Abstract Algebra, Lecture 13

Fields of fractions and Divisibility in Domains

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Linköping, fall 2019

Lecture notes availabe at course homepage
http://courses.mai.liu.se/GU/TATA55/

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

Summary

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

1. **Fields of fractions**
2. **Divisibility in domains**
   - Basic concepts
   - Non UFDs
   - Euclidean domains
   - Finite factorization
   - PIDs
   - Extensions of UFDs
3. **More about $\mathbb{Z}[x]$ and $\mathbb{Q}[x]$**

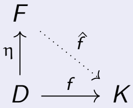
Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

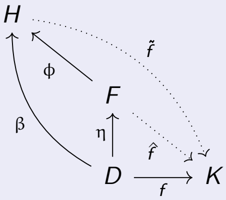
Throughout this lecture, D will denote an integral domain.

Theorem

There is an injective ring homomorphism $\eta : D \to F$, *with* F *a field, such that any injective ring homomorphism* $f : D \to K$ *to a field* K *factors through* F *as* $f = \hat{f} \circ \eta$.



The pair (F, η) *is unique up to isomorphism; if* (H, β) *solves the same universal problem, then there is a ring isomorphism* ϕ *such that* $\beta = \phi \circ \eta$.



Example

Think of $\mathbb{Z} \subset \mathbb{Q}$, and $f : \mathbb{Z} \to K$ extended by $f(a/b) = f(a)/f(b)$.

Example

Think also of the "rational functions", which are quotients of polynomials in $K[x]$.

Example

Somewhat similar: as an additive group, $\mathbb{Z}$ is the "difference group" of the monoid $\mathbb{N}$; we represent -3 as $0 - 3$ or $1 - 4$ or $2 - 5$ or...

Proof

Existence: Let $X = D \times (D \setminus 0)$, and introduce the relation

$$(a, b) \sim (c, d) \iff ad = bc$$

Think of (a, b) as a/b, and write it like so. We check that $\sim$ is an equivalence relation respecting multiplication and addition, turning $X/\sim = F$ into a commutative, unitary ring. But $1/(r/s) = (s/r)$ whenever $r \neq 0$, so F is a field.

The map

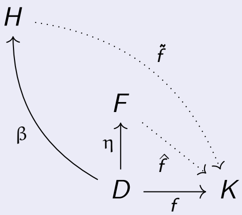
$$D \ni r \mapsto r/1 \in F$$

is an embedding of D into F.

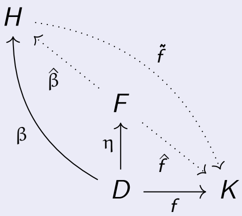
If $f : D \to K$ is injective, then we define $\hat{f} : F \to K$ by $\hat{f}(r/s) = f(r)/f(s)$. Clearly, $\hat{f}(\eta(r)) = \hat{f}(r/1) = f(r)/f(1) = f(r)$, since f is injective and hence $f(1) = 1$.

Proof, cont.

Uniqueness: consider the diagram

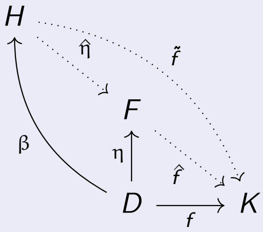


By the universal property, β factors through η:



Proof, cont.

Similarly, by the universal property, η factors through β:



So F embeds into H and H into F; they are thus isomorphic fields.

Definition

When $D = K[x]$, then the fraction field

$$F = K(x) = \left\{ \frac{f(x)}{g(x)} \middle| f(x), g(x) \in K[x], g(x) \neq z.p. \right\}$$

is called the "field of rational functions".

1. For $\frac{f(x)}{g(x)} \in K(x)$, it is natural to concern oneself with the quantity $\deg(f) - \deg(g)$
2. Some rational functions, like

$$\frac{1}{x-1} = 1 + x + x^2 + x^3 + \dots$$

lie in the ring of formal power series; all lie in the ring of formal Laurent series. As an example,

$$\frac{1}{x^2(1-x)} = x^{-2} + x^{-1} + 1 + x + x^2 + x^3 + \dots$$

Theorem

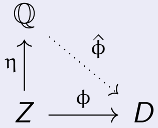
Any domain D contain a smallest subdomain: this is either an isomorphic copy of Z or of $\mathbb{Z}_p$; any field contains a smallest subfield, which is either Q or $\mathbb{Z}_p$.

