Abstract Algebra – II Rings and Algebras (环理论与代数)

2.5 notes, 2.8 Localizations

2012 年 12 月 12 日

Outline

2.5.1 Irreducible Polynomials

Proposition (Eisenstein's criterion)

Given a field $F = K[R]$ that is the field of fractions of a unique factorization domain R. Given further a polynomial $Q = a_0 + \cdots + a_n x^n \in R[x]$ and an irreducible $p \in R$ such that

1. *a_n is not divisible by p,*
2. *$a_0, \ldots, a_{n-1}$ are divisible by p,*
3. *a_0 is not divisible by p^2,*

then Q is irreducible in $F[x]$.

The problem is that the criterion cannot be applied to every irreducible polynomial. Using more localizations one can derive better irreducibility tests which we will briefly discuss in Section 2.8.
Instead we should consider a few more properties of polynomials over an UFD (such as a PID).

Irreducible Polynomials II

The following result is already due to Euclid:

Proposition (Euclid)

Given a UFD R, then $R[x]$ contains infinitely many different irreducible polynomials.

Remark

All the polynomials of degree 1 are irreducible. If R itself has infinitely many elements, then the $x - r \in R[x]$ for $r \in R$ are all different.

Irreducible Polynomials III

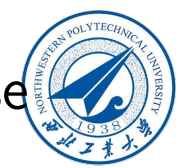
Proof.

Assume for the sake of an indirect proof that $p_1, \ldots, p_N$ are all different irreducible polynomials. Consider now their product $P := 1 + \prod_{k=1}^{n} p_k$. Since the list contains at least the linear monic polynomials the product has degree at least 2. Thus it is not a unit and not 0. But none of the p_k divides P, because it has remainder 1. On the other hand P does factor into a product of irreducible polynomials. Therefore there must be at least one other polynomial p_{n+1} that divides P. This is a contradiction to an assumed finite list. □

Theorem

Given a UFD R, then the polynomials over R (in one more indeterminate) form a UFD.

The first proof of the theorem was discovered by Gauss in the case of $\mathbb{Z}[x]$ and uses the following notions:



Primitive Polynomials and Content

Definition

Given a polynomial $p \in R[x]$ where R is a UFD. We say that p is primitive *if there is no irreducible $q \in R$ such that q divides all coefficients of p.*

The following lemma is immediate and its result will help in the proof of the Theorem.

Lemma

Every non-zero polynomial $p \in F[x]$ where $F = K[R]$ is the field of fractions of a UFD R can be written in the form $p = up^*$ where $u \in F^*$ and $p^* \in R[x]$ primitive. □

We denote $u \in F[x]$ the content of p. The content of a primitive polynomial is thus 1 (or any other unit $u \in R^*$).

Lemma (Gauss)

The product of two primitive polynomials is primitive.

Primitive Polynomials and Content II

Proof.

Let $p, q \in R[x]$ be primitive polynomials over the UFD R with coefficients $p = p_0 + p_1 x + \cdots + p_m x^m$, $q = q_0 + q_1 x + \cdots + q_n x^n$. And let $r \in R$ be any irreducible element. Since p and q are primitive, not all of the p_i, q_i are divisible by r. Let k be the smallest i such that r does not divide p_i and l the smallest i such that r does not divide q_i. But then r divides all p_i with $i < k$ and all q_j with $j < l$. Thus in particular for $pq = c_0 + c_1 x + \cdots + c_{m+n} x^{m+n}$, p does not divide $c_{k+l} = \sum_{\substack{i+j=k+l \\ i<k \text{ or } j<l}} p_i q_j + p_k q_l$. □

Proposition

A polynomial $p \in F[x]$ over the field of fractions of a UFD R, $F = K[R]$, then p is irreducible iff $p^* \in R[x]$ is.

Primitive Polynomials and Content III

Proof.

