Fields of Quotients (Cont’d)

**Theorem.** Let $F$ be a field of quotients for an integral domain $D$, and let $L$ be any field that contains $D$ as a subring. Then there is a unique homomorphism $\psi: F \to L$ such that $\psi(a) = a$ for all $a \in D$.

**Proof.** See the book for the existence of $\psi$, or use:

$$\psi([a,b]) = \psi(a/b) = \psi(a)/\psi(b) = a/Lb.$$

One also needs to show that it is well defined and is a homomorphism.

**Uniqueness:** It has to be as given. In detail, let $x \in F$ be given. Then $x = [(a,b)] = a/Fb$ for some $a,b \in D$, $b \neq 0$. Then $bx = a$ in $D$, hence in $F$. So $\psi(b)\psi(x) = \psi(a)$, therefore $b\psi(x) = a$, so $\psi(x) = a/Lb$. □

Integral Domains as Subrings of Fields

We also proved: Every integral domain is a subring of a field, which contains the unity element of the field.

**Conversely,** let $F$ be a field let $1_F$ be its unity element, and let $R$ be a subring of $F$ that contains $1_F$. Then $R$ is an integral domain:

- It is commutative because $F$ is
- It has $1 \neq 0$ because $F$ does and $1_F \in R$
- It has no zero divisors because $F$ has none.

So:

A ring $R$ is an integral domain

$$\iff$$ it is a subring of a field and contains the field’s unity element

$$\iff$$ it is a subring of a field and has $1 \neq 0$ .

(See Ex. 19.23: If $F$ is a division ring then $\{x \in F : x^2 = x\} = \{0,1\}$.)

Polynomials

**Definition.** Let $R$ be an integral domain. We define the set $R[x]$ to be the set of all formal infinite sums $a_0 + a_1x + a_2x^2 + \ldots$ such that all but finitely many of the $a_i$ are zero.

We define a binary operation $+$ on $R[x]$ by termwise addition:

$$(a_0 + a_1x + a_2x^2 + \ldots) + (b_0 + b_1x + b_2x^2 + \ldots) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \ldots .$$

We define a binary operation $\cdot$ on $R[x]$ as you’ve learned in grade school:

$$(a_0 + a_1x + a_2x^2 + \ldots) \cdot (b_0 + b_1x + b_2x^2 + \ldots) = c_0 + c_1x + c_2x^2 + \ldots ,$$
where
\[ c_n = \sum_{i=0}^{n} a_i b_{n-i} \text{ for all } n \in \mathbb{N} . \]

**Theorem.** With the above definitions, \( R[x] \) is a ring. It also contains \( R \) as a subring.

**Proof.** To show that it is a ring: Associativity of \( \cdot \) is proved on page 200, and the distributive law is Ex. 26.

To show that it contains \( R \) as a subring: The map \( R \to R[x] \) given by \( a \mapsto a \) is a ring homomorphism, and is injective. \( \square \)

**Proposition.** Since \( R \) is assumed to be an integral domain, \( R[x] \) is also an integral domain.

**Proof.** The ring \( R[x] \) is commutative because \( R \) is, and it has \( 1 \neq 0 \) because \( R \) does (with the same unity element). To show that it has no zero divisors, let
\[ f = a_0 + a_1 x + a_2 x^2 + \ldots \quad \text{and} \quad g = b_0 + b_1 x + b_2 x^2 + \ldots \]
be nonzero elements of \( R[x] \). Then there are integers \( n \) and \( m \) such that \( a_n \neq 0 \) but \( a_i = 0 \) for all \( i > n \) and \( b_m \neq 0 \) but \( b_j = 0 \) for all \( j > m \). Then
\[ c_{n+m} = \sum_{i=0}^{n-1} a_i b_{n+m-i} + a_n b_m + \sum_{i=n+1}^{n+m} a_i b_{n+m-i} = a_n b_m . \]
Indeed, the first sum vanishes because \( n + m - i > m \), and therefore \( b_{n+m-i} = 0 \) for all \( i < n \); and the second sum vanishes because \( a_i = 0 \) for all \( i > n \). Therefore \( fg \neq 0 \) because its coefficient of \( x^{n+m} \) is \( a_n b_m \neq 0 \). \( \square \)