Proof

Consider the ring homomorphism $\phi : \mathbb{Z} \to D$ with $\phi(n) = 1_D + \cdots + 1_D$, n times. If it is injective, then the image is isomorphic to $\mathbb{Z}$. If not, the image is a subring of a domain, so a domain; hence $Z/\ker(\phi)$ is a domain, so $\ker(\phi)$ is a prime ideal, so it is (p) for a prime p, so the image is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof, cont.

If D is a field, and ϕ is injective, then we can extend ϕ to $\mathbb{Q}$, embedding it inside D (note that all non-zero ringhomomorphisms between fields are injective):



If D is a field, and $\mathtt{ker}(\phi) = p\mathbb{Z}$, then as before, the image of ϕ is $\mathbb{Z}_p$ (so is the image of $\hat{\phi}$).

Definition

The unique smallest subfield of the field is called the *prime subfield*.

Definition

Let $u, v, w \in D \setminus \{0\}$.

1. If $u|1$ then u is a unit
2. If $u|v$ and $v|u$ then $u = cv$, with c a unit; we say that u, v are associate and write $u \sim v$. This is an equivalence relation.
3. If $w|u$ and $w|v$ then w is a common divisor of u and v; it is a greatest common divisor if it furthermore holds that w is divisible by any other common divisor. Gcd's are determined up to association.
4. We define $\gcd(u_1, \ldots, u_r)$ inductively as $\gcd(\gcd(u_1, \ldots, u_{r-1}), u_r)$. It is the greatest (w.r.t. divisibility) of the common divisors of $u_1, \ldots, u_r$.
5. w is irreducible if any divisor is either a unit, or associate to w
6. w is a prime element if $w|uv$ implies that $w|u$ or $w|v$
7. D has finite factorization if all (nonzero) elements are finite products of irreducible elements
8. D is a *unique factorization domain* if it has finite factorization, and this factorization is unique, up to order and associates

Example

Kronecker, and his student Kummer, studied so called "rings of algebraic integers". It was assumed that elements in such domains could be factored uniquely. However, in

$$\mathbb{Z}[\sqrt{-5}] \simeq \frac{\mathbb{Z}[t]}{(t^2+5)}$$

we have that

$$6 = 2 * 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

are two non-equivalent factorizations into irreducible elements. The world of algebraic number theory was shaken to its core! Kummer, in order to rectify the situation, introduced so-called "ideal elements", i.e. principal ideals. One often has unique factorization *of ideals* where unique factorization of elements do not hold.

Example

The subring of $\mathbb{C}[[x]]$ consisting of *convergent* power series is not a UFD, since some elements can have infinitely many irreducible factors. More precisely, Weierstrass factorization theorem says that

$$1 - z/n$$

is analytic, and irreducible, and has a single zero at $z = n$. Furthermore, every entire function whose zeroes are simple and contained in the natural numbers can be written as

$$e^{g(z)} \prod_{k=1}^{\infty} (1 - z/n).$$

Here $g(z)$ is an entire function, and $e^{g(z)}$ thus has no zeroes, and is invertible.

Definition

D is an Euclidean domain if there is a function $d : D \to \mathbb{N} \cup \{-\infty\}$ such that

$$
\begin{aligned}
d(u+v) &\leq \max d(u), d(v) \\
d(uv) &= d(u) + d(v) \\
d(0) &= -\infty
\end{aligned}
$$

Furthermore, this function should provide for a division algorithm: we demand that for $u, v \in D$, $v \neq 0$, there are unique k, r such that

$$u = kv + r, \qquad d(r) < d(v)$$

Theorem

The following are Euclidean domains:

1. $\mathbb{Z}$, *with* $d(u) = |u|$,
2. $K[x]$, *with* $d(u) = \deg(u)$,
3. *The Gaussian integers* $\mathbb{Z}[i] = \{ a + ib | a, b \in \mathbb{Z} \}$ *with* $d(a + ib) = a^2 + b^2$.

Theorem

Euclidean domains have an Euclidean algorithm, thus gcd's exist. Bezout's theorem hold. They are principal ideal domains.

Proof.

Extract the pertinent parts of the proofs in $K[x]$. □

Theorem

If D has finite factorization, and if irreducible elements are prime, then D is a UFD.