We may assume that $\deg p \geq 1$. If p is not irreducible over $F[x]$, then there are $f, g \in F[x]$ with $p = fg$. But then also $p^* = (fg)^* = f^* g^*$ by the last lemma and thus p^* factors over $R[x]$. If on the other hand $p^* = fg$ for some $f, g \in R[x]$. Since p is primitive, so must be f and g. In particular each of them has degree at least 1. But then also $p = up^* = ufg$ is not irreducible in $F[x]$. □

Remark

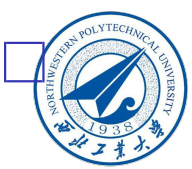
To say it more explicitely, the irreducible elements of $R[x]$ are the irreducible elements of R together with the $p^* \in R[x]$ where $p \in F[x]$ is an irreducible polynomial. In particular all the p^* are primitive.

Proof of the theorem

We work by induction over the number of indeterminates. Let us thus restrict to the case of one indeterminate. In order to show that $R[x]$ is a UFD, we consider $F := K[R]$, because R is in particular a domain, and embed the polynomials $R[x] \subset F[x]$. In the latter case we have already shown (see Proposition 2.5.2) that these form a UFD. Assume thus that $p \in R[x] \subset F[x]$ factors as $p = p_1 \dots p_n$ with $p_i \in F[x]$. By extracting the content, we can write $p = uP_1 \dots P_n$ where $P_i \in R[x]$ and $p_i = u_i P_i$, $u = u_1 \dots u_n \in F$. If $u_i \in R^*$, then also $p_i \in R[x]$ and thus we can keep this factor. If there are some $p_i \notin R[x]$ it means that also the corresponding $u_i \notin R$. We are thus left with factoring the polynomials p for which all $p_i \notin R[x]$, but then the polynomial is irreducible over R, while we claim that it splits over $F[x]$. This is a contradiction to Proposition 2.5.12.

Proof of the theorem II

It remains to show uniqueness of the factorization. Let thus $p = p_1 \cdots p_m = q_1 \cdots q_n$ with $p_i, q_i \in R[x]$. From the uniqueness of factorization over $F(x)$ we know that there is a bijection between the polynomials that are not constant, i.e. $p_i = u_i q_{\sigma i}$ for $u_i \in F^*$ and $1 \leq i \leq m' \leq m$. If the p_i are irreducible over R, then they must be either constant or of degree at least 1 and primitive. But then the $u_i \in R^*$ and the remaining $p_{m'+1} \cdots p_m$ as well as the remaining $q_{m'+1} \cdots q_n$ must multiply to an element of F^*. Since all p_i are primitive and of degree at least 1 and p^* is primitive as well, we have $p^* = up_1 \cdots p_{m'} = u' q_{\sigma 1} \cdots q_{\sigma m'}$ as well as the content of p equal some element in R, $u^{-1} p_{m'+1} \cdots p_m = u'^{-1} q_{\sigma(m'+1)} \cdots q_{\sigma n}$. But since R is a UFD, we know that we can modify the bijection σ such that $p_i = u_i q_{\sigma i}$ also for $m' + 1 \leq i \leq m$, $u_i \in R^*$ and in particular $n = m$. This completes the proof.



Example

1. We already know that the integers $\mathbb{Z}$ form a UFD, because they are a PID. Therefore also $\mathbb{Z}[x]$, the polynomials with integer coefficients, form a UFD. Note that they are no longer a PID.
2. In the same way polynomials in countably many indeterminates over a UFD (e.g. a field) form a UFD, because every (finite) polynomial lies in an extension with finitely many indeterminates which form a tower of UFDs.

Exercises

Exercise

Show that every family of elements $a_i \in R$ of a UFD has a

a. greatest common divisor;

b. least common multiple, if the family is finite;

c. show that there is an infinite family of elements that do not have a finite non-zero least common multiple.

Hint: You cannot assume that a UFD is a PID, but nevertheless the gcd is determined uniquely by the common irreducible divisors modulo equivalence, while the lcm is determined by the union of all irreducible divisors modulo equivalence.

Exercise

Find a UFD R together with two elements $a, b \in R$ such that their greatest common divisor cannot be written as a linear combination $\gcd(a, b) = fa + gb$ for any $f, g \in R$.

