ON FACTORIALITY AND IRREDUCIBILITY, *505,* WINTER 2021

DUE TUESDAY, JANUARY 12

1. Gauss's Lemma and consequences

Throughout A is a unique factorization domain. Recall that a UFD is an integral domain such that all elements are uniquely (up to order and associates) written as a product of irreducible elements, where a and b are associates if $a = ub$ for some unit u. Note also that in UFD, prime $\iff$ irreducible — recalling that an element p being prime means that (p) is a prime ideal, i.e. that $p \mid ab \implies p \mid a$ or $p \mid b$; and an element q being irreducible means that if $q = ab$ for some ab, then one of a, b must be a unit (and p, q must be non-zero and non-unit).

Definition 1. Let $f(x) \in A[x]$. The content of f, denoted $c(f)$, is the GCD of the coefficients of f.

One may ask what is a GCD? Although this should be intuitively clear, let's define it more formally. Let $a \in A$. For any $p \in A$, an irreducible element, we can define $\mathrm{ord}_p(a) \in \mathbb{Z}_{\geq 0}$, which is the power of p in the prime decomposition of a. This is well defined since A is a unique factorization domain. Now for $a, b \in A$ define

$$\mathrm{GCD}(a, b) = \prod_p p^{\min(\mathrm{ord}_p a, \mathrm{ord}_p b)},$$

and similarly for several elements of A. This is well-defined UP TO multiplication by a unit, and, hence, the GCD is formally speaking an equivalence class, where two elements are equivalent if they differ by a unit. In particular, being relatively prime means that the GCD is a unit. Also, $[n]$ denotes $\{1, \ldots, n\}$.

The following fact is called **GAUSS'S LEMMA**.

Theorem 2. *Let A be a unique factorization domain, and let $f, g \in A[x]$. Then* $\boxed{c(fg) = c(f)c(g)}$.

Proof. It's clear from the definition of GCD that $\mathrm{GCD}(x_1, \ldots, x_n)$ divides $x_1, \ldots, x_n$, because for any $i \in [n]$, $x_i = \mathrm{GCD}(x_1, \ldots, x_n) \cdot \prod_p p^{\mathrm{ord}_p(x_i) - \min\{\mathrm{ord}_p(x_1), \ldots, \mathrm{ord}_p(x_n)\}}$ where the product (let's call it y_i) is indeed an element of A because the exponents are all ≥ 0. Also, there is no non-zero, non-unit a that divides all the y_i (as one should expect, from the "greatest" in GCD), since then that would mean that there would be some p s.t. for all $i \in [n]$, $\mathrm{ord}_p(x_i) - \min\{\mathrm{ord}_p(x_1), \ldots, \mathrm{ord}_p(x_n)\} \geq 1$, which is impossible. In other words, $\mathrm{GCD}(y_1, \ldots, y_n)$ is a unit (or to be more precise since we are thinking of the GCD as an equivalence class, it is the set of all units).

That's all so we can see that there's some $\tilde{f}, \tilde{g} \in A[x]$ s.t. $c(\tilde{f}), c(\tilde{g})$ are units (more precisely they are the set of units), and $f \in c(f)\tilde{f}$ and $g \in c(g)\tilde{g}$ (i.e. $f = \gamma_f \tilde{f}$ and $g = \gamma_g \tilde{g}$, for some $\gamma_f \in c(f)$ and $\gamma_g \in c(g)$). Multiplying, we get that $fg = \gamma_f \gamma_g \tilde{f}\tilde{g}$, implying that $c(fg) = c(\gamma_f \gamma_g \tilde{f}\tilde{g}) = \gamma_f \gamma_g c(\tilde{f}\tilde{g}) = c(f)c(g)c(\tilde{f}\tilde{g})$. So we just need $c(\tilde{f}\tilde{g})$ to be the set of units (given that we know $c(\tilde{f}), c(\tilde{g})$ are units). That is, we want to prove that if $p \nmid \tilde{f}$ and $p \nmid \tilde{g}$ (i.e. that there is some coefficient of $\tilde{f}$ and some coefficient of $\tilde{g}$ not divisible by a prime/irreducible p), then $p \nmid \tilde{f}\tilde{g}$. Note that this is equivalent to showing $p \mid \tilde{f}\tilde{g} \implies p \mid \tilde{f}$ or $p \mid \tilde{g}$, or in other words showing that p (which is prime in A) is also prime in $A[x]$.

