KTH Teknikvetenskap

# SF2729 GROUPS AND RINGS
# LECTURE NOTES
# 2010-03-30

SANDRA DI ROCCO

## CONTENTS



## 2. POLYNOMIALS

2.1. **Last time.** Last time we used the fact that he number of nonzero elements in $\mathbb{Z}_n$ that are not zero divisors are exactly the number of invertible elements. We have already observed that invertible elements cannot be zero divisors. It is in fact true that:

**Theorem 2.1.** *Let $R$ be a FINITE ring. Then every non zero element which is not a zero divisor is invertible*

*Proof.* Let $0 \neq r \in R$, notice that the multiplication morphism $r\cdot : R \to R$ is a group homomorphism of abelian group, because $R$ is a ring. This morphism is injective if $r$ is not a zero divisor. In this case, because $R$ is finite it is an isomorphism and thus there is $r_1$ such that $r \cdot r_1 = 1_R$. □

Observe that the same is true if $R$ is a vector space over a field (ex $M_2(\mathbb{R})$). Remember that we have observed that every Field is an integral domain. From what proven above it follows that every finite integral domain is a field.

2.2. **The field of fractions.** There are many integral domains which are not fields ($\mathbb{Z}$ for example). The following constraction gives a way of building a field $Q(D)$ from an integral domain $D$. A field that contains $R$ and is "generated by "$D$ in the sense that every elemnt of $Q(D)$ is of the form $x/y$ for some element $x, y \in D$.

Consider the set:

$$\Omega = \{(a, r) \in D \times D : r \neq 0\},$$

one which we define the following relation:

$$(a, r) \sim (b, s) \Leftrightarrow a \cdot s = b \cdot r.$$

This relation defines an equivalence relation, in fact:

- It is reflexive: $(a, r) \sim (a, r) \Leftrightarrow a \cdot r = a \cdot r$.
- It is symmetric: if $(a, r) \sim (b, s)$ i.e. $a \cdot s = b \cdot r$ then $b \cdot r = a \cdot s$. i.e. $(b, s) \sim (a, r)$.
- It is transitive: if $(a, r) \sim (b, s)$ and $(b, s) \sim (c, t)$ i.e. $a \cdot s = b \cdot r$ and $b \cdot t = c \cdot s$, then, *because the multiplication is commutative*,

$$a \cdot t \cdot s = a \cdot s \cdot t = b \cdot r \cdot t = r \cdot b \cdot t = r \cdot c \cdot s = c \cdot r \cdot s$$

which implies that $(a \cdot t - c \cdot r) \cdot s = 0$ and thus $a \cdot t - c \cdot r$ since $s \neq 0$.

Let $Q(D)$ the set of equivalence classes and let $\frac{a}{r}$ denote the class $[(a, r)]$. We will now define two binary operations on $Q(D)$.

$$\frac{a}{r} + \frac{b}{s} = \frac{a \cdot s + b \cdot r}{r \cdot s}, \frac{a}{r} \cdot \frac{b}{s} = \frac{a \cdot b}{r \cdot s}$$

Note that $r \cdot s \neq 0$ *because $D$ is a domain.*

In order to make sure that this operations are well defined we have to show that they do not depend on the class representative. Let

$$\frac{a}{r} = \frac{a'}{r'} \text{ and } \frac{b}{s} = \frac{b'}{s'}.$$

This means that $a \cdot r' = a' \cdot r$ and $b \cdot s' = b' \cdot s$. It follows that:

$$(a' \cdot s' + b' \cdot r') \cdot r \cdot s = a' \cdot s \cdot r \cdot s' + b' \cdot r' \cdot r \cdot s = (a' \cdot r) s' \cdot s + (b' \cdot s) r' \cdot r = a \cdot r' \cdot s' \cdot s + b \cdot s' \cdot r' \cdot r = (a \cdot s + b \cdot r) \cdot r' \cdot s',$$

which implies that

$$\frac{a' \cdot s' + b' \cdot r'}{r' \cdot s} = \frac{a \cdot s + b \cdot r}{r \cdot s}.$$

Similarly for the multiplication.

