Algebraic Theory I

Thomas Fleming

May 7, 2018

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 $\mathrm{Cont}(f) = 1$ 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 $\deg(f) = \deg\left(\overline{f}\right)$ 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 Review of Ring Theory

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.

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

Theorem 1.1. All maximal ideals are prime.

Proof. Maximal ideals induce a field, hence an integral domain, hence a prime ideal. $\square$

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 1.2. 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 1.3. 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 1.4. 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 1.5. 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 1.6. 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. □