

Homework 6, Selected Solutions

1) a)  $\begin{bmatrix} 1 & 1 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{bmatrix}$  works.

b) Let  $A = \begin{bmatrix} 0 & 37 & 0 \\ 0 & 0 & 101 \\ 1 & 0 & 0 \end{bmatrix}$ . Then  $\det(A) = 37 \cdot 101$ . Over  $\mathbb{Q}$  we see  $A$  has rank 3. Over

$\mathbb{F}_{37}$  and  $\mathbb{F}_{101}$  we see  $A$  has determinant 0. Over these fields  $A$  becomes  $\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 27 \\ 1 & 0 & 0 \end{bmatrix}$  and

$\begin{bmatrix} 0 & 37 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$  respectively. These both have rank 2.

2) Let  $V$  be  $n$  dimensional. Following last week's homework, it is not hard to show that the dimension of the space of  $k$ -multilinear functions on  $V$  is  $n^k$ . This week, however we are interested in the  $k$ -multilinear *alternating* functions.

Let  $\{\vec{v}_1, \dots, \vec{v}_n\}$  be a basis of  $V$ . For each set of  $k$  distinct integers  $A = \{a_1 < a_2 < \dots < a_k\}$  we define a function  $\Psi_A(\sum_{j=1}^n \beta_{j1}, \sum_{j=1}^n \beta_{j2}, \dots, \sum_{j=1}^n \beta_{jk})$  to be the determinant of the  $k \times k$  matrix with  $rs$  entry equal to  $\beta_{a_r s}$ . From the properties of the determinant we immediately see that  $\Psi_A$  is alternating and  $k$ -multilinear. I claim that as we vary  $A$  through all sets  $\mathcal{S}$  of  $k$  distinct integers  $\{a_1 < a_2 < \dots < a_k\}$  we get a basis of the alternating and  $k$ -multilinear functions on  $V$ . Consider a dependence relation  $\sum_{B \in \mathcal{S}} \alpha_B \Psi_B = 0$ . Choose  $A = \{a_1 < a_2 < \dots < a_k\} \in \mathcal{S}$  and evaluate the left hand side at  $(\vec{v}_{a_1}, \vec{v}_{a_2}, \dots, \vec{v}_{a_k})$ . For  $B \neq A$  we have  $B = \{b_1 < b_2 < \dots < b_k\}$  and for some  $t$  we have  $b_t \notin A$ . We see that  $\Psi_B(\vec{v}_{a_1}, \vec{v}_{a_2}, \dots, \vec{v}_{a_k})$  is a determinant of a  $k \times k$  matrix whose  $t$ th column is all zeros, that is  $\Psi_B(\vec{v}_{a_1}, \vec{v}_{a_2}, \dots, \vec{v}_{a_k}) = 0$  for  $B \neq A$ . It is clear that  $\Psi_A(\vec{v}_{a_1}, \vec{v}_{a_2}, \dots, \vec{v}_{a_k}) = 1$  so  $\sum_{B \in \mathcal{S}} \alpha_B \Psi_B(\vec{v}_{a_1}, \vec{v}_{a_2}, \dots, \vec{v}_{a_k}) = \alpha_A \Psi_A(\vec{v}_{a_1}, \vec{v}_{a_2}, \dots, \vec{v}_{a_k}) = \alpha_A$ . Thus if  $\sum_{B \in \mathcal{S}} \alpha_B \Psi_B = 0$  we have  $\Psi_A = 0$  for all  $A \in \mathcal{S}$ . The functions  $\Psi_A$  for  $A \in \mathcal{S}$  are independent. It remains to show they span the space of alternating and  $k$ -multilinear functions.

Let  $\Gamma$  be alternating and  $k$ -multilinear. For  $A \in \mathcal{S}$  set  $\alpha_A = \Gamma_A(\vec{v}_{a_1}, \vec{v}_{a_2}, \dots, \vec{v}_{a_k})$ . I claim  $\Gamma = \sum_{A \in \mathcal{S}} \alpha_A \Psi_A$ . Since both sides are alternating and  $k$ -multilinear, we need only check that they agree on  $k$ -tuples of the form  $(\vec{v}_{c_1}, \vec{v}_{c_2}, \dots, \vec{v}_{c_k})$  where  $c_1 < c_2 < \dots < c_k$ . Setting  $C = \{c_1, \dots, c_k\}$  we get that  $\Gamma(\vec{v}_{c_1}, \vec{v}_{c_2}, \dots, \vec{v}_{c_k}) = \alpha_C$  by definition, and  $\sum_{A \in \mathcal{S}} \alpha_A \Psi_A(\vec{v}_{c_1}, \vec{v}_{c_2}, \dots, \vec{v}_{c_k}) = \alpha_C$  by the work we did in the proof of independence. Thus the functions  $\Psi_A$  for  $A \in \mathcal{S}$  span the space of alternating and  $k$ -multilinear functions. We need only find the cardinality of  $\mathcal{S}$ . It is well know this is  $\binom{n}{k}$ . Note the space of  $k$ -multilinear alternating functions is *trivial* if  $k > n$ .

If this seems like magic, remember the heavy lifting is done in the existence and uniqueness of the determinant function.

3) We know  $\det(A) = \det(A^T)$ . On the first day of class we learned that complex conjugation is a field automorphism, so  $\det(A^*) = \det(\overline{A^T}) = \det(\overline{A})$ . If  $AA^* = I_n$  we see  $\det(A)\det(A^*) = 1$  so  $\det(A)\det(\overline{A}) = 1$ . Setting  $\det(A) = a + bi$  we see  $a^2 + b^2 = 1$ , that is  $|\det(A)| = 1$ .

