading coefficient $\det(M_1)$ and constant term

$$C = \sum_{i=2}^n (-1)^{i+2} x_{1i} \det(M_i).$$

By induction we know that $\det(M_1)$ is irreducible, so it remains to prove that $\det(M_1)$ does not divide C in $K[x_{12}, \dots, x_{nn}]$.

Regard $C = \sum_{i=2}^n (-1)^{i+2} x_{1i} \det(M_i)$ as a linear polynomial in the ring $K[x_{13}, \dots, x_{nn}][x_{12}]$ with leading term $-\det(M_2)$. Then C is divisible by $\det(M_1) \in K[x_{13}, \dots, x_{nn}]$ if and only if all its coefficients are; in particular $\det(M_1)$ would have to divide $\det(M_2)$. This is absurd, e.g. because they are irreducible polynomials of the same degree and they certainly are not associates ($\det(M_1)$ contains the variable x_{22} while $\det(M_2)$ does not).

5. The identity $x_n^k = (x_n - a_n + a_n)^k = \sum_{i=0}^k \binom{k}{i} (x_n - a_n)^i a_n^{k-i}$ easily implies that any polynomial $f(x_1, \dots, x_n)$ can be written as

$$f(x_1, \dots, x_n) = q_n(x_1, \dots, x_n)(x_n - a_n) + r(x_1, \dots, x_{n-1}).$$

(Another way to see this is to note that although $k[x_1, \dots, x_{n-1}][x_n]$ does not have a division algorithm in general, we *can* divide by monic polynomials in x_n .) Now repeat the above observation for $r(x_1, \dots, x_{n-1})$ and $x_{n-1} - a_{n-1}$; continuing, we eventually find

$$(1) \quad f(x_1, \dots, x_n) = (x_n - a_n)q_n + \dots + (x_1 - a_1)q_1 + q_0$$

where q_i is a polynomial in x_1, \dots, x_i and $q_0 \in K$. Substituting $x_i = a_i$ for all i , we see that $q_0 = f(a_1, \dots, a_n)$.

In particular if $f(a_1, \dots, a_n) = q_0 = 0$ then in (1) we have expressed $f(x_1, \dots, x_n)$ as an element of I . The converse (that if $f \in I$ then $f(a_1, \dots, a_n) = 0$) is obvious, so we have proved the first part of the problem.

Now consider the ring homomorphism $\phi : K[x_1, \dots, x_n] \rightarrow K$ sending $x_i \mapsto a_i$. Since $K[x_1, \dots, x_n]/\ker(\phi) \cong K$ is a field, $\ker(\phi)$ is a maximal ideal. But by the first part of the problem $\ker(\phi)$ is exactly I , and so I is maximal ideal.

Finally, if $x_i - b \in I$ then by the above we have $a_i - b = 0$, i.e., $b = a_i$. It follows immediately that if $(x_1 - a_1, \dots, x_n - a_n) = (x_1 - b_1, \dots, x_n - b_n)$ then $a_i = b_i$ for all i .

6. $(1 + \theta)(1 + \theta + \theta^2) = 2\theta^2 + 4\theta + 3$, while $\frac{1+\theta}{1+\theta+\theta^2} = \frac{1}{3}(-\theta^2 + 2\theta + 1)$. To see the latter, use the Euclidean algorithm to write 1 as a linear combination of $1 + x + x^2$ and $x^3 - 2x - 2$:

$$(1 + x + x^2)(-2x^2 + x + 5) + (2x + 1)(x^3 - 2x - 2) = 3.$$

Substitute θ for x to deduce that $(1 + \theta + \theta^2)^{-1} = \frac{1}{3}(-2\theta^2 + \theta + 5)$.

7. If the polynomial $x^3 - 3$ were reducible over $\mathbb{Q}(i)$, it would have a root in that field (a cubic is reducible if and only if it has a root). But the polynomial $x^3 - 3 \in \mathbb{Z}[x]$ is irreducible over \mathbb{Q} since it is Eisenstein at 3, so a root of $x^3 - 3$ generates an extension of degree 3 over \mathbb{Q} . Since $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, this is a contradiction.

8.

