Algebraic Theory I

Thomas Fleming

December 5, 2021

Contents

Lecture 40: Polynomials (6)

Wed 01 Dec 2021 12:33

This was the last class.

Recall. If R was a UFD with K its quotient field, then a polynomial $f \in K[x]$ has a linear factor if and only if it has a root. Moreover, if $\deg(f) \leq 3$, then f has a linear factor if and only if it is irreducible (and has $\mathrm{Cont}(f) = 1$).

Theorem 0.1 (Eisenstein's Criterion)**.** Suppose R is a UFD with quotient field K and $f(x) = \prod_{i=0}^{n} a_i x^i \in R[x]$ with $n = \deg(f) \geq 1$ and $\mathrm{Cont}(f) = 1$. If $p \in R$ is prime with the following conditions holding

- $a_n \not\equiv 0 \mod (p)$,
- $a_i \equiv 0 \mod (p)$ for all $0 \leq i < n$,
- and $a_0 \not\equiv 0 \mod \left(p^2\right)$,

then f is irreducible.

Proof. Assume by contradiction that there is a factorization $f = gh$ with $\deg(g), \deg(h) \geq 1$ and $g = \sum_{i=0}^{m} b_i x^i$, $h = \sum_{i=0}^{d} c_i x^i$. Remove any trivial terms such that $\deg(g) = m$ and $\deg(h) = d$ with both being nonzero. Additionally, we can assume all coefficients live in R.
Then, we see $a_0 = c_0 b_0 \equiv 0 \mod (p)$ but $c_0 b_0 \not\equiv 0 \mod \left(p^2\right)$. This implies exactly one of c_0, b_0 is divisible by p. WLOG, suppose $p \mid c_0$ and $p \nmid b_0$.
Next, $a_n = b_m \cdot c_d \not\equiv 0 \mod (p)$, so $p \nmid c_d$. Then, there is a minimal index r such that $p \nmid c_r$ but $p \mid c_i$ for $0 \leq i < r$.
Now, collecting coefficients yields

$$a_r = b_0 c_r + b_1 c_{r-1} + \ldots + b_{r-1} c_1 + b_r c_0.$$

By the earlier conclusion, we see $p \mid b_j c_{r-j}$ for all $j \geq 1$. That is, p divides all but the first term since $p \nmid b_0$ and $p \nmid c_r$. Since p is prime, $p \nmid b_0 c_r$, and since p divides all other terms, we find $p \nmid a_r$, hence $a_r \not\equiv 0 \mod (p)$. Hence, the assumptions yield $r = n$ But by an earlier assumption, we see $d \geq r$, hence $d = n$ else a contradiction would arise. Hence since $\deg(h) = \deg(f)$, we see $\deg(g) = 0$, so g is constant. $\lightning$, since we assumed g nonconstant. $\square$

Example. $f(x) = x^{72} + 40x^7 + 10x + 50 \in \mathbb{Z}[x]$. Clearly $\text{Cont}(f) = 1$ and $\deg(f) = 72 \geq 1$. Since $2, 5$ divide all the coefficients these are our choices for p. Since $5^2 \mid 50$, this one will not work, so we choose 2. $2 \nmid 1 = a_n$, $2 \mid 40, 10, 50$ respectively, and $2^2 = 4 \nmid 50$, hence eisenstein yields that f is irreducible over $\mathbb{Z}$ (hence $\mathbb{Q}$).
$g(x) = x^4 + 1$. As no primes divide 1, this seems to be a poor case for eisenstein. However, if we consider the ring isomoprhism

$$\begin{aligned} h_a : R[x] &\longrightarrow R[x] \\ f(x) &\longmapsto h_a(f(x)) = f(x+a). \end{aligned}$$

We see this has inverse $f(x) \mapsto f(x-a)$. Since this is an isomorphism, we know it preserves irreducible. Hence, we need only choose a clever a, and show that $h_a(g(x))$ is irreducible.
For our a we choose 1, yielding $h_1(g) = (x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$. Taking $p = 2$, we see the conditions of eisenstein hold hence this is irreducible. Taking the pullback h_{-1} yields $x^4 + 1 = g$ irreducible.
As a final example, we take $\varphi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$. Again, taking the isomorphism h_1 yields $h_1(\varphi_p) = \sum_{n=1}^{p} \binom{p}{n} x^{n-1}$. When $n = 1$, we see $p \mid \binom{p}{1} = p$ but $p^2 \nmid p$. Moreover, every other $\binom{p}{n}$ has $p \mid \binom{p}{n}$ except $p \nmid \binom{p}{p} = 1$. Hence applying eisenstein and the pullback h_{-1} yields the result. $\diamond$