We proceed by contradiction: suppose we have $f = a_n x^n + \ldots + a_0$ and $g = b^m x^m + \ldots + b_0$ in $A[x]$ and a prime $p \in A$ s.t. $p \nmid f, g$ but $p \mid fg$. Because $p \nmid f, g$, there must be some minimal $I \in [n]$ and $J \in [m]$ s.t. $p \nmid a_I, b_J$. Now consider the coefficient of x^{I+J} in fg:

$$c_{I+J} = \sum_{k=0}^{I+J} a_k b_{(I+J)-k} = a_0 b_{I+J} + \ldots + a_{I-1} b_{J+1} + a_I b_J + a_{I+1} b_{J-1} + \ldots + a_{I+J} b_0$$

(considering coefficients with index-out-of-bounds to be 0). Rearranging, we get

$$a_I b_J = c_{I+J} - (a_0 b_{I+J} + \ldots + a_{I-1} b_{J+1}) - (a_{I+1} b_{J-1} + \ldots + a_{I+J} b_0).$$

This shows that $a_I b_J$ is divisible by p because we know from $p \mid fg$ that $p \mid c_{I+J}$, and by minimality of $I \in [n]$ and $J \in [m]$, the 2nd and 3rd terms respectively must also be divisible by p. But by primality of $p \in A$, $p \mid a_I b_J \implies p \mid a_I$ or $p \mid b_J$, a contradiction. □

Remark 3. To avoid dealing with equivalence classes, this can be stated as

$$\mathrm{ord}_p(f) + \mathrm{ord}_p(g) = \mathrm{ord}_p(fg)$$

for any $f, g \in A[x]$ and any irreducible element $p \in A$.

Proof. Perhaps it'd be wise to define explicitly what we mean by $\mathrm{ord}_p(f)$; of course, we would like to be like the original, i.e. "the power of p in the prime decomposition of f", but since we do not yet know that such a prime decomposition is unique in $A[x]$, we must make do with the following: let $\mathrm{ord}_p(f)$ be the power of p in $c(f)$, or more explicitly the minimum of the ord_p for all the coefficients of f. Following this definition, we have that $c(f) = \prod_p p^{\mathrm{ord}_p(f)}$ (up to units), and hence:

$$\begin{aligned} c(f)c(g) = c(fg) &\iff \prod_p p^{\mathrm{ord}_p(f)} \cdot \prod_p p^{\mathrm{ord}_p(g)} = \prod_p p^{\mathrm{ord}_p(fg)} \text{ (up to units)} \\ &\iff \mathrm{ord}_p(f) + \mathrm{ord}_p(g) = \mathrm{ord}_p(fg) \text{ for all } p \end{aligned}$$

□

Lemma 4. *Let $f(x) \in A[x]$, and let $K = \mathrm{Frac}(A)$. If f is non-constant and irreducible in $A[x]$, then f is irreducible in $K[x]$.*

Proof. Suppose on the contrary that f is irreducible in $A[x]$, but that f is reducible in $K[x]$, say $f = gh$ for $g, h \in K[x]$ (both non-constant). Let β be the product of all the denominators of the coefficients of g; this makes it so that $\beta f \in A[x]$. Then, we pull out all the common factors of βg in front: we have some $\alpha \in c(\beta g)$ and $\tilde{g}$ satisfying $c(\tilde{g}) = \mathbf{1}$ (where $\mathbf{1}$ denotes the set of units) s.t. $\beta g = \alpha \tilde{g}$. We can do the same for h, yielding $\delta h = \gamma \tilde{h}$ where $c(\tilde{h}) = \mathbf{1}$.