It is straight forward to see (EXERCISE) that with this two operations $Q(D)$ is a commutative ring, where $0 = [(0, 1)] = \frac{0}{1}, 1 = [(1, 1)]$.

Notice that any element $\frac{a}{b} \neq 0$, i.e. where $a \neq 0$, has $\frac{b}{a}$ as multiplicative inverse. This proves that $Q(D)$ is a field.

[EXERCISE] Show that $S = \{[(a, 1)], a \in D\} \subset Q(D)$ is a subring and that the map $i : S \to D$, assigning $i([a, 1]) = a$, is a ring-isomorphism.

**Example 2.2.**
- $Q(\mathbb{Z}) = \mathbb{Q}$.
- $Q(F) = F$ if $F$ is a field. [EXERCISE]

We can conclude that the field $Q(D)$ contains $D$ as a subring (subdomain). The following theorem shows that such a field is *unique* and it is the *minimal such*.

**Theorem 2.3.** *Let $D$ be an integral domain and let $F$ be a field containing $D$. Then there exists $\phi : Q(D) \to F$ that gives an isomorphism of $Q(D)$ with a subfield of $F$ and such that $\phi([a,1]) = a$ for all $a \in D$.*

*Proof.* We start defining the map with $\phi([a,1]) = \phi(a) = a$, i.e. $\phi|_D = id_D$, and then with $\phi([a,b]) = [\phi(a), \phi(b)]_F$. Notice that since $b \neq 0$, then it is $\phi(b) \neq 0$ and that if $[a,b] = [a',b']$, i.e. $ab' = a'b$ then $\phi(ab') = \phi(a)\phi(b') = \phi(a'b) = \phi(a')\phi(b)$ which implies $[\phi(a), \phi(b)]_F = [\phi(a'), \phi(b')]_F$. The morphism is then well defined.

$$\phi(\frac{a}{r} + \frac{b}{s}) = \phi(\frac{as+br}{rs}) = [\phi(as+br), \phi(rs)]_F =$$

$$= [\phi(a)\phi(r) + \phi(b)\phi(r), \phi(r)\phi(s)]_F = [\phi(a), \phi(r)]_F + [\phi(b), \phi(s)]_F = \phi(\frac{a}{r}) + \phi(\frac{b}{s}).$$

Similarly with the multiplication. This shows that $\phi$ is a ring-homomorphism. To see that is is one-to-one note that $\phi(\frac{a}{r}) = \phi(\frac{b}{s})$ if and only if $[\phi(a), \phi(r)] = [\phi(b), \phi(s)]$, i.e. $\phi(a)\phi(s) = \phi(as) = \phi(b)\phi(r) = \phi(br)$ which implies that $\frac{a}{r} = \frac{b}{s}$ since $\phi$ is the identity on $D$. □

So $Q(D)$ can be thought as the "smallest" field containing $D$.

### 2.3. **One more example: the ring of polynomials.**

**Definition 2.4.** Lt $R$ be a ring. A polynomial in the variable $x$ with coefficients in $R$ is an expression of the form:

$$p(x) : a_0 + a_1x + \ldots + a_nx^n,$$

where $a_1 \in R$. Equivalently $p(x) = \sum_0^\infty a_ix^i$, where $a_i = 0$ for all but a finite number of $i$. This means that there is a positive integer $n$ such that $a_i = 0$ for all $i > n$.

We say that the $a_i$s are the coefficients of $p$.

Two polynomials $\sum a_ix^i, \sum b_ix^i$ are equal if nd only id $a_i = b_i$ for all $i$.

The degree of $0 \neq p(x) = \sum a_ix^i$ is $\deg(p(x)) = n$ if $n$ is the largest integer such that $a_n \neq 0_R$. Notice that the degree is not defined for the trivial polynomial, i.e. if $a_i = 0$ for all $i$.

