Some slides for 17th Lecture, Algebra

Diego Ruano

Department of Mathematical Sciences
Aalborg University
Denmark

18-11-2010

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

$$a = u p_1^{r_1} \cdots p_n^{r_n}$$

$$b = v p_1^{s_1} \cdots p_n^{s_n}$$

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?

Euclidean domains

A domain R is called Euclidean if there exists a Euclidean function $N : R \setminus \{0\} \to \mathbb{N}$.

A Euclidean function satisfies that for every $x \in R, d \in R \setminus \{0\}$, there exists $q, r \in R$ s.t.

$$x = qd + r$$

where either $r = 0$ or $N(r) < N(d)$

Proposition 3.5.9

A Euclidean domain is a principal ideal domain.

$\langle a, b\rangle = \langle \gcd(a, b)\rangle$

How do we compute $\gcd(a, b)$? In the same way as for integers!

Remark 3.5.10

There are principal ideal domains that are not Euclidean domains, for instance $\mathbb{Z}[\xi] = \{a + b\xi : a, b \in \mathbb{Z}\}$, where $\xi = (1 + \sqrt{-19})/2$.

Recall:

- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
- $N(\pi) = |\pi|^2 = \pi\overline{\pi} = (a + bi)(a - bi) = a^2 + b^2$

$\mathbb{Z}[i]$ is a Euclidean domain.

- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
- $N(\pi) = |\pi|^2 = \pi\overline{\pi} = (a + bi)(a - bi) = a^2 + b^2$
- $5 = (1 + 2i)(1 - 2i)$, 5 is not prime.

Proposition 3.5.11

Let $\pi = a + bi \in \mathbb{Z}[i]$ be a Gaussian integer with $N(\pi) = p$, where p is a prime integer. Then π is a prime element in $\mathbb{Z}[i]$.

Proof:

- We have already seen that $\mathbb{Z}[i]$ is a principal ideal domain (Theorem 3.1.11).
- In a unique factorization domain every irreducible element is prime (Prop. 3.5.3).
- We may check that π is irreducible.
- If $\pi = ab$ then $p = N(\pi) = N(a)N(b)$.
- Therefore, $N(a) = p$ (wlog) and $N(b) = 1$. Hence b is a unit and π irreducible.

Interesting applications of $\mathbb{Z}[i]$ in pages 133 to 138, but we will concentrate in a special ring: Polynomials

Let R be a ring and $R[\mathbb{N}]$ the set of functions $f : \mathbb{N} \to R$ such that $f(n) = 0$ for n large enough. Think in $f(i)$ as the coefficient of X^i

Given $f, g \in R[\mathbb{N}]$ we define $+$ and $\cdot$

$$(f+g)(n) = f(n) + g(n)$$

$$(fg)(n) = \sum_{i+j=n} f(i)g(j)$$

where $i, j \in \mathbb{N}$

We denote by $X^i \in R[\mathbb{N}]$ the function with $X^i(i) = 1$ and $X^i(n) = 0$ if $n \neq i$

Notice that: $X^i X^j = X^{i+j}$

We view an element of $a \in R$ as the function with $a(0) = a$ and $a(n) = 0$ if $n > 0$.

So an element $f \in R[\mathbb{N}]$ can be written as

$$f = a_0 + a_1 X + \cdots + a_n X^n$$

were $a_i = f(i)$ and $f(i) = 0$ if $i > n$.

- 0 is the neutral element for the sum
- $1 = X^0$ is the neutral element for multiplication
- $fg = gf$
- $f(g+h) = fg + fh$
- $f(gh) = (fg)h$

Definition 4.1

We define $R[X]$ the polynomial ring in one variable over the ring R as $R[\mathbb{N}]$. Here X denotes the function X^1.

Concepts: Term, coefficient, degree, leading term, leading coefficient, monic polynomial.

Proposition 4.2.2

Let $f, g \in R[X] \setminus \{0\}$. If the leading coefficient of f or g is not a zero divisor then

$$\deg(fg) = \deg(f) + \deg(g)$$

$2X + 1$ is a unit in $\mathbb{Z}/4\mathbb{Z}[X]$, but in a domain the units have degree 0:

Proposition 4.2.3

Let R be a domain. Then $R[X]^* = (R[X])^* = R^*$