Exercise

Prove the following: Assume R is a UFD, $I \triangleleft R$ any ideal and $\pi : R \to R/I$ the quotient map. If $f \in R[x]$ is monic and $f_\pi \in (R/I)[x]$ irreducible, then p is irreducible over R.

Exercise

Apply the previous result to show that the following polynomials are irreducible in $\mathbb{Q}[x]$:

a. $x^3 - 10$,

b. $x^3 + 3x^2 - 6x + 3$,

c. $x^3 + 3x^2 - 6x + 9$,

d. $x^3 - 3x + 4$.

Localizations (环的局部化)

Remember the trick in the proof of Eisenstein's criterion (Proposition 2.5.4). Given a polyonomial $Q \in R[x]$ over an integral domain R together with a prime ideal $\mathfrak{p} \lhd R$, then Q reducible in $R[x]$ implies that $Q_{\mathfrak{p}}$ is reducible in $(R/\mathfrak{p})[x]$, because the projection $\pi : R[x] \to (R/\mathfrak{p})[x] : a \mapsto a + \mathfrak{p}, x \mapsto x$ can be extended as a ring homomorphism. Therefore, given a prime ideal $\mathfrak{p} \lhd R$ such that $Q_{\mathfrak{p}}$ is irreducible, then also Q must be irreducible.

You will see in the homework what can be done if there is no prime ideal $\mathfrak{p} \lhd R$ such that $Q_{\mathfrak{p}}$ is irreducible, but you have the strong feeling that Q should be irreducible.

Localizations (环的局部化)

Remember the trick in the proof of Eisenstein's criterion (Proposition 2.5.4). Given a polyonomial $Q \in R[x]$ over an integral domain R together with a prime ideal $\mathfrak{p} \lhd R$, then Q reducible in $R[x]$ implies that $Q_{\mathfrak{p}}$ is reducible in $(R/\mathfrak{p})[x]$, because the projection $\pi\colon R[x] \to (R/\mathfrak{p})[x] : a \mapsto a + \mathfrak{p}, x \mapsto x$ can be extended as a ring homomorphism. Therefore, given a prime ideal $\mathfrak{p} \lhd R$ such that $Q_{\mathfrak{p}}$ is irreducible, then also Q must be irreducible.

You will see in the homework what can be done if there is no prime ideal $\mathfrak{p} \lhd R$ such that $Q_{\mathfrak{p}}$ is irreducible, but you have the strong feeling that Q should be irreducible.

The biggest problem that prevents us from constructing the quotient field of an arbitrary (commutative) ring R are the zero divisors. Namely if we write a/b for some $a, b \in R$ we do not only have to exclude $b = 0$, but also every possible $d_{1/2}$ such that $d_1 d_2 = 0$, i.e. the zero divisors, because they would eventually lead to $(1/d_1)(1/d_2) = 1/0$.

Localizations (环的局部化) I

The abstraction gives the following concept.

Definition

Given a ring $(R, +, \cdot)$, then a multiplicative set is a nonempty subset $S \subset R$ that does not contain 0, contains all units $R^* \subset S$, and is closed under multiplication, i.e. $S \cdot S \subset S$.

Example

1. The complements $S = R \setminus \mathfrak{p}$ of prime ideals $\mathfrak{p} \triangleleft R$ are multiplicative sets, because for a prime ideal we have that $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$ and in particular $0 \in \mathfrak{p}$ thus $0 \notin S$.
2. For domains (such as the integers $\mathbb{Z}$) (0) is a prime ideal and we can thus choose $S = R \setminus \{0\}$.

The localization is now defined as follows.

Localizations (环的局部化) II

Definition

Let R be a ring and $S \subset R$ be a multiplicative subset. The localization of R at S, denoted as $S^{-1}R$ is the set $R \times S/\sim$ with elements denoted as a/s where $a \in R$ and $s \in S$ under the equivalence relation $r/s \sim r'/s'$ iff there is a $t \in S$ such that

$$t(rs' - r's) = 0.$$

Addition is done via expansion to a common denominator, i.e. $a/s + b/t = (at + bs)/(st)$. Multiplication is done componentwise, i.e. $(a/s)(b/t) = (ab)/(st)$.

