MAT 150C - Homework 1

Markus Tran

Computational Exercises

1. (a) $(3+\alpha)(-1+2\alpha) = -3+6\alpha-\alpha+2\alpha^2 = 3+5\alpha = 3.$

   (b) $(4+2\alpha)(x+y\alpha) = 4x+4y\alpha+2x\alpha+2y\alpha^2 = (4x+6y)+(2x+4y)\alpha.$

   Solving the system

$$\begin{aligned} 4x+6y &= 1 \\ 2x+4y &= 0 \end{aligned}$$

   in $\mathbb{F}_5$ gives $x=1, y=2$.

2. $\mathbb{F}_7[x]/(x^2-c)$ is a field whenever (x^2-c) is irreducible, which occurs whenever c is not a square in $\mathbb{F}_7$. In $\mathbb{F}_7$, we have

x	x^2
0	0
1	1
2	4
3	2
4	2
5	4
6	1

   Thus $c = 3, 5, 6$.

3. (a)

$$(1+x+x^2)\cdot\sum_{i=0}^{\infty} a_i x^i = a_0 + (a_0+a_1)x + (a_0+a_1+a_2)x^2 + (a_1+a_2+a_3)x^3 + \cdots.$$

   We have $a_0 = 1$ and $a_1 = -1$. The relation $a_n = -a_{n-1} - a_{n-2}$ for $n \geq 2$ gives the sequence $(a_n) = (1, -1, 0, 1, -1, 0, \ldots)$, so

$$(1+x+x^2)^{-1} = 1 - x + x^3 - x^4 + x^6 - x^7 + \cdots.$$

   (b)

$$\left(\sum_{i=0}^{\infty} x^i\right)\left(\sum_{i=0}^{\infty} a_i x^i\right) = \sum_{i=0}^{\infty}\left(\sum_{k=0}^{i} a_k\right) x^i.$$

Similarly, we have $a_0 = 1$ and $a_1 = -1$, and the relation $a_n = -\sum_{i=0}^{n-1} a_i$ for $n \geq 2$ gives $a_n = 0$. Thus

$$\left(\sum_{i=0}^{\infty} x^i\right)^{-1} = 1 - x.$$

Theoretical Exercises

1. (a) Let $x, y \in IJ$, so that $x = \sum_{i=1}^{n} f_i g_i$ and $y = \sum_{j=1}^{m} f_j g_j$ with $f_i, f_j \in I$ and $g_i, g_j \in J$. Then $x + y$ can be written as $x + y = \sum_{k=1}^{n+m} f_k g_k$, and IJ is closed under addition.

   Let $x \in IJ$ and $r \in R$ with $x = \sum_{i=1}^{n} f_i g_i$. Then $rx = \sum_{i=1}^{n} r f_i g_i$. Since I is an ideal and $f_i \in I$, then $rf_i \in I$ and so $rx \in IJ$. Therefore IJ is an ideal in R.

   (b) Let $x \in IJ$ and $x = \sum_{i=1}^{n} f_i g_i$. Since I is an ideal and $f_i \in I$, then $f_i g_i \in I$. This means that x is a sum of elements in I, and so $x \in I$. By a similar argument, $x \in J$, and altogether $x \in I \cap J$.

   (c) Let $R = \mathbb{R}[x]$, and let $I = J = (x^2)$ be the ideal consisting of polynomials where every term has degree at least 2. Then $I \cap J = (x^2)$, but $IJ = (x^4)$, the ideal of polynomials where every term has degree at least 4.

2. (a) Let a, b be nilpotent elements in R such that $a^n = b^m = 0$. Let $N = \max(n, m)$, so that $a^N = b^N = 0$. Then

   $$(a+b)^{2N} = \sum_{k=0}^{2N} \binom{2N}{k} a^k b^{2N-k}.$$

   Since either $k \geq N$ or $2N - k \geq N$, then $a^k b^{2N-k} = 0$, and the whole sum equals 0. Thus $a + b$ is nilpotent.

   Let a be a nilpotent element in R such that $a^n = 0$, and let $r \in R$. Then $(ra)^n = r^n a^n = 0$, and ra is a nilpotent element. Therefore $\mathfrak{nil}(R)$ is an ideal.

   (b)

Let $\overline{x}$ be a nonzero element of $R/\mathfrak{nil}(R)$ with representative x where x is not nilpotent in R. Then $(\overline{x})^n = \overline{x^n} \neq \overline{0}$, since x^n is also never nilpotent. Thus $\overline{x}$ is not nilpotent in $R/\mathfrak{nil}(R)$.

(c) Let a be a nilpotent element and u a unit in R. Then $u^{-1}a$ is another nilpotent element, and say $(u^{-1}a)^n = 0$. Then

$$(u+a) \cdot u^{-1} \sum_{i=0}^{n-1} (-1)^i (u^{-1}a)^i = (1 + u^{-1}a) \cdot \sum_{i=0}^{n-1} (-1)^i (u^{-1}a)^i = 1 \pm (u^{-1}a)^n = 1.$$

Thus $u + a$ is a unit.

3. (a) Let $f_a \in \mathbb{F}_q[x]$ be defined as

$$f_a(x) = \prod_{b \neq a} (x-b)(a-b)^{-1}.$$

This is well defined, since $a - b \neq 0$. Furthermore, $f_a(a) = 1$ and $f_a(b) = 0$ for $b \neq a$.

(b) Let $f \in \mathbb{F}_q[x]$ be defined as

$$gf = \sum_{a \in \mathbb{F}_q} \Phi(a) \cdot f_a.$$

Then for any $a \in \mathbb{F}_q$,

$$f(a) = \underbrace{\Phi(a) \cdot f_a(a)}_{\Phi(a)} + \sum_{b \neq a} \underbrace{\Phi(b) \cdot f_b(a)}_{0} = \Phi(a).$$

(c) Part (b) shows that ev is surjective.

Let $f \in \ker(\mathrm{ev})$, so $f(a) = 0$ for all $a \in \mathbb{F}_q$. Therefore $(x - a)$ divides f, and $p = \prod_{a \in \mathbb{F}_q} (x - a)$ divides f. Every element of $\ker(\mathrm{ev})$ can be written as pq where q is a polynomial in $\mathbb{F}_q[x]$, so $\ker(\mathrm{ev}) \subseteq (p)$. Clearly $(p) \subseteq \ker(\mathrm{ev})$, and altogether $\ker(\mathrm{ev}) = (p)$.