Math 103B, Winter 2018

Modern Algebra II, HW 8

Due Friday March 9th by 5PM in your TA's box

From Lauritzen's book:

- Exercises 4.10 (starting page 179): *8, 16, 17, 22, 23 (here* $p \nmid 10$*), 33*[1]

Problem A. Let p be a prime and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. The polynomial ring $\mathbb{F}_p[X]$ is a domain; consider its fraction field which is denoted by $\mathbb{F}_p(X)$.

(a) Explain why $\mathbb{F}_p(X)$ is an infinite field of characteristic p.

(b) Let $\varphi : \mathbb{F}_p(X) \to \mathbb{F}_p(X)$ be the Frobenius homomorphism ($r \mapsto r^p$). Why is φ injective? Show that φ is **not** surjective by verifying that the element X is not in its image. (`Hint`: Suppose $X = (\frac{f}{g})^p$ for some $f, g \in \mathbb{F}_p[X]$. Differentiate both sides of the relation $f^p = Xg^p$ and deduce that $g = 0$.)

Problem B. We define the **content** of a nonzero polynomial $f \in \mathbb{Z}[X]$ to be the GCD of all its coefficients. That is, if $f = a_0 + a_1X + \cdots + a_nX^n$ we let

$$\text{cont}(f) := \text{GCD}(a_0, a_1, \ldots, a_n) \in \mathbb{Z}_{>0}.$$

We say $f \in \mathbb{Z}[X]$ is **primitive** if $\text{cont}(f) = 1$ (in other words if its coefficients a_i have no common factor > 1).

(a) Let $f, g \in \mathbb{Z}[X]$ be primitive polynomials. Show that their product fg is primitive. (`Hint`: Otherwise choose a prime p dividing all coefficients of fg. Let a_r be the first coefficient of f which is not a multiple of p; and let b_s be the first coefficient of g which is not a multiple of p. The coefficient of X^{r+s} in fg is given by

$$\sum_{i+j=r+s} a_i b_j.$$

In this sum the term $a_r b_s$ is not a multiple of p, but all other terms *are* divisible by p since either $i < r$ or $j < s$. This leads to a contradiction.)

[1] `Hint`: Try something of the form $\mathbb{F}_2[X]/(X^3 + aX^2 + bX + c)$ for suitable $a, b, c \in \mathbb{F}_2$.

(b) Now let $f, g \in \mathbb{Z}[X]$ be arbitrary nonzero polynomials. Use the special case in (a) to show that more generally

$$\boxed{\mathrm{cont}(fg) = \mathrm{cont}(f)\mathrm{cont}(g)} \tag{1}$$

(`Hint`: Note that $\mathrm{cont}(f)^{-1}f$ is primitive.)

(c) We extend the definition of content to $\mathbb{Q}[X]$ as follows. For a nonzero $f \in \mathbb{Q}[X]$ choose an $N \in \mathbb{Z}_{>0}$ such that $Nf \in \mathbb{Z}[X]$ and let

$$\mathrm{cont}(f) := N^{-1}\mathrm{cont}(Nf) \in \mathbb{Q}_{>0}.$$

Check that this is well-defined (that is independent of the choice of N) and that the relation (1) in (b) continues to hold for $f, g \in \mathbb{Q}[X]$.

(d) Observe that if $f \in \mathbb{Q}[X]$ is <u>monic</u> its content is of the form $\frac{1}{c}$ for some $c \in \mathbb{Z}_{>0}$. (`Hint`: N is the leading coefficient of Nf and therefore a multiple $c \cdot \mathrm{cont}(Nf)$.) Moreover, if $\mathrm{cont}(f) = 1$ then $f \in \mathbb{Z}[X]$.

(e) (A very useful application!) Suppose the polynomial $h \in \mathbb{Z}[X]$ factors as $h = fg$ with $f, g \in \mathbb{Q}[X]$ both <u>monic</u>. Then necessarily $f, g \in \mathbb{Z}[X]$. (`Hint`: Observe that h is monic too and has integer coefficients; therefore it has content $1 = \mathrm{cont}(f)\mathrm{cont}(g) = \frac{1}{c} \cdot \frac{1}{d}$ by (c) and (d). We conclude that $c = d = 1$.)

The equation (1) for $\mathbb{Q}[X]$ is known as the *Gauss Lemma*. If you're interested you can try to mimic the above arguments with $\mathbb{Z}$ replaced by a UFD R (this is <u>not</u> required for full credit).