Algebraic Theory I

Thomas Fleming

May 7, 2018

Contents

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 $x - y \in I$.

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. □

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. □

Theorem 1.7. 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. □

Theorem 1.8. 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. □

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

Theorem 1.9. 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. □

Theorem 1.10 (CRT)**.** If R a commutative ring with $I_1, \ldots, I_n$ ideals which are pairwise co-maximal ($I_i + I_j = R$), then any $x_1, \ldots, x_n$ 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 $x = \prod_{i=1}^{n} x_i y_i$ yields our general solution. □

Theorem 1.11. 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. □

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. $V_p(0) \coloneqq \infty$.
Let $V_p(f) = \inf\{V_p(a_i)\}$. Then, $\text{Cont}(f) = \prod_{p \text{ prime}} p^{V_p(f)}$ is the **Content** of f.
If R is a UFD with K its quotient field, then $f \in K[x]$ is primitive if $\text{Cont}(f) = 1$.

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

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

Theorem 1.13. $R[x]$ 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 1.14. 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 1.15 (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 1.16. 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 $\operatorname{ord}(x) = p^m$ implies x generates P_i. □

Theorem 1.17 (Gauss Lemma)**.** Let R be a UFD with K its quotient field, then $\operatorname{Cont}(fg) = \operatorname{Cont}(f)\operatorname{Cont}(g)$.

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 $\operatorname{Cont}(f) = 1 \Rightarrow f \in R[x]$.

Theorem 1.18. 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 $\operatorname{Cont}(f) = \operatorname{Cont}(g)\operatorname{Cont}(h) = 1$, 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 1.19. 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 $\operatorname{Cont}(f) = 1$.

Proof. We show the first part of the converse first. If $f = p$, suppose $p \mid gh$ with $g, h \in R[x]$, then $p \mid \operatorname{Cont}(g)$ or $\operatorname{Cont}(h)$, 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 $\operatorname{Cont}(t) \in R$, 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 1.20. 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 $\text{Cont}(f)$ and the product of irreducible polynomials in $K[x]$. Since the factorization of $\text{Cont}(f)$ is unique and we know $K[x]$ is a UFD, then the claim immediately follows. □

Theorem 1.21 (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 $\lightning$. □

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. ◇

Theorem 1.22. 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. ◇