Proof.

If $u = p_1 \cdots p_r = q_1 \cdots q_s$, we can cancel p_1 and some q_i, then proceed by induction. □

Lemma

In a PID, (u) is maximal iff u is irreducible.

Proof.

If $u = vw$ with v, w non-units, then $(u) \subsetneq (v)$, so (u) is not maximal. Conversely, if u is irreducible, and $(u) \subseteq (v)$, then $v|u$, so v is either a unit or associate to u, so $(v) = D$ or $(v) = (u)$. So (u) is maxial. □

Theorem

In a PID, irreducible elements are prime.

Proof.

Let w be irreducible. If $w|uv$ then $(w) \supseteq (uv)$. But (w) is a maximal ideal, hence a prime ideal, hence either u or v belong to (w), hence either u or v is divisible by w. □

Theorem

In a PID, and strictly increasing chain of ideals

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$$

stabilizes, i.e., $I_n = I_{n+1} = \ldots$ *for some* n*.*

Proof.

Put $I = \cup I_n$. This is an ideal! It has a generator, so $I = (u)$. Since $u \in I = \cup I_n$, $u \in I_n$ for some n. Then $I_n = (u) = I \supseteq I_m$ for all m. □

Theorem

Any PID has finite factorization.

Proof.

Take $u \in D \setminus \{0\}$. If u is irreducible, done. Otherwise, $u = vw$, with $(u) \subsetneq (v)$. If v irreducible, fine; otherwise $v = v_2 w_2$ with $(u) \subsetneq (v) \subsetneq (v_2)$. Continue, by the previous lemma we'll eventually get $(v_{n-1}) = (v_n)$, i.e., $v_n = c v_{n-1}$ with c a constant, and v_{n-1} could not be divided further; it was irreducible.

So we have $u = \hat{v} g$ with $\hat{v}$ irreducible. Repeating the above argument with g, it is either irreducible or contains an irreducible factor. But if we could keep splitting of factors indefinitely, we would get an infinite ascending chain of principal ideals, which is impossible. □

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Theorem

Any PID is a UFD.

Proof.

It has finite factorization, and irreducible elements are prime. □

Corollary

Any Euclidean domain is a UFD.

Proof.

They are PIDs. □

Example

In $\mathbb{Z}[i]$, we can uniquely (up to the units $\{1, -1, i, -i\}$) factor into irreducibles, which are (Gaussian) primes. The ordinary primes in the subring $\mathbb{Z} \subset \mathbb{Z}[i]$ may factor:

$$13 = (2+3i)(2-3i)$$

Since $d(13) = 13^2 = d(2+3i)d(2-3i) = 13^2$ we have $13 = d(2+3i) = 2^2 + 3^2$, showing that $(2, 3, 13)$ is a Pythagorean triple, i.e., there is a right triangle with these sidelengths.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Theorem

If D is a UFD, then so is $D[x]$

The proof, which is somewhat technical, uses the so-called

Lemma (Gauss's lemma)

Let $f(x) = \sum_j a_j x^j \in D[x]$, with D a UFD. Let the content of $f(x)$ be $\mathrm{cn}(f) = \gcd(a_0, \ldots, a_n)$. Then

$$\mathrm{cn}(fg) = \mathrm{cn}(f)\mathrm{cn}(g)$$

Theorem

If $f(x) \in D[x]$ factors as $f(x) = g(x)h(x)$, with $g(x), h(x) \in K[x]$, where K is the fraction field of D, then there are $c, d, e \in D$ such that $f(x) = c(dg(x))(eh(x))$ and $dg(x), eh(x) \in D[x]$.

The proofs are in your textbook!

Corollary

Let D be a UFD. Then $D[x_1, \ldots, x_n]$ is a UFD.

Proof.

$D[x_1]$ is a UFD, hence so is $D[x_1, x_2] \simeq D[x_1][x_2]$, and so forth. □

Theorem

If K is a field, then $K[x_1, x_2, x_3, \ldots]$ (infinitely many indeterminates) is a UFD.

Proof.

This is an exercise in Bourbaki's *Algèbre commutatif*. □

Theorem

Let K be a field. The ring of formal power series $K[[x]]$ is a UFD.

Proof.

It is a PID; in fact, every ideal is of the form (x^m). □

Theorem

Let K be a field. The ring of formal power series $K[[x_1, \ldots, x_n]]$ is a UFD.