Localizations (环的局部化) III

Proposition

The relation $\sim$ is an equivalence relation. $a/s \sim (at)/(st)$ and addition and multiplication are representation independent and thus $S^{-1}R$ a ring together with a ring homomorphism $i\colon R \to S^{-1}R : a \mapsto a/1$ that maps all elements of $S \subset R$ to units.

It is obvious that this generalizes the definition of the field of fractions in Proposition 2.3.3. The difference to the quotient field of a domain is that R can have zero divisors.

Proof.

Reflexivity $a/s \sim a/s$ is clear with any $t \in S$, e.g. $t = 1$. Suppose $a/s \sim b/s'$ with $t \in S$, then $t(bs - as') = -t(as' - bs) = 0$, and for transitivity assume that $a/s \sim a'/s'$ via $t \in S$ and $a'/s' \sim a''/s''$ via $t' \in S$, then $tt's'(as'' - a''s) = t's''(t(as' - a's)) + ts(t'(a's'' - a''s')) = 0$. The second statement is obvious.

Localizations (环的局部化) IV

In order to see that addition is representation independent, let $a/s \sim a'/s'$ via t and $b/u \sim b'/u'$ via t'. Then $a/s + b/u = (au + bs)/(su)$ and $a'/s' + b'/u' = (a'u' + b's')/(s'u')$. The right hand expressions are equivalent via tt', because $tt'[(au + bs)s'u' - (a'u' + b's')su] =$ $tt'[(as' - a's)uu' + (bu' - b'u)ss'] = 0$. An analogous but simpler computation leads to representative independence of the multiplication.

It is obvious that i is a ring homomorphism. The inverse elements of s are $1/s$. This completes the proof. □

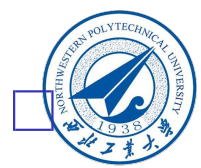
Localizations (环的局部化) V

Proposition

The above construction fulfills the universality condition that every ring homomorphism $\phi\colon R \to R'$ that sends S to R'^* extends uniquely to $S^{-1}R$.

Proof.

Remember that the elements of $S^{-1}R$ are generated by pairs a/s with $a \in R$ and $s \in S$. Since $\phi(s) \in R'^*$ there are inverse elements $\phi(s)^{-1} \in R'$. We thus send $a/s \mapsto \phi(a)\phi(s)^{-1}$. It remains to check that this is representation independent. Let thus $a/s \sim a'/s'$ via $t \in S$. We thus have $t(as' - a's) = 0 \in R$ but since ϕ is a ring homomorphism, we obtain $\phi(t)(\phi(a)\phi(s') - \phi(a')\phi(s)) = 0 \in R'$. Since $\phi(t)$, $\phi(s)$, and $\phi(s')$ are invertible, we obtain $\phi(a)\phi(s)^{-1} = \phi(a')\phi(s')^{-1}$. The homomorphism property of the extension of ϕ is now obvious. This completes the proof.



Exercises

Exercise

Given the ring of integers $R = \mathbb{Z}$ and the multiplicative set $S = R \setminus (2)$. Determine the localization $S^{-1}R$ and show that it is embedded into $K[R] = \mathbb{Q}$. What is its image?

Exercise

Show that the polynomial $Q = x^4 + 4x^3 + 5x^2 + 1 \in \mathbb{Z}[x]$ is irreducible in $\mathbb{Q}[x]$. You may proceed as follows:

. Note that you cannot apply Eistenstein's criterion directly;

a. localize the polynomial w.r.t. $p = 2$ and note that it factors. This says, that one localization is not sufficient;

b. localize the polynomial w.r.t. $p = 3$ and note that it also factors. Thus this localization is not sufficient either;

c. assume that Q factors in $\mathbb{Q}[x]$ as $Q = fg$ and compare their localizations for $p = 2, 3$ with the factors you obtained earlier. Conclude that either f or g must have degree 4 and thus Q is irreducible;

Next week we will start with Field extensions and Galois theory.