Math 504 HW7

Rohan Mukherjee

December 31, 2023

1. We begin by proving the following lemma:

   Lemma 1. *Let p be a prime element of a UFD A. Then*

   $$(p) = \left\{ \begin{array}{c} \textit{Polynomials with coefficients in } A \\ \textit{divisible by } p \end{array} \right\}$$

   is a prime ideal of $A[x]$.

   Proof. Let $f(x) = a_0 + a_1 x + \cdots a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ with $fg \in (p)$. Obviously $p \mid a_n b_m$, so WLOG $p \mid a_n$. Then,

   $$fg = (a_0 + \cdots + a_n x^n)(b_0 + b_1 x + \cdots + b_m x^m) = (a_0 + \cdots a_{n-1}x^{n-1})g + a_n x^n g$$

   Clearly showing that $(a_0 + \cdots a_{n-1}x^{n-1})g \in (p)$. Now repeat the procedure: if $p \mid a_{n-1}$, we can run the above again, and eventually either all the a_i's are divisible by p or there is a k such that a_k is not divisible by p, and $(a_0 + \cdots + a_k x^k)g \in (p)$. In this case, we have $p \mid a_k b_m$ but $p \nmid a_k$, so $p \mid b_m$. Using the above argument again, we can get $(a_0 + \cdots + a_k x^k)(b_0 + \cdots + b_{m-1}x^{m-1}) \in (p)$, which shows $p \mid a_k b_{m-1}$ which forces $p \mid b_{m-1}$. Continuing this process *ad infinitum* shows that $p \mid b_i$ for every i, i.e. that $g \in (p)$, which completes the proof. □

   Sketch of second proof. A simple exercise shows that if $A \subset R$ is an ideal, then $R[x]/A[x] \cong (R/A)[x]$. Also, if S is an integral domain, then $S[x]$ is too (one could see this by looking at just the leading coefficient). So, if p is prime in R, then (p) is a prime ideal of R, so $R[x]/(p)[x] \cong (R/(p))[x]$ which is clearly an integral domain, completing the sketch. □

Let p be a prime dividing the gcd of the coefficients of fg and m be the max power of p appearing in the gcd of the coefficients. Then $fg \in (p^n)$ and in particular $fg \in (p)$, which by the lemma shows that (WLOG) $f \in (p)$. Then $\frac{f}{p} \in A[x]$, and,

$$\frac{f}{p}g \in (p^{n-1}) \subset (p)$$

Then $\frac{f}{p} \in (p)$ or $g \in (p)$. Repeating this process will yield a $k \in \mathbb{N}$ such that $\frac{f}{p^k} \in A[x]$ and $\frac{g}{p^{n-k}} \in A[x]$, which shows that $p^k \mid c(f)$ and $p^{n-k} \mid c(g)$, so $p^n \mid c(fg)$. Now, since $c(f)c(g) \mid a_i b_{n-i}$ for every i, we have $c(f)c(g) \mid c(fg)$. Since the above holds for every prime p dividing $c(fg)$, we have $c(fg) \mid c(f)c(g)$, so $c(fg) = c(f)c(g)$, which completes the proof.

2. Suppose that $f \in A[x]$ is reducible in $K[x]$ and write $f = gh$ for $g(x) = \frac{c_0}{a_0} + \cdots + \frac{c_n}{a_n}x^n$ and $h(x) = \frac{d_0}{b_0} + \cdots + \frac{d_m}{b_m}x^m \in K[x]$, and assume that $c(f) = 1$. Then,

$$\prod a_i b_i f = \prod a_i g \cdot \prod b_i h$$

Now, $\prod a_i g, \prod b_i h \in A[x]$, so, since $\gcd(da, db) = d\gcd(a, b)$, we have that $\prod a_i b_i = \prod a_i b_i c(f) = c(\prod a_i b_i f) = c(\prod a_i g)c(\prod b_i h)$. Now let p be a prime divisor and α its maximal power in the prime decomposition of $\prod a_i b_i$. Then $p \mid c(\prod a_i g)c(\prod b_i h)$ so $p \mid c(\prod a_i g)$ or $p \mid c(\prod b_i h)$, WLOG suppose its the first case. Repeat this process inductively until we find k such that $c(\prod a_i g)/p^k \in A$ and $c(\prod b_i h)/p^{\alpha-k} \in A$. Then we see that $\prod a_i b_i/p^{\alpha} \cdot f = g/p^k \cdot h/p^{\alpha-k}$ where $g/p^k \in A[x]$ and $h/p^{\alpha-k} \in A[x]$. Since this holds for every prime divisor of $\prod a_i b_i$, we can repeat this to eventually get $f = kl$ for $k, l \in A[x]$, which shows that f is reducible in $A[x]$.

3. We shall first prove that all polynomials with content 1 can be factored as a product of irreducibles, and we shall do so by strong induction on the degree. Let $f(x) = ax + b$ be a degree 1 polynomial with $a \neq 0$ and content 1. If $f(x) = g(x)h(x)$, then WLOG $\deg g(x) = 1$ and $\deg h(x) = 0$ by some simple casework. Now, by the above we have that $1 = c(f) = c(g) \cdot c(h) = c(g) \cdot h$, so h is a unit and f is irreducible. Suppose that all polynomials with degree $\leq n$ can be factored as a product of irreducibles for some $n > 1$, and let $f(x)$ be degree $n + 1$ with content 1. If $f(x)$ is irreducible we are done, otherwise we have $f(x) = g(x)h(x)$ where neither g nor h are units. Re-using the above if g or h had degree 0 then they would be units a contradiction, so each has degree ≥ 1 and $\deg g, \deg h \leq n$. Then g, h can be factored as a product of irreducibles and henceforth f can do. Now, if f is any polynomial in $A[x]$, then write $f = c(f)g$ for some g with content 1. Now, since A is a UFD $c(f)$ can be written as a product of irreducibles in A, which are

also irreducible in $A[x]$ by degree considerations, and g can be written as a product of irreducibles by the above so f can too.

