Assignment 6 – All 2 parts – Math 412

Due in class: Thursday, Oct. 10, 2019

Textbook exercises:[1]

Section 4.1: 10, 16(WI), 22

Section 4.2: 3

Section 4.3: 15

Other exercises:

(1) Let R be a commutative ring and let $f, g \in R[x]$.

(a) Show that $\deg(f+g) \leq \max(\deg(f), \deg(g))$.

(b) Show that if $\deg(f) \neq \deg(g)$, then $\deg(f+g) = \max(\deg(f), \deg(g))$.

(2) (a) Show that $1+2x$ is a unit in $(\mathbf{Z}/4\mathbf{Z})[x]$.

(b) Show that $1+10x$ is a unit in $(\mathbf{Z}/25\mathbf{Z})[x]$.

(c) Is $1+3x$ a unit in $(\mathbf{Z}/6\mathbf{Z})[x]$?

(3) Let F be a field. For $m \in \mathbf{R}$, define $m+\infty = \infty$ and $\infty+\infty = \infty$, and extend the usual ordering on $\mathbf{R}$ by setting $\infty \geq m$. A *valuation* on F is a function $v : F \to \mathbf{R} \cup \{\infty\}$ such that for all $a, b \in F$

(i) $v(a) = \infty$ if and only if $a = 0$,

(ii) $v(ab) = v(a) + v(b)$,

(iii) $v(a+b) \geq \min(v(a), v(b))$.

(a) (WI) Let $R = \{a \in F : v(a) \geq 0\}$. Show that R is a subring of F. It is called the *valuation ring of* v. (Hint: to show that $1 \in R$, consider $v(1 \cdot 1)$.)

(b) (WI) Show that $R^\times = \{a \in R : v(a) = 0\}$.

(c) Let p be a prime. For $\frac{a}{b} \in \mathbf{Q}$ (with $\gcd(a,b) = 1$), define $v_p(a/b) = e$ where $\frac{a}{b} = p^e \frac{a'}{b'}$ with $p \nmid a'$ and $p \nmid b'$ (and $e = \infty$ if $a/b = 0$). So, for instance,

$$v_3(3) = 1, \quad v_3(2/9) = -2, \quad \text{and} \quad v_3(10) = 0.$$

Show that v is a valuation on $\mathbf{Q}$ and that $\mathbf{Z}_{(p)}$ is its valuation ring (where $\mathbf{Z}_{(p)}$ is the ring defined in Question 1 of Assignment 4).

[1] From Hungerford's *Abstract algebra, An introduction, Third edition*

(4) Let F be a field.

(a) Let $f(x) \in F[x]$. Show that $f(x)$ is irreducible if and only if $cf(x)$ is irreducible for all $c \in F^\times$. (Remark: therefore when discussing general results on irreducibility, we may assume $f(x)$ is monic.)

(b) Let $f(x) = x^2 + bx + c \in F[x]$ be a (monic) quadratic polynomial. Show that $f(x)$ is reducible if and only if there exist $\alpha, \beta \in F$ such that

$$x^2 + bx + c = (x - \alpha)(x - \beta).$$

(c) For $f(x) = x^2 + bx + c$, let $\Delta = b^2 - 4c$. This is called the *discriminant of* $f(x)$. This part, and the next, lead you along a path to showing that when the characteristic of F is not 2

$$f(x) \text{ is reducible if and only if } \Delta \text{ is a square in } F.$$

So suppose $\mathrm{char}(F) \neq 2$ (so that we can divide by 2) and suppose $\Delta = \delta^2$ for some $\delta \in F$. Show that taking

$$\alpha = \frac{-b + \delta}{2} \quad \text{and} \quad \beta = \frac{-b - \delta}{2}$$

yields a factorization of $f(x)$ as in the previous part, so that $f(x)$ is reducible.

(d) Conversely, show that if $f(x) = (x - \alpha)(x - \beta)$, then $(\alpha - \beta)^2 = \Delta$. (Hint: show that $\alpha + \beta = -b$ and $\alpha\beta = c$, and use that $(x - y)^2 = (x + y)^2 - 4xy$.)

(5) Quadratic equations in characteristic 2. When $\mathrm{char}(F) \neq 2$, we can start with a quadratic polynomial $f(x) = x^2 + bx + c$ and make a linear change of variable $x' = x + \frac{b}{2}$ to get

$$\begin{aligned} x^2 + bx + c &= (x' - b/2)^2 + b(x' - b/2) + c \\ &= x'^2 - bx' + \frac{b^2}{4} + bx' - \frac{b^2}{2} + c \\ &= x'^2 - \frac{\Delta}{4}. \end{aligned}$$

The roots of this latter polynomial are $\pm\frac{\delta}{2}$ (if Δ has square root δ in F). Since $x = x' - \frac{b}{2}$, translating back in terms of x gives the usual quadratic formula we are used to

$$x = \frac{-b \pm \delta}{2}.$$

(And note that this gives another way of showing that $f(x)$ is reducible if and only if Δ is a square). Doing the change of variable above is called "completing the square". In characteristic 2, we cannot generally "complete the square" and put a polynomial into the form $x^2 - d$ since the change of variable involved has a 2 in the denominator (and in characteristic 2, $2 = 0$!!).

So, suppose $\mathrm{char}(F) = 2$ and that $f(x) = x^2 + bx + c \in F[x]$ is such that $b \neq 0$ (otherwise, we can immediately say that $f(x)$ is reducible if and only if c is a square in F). This exercise will develop a "quadratic formula in characteristic 2" for such $f(x)$. Note first that, since $b \neq 0$, $f(x)$ has roots α and β if and only if $b^{-2}f(x)$ has roots α and β.

(a) Take the change of variable $x' = b^{-1}x$ and let $\widetilde{f}(x') = b^{-2}f(bx')$. Show that

$$\widetilde{f}(x) = x^2 + x + D \text{ where } D = cb^{-2}.$$

(b) A polynomial of the form $x^2 + x + D$ in characteristic 2 is called an *Artin–Schreier polynomial*. The map $\wp : F \to F$ defined by

$$\wp(a) = a^2 + a$$

is called the *Artin–Schreier map*. Show that $\wp$ is *additive*, i.e. show that for all $a_1, a_2 \in F$

$$\wp(a_1 + a_2) = \wp(a_1) + \wp(a_2).$$

(c) Suppose that δ is a root of $x^2 + x + D$, i.e. $\delta \in F$ is such that $\wp(\delta) = D$. Show that the roots of $x^2 + x + D$ are δ and $\delta + 1$. (Hint: just show that if $\wp(\delta) = D$, then $\wp(\delta + 1) = D$, too.)

(d) The function $\wp$ is playing the role the squaring function usually plays. So prove the following: given $f(x) = x^2 + bx + c \in F[x]$ with $b \neq 0$, let $D = cb^{-2}$; then $f(x)$ is reducible if and only if there is a $\delta \in F$ such that $D = \wp(\delta)$, in which case the roots of $f(x)$ are

$$\alpha = b^{-1}\delta, \beta = b^{-1}(\delta + 1).$$