**Some Notes**

- In the definition of \( R[x] \) the book allows \( R \) to be any ring, but we are requiring \( R \) to be an integral domain.
- \( \mathbb{Q} \) is a field, but \( \mathbb{Q}[x] \) is not (\( x \) has no inverse).
- If \( a_i = 0 \) for all \( i > n \) then we may write \( a_0 + a_1 x + a_2 x^2 + \ldots \) as the finite sum \( a_0 + \cdots + a_n x^n \) or \( a_n x^n + \cdots + a_0 \).
- In algebra, we don’t have infinite sums, unless:
  1. all but finitely many of the terms are zero (so it’s really a finite sum), or
  2. there is some notion of convergence in the ring (not in Math 113).

**Polynomials in Several Variables, and Rational Functions**

**Definition.** Let \( R \) be an integral domain. For all \( n \in \mathbb{N} \), the polynomial ring \( R[x_1, \ldots, x_n] \) is defined to be \( R \) if \( n = 0 \), or \( (R[x_1, \ldots, x_{n-1}])[x_n] \) if \( n > 0 \).

**Definition.** Let \( F \) be a field and let \( n \in \mathbb{N} \). Then the **field of rational functions in \( n \) indeterminates** \( x_1, \ldots, x_n \) **over** \( F \) is the field of quotients of \( F[x_1, \ldots, x_n] \).
Clicker Questions!

Evaluation Homomorphisms

Theorem. Let \( F \leq E \) be fields, let \( \alpha \in E \), and let \( x \) be an indeterminate.
Then the map \( \phi_\alpha : F[x] \to E \) defined by
\[
\phi_\alpha(a_n x^n + \cdots + a_1 x + a_0) = a_n \alpha^n + \cdots + a_1 \alpha + a_0
\]
is a well-defined homomorphism from \( F[x] \) to \( E \). This map is called evaluation at \( \alpha \). It also satisfies (1) \( \phi_\alpha(a) = a \) for all \( a \in F \) and (2) \( \phi_\alpha(x) = \alpha \) for all \( \alpha \in E \).

Proof. (1) and (2) are clear.

Addition:
\[
\phi_\alpha \left( \sum a_i x^i + \sum b_i x^i \right) = \phi_\alpha \left( \sum (a_i + b_i) x^i \right) = \sum (a_i + b_i) \alpha^i = \sum a_i \alpha^i + \sum b_i \alpha^i
\]
\[
= \phi_\alpha \left( \sum a_i x^i \right) + \phi_\alpha \left( \sum b_i x^i \right).
\]

Multiplication: Similar but harder. □

Examples
(1). \( \phi_0 : F[x] \to F \) is \( \sum a_i x^i \mapsto a_0 \)
(2) Take \( F = \mathbb{Q} \) and \( E = \mathbb{R} \). It is a deep theorem in number theory that \( \phi_\pi : \mathbb{Q}[x] \to \mathbb{R} \) and \( \phi_\epsilon : \mathbb{Q}[x] \to \mathbb{R} \) are injective.

Polynomials vs. Functions

For us, it’s OK to write \( f(\alpha) \) instead of \( \phi_\alpha(f) \).

However: Polynomials in \( R[x] \) are not the same as functions \( R \to R \).

You know from grade school that if \( f \in \mathbb{R}[x] \) and \( \phi_\alpha(f) = 0 \) for all \( \alpha \in \mathbb{R} \) then \( f = 0 \).

But: Let \( p \) be a prime number. Then
\[
\phi_\alpha(x^p - x) = 0 \quad \text{for all } \alpha \in \mathbb{Z}_p
\]
(by Fermat). So both \( x^p - x \in \mathbb{Z}_p[x] \) and \( 0 \in \mathbb{Z}_p[x] \) give rise to the same function \( \mathbb{Z}_p \to \mathbb{Z}_p \).

Our “Basic Goal”

Definition. Let \( F \leq E \) be fields, and let \( f \in F[x] \) (with \( x \) an indeterminate).
Then a zero of \( f \) in \( E \) is an element \( \alpha \in E \) such that \( \phi_\alpha(f) = 0 \) (i.e., \( f(\alpha) = 0 \)).