Theorem 0.2. Suppose R and $\overline{R}$ are both integral domains with $\alpha : R \to \overline{R}$ being a ring homomorphism. We know this extends to homomorphism

$$\begin{aligned} \overline{\alpha} : R[x] &\longrightarrow \overline{R}[x] \\ f = \sum_{i=0}^{n} a_i x^i &\longmapsto \sum_{i=0}^{n} f(a_i) x^i = \overline{f}. \end{aligned}$$

If $f(x) \in R[x]$ with $\deg(f) = \deg(\overline{f})$ and $\overline{f}$ being irreducible, then f has no nontrivial factorizations (no factorization $f = gh$ with $\deg(g), \deg(h) \geq 1$).

This theorem is generally used when $R = \mathbb{Z}$ and $\overline{\mathbb{R}} = \mathbb{Z}/p\mathbb{Z}$. The proof is omitted for now, so see Lang.

Example. If $f = x^5 + (2k+1)x^2 + (2\ell + 1)$. Reducing $\mod 2$ yields $\overline{f} = x^5 + x^2 + 1$. Clearly, there are no linear factors, hence as all partitions of 5 into 2 integers admit either a 1 or 2 we need only show there are no quadratic factors. Moreover, the quadratic factor must be irreducible (else it would admit a linear factor). The only four quadratic factors in $\mathbb{Z}/2\mathbb{Z}$ are $x^2, x^2+1, x^2+x, x^2+x+1$. We know $x^2 = x \cdot x$, $x^2 + 1 = (x+1)^2$ over characteristic 2, $x^2 + x = x(x+1)$. Hence we need only see if $x^2 + x + 1$ is irreducible. This is a trivial fact to show, so we need only see if it divides the original polynomial. Performing long division yields remainder 1, so $x^2 + x + 1 \nmid x^5 + x^2 + 1$. Hence, as this polynomial is irreducible over $\mathbb{Z}/2\mathbb{Z}$ applying the pullback yields the original family of polynomials to be irreducible. $\diamond$

1 Summary of Ring Theory

Lecture 41: Summary of Ring Theory

Mon 07 May 2018 19:15

1.1 Rings and Ideals

Definition 1.1 (Rings)**.** A **Ring** is a set and two operations, $+, \cdot$.
A **Unit** is an element with multiplicative inverse.
A **Field** is a commutative ring with all nonzero elements units.
An **Integral Domain** is a Ring with the zero product property.
A **Division Ring** is a noncommutative field.
A **Ring Homomorphism** respects $+$ and $\cdot$.
An **Ideal** is a subset of R which is a subgroup under addition and has absorbtion property.
A **Quotient Ring** Is simply the set of additive cosets of a given ideal.
(X) is the smallest ideal containing the set X. Arbitrary elements are linear combinations of elements from X with elements from R.
A **Prime Ideal** has $xy \in P \Rightarrow x \in P$ or $y \in P$. Alternatively, R/P is an ID.
Maximal Ideals are maximal by containment. Equivalently R/I is a field $\Leftrightarrow I$ is maximal.
A **Principal Ideal** is generated by 1 element. $x \mid y$ if $y = rx$ for $r \in R$.
Two elements are **Associate** if they are equal up to units.
A **Principal Ideal Domain** is an ID where all ideals are principal.
A **Euclidean Domain** is an ID with a norm and well defined division with remainders.
An element is **Prime** if $p \mid xy \Rightarrow p \mid x$ or $p \mid y$.
An element is **Irreducible** if $x = yz \Rightarrow y$ or z a unit.
A **Factorization** is an equivalence to a unit times a product of irreducibles.
A **UFD** is an ID with all nonzero elements having Unique factorization.
An ideal is **finitely generated** if its generated by a finite number of elements.
A ring is **Noetherian** if all properly ascending chains of ideals are finite in length. Alternatively, it is noetherian if all ideals are finitely generated.
A **Localiztion** of R is the ring of fractions $S^{-1}R = \{X/s : x \in R, s \in S\}$. Fractions are equal iff their crossmultiples are zero divisors or 0. Moreover, multiplication and addition are defined in the usual way. Two elements have $x \equiv y \mod I$ if $x - y \in I$.