4) Note that if  $D$  is invertible we have  $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} I & 0 \\ -D^{-1}C & I \end{pmatrix} = \begin{pmatrix} A - BD^{-1}C & B \\ 0 & D \end{pmatrix}$ .

Recalling from a previous assignment that  $\det \begin{pmatrix} X & Y \\ 0 & Z \end{pmatrix} = \det(X)\det(Z)$  we see that

$\det \begin{pmatrix} A & B \\ C & D \end{pmatrix} = \det(AD - BD^{-1}CD) = \det(AD - BC)$  where the last equality uses that  $D$  and  $C$  commute. We can also get the result if  $A$  is invertible in a similar manner.

Considering  $x$  as a variable, observe that for a  $k \times k$  matrix  $P$  that  $\det(P - xI_k)$  is a polynomial in  $x$  of degree  $k$ . Indeed, using the permutation description of determinants, the identity permutation contributes a degree  $k$  term in  $x$ . For all other permutations  $\sigma$  there is some  $i$  with  $\sigma(i) \neq i$  and  $(P - xI_k)_{i\sigma(i)} = P_{i\sigma(i)}$  so the contribution to the determinant from  $\sigma$  is at most degree  $k - 1$  in  $x$ . Thus  $P - xI_k$  is invertible over  $\mathbb{F}(x)$ , the field of fractions of  $\mathbb{F}[x]$ .

Note that if  $A, B, C$  and  $D$  pairwise commute, then so do  $A - xI_n, B, C$  and  $D - xI_n$ . By our initial reasoning, since  $D - xI_n$  is invertible over  $\mathbb{F}(x)$ , we have  $\det \begin{pmatrix} A - xI_n & B \\ C & D - xI_n \end{pmatrix} = \det(AD - B(D - xI_n)^{-1}C(D - xI_n)) = \det((A - xI_n)(D - xI_n) - BC)$ . Thus the polynomials  $\det \begin{pmatrix} A - xI_n & B \\ C & D - xI_n \end{pmatrix}$  and  $\det((A - xI_n)(D - xI_n) - BC)$  of degree  $2n$  in the variable  $x$  are identical. Evaluating them at  $x = 0$  gives the desired result.

5) The elements  $x$  and  $5$  of  $\mathbb{Z}[x]$  have no common factors, but if  $5f_1(x) + xf_2(x) = 1$ , plugging in  $x = 0$  we see  $5f_1(0) = 1$ . But  $1$  is not a multiple of  $5$ . corollary 20.16 does not hold here. Of course the corollary is only asserted for polynomials over a *field*.

6) a)  $x^2 - 2$  is prime over  $\mathbb{Q}[x]$ . If it weren't, it would factor and we would have that  $\sqrt{2} \in \mathbb{Q}$ . Over  $\mathbb{R}[x]$  we see  $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ .

b)  $x^2 + 1$  is prime over  $\mathbb{R}[x]$ . If it weren't, it would factor and we would have that  $\sqrt{-1} \in \mathbb{R}$ . Over  $\mathbb{C}[x]$  we see  $x^2 + 1 = (x - \sqrt{-1})(x + \sqrt{-1})$ .

c)  $x^2 - 5$  is prime over  $\mathbb{F}_7[x]$ . If it weren't, it would factor as  $(x - \alpha)(x - \beta)$ . Thus  $x^2 - 5$  would have a root in  $\mathbb{F}_7$ . Plugging in  $0, 1, 2, 3, 4, 5$  and  $6$  into  $x^2 - 5$  gives  $2, 3, 6, 4, 6$  and  $3$ . Clearly  $x^2 + 5$  becomes  $x^2$  over  $\mathbb{F}_5[x]$  which factors to  $x \cdot x$ .

d) Consider  $x^5 - 2$ . Over  $\mathbb{F}_5[x]$  this becomes  $(x + 2)^5$ . (Check it!) I claim  $x^5 - 2$  is prime over  $\mathbb{Q}[x]$ . Suppose  $x^5 - 2 = p(x)q(x)$ . If either  $p(x)$  or  $q(x)$  is degree 1, that is of the form  $x - \alpha$ , then we would have  $\alpha \in \mathbb{Q}$  and  $\alpha^5 = 2$ . But  $2^{1/5}$  is irrational by the same standard proof that  $\sqrt{2}$  is irrational. Thus we must have that one of  $p(x)$  or  $q(x)$  is quadratic with roots  $r \pm s\sqrt{d}$  with  $r, s, d \in \mathbb{Q}$  and  $(r \pm s\sqrt{d})^5 = 2$ . Suppose  $p(x) = x^2 + rx + s \in \mathbb{Q}[x]$  is the quadratic. If  $p(x)$  has distinct real roots, then their 5th powers are distinct. But the 5th powers are 2, so  $p(x)$  does not have distinct real root. If  $p(x)$  has a real double root, this is necessarily rational (why?). Thus  $2^{1/5}$  is rational, a contradiction. We see  $p(x)$  has

distinct complex roots  $u + iv\sqrt{w}$  and  $u - iv\sqrt{w}$  where  $u, v, w \in \mathbb{Q}$  and  $w > 0$ . Furthermore  $(u + iv\sqrt{w})^5 = 2 = (u - iv\sqrt{w})^5$  so  $(u + iv\sqrt{w})^5(u - iv\sqrt{w})^5 = (w^2 + v^2w)^5 = 4$ . Thus we have  $4^{1/5}$  is rational. But  $4^{1/5}$  is irrational by the same standard proof that  $\sqrt{2}$  is irrational. No factorization of  $x^5 - 2$  exists over  $\mathbb{Q}[x]$ . It is prime.