(a) Suppose D is not a square in F , and suppose $z \in F$ is a square in $F(\sqrt{D})$. Then

$$z = (x + y\sqrt{D})^2 = x^2 + Dy^2 + 2xy\sqrt{D}.$$

Since $\sqrt{D} \notin F$, we see that $x = 0$ or $y = 0$; that is, either $z = x^2$ is a square in F , or else z has the form y^2D for $y \in F$. The converse is clear.

Applying this to our problem, D_2 (which is assumed not to be square in F) is a square in $F(\sqrt{D_1})$ if and only if D_2 has the form y^2D_1 , if and only if D_1D_2 is a square. The problem follows.

(b) Write $\alpha = \sqrt{2} + \sqrt{3}$. The inclusion $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$ is clear. But $(\alpha - \sqrt{2})^2 = 3$, which implies (after a bit of algebra) that

$$(2) \quad \sqrt{2} = \frac{\alpha^2 - 1}{2\alpha} \in \mathbb{Q}(\alpha).$$

Then $\sqrt{3} = \alpha - \sqrt{2} \in \mathbb{Q}(\alpha)$ as well, and we obtain the reverse inclusion.

Now squaring (2) gives

$$2(2\alpha)^2 = (\alpha^2 - 1)^2$$

which simplifies to

$$\alpha^4 - 10\alpha^2 + 1 = 0.$$

By (a) we have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ and the minimal polynomial of α has degree 4; thus the minimal polynomial of α is $x^4 - 10x^2 + 1$.

9. The extension $F(\alpha)/F(\alpha^2)$ is generated over $F(\alpha^2)$ by a root of the polynomial $x^2 - \alpha^2$. Therefore the extension has degree 1 or 2. The latter is ruled out by the assumption that $[F(\alpha) : F]$ is odd, so $[F(\alpha) : F(\alpha^2)] = 1$ and $F(\alpha) = F(\alpha^2)$.

10. Part (i) is a trivial verification. For part (ii), chose any basis \mathcal{B} for K as an n -dimensional vector space over F , and let $\iota(\alpha)$ be the matrix for the multiplication-by- α map in this basis. That is, the entries in the j th column of $\iota(\alpha)$ are the elements $a_{1j}, \dots, a_{nj} \in F$ such that $\sum_{i=1}^n a_{ij}v_i = \alpha v_j$. This gives a homomorphism $\iota : K \rightarrow M_n(F)$.

(iii) **Solution 1:** We'd like to show that α is an eigenvalue of $\iota(\alpha)$. The problem is that since $\alpha \notin F$, we certainly aren't going to be able to exhibit a vector in the F -vector space K on which $\iota(\alpha)$ acts via α . Fortunately we can regard the matrix $\iota(\alpha) = (a_{ij})$ as a matrix A with entries in K ; we have some hope that we could write down a vector in K^n on which $\iota(\alpha)$ acts via α . Actually, we'll write down a vector on which the transpose A^T acts via α ; since A^T and A have the same characteristic polynomial, this will suffice.

Let our basis $\mathcal{B} = (v_1, \dots, v_n)$ and let \mathbf{v} be the column vector with entries $v_1, \dots, v_n \in K$. Then the j th entry of $A^T \mathbf{v}$ is $\sum_{i=1}^n a_{ij} v_i$; by definition of A this is αv_j . So $A^T \mathbf{v} = \alpha \mathbf{v}$, as desired.

Solution 2: We use the Cayley-Hamilton theorem. If $f(x) \in F[x]$ is any polynomial, then $\iota(f(\alpha)) = f(\iota(\alpha))$ since ι is a ring homomorphism, and since each element $a \in F$ maps to the corresponding scalar matrix $aI \in M_n(F)$. Let $P(x)$ be the characteristic polynomial of $\iota(\alpha)$. Then

$$\iota(P(\alpha)) = P(\iota(\alpha)) = 0$$

by Cayley-Hamilton, and since ι is injective we conclude that $P(\alpha) = 0$.

(iv) With respect to this basis, the element $a + b\sqrt{D}$ maps to the matrix

$$\begin{pmatrix} a & bD \\ b & a \end{pmatrix}.$$