ANSWERS TO SOME OF THE HOMEWORK PROBLEMS

Eighth problem set

1. The derivative of $x^n - 1$ is nx^{n-1}. If the characteristic of F divides n, then $nx^{n-1} = 0$, and hence there exists a multiple root of $x^n - 1$. In fact, if $n = pk$, then $x^n - 1 = (x^k - 1)^p$. If the characteristic of F does not divide n or is zero, then nx^{n-1} is a nonzero polynomial whose only root is 0. Since 0 is not a root of $x^n - 1$, $x^n - 1$ does not have a multiple root.

2. (i) This is just a geometric series:

$$\frac{y^n - x^n}{y - x} = y^{n-1} + y^{n-2}x + \cdots + yx^{n-2} + x^{n-1}.$$

(ii) Follows by looking term by term at $Q_f(x, y)$: if $f(x) = \sum_{i=1}^n a_i x^i$, then

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

and each individual summand is by (i) a polynomial in x and y. (iii) The identities $Q_{cf}(x, y) = cQ_f(x, y)$ and $Q_{f+g}(x, y) = Q_f(x, y) + Q_g(x, y)$ are straightforward. As for $Q_{fg}(x, y)$, we have

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

and hence, after dividing by $y - x$, we see that

$$Q_{fg}(x, y) = f(y)Q_g(x, y) + Q_f(x, y)g(x).$$

(iv) If $f(x) = x^n$, then by (i)

$$Q_f(x, x) = x^{n-1} + x^{n-2}x + \cdots + xx^{n-2} + x^{n-1} = nx^{n-1}.$$

The remaining statements follow from (iii).

3. Clearly, $M_r(s_1 + s_2) = r(s_1 + s_2) = rs_1 + rs_2 = M_r(s_1) + M_r(s_2)$ and, for $a \in F$, $M_r(as) = ras = ars = aM_r(s)$. Hence M_r is F-linear. As $\operatorname{Ker} M_r = \{s \in R : rs = 0\}$, M_r is injective $\iff$ $\operatorname{Ker} M_r = \{0\}$ $\iff$ r is not a zero divisor. If M_r is surjective, then in particular $M_r(s) = 1$

for some $s \in R$, i.e. there exists an $s \in R$ such that $rs = 1$, so that r is a unit. Hence M_r surjective $\implies$ r is a unit. Next, if r is a unit, then clearly $M_r \circ M_{r^{-1}} = M_{r^{-1}} \circ M_r = M_{rr^{-1}} = M_1 = \mathrm{Id}$. Hence r is a unit $\implies$ M_r is an isomorphism, and clearly M_r is an isomorphism $\implies$ M_r is surjective.

4. (i) $M_{r+s\sqrt{2}} = \begin{pmatrix} r & 2s \\ s & r \end{pmatrix}$. (ii) $a = d$, $b = 2c$. (iii) $\det M_{r+s\sqrt{2}} = r^2 - 2s^2$. By Problem 3, $M_{r+s\sqrt{2}}$ is injective, hence invertible, hence $\det M_{r+s\sqrt{2}} \neq 0$. (iv) We use the general formula that, if $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is an invertible 2×2 matrix, then $A^{-1} = \dfrac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$. Thus

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

By (ii), this is of the form $M_{t+u\sqrt{2}}$, where $t = \dfrac{r}{r^2 - 2s^2}$ and $u = \dfrac{-s}{r^2 - 2s^2}$. Thus we see that

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

5. (i) $M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2} = \begin{pmatrix} a & 2c & 2b \\ b & a & 2c \\ c & b & a \end{pmatrix}$. (ii) If $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, then the conditions are $a_{11} = a_{22} = a_{33}$, $a_{13} = 2a_{21} = 2a_{32}$, $a_{12} = a_{23} = 2a_{31}$. (iii) $a^3 + 2b^3 + 4c^3 - 6abc$. It is nonzero if $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \neq 0$ for the same reason as Problem 4, Part (iii). (iv) By Cramer's rule,

$$M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2}^{-1} = \frac{1}{a^3 + 2b^3 + 4c^3 - 6abc} \begin{pmatrix} a^2 - 2bc & 2b^2 - 2ac & 4c^2 - 2ab \\ 2c^2 - ab & a^2 - 2bc & 2b^2 - 2ac \\ b^2 - ac & 2c^2 - ab & a^2 - 2bc \end{pmatrix}.$$