Example

The ring of formal power series $D[[x]]$, where D is a UFD, need not be a UFD!

For an example, let K be a field, form the polynomial ring $K[x,y,z]$, then the quotient $S = \frac{K[x,y,z]}{(x^2+y^3+z^7)}$. Then we form, not the fraction field, but something similar, namely the *localization*; we put

$$S = \{ f/g \mid f, g \in S,\ g(0,0,0) \neq 0 \}$$

It is well-defined whether $g(0,0,0) = 0$ or not, even though it is an element in the quotient.

Then S is a local ring, and a UFD, but $S[[t]]$ is not!

Thank you, Wikipedia!

Theorem (Cashwell-Everett)

$K[[x_1, x_2, x_3, \ldots]]$ is a UFD.

Jan Snellman

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

In a similar fashion to Weierstrass factorization thm:

Theorem (Snellman)

The subring $\varprojlim K[x_1, \ldots, x_n] \subset K[[x_1, x_2, x_3, \ldots]]$ *of formal power series, whose restrictions to finitely many indeterminates are polynomials, is a "topological UFD" in which every element can be uniquely written as a countable convergent product of irreducibles.*

We reiterate the following consequence of Gauss's lemma:

Lemma

The polynomial

$$f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$$

is irreducible iff it is irreducible viewed as a polynomial in $\mathbb{Q}[x]$.

We can check for linear factors:

Lemma

If $f(x) = \sum_{j=0}^{n} a_j x^j \in \mathbb{Z}[x]$ *has a rational zero* r/s*, with* $\gcd(r,s) = 1$*, then* $r|a_0$ *and* $s|a_n$*.*

Proof.

If

$$a_0 + a_1 r/s + \cdots + a_n r^n/s^n = 0,$$

then

$$s^n a_0 + s^{n-1} a_1 r + \cdots + a_n r^n = 0,$$

so

$$s^n a_0 = -rs^{n-1} a_1 - \cdots - r^n a_n.$$

Since $r|RHS$, $r|s^n a_0$. But $\gcd(r,s) = 1$, so $r|a_0$. A similar argument shows that $s|a_n$. □

- Let D, L be domains, and $\phi : D \to L$ a ring homomorphism
- If $w = uv$ in D, then $\phi(w) = \phi(u)\phi(v)$ in L
- However, ϕ can turn non-units into units
- A special case of the technique: ϕ induces

$$\hat{\phi} : D[x] \to L[x]$$
$$\hat{\phi}(\sum_j a_j x^j) = \sum_j \phi(a_j) x^j$$

- A special case of the special case: $\phi : \mathbb{Z} \to \mathbb{Z}_p$, and $\hat{\phi} : \mathbb{Z}[x] \to \mathbb{Z}_p[x]$, reducing the coefficients mod p

Example

Let $f(x) = x^2 + 10x + 21 \in \mathbb{Z}[x]$. Reducing modulo 3 we see that

$$f(x) \equiv x(x+1) \mod 3.$$

A technique known as "Hensel lifting" lifts this factorization uniquely modulo 3^2

$$f(x) \equiv (x + 1 * 3)(x + 1 + 2 * 3) \equiv (x+3)(x+7) \mod 9.$$

This lifting extends to any power of 3, but already modulo 9 we have recovered the correct factors over $\mathbb{Z}$.

Another useful result which follows from reducing modulo a prime is

Lemma (Eisenstein)

Let

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{Z}[x],$$

with

- p *prime*
- $p | a_i$ *for* $0 \leq i < n$
- $p \not| a_n$
- $p^2 \not| a_0$

Then $f(x)$ *is irreducible.*

Proof.

Consult your textbook! □

Example

Is $x^5 - 1 \in \mathbb{Z}[x]$ irreducible? Obviously not, since

$$x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1).$$

Is this the factorization into irreducibles? Put

$$h(x) = x^4 + x^3 + x^2 + x + 1,$$

then

$$h(x+1) = (x+1)^4 + (x+1)^3 + (x+1)^2 + (x+1) + 1 = x^4 + 5x^3 + 10x^2 + 10x + 5,$$

which is irreducible by Eisenstein. But if $h(x) = a(x)b(x)$ then surely $h(x+1) = a(x+1)b(x+1)$, so $h(x)$ is irreducible.