MATH3030 Tutorial 10-11

J. SHEN

23 November, 2023

10 Factorization in $\mathbb{Z}[i]$

10.1 Factorization, PID and UFD

We record here some relations among prime elements, irreducible element, prime ideals, and maximal ideals.

Proposition 10.1. *Let R be an integral domain. Let $r \in R$,*

$$\begin{tikzcd}
\text{1. } r \text{ is irreducible.} & \text{2. } r \text{ is a prime element.} \arrow[l, Rightarrow] \arrow[d, Leftrightarrow] \\
\text{4. } (r) \text{ is a maximal ideal.} \arrow[r, Rightarrow] & \text{3. } (r) \text{ is a prime ideal.}
\end{tikzcd}$$

When R is a PID, $1 \implies 4$, and so the four statements 1-4 are all equivalent.

An integral domain R is called a unique factorization domain (UFD) if
(U1) Any element in $R - (R^\times \cup \{0\})$ is a product of irreducible elements.
(U2) The factorization is unique up to associates and reordering.

Proposition 10.2. (a) *Condition (U1) is equivalent to ACCPI: If $(a_1) \subseteq (a_2) \subseteq \ldots \subseteq (a_n) \subseteq \ldots$, then there exists some n such that $(a_n) = (a_{n+1}) = \ldots$*

(b) *Under (U1), (U2) is equivalent to $1 \implies 2$ in proposition 9.2, that is, any irreducible element is a prime.*

(c) *Any PID is a UFD.*

10.2 Euclidean domains, Gaussian integers

An integral domain R is called an Euclidean domain (ED) if there is a size function $\sigma : R - \{0\} \to \mathbb{Z}_{\geq 0}$ on R such that the division with remainder is possible in the following sense:
(ED1) Let $a, b \in R$ with $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\sigma(r) < \sigma(b)$.
(ED2) When $a \neq 0$, $\sigma(ab) \geq \sigma(b)$.

Artin's definition does not require (ED2), which is included for discussion of units.

Proposition 10.3. *Any ED is a PID.*

Examples. $\mathbb{Z}$ is an ED with $\sigma(n) = |n|$.
$\mathbb{F}[x]$ is an ED with $\sigma(f) = \deg(f)$.
Recall the definition the ring of Gaussian integers $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$.

Proposition 10.4. $\mathbb{Z}[i]$ *is an ED with* $\sigma(a) = |a|^2$ *for any* $a \in \mathbb{Z}[i]$.

10.3 Factorization in $\mathbb{Z}[i]$

We characterize units and prime (irreducible) elements in $\mathbb{Z}[i]$.

Proposition 10.5. (a) *Units in $\mathbb{Z}[i]$ are $\pm 1, \pm i$.*

(b) *If $a \in \mathbb{Z}[i]$ is a prime element, then either a is associate to an integer prime, or $a\bar{a}$ is an integer prime.*

(c) *Let p be an integer prime, then either p remains a prime in $\mathbb{Z}[i]$, or p factors into $\pi\bar{\pi}$ for some prime $\pi \in \mathbb{Z}[i]$.*

(d) *An integer prime p remains a prime in $\mathbb{Z}[i]$ exactly when $p \equiv 3 \pmod 4$, and p factors in $\mathbb{Z}[i]$ exactly when $p = 2$ or $p \equiv 1 \pmod 4$.*

Therefore, up to associates, we can list all primes in $\mathbb{Z}[i]$ as $\{3, 7, 11, 19, ...\} \cup \{1+i, 2+i, 2-i, 3+2i, 3-2i, ...\}$.

Corollary. *An integer prime p can be written as $a^2 + b^2$ for some $a, b \in \mathbb{Z}$ exactly when $p = 2$ or $p \equiv 1 \pmod 4$.*

10.4 Using Gauss's Lemma

Let R be a UFD. Let $F = \mathrm{Frac}(R)$. Then $\{p : p \text{ is a prime in } R[x]\} = \{p : p \text{ is a prime in } R\} \bigcup \{f : f \text{ is irreducible in } F[x], \text{ and the content } c(f) = 1\}$.

Recall that in MATH2070, we have the following tools to decide whether a polynomial f is irreducible.

(a) When $f \in \mathbb{F}[x]$, if $\deg(f) = 2$ or 3, and if f has no root in $\mathbb{F}$, then f is irreducible in $\mathbb{F}[x]$.

(b) Reduce f mod p. If $\overline{f} \in \mathbb{F}_p[x]$ is irreducible, and $\deg(f) = \deg(\overline{f})$, then f is irreducible in $\mathbb{Z}[x]$.

(c) Eisenstein's criterion. Let $f = \sum_{i=0}^{n} a_i x^i$ be primitive. Let p be a prime. Suppose $p \mid a_0, a_1, ..., a_{n-1}$, $p \nmid a_n$, and $p^2 \nmid a_0$, then f is irreducible in $\mathbb{Z}[x]$.

Note that method (b) and (c) generalize: We can replace $\mathbb{Z}$ by any UFD R, and replace $p \in \mathbb{Z}$ by a prime $p \in R$.

Exercise. (a) Factorize $x^p + y^p$ in $\mathbb{C}[x, y]$.

(b) Show that $x^p + y^p + z^p$ is irreducible in $\mathbb{C}[x, y, z]$. (Hint: Eisenstein criterion)

(c) Show that $xy + zw$ is irreducible in $\mathbb{C}[x, y, z, w]$.