Multiplying, we get that $\beta\delta f = \beta\delta gh = \alpha\gamma\tilde{g}\tilde{h}$. Thus, $c(\beta\delta f) = c(\alpha\gamma\tilde{g}\tilde{h})$, and applying Theorem 2, we get that $c(\beta)c(\delta) = c(\alpha)c(\gamma)$ (where $c(f) = \mathbf{1}$ due to f being irreducible). But for any $a \in A$, $c(a)$ is just a (up to units), so we have that $\beta\delta = u\alpha\gamma$, where u is some unit. This yields $u\alpha\gamma f = \alpha\gamma\tilde{g}\tilde{h}$, and cancelling (which we can do because A is in particular an integral domain) and multiplying by u^{-1}, we get that $f = u^{-1}\tilde{g}\tilde{h}$. But $\deg(\tilde{g}) = \deg(g) > 0$ and similarly for $\deg(\tilde{h})$, because g, h are non-constant. And so we find that f is in fact reducible — contradiction. □

Does the converse (i.e. that f reducible in $A[x]$ implies that f reducible in $K[x]$) hold? Obviously, since $A[x] \subseteq K[x]$.

Theorem 5. *Let A be a unique factorization domain. Then $A[x]$ is a unique factorization domain.*

Proof. Part 1: Existence. Given some $f \in A[x]$ (non-zero and non-unit), we know we can write it as $f = \alpha\tilde{f}$ where $\alpha \in c(f)$ and $c(\tilde{f}) = \mathbf{1}$. The α is some element of A, and so because A is a UFD, it can be factored into irreducibles (or it is a unit). If $\tilde{f}$ is reducible, then we can find non-unit $g, h \in A[x]$ s.t. $f = gh$. Because $c(f) = \mathbf{1}$, $c(g)$ and $c(h)$ both have to be $\mathbf{1}$ as well (if some irreducible $p \in A$ divides g, it would obviously divide f as well); this furthermore gives that g, h can not be constant, since g, h are non-zero and non-unit as well as not divisible by any irreducible $p \in A$, implying that $0 < \deg(g), \deg(h) < \deg(f)$.

Thus we see that given any reducible $\tilde{f}$ s.t. $c(\tilde{f}) = \mathbf{1}$, we can factor it into g, h with $c(g), c(h) = \mathbf{1}$ with strictly less (but still positive) degree. The "strictly less but still positive degree" part tells us that if we run this process over and over, it finishes in finitely many steps, yielding $\tilde{f}$ as a product of irreducible non-constant polynomials.

PART 2: UNIQUENESS. With PART 1 in place, let's now say we have f factored as $\alpha_1 \cdots \alpha_k \cdot g_1 \cdots g_m$ and also $\beta_1 \cdots \beta_\ell \cdot h_1 \cdots h_n$, where all the α's and β's are irreducible (or units) in A and all the g's and h's are irreducible non-constant polynomials in $A[x]$ (with content **1**). Like we did in the second paragraph of the proof of Lemma 4, we can apply $c(\cdot)$ to both sides and use Theorem 2 to get that $\alpha_1 \cdots \alpha_k = u\beta_1 \cdots \beta_\ell$ (where u is some unit), and furthermore that $g_1 \cdots g_m = u^{-1} h_1 \cdots h_n$.

Because A is a UFD, and the α_i, β_i are all in A, it must be that $k = \ell$ and the α_i and β_i are the same up to re-ordering and units.

Now to show that $m = n$ and the g_i are the h_i up to re-ordering and units: we have that $ug_1 \cdots g_m = h_1 \cdots h_n$. Thus in particular, we have that $g_1 \mid h_1 \cdots h_n$, so by the definition of prime, we can say that $g_1 \mid h_1$ (h_1 chosen w.l.o.g., since we can just rename/reorder the indices). But because h_1 is also irreducible, it must be that g_1 is either a unit or a unit times h_1, and g_1 can't be a unit because it's irreducible. Thus, we now have that $g_1 = u_1 h_1$ for some unit u_1. Plugging in and cancelling (which we can do because $A[x]$ is an integral domain), we get that $uu_1 g_2 \cdots g_m = h_2 \cdots h_n$. We iterate this process (yielding $g_1 = u_1 h_1, g_2 = u_2 h_2, \ldots$) until we run out of g_i or h_i; if w.l.o.g. we assume that $n > m$, then we get that $h_{m+1} \cdots h_n$ is equal to a product of units, which is impossible since the h_i are irreducible and hence non-units. Thus, we must run out of g_i and h_i at the same time, i.e. $n = m$, and we are done (since we already said above that this process yields $g_1 = u_1 h_1, g_2 = u_2 h_2, \ldots$. □

Corollary 6. *Let K be a field. Then $K[x_1, \ldots, x_n]$ is a unique factorization domain.*

Note that when $n > 1$, $K[x_1, \ldots, x_n]$ is NOT a principal ideal domain.