Now, suppose that f has the following factorizations:

$$f = wp_1^{\alpha_1} \cdots p_n^{\alpha_n} = vq_1^{\beta_1} \cdots q_m^{\beta_m}$$

where w, v are units and the rest are irreducibles. Notice that these are also factorizations of f into a product of irreducibles in the UFD $\mathrm{Frac}(A)[x]$ by the previous lemma. Thus, $m = n$ and there is a bijection $\varphi : \{ p_1, \ldots, p_n \} \to \{ q_1, \ldots, q_n \}$ such that $\varphi(p_i)$ is an associate of q_j. Now, suppose that $p(x) = \frac{r}{s}q(x)$ where $\frac{r}{s}$ is a unit in $\mathrm{Frac}(A)$. Then $sp(x) = rq(x)$, so $sc(p) = rc(q)$ meaning $\frac{s}{r} = c(p)^{-1}c(q) \in A$ since $c(p)$ is a unit, showing that $\frac{r}{s}$ is a unit in A and so p is an associate of q in $A[x]$, verifying uniqueness on polynomials with content 1. In the more general case, we can write $f = c(f) \cdot g$ for a polynomial of content 1 g. This decomposition is clearly unique up to units (since $c(f)$ is unique up to a unit). Now, g can be written uniquely as the product of irreducibles, and $c(f)$ can too since A is a UFD. Also, given any factorization of f as $w \cdot p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ where p_i are not necessarily content-1, we can just factor out the content from each and collect it towards the front yielding a decomposition of the above form, which is unique.

4. We start by proving the following lemma:

Lemma 2. *Let R be an integral domain and $n \geq 1$. Then the only divisors of cx^n for $0 \neq a \in R$ in $R[x]$ are dx^k for $0 \leq k \leq n$ and $d \mid c$.*

Proof. Let $f(x) = a_k x^k + \cdots + a_0$ be a divisor of cx^n. Then there is a $g(x) = b_{n-k}x^{n-k} + \cdots + b_0$ such that $f(x)g(x) = x^n$ since $\deg g = n - \deg f = n - k$. Now, $f(x)g(x) = a_k b_{n-k} x^n + \cdots + a_0 b_0$. In particular, $a_k b_{n-k} = c$, so $a_k \mid c$. Now, suppose that there was an $i < k$ so that $a_i \neq 0$, and then find the minimum such j. Simultaneously find the minimum l such that $b_l \neq 0$ (this could be b_{n-k}). Then the term with the smallest power in $f(x)g(x)$ is $a_j b_l x^{j+l}$. Since $j < k$ and $l \leq n - k$ we have $j + l < n$, which shows that this product has a term other than cx^n, a contradiction. Thus $f(x) = a_k x^k$ for $a_k \mid c$. It is obvious to see that this is indeed a divisor, so we are done. $\square$

Now let bars denote passage to $A/(p)[x]$ (i.e., reducing the coefficients mod (p)). Suppose that f has content 1. We shall show that f is irreducible in $A[x]$. Indeed, let $f(x) = g(x)h(x)$ where neither $g(x)$ nor $h(x)$ are units. By the same content considerations as above, this shows that neither $g(x)$ nor $h(x)$ are constant, otherwise they would be units. By the lemma $\bar{g}(x)$ and $\bar{h}(x)$ are of the form dx^k for some k. In particular, the constant term of both $g(x)$ and $h(x)$ is divisible by p. But then the product of their constant terms would be divisible by p^2, a contradiction, which shows that f is irreducible in $A[x]$. In the more general case, write $f(x) = c(f)g(x)$ for a content-1 polynomial $g(x)$. $g(x)$ is now irreducible in $K[x]$ and $c(f)$, being in A, is a unit in K and therefore $K[x]$, so $f(x)$ is an associate of a irreducible and hence itself irreducible, which completes the proof.

5. Let $f(x) = x^{p-1} + \cdots + x + 1$, and notice that $f(x)(x-1) = x^p - 1$. Thus, $f(x+1)x = (x+1)^p - 1$, and,

$$f(x+1) = \frac{(x+1)^p - 1}{x} = \sum_{k=1}^{p} \binom{p}{k} x^{k-1} = \sum_{k=0}^{p-1} \binom{p}{k+1} x^k$$

Notice that the constant term is $\binom{p}{1} = p$, and the leading coefficient is $\binom{p}{p} = 1$. For $1 \leq k \leq p-1$, $\binom{p}{k}$ is divisible by p since,

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdots (p-k+1)}{k \cdot (k-1) \cdots 1}$$

And no term on the bottom can cancel the p on the top since p is a prime greater than k, meaning its only divisors are p and 1 so to cancel it p would have to appear on the bottom. We are now in the case to apply Eisenstein: p^2 does not divide the constant term, p does not divide the leading coefficient, and p divides every other coefficient, so $f(x+1)$ is irreducible. If $f(x) = g(x)h(x)$ where neither g nor h are constants, then $f(x+1) = g(x+1)h(x+1)$, where neither $g(x+1)$ nor $h(x+1)$ are constant, a contradiction. So $f(x)$ is irreducible too, and we are done.