Theorem 1.1. fields $\subset$ ED's $\subset$ PIDs $\subset$ UFDs $\subset$ IDs.

Proposition 1.1 (1st Isomorphism Theorem)**.** A surjective homomorphism is an ideal.

Theorem 1.2. All maximal ideals are prime.

Proof. Maximal ideals induce a field, hence an integral domain, hence a prime ideal. □

Definition 1.2 (Zorn's Lemma)**.** A non-empty partially ordered set with every totally ordered subset having an upper bound admits a maximal element.

Theorem 1.3. All proper ideals are contained in a maximal ideal.

Proof. Take set of all proper ideals containing I po'd by inclusion. It is nonempty and the union of nested ideals is itself an ideal and it is an upper bound, hence there is a maximal element by zorn's lemma. □

Proposition 1.2. $x \mid y$ and $y \mid x$ iff $(x) = (y)$.
If R is an integral domain, then x, y are associate.

Proposition 1.3. p prime implies (p) prime.

Theorem 1.4. If p irreducible, then (p) is maximal by inclusion among proper PI's.

Proof. If (p) is in a proper PI, then $p = rx$ implying r is a unit, so p, x are associate $\lightning$. □

Corollary 1. p irreducible implies (p) maximal.

Theorem 1.5. If R is an ID, then maximal among PI's implies irreducible.

Proof. If $p = xy$, then $p \in (x)$ and (y), so $(y) = (p)$ or $(y) = R$. If $(y) = (p)$, then p, y are associate implying x a unit. Else $(y) = R$, so y is a unit. □

Theorem 1.6. If R is an ID, prime implies irreducible.

Proof. If $p = xy$, then WLOG $x \in (p)$, so $x = rp$ hence $p = rpy$ implying y a unit. □

Theorem 1.7. In a UFD, prime iff irreducible.

Proof. Let p be irreducible with $p \mid xy$. then $xy = rp$, so setting up factorization yields $r \operatorname{Fac}(x) \operatorname{Fac}(y) = rp$. Since its an ID, $p \in \operatorname{Fac}(x)$ WLOG, hence $p \mid x$ so p prime. □

Theorem 1.8. A ring is noetherian iff its ideals are finitely generated.

Proof. First, take a sequence of ideals constructed from the elements of a desired ideal. Eventually this must stop, yielding the finite generation of the ideal. Conversely, chains must end otherwise we could obtain an infinitely generated ideal. $\square$

Theorem 1.9. If R satisfies the ascending chain condition for principal ideals, then all nonzero elements have factorization.

Proof. Do the combinatorial infinite tree argument, repeatedly splitting an element into the product of irreducibles in order to obtain an infinite chain of ideals. Conclude a contradiction. $\square$

Proposition 1.4. R is noetherian and UFD iff irreducible $\Rightarrow$ prime.

Theorem 1.10. A multiplicative subset admits an identity map into the localization.

Proof. Apply definition of $\ker(\varphi)$ to see $sx = 0$ implying $x = 0$ or $s = 0$, so $x = 0$ by assumption. $\square$

Theorem 1.11 (CRT)**.** If R a commutative ring with $I_1, \dots, I_n$ ideals which are pairwise co-maximal ($I_i + I_j = R$), then any $x_1, \dots, x_n$ there is a solution to the system $x \equiv x_i \; 1 \leq i \leq n$.

Proof. Use induction. Case 1 is trivial, case 2 is accomplished by taking $a_1 + a_2 = 1$ by assumption and choosing $x = x_1a_2 + x_2a_1$. For the case n, we find $1 = a_i + b_i$ for $a_i \in I_1$ and $b_i \in I_i$. Hence $1 = \prod_{i=1}^n (a_i + b_i) \in I_1 + \prod_{i=2}^n I_i$. Applying the case $n = 2$ we find a solution to the system $y_1 \equiv 1 \mod I_1$, $y_1 \equiv 0 \mod \prod_{i=2}^n I_i$. Repeating yields y_i for each i, hence $x = \prod_{i=1}^n x_iy_i$ yields our general solution. $\square$

Theorem 1.12. Under the same assumptions as CRT, the map sending x to the cartesian product of its congruenceies mod I_i is a surjective ring homomorphism with $\ker(\varphi) = \bigcap_{i=1}^n I_i$. Moreover, its quotient ring is isomorphic to the product of the individual quotient rings.