2. Eisenstein criterion

Prove the following criterion of irreducibility for polynomials:

Theorem 7. *Let A be a UFD, and let $K = \operatorname{Frac} A$. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 \in A[x]$. If there exists an irreducible element $p \in A$ such that*

1. *p divides a_i for all $0 \le i \le n-1$*
2. *p does not divide a_n*
3. *p^2 does not divide a_0*

then $f(x)$ is irreducible in $K[x]$ (and hence in $A[x]$ too by the converse of Lemma 4).

Proof. Suppose on the contrary that there is some f that satisfies these conditions, but is reducible in $K[x]$. Then, by Lemma 4, f must be reducible in $A[x]$, say $f = (b_m x^m + \ldots + b_0)(c_k x^k + \ldots + c_0)$. Then, for any $i \in \{0, \ldots, n\}$, $a_i = \sum_{\iota=0}^{i} b_\iota c_{i-\iota} = b_0 c_i + \ldots + b_i c_0$ (considering coefficients with index-out-of-bounds to be 0). Rearranging, we get that

$$b_i c_0 = a_i - (b_0 c_i + \ldots + b_{i-1} c_1).$$

If we somehow manage to get (for some index I) that the RHS is divisible by some prime p (say because $a_i, b_0, \ldots, b_{i-1}$ are all divisible by p), but the LHS is not, we get a contradiction and hence f would have to be irreducible. Indeed, the three conditions guarantee exactly this possibility:

First, (3) and $p \mid a_0$ (part of (1)) guarantee (w.l.o.g.) that p divides b_0 but not c_0 (since $a_0 = b_0 c_0$). Letting I be the minimal index s.t. $p \nmid b_I$, (2) gives that I indeed exists and is $\le m$ (ensuring that I is a valid index for the b_i), because $p \nmid a_n \implies p \nmid b_m$ and $p \nmid c_k$ (since $a_n = b_m c_k$). The minimality of I, and the fact that $I \le m < n \implies p \mid a_I$ (by (1)) prove that p indeed divides every term on the RHS, and since we already said that $p \nmid c_0$, we know also that the LHS is not divisible by p. This is our predicted contradiction, and we are done. □

Corollary 8. *For a prime number p, the polynomial $f = x^{p-1} + x^{p-2} + \ldots + x + 1$ is irreducible over $\mathbb{Z}$.*

Proof. First, note that $f(x)(x-1) = x^p - 1$. Substituting $x+1$ in place of x, we get that $xf(x+1) = (x+1)^p - 1$. Using the binomial theorem, we can expand the RHS to be $x^p + \binom{p}{p-1}x^{p-1} + \ldots + \binom{p}{1}x$, which means that $f(x+1)$ must be exactly

$$f(x+1) = x^p + \binom{p}{p-1}x^{p-1} + \ldots + \binom{p}{1}x.$$

Since $\binom{p}{k} = \frac{p!}{k!(p-k)!}$, we see that for any $k \in \{1, \ldots, p-1\}$, the numerator has one factor of p while the denominator has none (all the numbers are smaller than p, so no factor of p can be found in the prime factorization of the denominator). Furthermore, the constant coefficient, $\binom{p}{1}$, is just equal to p, and so Eisenstein's criterion are met, telling us that $f(x+1)$ is irreducible. Thus, $f(x)$ must be irreducible as well, since if it were instead reducible, then $f(x+1)$ would be reducible as well (since $f(x) = g(x)h(x) \implies f(x+1) = g(x+1)h(x+1)$). $\square$