The basic goal for much of the remainder of the course is:
Theorem (29.3). Let $F$ be a field. Then for any nonconstant polynomial $f \in F[x]$ there is a field $E$, containing $F$ as a subfield, such that $f$ has a zero in $E$.

Note: If $F \leq E$ and $f, g \in F[x]$ are such that their product $fg$ has a zero $\alpha \in E$, then $\alpha$ is a zero of $f$ or of $g$ (or both):

$$(fg)(\alpha) = 0 \iff f(\alpha)g(\alpha) = 0 \iff f(\alpha) = 0 \text{ or } g(\alpha) = 0.$$ 

The Degree of a Polynomial

Definition. Let $R$ be an integral domain and let $f = \sum a_i x^i \in R[x]$ be a polynomial (in one variable). Then the degree of $f$, denoted $\deg f$, is the largest integer $n$ such that $a_n \neq 0$, or $1$ if $f = 0$.

Note that $\deg(fg) = \deg f + \deg g$ for all $f, g \in R[x]$.
(The book says that $\deg f$ is undefined when $f = 0$; we are defining it to be $-\infty$.)

The Division Algorithm for $F[x]$ 

Theorem (Division Algorithm for $F[x]$). Let $F$ be a field, and let $f$ and $g$ be elements of $F[x]$ with $g \neq 0$.

Then there are unique polynomials $q, r \in F[x]$ such that

$$f = qg + r \quad \text{and} \quad \deg r < \deg g.$$ 

Proof. Existence. Write

$$f(x) = a_n x^n + \cdots + a_0$$
and $$g(x) = b_m x^m + \cdots + b_0$$

with $b_m \neq 0$ (we don’t need to assume $a_n \neq 0$ or $m > 0$).

Let $S = \{f - sg : s \in F[x]\}$ and let $r \in S$ be an element of smallest degree. Then $r = f - sg$ for some $q \in F[x]$, so $f = qg + r$, and we’ll be done if we can show that $\deg r < m$.

Suppose not. Then $r(x) = c_t x^t + \cdots + c_0$ with $c_t \neq 0$ and $t \geq m$. Also

$$f - qg - \left(\frac{c_t}{b_m}\right)x^{t-m}g = r(x) - \left(\frac{c_t}{b_m}\right)x^{t-m}g$$

$$= (c_t x^t + \cdots + c_0) - \frac{c_t}{b_m} (b_m x^t + b_{m-1} x^{t-1} + \cdots + b_0 x^{t-m})$$

$$= \left(\frac{c_t}{b_m} - b_{m-1}\right) x^{t-1} + \text{(lower-order terms)}.$$
This is an element of $S$ (with $s(x) = q(x) - (c_t/b_m)x^{t-m}$) of degree $< t$, contradicting the choice of $r(x)$.

Therefore we have $q$ and $r$ with $\deg r < m$.

Uniqueness. See book. \hfill \Box

**Example.** Long division of $x^2 + x + 1$ by $x - 2$ (on board).

**Definition.** Let $F$ be a field and let $f, g \in F[x]$. Then we say that $f \mid g$ (f divides g) if $f \cdot q = g$ for some $q \in F[x]$.

If $f \neq 0$ then $f \mid g$ is equivalent to $g/f \in F[x]$. In the context of the division algorithm, $f \mid g$ if and only if the division algorithm gives $g = qf + r$ with $r = 0$.

**Corollary** (of the Division Algorithm). Let $f \in F[x]$ and let $a \in F$. Then $a$ is a zero of $f$ if and only if $(x - a) \mid f$.

**Proof.** There exist $q, r \in F[x]$ such that $f(x) = q(x)(x - a) + r(x)$ and $\deg r < 1$. Since $\deg r < 1$, $r$ is a constant $c$. Then

$$c = r(a) = f(a) - q(a)(a - a) = f(a) - q(a) \cdot 0 = f(a).$$

So $f(a) = 0$ if and only if $r = 0$, if and only if $(x - a) \mid f$. \hfill \Box