Proof. φ is obviously a homomorphism with the given kernel. For f to be surjective, we see an arbitrary congruence system must have a solution, but this is true by CRT. $\square$

1.2 Polynomials

Definition 1.3. A **Polynomial Ring** $R[x]$ is the ring of formal sums with coefficients in R $f = \sum_{i=0}^{n} a_i x^i$ for some $n \geq 0$. We define a_0 the **constant**, a_n the **leading coefficient** and n the **degree.**
$f = g$ iff their coefficients are equal.
A **Multivariate** polynomial ring is created by induction $R[x_1, \ldots, x_n] = (R[x_1, \ldots, x_{n-1}])[x_n]$. For these rings the leading coefficient is poorly defined.
The **evaluation** map is the ring homomorphism sending all $f \in R[x]$ to $f(a)$.
The **p-adic** valuation of $\frac{a}{b}$ is $V_p\left(\frac{a}{b}\right) = V_p(a) - V_p(b)$ for a prime p, where $V_p(a)$ is the power of p in the factorization of a. $V_p(0) := \infty$.
Let $V_p(f) = \inf\{V_p(a_i)\}$. Then, $\mathrm{Cont}(f) = \prod_{p \text{ prime}} p^{V_p(f)}$ is the **Content** of f.
If R is a UFD with K its quotient field, then $f \in K[x]$ is primitive if $\mathrm{Cont}(f) = 1$.

Proposition 1.5. If φ is a ring homomorphism of R, then it is a ring homomorphism of $R[x]$ simply applying φ to each coefficient.

Proposition 1.6. If R is an ID, then $R[x]$ is an ID with $\deg(fg) = \deg(f) + \deg(g)$.

Theorem 1.13. If F is a field, then $F[x]$ is a ED.

Proof. Applying polynomial division with norm $\deg(\cdot)$ yields the result. ☐

Theorem 1.14. $R[x]$ is a PID iff R is a field.

Proof. It is clear R is an ID embedded in $R[x]$. Then, take the ideal $(y, x) = (f)$ for some f. We find f constant. So, $x \in (f) = (\alpha)$ for $\alpha \in R$, implying $x = g\alpha = \alpha a x + \alpha b.$, so $\alpha a = 1$, $\alpha b = 0$, so $I = R[x]$, implying $1 = g_1 y + g_2 x$, and we find this implies y a unit. ☐

Theorem 1.15. If F a field, then $F[x, y]$ is not a PID.

Proof. We know $F[x]$ is not a field, hence the result. ☐

Theorem 1.16 (FTA)**.** Suppose F is a field with $f \in F[x]$ and $\deg(f) = n \geq 0$. Then $f(a) = 0$ implies $(x - a) \mid f$. Lastly, f has at most n roots in F.

Proof. Long division yields $f = q(x - a) + r$ implying r constant, hence $r = 0$, hence $(x - a) \mid f$. Then, long division yields it obvious the second claim. ☐

Theorem 1.17. If K is a field with U being a finite multiplicative subgroup, then U is cyclic.

Proof. Since U is a finite additive group, it is the produce of sylow p_i-groups. It suffices to show each P_i is cyclic. Taking an element of maximal order m and denoting $|P_i| = p^n$, we see a $y \in P_i$ is a rot of $f = x^{p^m} - 1$, hence $n \leq m$, so $n = m$, so $\text{ord}(x) = p^m$ implies x generates P_i. □

Theorem 1.18 (Gauss Lemma)**.** Let R be a UFD with K its quotient field, then $\text{Cont}(fg) = \text{Cont}(f)\,\text{Cont}(g)$.

Proof. It suffices to show the claim holds for primitive polynomials. Suppose there is a p dividing all coefficients of f, g, then $\varphi : R[x] \to \overline{R}[x]$ has (p) being a prime ideal so $\overline{R}$ is an ID implying $\varphi(f) = 0$ of $\varphi(g) = 0$. If either is the case $\lightning$, hence the claim holds. □

Proposition 1.7. If R is a UFD with K its quotient field, then $\text{Cont}(f) = 1 \Rightarrow f \in R[x]$.

