Problem Set 2

Most of these problems are taken from the 4th edition of Cox-Little-O'Shea, § 1.4, § 1.5.

1. Use the Euclidean algorithm to do the following.

   (a) Find $\gcd(112, 84)$ and find integers a, b so that $\gcd(112, 84) = a \cdot 84 + b \cdot 112$.

   (b) Find h so that $\langle x^3 + x + 1, x^2 + 2x + 3\rangle = \langle h\rangle$.

   (c) Find h so that $\langle x^3 - x, x^2 + 3x + 2\rangle = \langle h\rangle$.

   (d) Find h so that $\langle x^4 - x, x^5 - x, x^6 - x\rangle = \langle h\rangle$.

2. Find the row reduced echelon form of the matrix M below over $\mathbb{Q}(x)$ and over $\mathbb{F}_2[x]/\langle x^3 + x + 1\rangle$.

$$\begin{bmatrix} 1 & x & x^2 \\ 0 & 1+x & 1+x^2 \end{bmatrix}$$

3. Some more practice with linear algebra over finite fields:

   (a) Show that $x^3 + x^2 + 2$ is irreducible over $\mathbb{F}_3[x]$.

   (b) Conclude that $F = \mathbb{F}_3[x]/\langle x^3 + x^2 + 2\rangle$ is a field.

   (c) Consider the matrix

$$M = \begin{bmatrix} 1 & 0 & x & 2 \\ 0 & 1 & x+1 & x^2 \end{bmatrix}$$

   defined over the field F. Is the vector $\begin{bmatrix} x & 2 & 1+x & 1 \end{bmatrix}$ in the row space of M?

4. Prove the following equalities of ideals in $\mathbb{Q}[x, y]$:

   (a) $\langle x + y, x - y\rangle = \langle x, y\rangle$

   (b) $\langle x + xy, y + xy, x^2, y^2\rangle = \langle x, y\rangle$

   (c) $\langle y^2 - xz, xy - z, x^2 - y\rangle = \langle y - x^2, z - x^3\rangle$

5. A *radical* ideal is an ideal $I \subset \mathbb{K}[x_1, \ldots, x_n]$ satisfying that if $f^k \in I$ for some integer k, then $f \in I$.

   (a) Prove that $I(V)$ is a radical ideal for any set $V \subset \mathbb{K}^n$.

   (b) Prove that $\langle x^2, y^2\rangle$ is not a radical ideal, so it is not the ideal of any set.

6. Let $V \subset \mathbb{R}^3$ be parametrized by $x = t, y = t^3, z = t^4$.

   (a) Prove that V is an affine variety.

   (b) Determine the ideal $I(V)$.

7. Suppose $I \subset \mathbb{K}[x_1, \ldots, x_n]$ is an ideal and f, g are polynomials.

   (a) If $f^2, g^2 \in I$, show that $(f + g)^3 \in I$.

   (b) More generally, if $f^r, g^s \in I$, show that $(f + g)^{r+s-1} \in I$.

8. Show that the Vandermonde determinant

$$\det \begin{bmatrix} 1 & a_1 & a_1^2 & \cdots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \cdots & a_2^{n-1} \\ & \vdots & & & \vdots \\ 1 & a_n & a_n^2 & \cdots & a_n^{n-1} \end{bmatrix}$$

is non-zero when all the a_i are distinct. Hint: if the determinant is zero, show that cofactor expansion along a row leads to a polynomial of degree $n-1$ which has at least n roots.

9. Suppose $f \in \mathbb{C}[x]$.

   (a) If $f = (x-a)^r h$, where $a \in \mathbb{C}$ and $h \in \mathbb{C}[x]$ does not vanish at a, show that $f' = (x-a)^{r-1}h_1$, where h_1 does not vanish at a.

   (b) Let $f = c(x-a_1)^{r_1}\cdots(x-a_\ell)^{r_\ell}$ be the factorization of f, where $a_1,\dots,a_\ell$ are distinct. Prove that $f' = (x-a_1)^{r_1-1}\cdots(x-a_\ell)^{r_\ell-1}H$, where $H \in \mathbb{C}[x]$ does not vanish at any of $a_1,\dots,a_\ell$.

   (c) Prove that $\gcd(f,f') = (x-a_1)^{r_1-1}\cdots(x-a_\ell)^{r_\ell-1}$.

10. If $f \in \mathbb{C}[x]$ factors as $f = c(x-a_1)^{r_1}\cdots(x-a_\ell)^{r_\ell}$, then the *squarefree part* of f, denoted f_{red} is defined as $f_{red} = c(x-a_1)\cdots(x-a_\ell)$.

    (a) Use the previous exercise to show that

    $$f_{\text{red}} = \frac{f}{\gcd(f,f')}.$$

    This allows for quick computation of f_{red} *without* factoring f.

    (b) Use Macaulay2 to find f_{red} if

    $$f = x^{11} - x^{10} + 2x^8 - 4x^7 + 3x^5 - 3x^4 + x^3 + 3x^2 - x - 1.$$

11. List all the monomials of degree at most two in $\mathbb{K}[x,y,z]$ (there are ten of these) from *smallest* (starting with $1 = x^0y^0z^0$) to *largest* according to the following monomial orders:

    - Lexicographic order.
    - Graded lexicographic order.
    - Graded reverse lexicographic order.

    In Macaulay2 when you define a polynomial ring, one of the options you can give is a monomial order (the default order is graded reverse lexicographic). The 'sort' command, when applied to a list of monomials, will automatically use the monomial order of the polynomial ring. See if you can reproduce the three lists you obtained above by using Macaulay2.

Some additional suggested exercises from Cox-Little-O'Shea:

- § 1.4, problem 6