# Some slides for 6th Lecture, Algebra 2

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

21-02-2012

# Divisibility and greatest common divisor in a domain

We assume from now on that $R$ is a domain.

Suppose that $x, y \in R$. If $x = ry$ for some $r \in R$, we say that $y$ is a divisor of $x$ and we denote it by $y|x$

- $y|x$ if and only if $\langle x \rangle \subset \langle y \rangle$.
- If $x = uy$, where $u \in R^*$, then $\langle x \rangle = \langle y \rangle$.
- If $\langle x \rangle = \langle y \rangle$, then $x = ry$ and $y = sx$ for some $s, r$. Therefore $x = (rs)x$ and $rs = 1$. This implies that $r, s \in R^*$ and there exists $u \in R^*$ s.t. $x = uy$ and we say that $x$ and $y$ are associated elements of $R$.

An element $d \in R$ is a greatest common divisor of $a, b \in R$ if $d$ is a common divisor of $a$ and $b$ and every common divisor of $a$ and $b$ divides $d$.

Let $R$ be a principal ideal domain. We know that for every $a, b \in R$ there is $d \in R$ s.t.

$$\langle a, b \rangle = \langle d \rangle$$

What is $d$?, $d$ is the greatest common divisor of $a$ and $b$.

Proof:

- $d$ is a common divisor of $a$ and $b$ since $\langle a \rangle \subset \langle d \rangle$ and $\langle b \rangle \subset \langle d \rangle$
- If $e$ is a common divisor of $a$ and $b$, then $\langle e \rangle \supset \langle a, b \rangle = \langle d \rangle$. That is $e$ divides $d$.

$r \in R \setminus R^*$ is called irreducible if $r = ab$ for $a, b \in R \Rightarrow a$ or $b$ is a unit.

Remark: $r$ irreducible, $u$ unit $\Rightarrow$ $ur$ is irreducible.

$x \in R \setminus R^*$ has factorization into irreducible elements if: there exists $p_1, \ldots, p_r \in R$ irreducible such that

$$x = p_1 \cdots p_r$$

$x$ has a unique factorization into irreducible elements if for any other factorization

$$x = q_1 \cdots q_s$$

for every $i = 1, \ldots, s$, $p_i | q_j$ for some $j$, that is, $pi = uq_j$, with $u$ unit (and one says that $p_i$ and $q_j$ are related).

According to the book, the fact that $r = s$ is a consequence of the definition (by applying Prop. 3.1.3). However, the usual definition is:

$x$ has a unique factorization into irreducible elements if for any other factorization

$$x = q_1 \cdots q_s$$

$r = s$ and for every $i = 1, \ldots, s$, $p_i | q_j$ for some $j$, that is, $pi = uq_j$, with $u$ unit (and one says that $p_i$ and $q_j$ are related).

A domain $R$ such that every non-zero element in $R \setminus R^*$ has unique factorization into irreducible elements is called a unique factorization domain (or factorial ring).

The uniqueness part is usually hard to verify. One uses proposition 3.5.3 to check this.

A non-zero element $p \in R \setminus R^*$ is called prime element if $p|xy$ for $x, y \in R$ implies that $p|x$ or $p|y$

**Proposition 3.5.2**

A prime element is irreducible

**Proposition 3.5.3**

Let $R$ be a ring for which every non-zero element $x \in R \setminus R^*$ has a factorization into irreducible elements. Every irreducible element is a prime element in $R$ if and only if $R$ is a unique factorization domain.

Proof:
$\Longrightarrow$ The proof is the same as the unique factorization for integers (Theorem 1.8.5)

$\Longrightarrow$ The proof is the same as the unique factorization for integers (Theorem 1.8.5). Assume every irreducible element is a prime.

