MATH 357 hw 1

Patrick Y

March 19, 2021

0.1 Table.

See the attached image for the completed table.

0.2 Goodman 6.6.1

The proof of (a) is by contraposition. Suppose $d \neq \gcd(a_1...a_s)$. If d does not divide one of the a_j's ($0 \leq j \leq s$) the result holds trivially. Suppose that d divides each of the a_j's. Since $d \neq \gcd(a_1...a_s)$, there is an element $x \neq d$ which divides each $a_1...a_s$ and $d|x$. Then $bd|ba_j$ and $bx|ba_j$ for each j. But clearly, $bd|bx$, since $d|x$. Since $bd \neq bx$, we conclude that $bd \neq \gcd(ba_1, ...ba_s)$ as desired.

For the proof of part (b), suppose $f(x) = bf_1(x)$, where f_1 is primitive. Put

$$f_1 = a_s x^s + ... + a_1 x + a_0$$

where $\gcd(a_1...a_s) = 1$. By the distributive property,

$$f = bf = ba_s x^s + ... + ba_1 x + ba_0$$

By part (a), $b = b \cdot 1 = \gcd(ba_1...ba_s)$, which are precisely the coefficients of f, and we are done.

0.3 Goodman 6.6.2

Let $C_{\alpha_1...\alpha_n}$ be the coefficient of $x^{\alpha_1}...x^{\alpha_n}$ in $R[x_1, ...x_n]$. Let $\varphi : R[x_1, ...x_n] \to R[x_1, x_{n-1}][x_n]$ be given by

$$\varphi\left(\sum_{(\alpha_1,...\alpha_n)\in\mathbb{N}} C_{\alpha_1...\alpha_n} x_1^{\alpha_1}...x_n^{\alpha_n}\right) = \sum_{j\in\mathbb{N}}\left(\sum_{\alpha_1,...\alpha_{n-1}} C_{\alpha_1...\alpha_n} x_1^{\alpha_1}...x_{n-1}^{\alpha_{n-1}}\right) x_n^{\alpha_j} \tag{1}$$

By the distributive property, φ is the identity map, and hence a ring isomorphism. The proof of part (2) is by induction. The base case $n = 1$ is trivial by a previous theorem. Then suppose the result holds for a nonnegative intreger n. Then

$$R[x_1, ...x_n]$$

is a UFD. By part (a), we have

$$R[x_1...x_{n+1}] \cong R[x_1, ...x_n][x_{n+1}] \tag{2}$$

which is a UFD by Theorem 6.6.7.

0.4 Goodman 6.6.3

Suppose $a_n x^n ... a_1 x + a_0 \in \mathbb{Z}[x]$ has a rational root r/s. Write $f = ef_1(x)$, where $e = \gcd(a_n...a_1, a_0)$. Of course, f_1 is primitive. Clearly, the roots of f_1 are the same as the roots of f, since multiplication by a constant does not change roots of polynomials in $\mathbb{Z}[x]$. Then r/s is a root of f_1, so $(x - r/s)$ is a factor of f_1. Again multiplying by the constant s, we can rewrite $(x - r/s) \to (sx - r)$, which is primitive since s, r are relatively prime. Since f_1 is a primitive multiple of $(sx - r)$, s must divide the leading term and r must divide the constant term, as desired.

0.5 Goodman 6.6.5

In this exercise, we give an alternate proof of Guass's lemma using a prescribed outline. Let R be a UFD. For any irreducible (prime) $p \in R$, let $\pi_p : R \to R/pR$ be the quotient map. Of course, π_p is a ring homomorphism. By Corollary 6.2.9, we can extend π_p to a ring homomorphism $\tilde{\pi_p} : R[x] \to (R/pR)[x]$ given by

$$\tilde{\pi_p}\left(\sum a_i x^i\right) = \sum \pi_p(a_i) x^i$$

Claim. First, we are asked to show that $h(x) \in \ker(\tilde{\pi_p})$ if and only if p divides all the coefficients of h. Suppose $h(x) \in \ker(\tilde{\pi_p})$. Then $\tilde{\pi_p}(h(x)) = \tilde{\pi_p}(a_i x^i + ... + a_0) = \tilde{\pi_p}(a_i)x^i + ... + \tilde{\pi_p}(a_0) = 0 + 0 + ... + 0$, so the quotient map $R \mapsto R/pR$ takes each a_i to 0. This implies that p divides each a_i, as desired. (In particular, $\ker \tilde{\pi_p}$ is the principle ideal generated by p). The reverse direction is straightforward – if p

divides each a_i, then the quotient map $R \mapsto r/pR$ again takes each a_i to 0, so $\tilde{\pi_p}(h) = \sum 0 = 0$, and we are done.

Claim. Next, we are asked to show that $f(x) \in R[x]$ is primitive if and only if for every irreducible p, we have $\tilde{\pi_p}(f(x))$ is nonzero. For the proof of the forwards direction, suppose $f = a_i x^i$ is primitive. Since $\gcd(a_i...a_0) = 1$, p does not divide some $a_k, 0 \leq k \leq i$. Then by the previous claim, the quotient map $R \mapsto R/sR$ does not take a_k to 0. Then $\tilde{\pi_p}(f)$ is nonzero, since it has a nonzero coefficient $\pi_p(a_k)$. Next, we prove the reverse direction. Let p be irreducible, and suppose $\tilde{\pi_p}(f(x))$ is nonzero. By the previous claim, p does not divide all the coefficients $a_i...a_0$ of $f(x)$. Since p was arbitrary, there is no irreducible p which divides each $a_i...a_0$. Now, since R is a UFD, we can write each a_k as the unique product of irreducibles

$$a_k = p_k^1, p_k^2 ... \quad : 0 \leq k \leq i$$

where no p_k^j divides every coefficient $a_i...a_0$. We conclude that $\gcd(a_i...a_0) = 1$, as desired.

Claim. The third statement we are asked to show is straightforward. Let p be irreducible. Suppose $\tilde{\pi_p}(f), \tilde{\pi_p}(g) \in (R/pR)[x]$ are nonzero. By the previous claim, f, g are primitive, and hence nonzero. Then of course fg is nonzero, since it has at least one nonzero coefficient. By corollary 6.2.9, the projection map $\tilde{\pi_p} : R[x] \to (R/pR)[x]$ is a ring homomorphism, hence it takes nonzero elements into nonzero elements. This implies that $\tilde{\pi_p}(f) \cdot \tilde{\pi_p}(g)$ is nonzero, as desired.

To conclude the proof of Gauss's lemma, suppose $f, g \in R[x]$ are primitive. By part (b), $\tilde{\pi_p}(f), \tilde{\pi_p}(g)$ are nonzero. By part (c), the product $\tilde{\pi_p}(f) \cdot \tilde{\pi_p}(g) = \tilde{\pi_p}(f \cdot g)$ is nonzero. Appealing to part (b) again, we conclude that $f \cdot g$ is primitive, as desired.