By (ii), setting $d = a^3 + 2b^3 + 4c^3 - 6abc$, $M_{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2}^{-1} = M_{r+s\sqrt[3]{2}+t(\sqrt[3]{2})^2}$, where

$$r = \frac{1}{d}(a^2 - 2bc); \quad s = \frac{1}{d}(2c^2 - ab); \quad t = \frac{1}{d}(b^2 - ac).$$

This then gives an explicit formula for $(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2)^{-1}$.

Ninth problem set

1. (i) Suppose that $f(x) \in F[x]$ is irreducible but that $f(x)$ has multiple roots. As we have seen, $Df(x) = 0$ and hence $f(x) = \sum_{i=0}^{n} a_i x^{ip}$ for some $a_i \in F$. Since F is perfect, there exist $b_i \in F$ such that $a_i = b_i^p$. Thus $f(x) = \sum_{i=0}^{n} a_i x^{ip} = \sum_{i=0}^{n} b_i^p x^{ip}$. Since raising to the p^{th} power is a homomorphism in characteristic p, $f(x) = \sum_{i=0}^{n} b_i^p x^{ip} = (\sum_{i=0}^{n} b_i x^i)^p$. Hence $f(x)$ is a p^{th} power and in particular is not irreducible, a contradiction. (ii) (Done in class.) If F is a finite field then $\sigma_p \colon F \to F$ is a homomorphism, automatically injective since F is a field, hence surjective by the pigeonhole principle. (iii) No, for example if $\#(F) = q$ and k and $q-1$ are not relatively prime, then not every element of F is a k^{th} power. For example, suppose that q is odd. Then not every element of F is a square, because the function $f \colon F \to F$ defined by $f(a) = a^2$ is not injective ($a^2 = (-a)^2$ but $a \neq -a$ since the characteristic of F is not 2) and hence f is not surjective. The argument in (ii) breaks down because, if $f \colon F \to F$ is defined by $f(a) = a^k$, then f is not a homomorphism if k is not a power of p, and so the statement $f^{-1}(0) = \{0\}$ does not necessarily imply that f is injective.

2. (i) Clearly $[\mathbb{F}_2(\alpha) : \mathbb{F}_2] = 2$. Also,

$$(\alpha+1)^2 + (\alpha+1) + 1 = \alpha^2 + 1 + \alpha + 1 + 1 = \alpha^2 + \alpha + 1 = 0.$$

Thus $x^2 + x + 1$ has two distinct roots in $\mathbb{F}_2(\alpha)$ and hence factors into linear factors:

$$x^2 + x + 1 = (x - \alpha)(x - (\alpha + 1)) = (x + \alpha)(x + \alpha + 1).$$

(ii) Clearly $[\mathbb{F}_2(\beta) : \mathbb{F}_2] = 3$ and $\#(\mathbb{F}_2(\beta)) = 2^3 = 8$. If $\sigma_{2^k} = (\sigma_2)^k$, where σ_2 is the Frobenius homomorphism, then $\beta^2 = \sigma_2(\beta)$ and $\beta^4 = \sigma_4(\beta)$. Since σ_2 is a homomorphism,

$$0 = \sigma_2(0) = \sigma_2(\beta^3 + \beta + 1) = (\sigma_2(\beta))^3 + \sigma_2(\beta) + 1 = (\beta^2)^3 + (\beta^2) + 1.$$

Hence β^2 is a root of $x^3 + x + 1$, and a similar argument works for $\beta^4 = \sigma_4(\beta)$. Since $\beta^3 = -\beta - 1 = \beta + 1$, $\beta^4 = \beta^2 + \beta$. Thus $x^3 + x + 1$ has three distinct roots in $\mathbb{F}_2(\beta)$ and hence factors as