- Suppose that $x \in R$ is a non-zero element with two factorizations

$$x = p_1 \cdots p_r = q_1 \cdots q_s$$

  into irreducible elements .
- If an irreducible factor associated with a $p_j$ appears on the right hand side for some $q_j$, we divide both sides by $p_j$.
- We can therefore assume from the beginning that the left and right hand side of the above equation have no associated irreducible elements in common and $r \geq 1$ and $s \geq 1$.
- Now, since $p_1$ is a prime element, it follows that $p_1 | q_j$ for some $j$. However, this can only happen if $p_1$ and $q_j$ are associated, contradiction.

Proof: $\Longleftarrow$ Assume $R$ is a unique factorization domain.

- Let $p \in R$ irreducible and suppose $p \mid ab$, with $a, b \in R$. We win if we show that $p \mid a$ or $p \mid b$.
- Assume $ab \neq 0$, then $a = q_1 \cdots q_s$ and $b = q'_1 \cdots q'_{s'}$ have factorizations into irreducible elements.

$$p \mid q_1 \cdots q_s q'_1 \cdots q'_{s'}$$

- Because of unique factorization, one of these factorizations must contain an irreducible element divisible by $p$ and the proof holds.

Example:

- $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}, a, b \in \mathbb{Z}\} \subset \mathbb{C}$
- $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$
- 2 is irreducible but not prime

**Lemma 3.5.5**

Let $R$ be a principal ideal domain and $r$ a non-zero element such that $r \notin R^*$. Then $r$ has an irreducible factorization.

## Proposition 3.5.6

Suppose that $R$ is a principal ideal domain that is not a field. An ideal $\langle x \rangle$ is a maximal ideal if and only if $x$ is an irreducible element in $R$.

Proof: $\Longleftarrow$

- $x$ irreducible and $\langle x \rangle \subset \langle y \rangle$ then $x = ys$ for some $s \in R$.
- Then $s$ or $y$ is a unit. That is, $\langle y \rangle = \langle x \rangle$ or $\langle y \rangle = R$ and $\langle x \rangle$ is maximal.

Proof: $\Longrightarrow$

- $\langle x \rangle$ is a maximal ideal and $x = ys$, $y, s \in R$
- Then one of $y$ or $s$ is a unit because in other case:
  - $\langle x \rangle \subsetneq \langle y \rangle$, since $s$ is not a unit.
  - $\langle y \rangle \subsetneq R$, since $y$ is not a unit.
- Contradiction: $\langle x \rangle$ is a maximal ideal

## Theorem 3.5.7

A principal ideal domain $R$ is a unique factorization domain.

Proof:

- Consider the factorization of the previous lemma. We should just prove that it is unique.
- But we are not going to prove it. We are going to prove that the irreducible elements are prime.
- $\pi \in R$ irreducible s.t. $\pi | ab$ but $\pi \nmid a$. Does $\pi | b$?
- $\langle \pi \rangle \subsetneq \langle \pi, a \rangle$, since $a \notin \langle \pi \rangle$
- Since $\langle \pi \rangle$ is maximal (previous prop) we have $\langle \pi, a \rangle = R$. Therefore, $x\pi + ya = 1$ for some $x, y$
- Then $xb\pi + yab = b$ and since $\pi | ab$ we have that $\pi | b$

Example:

- $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5}, a, b \in \mathbb{Z}\} \subset \mathbb{C}$
- $\mathbb{Z}[\sqrt{-5}]$ is not a principal ideal domain since 2 is an irreducible element that is not prime.
- Actually we can give a non-principal ideal $I = \langle 2, 1 + \sqrt{-5} \rangle$

# Computing the GCD from prime factorizations

Let $R$ be a unique factorization domain and there are prime elements $p_1, \ldots, p_n$ that are pair-wise non-associated such that

$$a = up_1^{r_1} \cdots p_n^{r_n}$$

$$b = vp_1^{s_1} \cdots p_n^{s_n}$$

where $r_i, s_i \geq 0$, $u, v$ are units and $p_1, \ldots, p_n$ are pairwise non-associated.

Then

$$\gcd(a, b) = p_1^{t_1} \cdots p_n^{t_n},$$

where $t_i = \min(r_i, s_i)$

What about the Euclidean algorithm?