We will denote the set of polynomials in $x$ and coefficients in $R$ with $R[x]$. We can define two binary operations:

$$\sum a_ix^i + \sum b_ix^i = \sum(a_i + b_i)x^i$$

$$\sum_0^\infty a_ix^i \cdot \sum_0^\infty b_ix^i = \sum_{k=0}^\infty (\sum_{i,j\, i+j=k} a_ib_j)x^k$$

The trivial polynomial is the additive unity and the polynomial $1_R$ is the multiplicative unity.

**Remark 2.5.**
- One sees that $R[x]$ is ring, with unity if $R$ has a multiplicative unity and commutative if and only if $R$ is commutative.

- Moreover $R \subset R[x]$ is a subring and $R[x]$ is an integral domain if $R$ is an integral domain. In this case it holds that:

$$\deg(f \cdot g) = deg(f) + \deg(g).$$

**Example 2.6.** $\mathbb{R}[x]$ and $\mathbb{C}[x]$ are integral domains.

Notice that one can define inductively $R[x_1, \dots, x_m] = R[x_1, \dots, x_{m-1}][x_m]$.

### 2.4. **evaluation at subfields.**

**Definition 2.7.** Let $(F, +, \cdot)$ be a field, $E \subset F$ is a *subfield* if $(E, +, \cdot)$ is a field.

For every $a \in F$, the *evaluation morphism* is defined as:

$$ev_a : F[x] \to F, ev_a(\sum a_i x^i) = \sum a_i a^i.$$

It is a ring homomorphism:

$$ev_a(\sum_0^\infty a_i x^i \cdot \sum_0^\infty b_i x^i) = ev_a(\sum_{k=0}^\infty (\sum_{i,j\, i+j=k} a_i b_j) x^k) = \sum_{k=0}^\infty (\sum_{i,j\, i+j=k} a_i b_j) a^k =$$

$$= \sum_0^\infty a_i a^i \cdot \sum_0^\infty b_i a^i = ev_a(\sum_0^\infty a_i x^i) \cdot ev_a(\sum_0^\infty b_i x^i).$$

Let $E$ be a subfield, then for every $e \in F$ then one can define:

$$ev_e : E[x] \to F$$

which is a ring-homomorphism such that $ev_a(x) = a$ and $ev_a(b) = b$ for all $b \in E$.

This gives a way of defining what we mean by a "zero" of a polynomial:

**Definition 2.8.** Let $E$ be a subfield of $F$ and let $\alpha \in F$. We say that $\alpha$ is a zero (in $F$ ) of a polynomial $p(x) \in E[x]$ if $ev_\alpha(f(x)) = 0_F$.

**Example 2.9.** We all know that the polynomial $p(x) = x^2 + 1 \in \mathbb{R}[x]$ has no zeroes in $\mathbb{R}$ but it does in $\mathbb{C}$. In fact if

$$ev_i : \mathbb{R}[x] \to \mathbb{C},$$

then $ev_i(x^2 + 1) = i^2 + 1 = 0$. The same happens for $-i$.

**Example 2.10.** Let $K$ be a field. the field of fraction of $K[x]$ is usually denoted by

$$K(x) = \{\frac{f(x)}{g(x)}, g(x) \neq 0\}.$$

2.5. **factorization.** Observe that if a plynomial $p(x) \in E[x]$ can be written as $p(x) = f(x)g(x)$, then

$$ev_\alpha(p(x)) = ev_\alpha(f(x))ev_\alpha(g(x))$$

and thus $\alpha$ is a zero of $p$ if and only if it is a zero of $f$ or $g$. This is one of the reasons why it is convenient to be able to factor polynomials.