Theorem 1.19. Let R be a UFD with quotient field K, then f is irreducible in $R[x]$ iff f is irreducible in $K[x]$.

Proof. First, suppose f irr. in $K[x]$ but not $R[x]$. Then, $f = gh \in R[x]$. Since $\text{Cont}(f) = \text{Cont}(g)\,\text{Cont}(h) = 1$, we see gh is a factorization in K unless g, h is a unit. Assuming WLOG g a unit in $K[x]$, then g is a unit in R, $\lightning$. So f is irr. in $R[x]$.
Conversely, the same argument yields a contradiction to show the claim. □

Theorem 1.20. If R is a UFD with quotient field K, then $f \in R[x]$ is prime iff $f = p \in R$ for a constant prime $p \in R$ or f is irreducible over $K[x]$ and $\text{Cont}(f) = 1$.

Proof. We show the first part of the converse first. If $f = p$, suppose $p \mid gh$ with $g, h \in R[x]$, then $p \mid \text{Cont}(g)$ or $\text{Cont}(h)$, WLOG choose the first. Then $p \mid g$ implies p prime in $R[x]$.
Now, f is primitive and irreducible over $K[x]$, then $K[x]$ is a UFD, so primes are irreducible, hence f is a prime in $K[x]$. Suppose $f \mid_R gh$, then $f \mid_{K[x]} gh$, so $f \mid_{K[x]} g$ WLOG. Then, we find $f = gt$ for $t \in K[x]$, so $\text{Cont}(t) \in R$, hence $t \in R[x]$, so $f \mid_{R[x]} g$, so f is prime.
Lastly, If $f \in R[x]$ is prime, then if $f = p \in R$ is a constant prime polynomial in $R[x]$ a similair division juggling argument yields the claim.
Otherwise, we wish to show f primitive. The preceding lemma handles this case. □

Theorem 1.21. R is a UFD iff $R[x]$ is a UFD.

Proof. Taking a nonzero polynomial, we see it is factorized into the factorization over R of $\mathrm{Cont}(f)$ and the product of irreducible polynomials in $K[x]$. Since the factorization of $\mathrm{Cont}(f)$ is unique and we know $K[x]$ is a UFD, then the claim immediately follows. $\square$

Theorem 1.22 (Eisenstein Criterion)**.** If R is a UFD with quotient field K and $f(x) = \prod_{i=0}^{n} a_i x^i$ with f primitive, and $p \in R$ is a prime with the following holding

- $a_n \not\equiv 0 \mod (p)$,
- $a_i \equiv 0 \mod (p)$,
- $a_0 \not\equiv 0 \mod \left(p^2\right)$,

then f is irreducible.

Proof. Assuming by contradiction $f = gh$ with $g = \prod_{i=0}^{k} b_i x^i$ and $h = \prod_{i=0}^{m} c_i x^i$, we see $a_0 = c_0 b_0 = 0$ and the conditions imply $p \mid c_0$ xor $p \mid b_0$. Similairly, $a_n = b_k c_m$, so $p \nmid b_k$ or c_m. Collecting coefficients yields $a_r = b_0 c_r + \ldots + b_{r-1} c_1 + b_r c_0$. The earlier conclusion yields p divides all but the first term, hence $p \nmid a_r$ implying $r = n$. Since we assumed $m \geq r$, we find $m = r = n$ else a contradiction. Hence, since $\deg(f) = \deg(h)$ implying $\deg(g) = 0$, so g is constant, hence a unit, so $\lightning$. $\square$

Example. Some cases are obvious, other times we use the translation homomorphism $h_a : f(x) \mapsto f(x + a)$ and the pullback to show the claim. $\diamond$

Theorem 1.23. Suppose R, $\overline{R}$ are integral domains with a ring homomorphism α between them. Then, if the extended homomorphism $\overline{\alpha}$ has $\deg(f) = \deg\left(\overline{f}\right)$ and $\overline{f}$ being irreducible, then f has no non-constant factorizations.

Example. Reduce a given polynomial $\mod n$ to yields the disappearance of coefficients. Then enumerate all possible factors in the finite field to prove the claim. $\diamond$