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

(iii) The polynomial $x^3 + x^2 + 1$ is irreducible as it has degree 3 and does not have a root in $\mathbb{F}_2$. Then there is a simple extension $\mathbb{F}_2(\gamma)$, where γ is a

root of x^3+x^2+1, and $[\mathbb{F}_2(\gamma):\mathbb{F}_2]=3$ and hence $\#(\mathbb{F}_2(\gamma))=2^3=8$. Since $\mathbb{F}_2(\gamma)$ and $\mathbb{F}_2(\beta)$ have the same number of elements, they are isomorphic. If $\varphi\colon \mathbb{F}_2(\gamma)\to\mathbb{F}_2(\beta)$ is an isomorphism, let $\delta=\varphi(\gamma)$. Then

$$0=\varphi(0)=\varphi(\gamma^3)+\varphi(\gamma^2)+\varphi(1)=\delta^3+\delta^2+1.$$

Thus δ is a root of x^3+x^2+1 in $\mathbb{F}_2(\beta)$.

Another way to think about this is as follows. If $\xi\in\mathbb{F}_2(\beta)$, then $[\mathbb{F}_2(\xi):\mathbb{F}_2]$ divides 3, hence is equal to 1 or 3. The case $[\mathbb{F}_2(\xi):\mathbb{F}_2]=1$ corresponds to the two elements of $\mathbb{F}_2$. The three roots of x^3+x+1, namely $\beta,\beta^2,\beta^2+\beta$, give 3 more elements of $\mathbb{F}_2(\beta)$. Since $\mathbb{F}_2(\beta)$ has 8 elements, there are three elements left over, and by the above each must be the root of some irreducible degree three polynomial not equal to x^3+x+1. Since there are only two irreducible polynomials in $\mathbb{F}_2[x]$ of degree 3, namely x^3+x+1 and x^3+x^2+1, the remaining three elements must all be roots of x^3+x^2+1.

Finally, we have seen that every element of $\mathbb{F}_2(\beta)$ is a root of x^8-x, and hence the irreducible polynomials x, $x+1$, x^3+x+1, and x^3+x^2+1 all divide x^8-x. Counting degrees, we see that

$$x^8-x=x(x+1)(x^3+x+1)(x^3+x^2+1).$$

(An alternative argument which works more generally is as follows: the polynomials on both sides of the above equality have the same set of roots, namely all elements of $\mathbb{F}_2(\beta)$, and it is easy to see that neither side has multiple roots. Hence, as both sides are monic, they are equal.)

3. (i) $\implies$ (ii): if I is a maximal ideal, then it is a prime ideal. Also, if R is not a field, then $\{0\}$ is not a maximal ideal (since $R/\{0\}\cong R$). Hence I is a nonzero prime ideal. (ii) $\implies$ (iii): we can write $I=(r)$ since R is a PID. Also, $r\neq 0$ since $I\neq\{0\}$ and $r\notin R^*$ since a prime ideal is not equal to R by definition. Suppose that $r=st$. Since $I=(r)$ is prime and $st=r\in(r)$, either $s\in(r)$ or $t\in(r)$, and after relabeling we can assume that $s\in R$, i.e. $s=ru$ for some $u\in R$. The $r=st=(tu)r$ and $r\neq 0$, so that $tu=1$. Hence t is a unit. It follows that r is irreducible. (iii) $\implies$ (i): Suppose that $I=(r)\subseteq J$. Since R is a PID, $J=(s)$ for some $s\in R$, hence $r=st$ is a multiple of s. Then either s is a unit and $J=R$, or t is a unit and hence $s=t^{-1}r$, so that $s\in I$, $J\subseteq I$ and hence $J=I$. Thus I is maximal (note that $I\neq R$ since by definition the irreducible r is not a unit).

4. (a) Follows from $N(1)\leq N(1\cdot r)=N(r)$. (b) By what we showed in class, either r is not a unit and $N(1)<N(1\cdot r)=N(r)$ or r is a unit and $N(1)=N(r)$. (c) If $r=st$ and s is not a unit, then $N(t)<N(st)=N(r)$.

By the assumption on r, $N(t) = N(1)$, and by (ii) t is a unit. Thus r is irreducible.