**Theorem 2.11** (division algorithm)**.** *Let $F$ be a filed and let $f(x), g(x) \in F[x]$, with $\deg(g(x)) > 0$. Then there are unique polynomials $q(x), r(x) \in F[x]$ such that*

$$f(x) = g(x)q(x) + r(x),$$

*where $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$. The prove is in the book pg. 210.*

In practice one performs long divisions of polynomials as we are used to (when $F = \mathbb{R}$.)

**Theorem 2.12.** *A non zero polynomial $f(x) \in F[x]$ with $\deg(f(x)) = n$ has at most $n$ zeroes in the field $F$.*

*Proof.* Observe that an element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $f(x) = (x-a)g(x)$. Assume that $a \in F$ is a zero of $f(x)$. In fact by the factorization theorem we can factor:

$$f(x) = (x-a)g(x) + r(x), \deg(r(x)) < 1.$$

It follows that $0 = f(a) = 0 + r(x)$ and thus $f(x) = (x-a)g(x)$, because the evaluation morphism is a ring-homomorphism.

Let $a_1, \ldots a_s$ be the zeroes of $f$, then

$$f(x) = (x-a_1)\ldots(x-a_r)g(x)$$

For the degree reasons and because $F[x]$ is an integral domain it is $r \leq n$. □

EXERCISE Show that any finite subgroup of the group $F^*$ is cyclic for a finite field $F$.

**Definition 2.13.** A non constant polynomial $f(x) \in F[x]$ is irreducible over $F$ if it cannot be factored as a product of two polynomials of lower degree:

$$f(x) = g(x)h(x),$$

where $g(x), h(x) \in F[x]$.

**Example 2.14.** $x^2 + 1$ is irreducible over $\mathbb{R}$ and it is reducible over $\mathbb{C}$.

There is a special relation between $\mathbb{Z}$ and $\mathbb{Q}$ :

**Theorem 2.15.** *A polynomial $f(x) \in \mathbb{Z}[x]$ factors as $f(x) = g(x)h(x)$ in $\mathbb{Q}[x]$, with $\deg(f) = r, \deg(g) = s$ if and only if it factors as $f(x) = g'(x)h'(x)$ in $\mathbb{Z}[x]$, with $\deg(f') = r, \deg(g') = s$.*

A consequence of this is the so called *Eisenstein Criterion*:

**Theorem 2.16.** *Let $p$ be a prime and let $f(x) = a_nx^n + \ldots + a_0 \in \mathbb{Z}[x]$, with $a_n \not\equiv_p 0$ and $a_i \equiv_p 0$ for all $i < n$, $a_0 \not\equiv_{p^2} 0$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

*Proof.* It is a direct consequence of the previous theorem that if a polynomial $f(x) \in \mathbb{Z}[x]$ with $a_0 \neq 0$ has a zero in $\mathbb{Q}$ then it has a zero in $\mathbb{Z}$ that must divide $a_0$.

Assume that $f(x) = (b_r x^r + \ldots b_0) \cdot (k_s x^s + \ldots k_0)$, then because $b_0 k_0 = a_0 \not\equiv_{p^2} 0$, $b_0, k_0$ cannot be congruent modulo $p$ at the same time, say $b_0 \not\equiv_p 0$ or $k_0 \equiv_p 0$. Moreover $a_n = b_r k_s \not\equiv_p 0$ implies $b_r, k_s \not\equiv_p 0$. Let now $t$ be the smallest value so that $k_t \not\equiv_p 0$. This implies that $a_t \not\equiv_p 0$ and thus $t = n$ which is a contraddiction. □

EXERCISE. Use induction to prove that **every polynomial in $\mathbb{Z}[x]$ factors in a product of irreducible polynomials, uniquely determined except for the order and up to non zero constants.**

## RECOMMENDED EXCERCISES

**IV-21 Fields of quotients and Integral domains.** 12,14,16.

**IV-22 Rings of Polynomials.** 24,25,26

**IV-23 Factorization of polynomials.** 9-11,18-21,26,34,35,37.

---