Lecture 3

M. Klazar

October 21, 2025

We treat the two auxiliary results we used last time. The first one is the proof of non-vanishing of a sum by the p-adic argument. The second one is the result that the domain of Gaussian integers $\mathbb{Z}[i]_{\mathrm{do}}$ is UFD.

Properties of the p-adic order

Recall that for a prime p and $\alpha \in \mathbb{Q}$, the p-adic order $\mathrm{ord}_p(\alpha)$ of α is $+\infty$ if $\alpha = 0$, and that for $\alpha \neq 0$ it is the unique $k \in \mathbb{Z}$ such that $\alpha = p^k\beta$ where $\beta \in \mathbb{Q}$ has both numerator and denominator coprime to p.

Proposition 1. *Let $\alpha, \beta \in \mathbb{Q}$.*

1. $\mathrm{ord}_p(\alpha\beta) = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta)$.
2. $\mathrm{ord}_p(\alpha+\beta) \geq \min(\{\mathrm{ord}_p(\alpha), \mathrm{ord}_p(\beta)\})$, *with equality if* $\mathrm{ord}_p(\alpha) \neq \mathrm{ord}_p(\beta)$.

Proof. 1. Let $\alpha = p^k\alpha_0$ and $\beta = p^l\beta_0$ in $\mathbb{Q}$ be two arbitrary fractions, where $k = \mathrm{ord}_p(\alpha)$, $l = \mathrm{ord}_p(\beta)$ and the fractions α_0 and β_0 have numerators and denominators coprime to p. Then

$$\alpha\beta = p^{k+l}\alpha_0\beta_0 =: p^{k+l}\gamma$$

where the fraction γ has numerator and denominator coprime to p. Thus

$$\mathrm{ord}_p(\alpha\beta) = k + l = \mathrm{ord}_p(\alpha) + \mathrm{ord}_p(\beta\,.)$$

2. We take α and β as in 1 and assume w.l.o.g. that $k \leq l$, so that

$$k = \min(\{\mathrm{ord}_p(\alpha),\, \mathrm{ord}_p(\beta)\})\,.$$

Then

$$\alpha + \beta = p^k(\alpha_0 + p^{l-k}\beta_0) =: p^k\gamma\,.$$

If $k < l$ then γ can be written as a fraction with numerator and denominator coprime to p, so that $\mathrm{ord}_p(\alpha + \beta) = k$. If $k = l$ then γ can be written with denominator coprime to p, and it follows that $\mathrm{ord}_p(\alpha + \beta) \geq k$. $\square$

Corollary 2. *If p is a prime and $\alpha_1, \ldots, \alpha_n$ are $n \geq 2$ fractions such that*

$$\mathrm{ord}_p(\alpha_n) < \mathrm{ord}_p(\alpha_i) \text{ for every } i = 1, 2, \ldots, n-1\,,$$

then $\sum_{j=1}^{n} \alpha_j \neq 0$.

Proof. Let $k := \min(\{\mathrm{ord}_p(\alpha_i)\colon\ i = 1, \ldots, n-1\})$ ($\in \mathbb{Z} \cup \{+\infty\}$) and let $\alpha := \sum_{j=1}^{n-1} \alpha_j$. Applying repeatedly item 2 of Proposition 1 we get that $\mathrm{ord}_p(\alpha) \geq k$. Since $\mathrm{ord}_p(\alpha_n) < k$, we get by this item that

$$\mathrm{ord}_p\big(\textstyle\sum_{j=1}^{n} \alpha_j\big) = \mathrm{ord}_p(\alpha + \alpha_n) = \mathrm{ord}_p(\alpha_n) < +\infty\,.$$

Thus $\sum_{j=1}^{n} \alpha_j \neq 0$. □

UFD = unique factorization domain

We define unique factorization domains. Recall that an *(integral) domain*

$$R_{\mathrm{do}} = \langle R,\, 0_R,\, 1_R,\, +,\, \cdot\rangle$$

is a commutative ring with 1_R such that for every $a, b \in R^* = R \setminus \{0_R\}$ also $ab \neq 0_R$. If $a, b \in R$, we say that *a divides b (in R_{do})*, written $a \,|\, b$, if $b = ac$ ($= a \cdot c$) for some $c \in R$. We say that $a \in R$ is a *unit* if $a \,|\, 1_R$ (i.e., a is multiplicatively invertible). The set of units in R_{do} is denoted by $R^\times$. It is easy to see that

$$\langle R^\times,\, 1_R,\, \cdot\rangle$$

is an Abelian group, the *group of units* of R_{do}. For $a, b \in R$ we write $a \sim b$ if $a = bc$ for some $c \in R^\times$. It is easy to see that $\sim$ is an equivalence relation. For example, in the domain

$$\mathbb{Z}_{\mathrm{do}} = \langle \mathbb{Z},\, 0,\, 1,\, +,\, \cdot\rangle$$

of integers we have $m \sim n$ iff $m = \pm n$. Two elements $a, b \in R$ are *coprime*, written $(a, b) = 1_R$, if they can be simultaneously divided only by units.

Let $R_{\mathrm{do}} = \langle R, 0_R, 1_R, +, \cdot\rangle$ be a domain. We say that an element $a \in R$ is *irreducible* iff $a \in R^* \setminus R^\times$ and in every decomposition

$$a = bc \text{ with } b,\, c \in R\,,$$

b or c is a unit.

Definition 3 (UFD). *We say that R_{do} is a* unique factorization domain*, or* UFD*, if every element in $R^* \setminus R^\times$ expresses as a product of irreducibles, and this product is unique up to the order of factors and the $\sim$ relation.*

So for every $a \in R^* \setminus R^\times$ there exist $m \in \mathbb{N}$ irreducibles $a_1, \ldots, a_m$ such that

$$a = a_1 \cdot a_2 \cdot \ldots \cdot a_m\,,$$

and if

$$a_1 \cdot a_2 \cdot \ldots \cdot a_m = b_1 \cdot b_2 \cdot \ldots \cdot b_n$$

where $m, n \in \mathbb{N}$ and every a_i and b_i is irreducible, then $m = n$ and there exists a permutation π of the numbers $1, 2, \ldots, m = n$ such that for every $i = 1, 2, \ldots, m = n$ we have

$$a_i \sim b_{\pi(i)}\,.$$

The coprime squares argument in UFD

In the next two propositions we generalize to UFD the argument used in the two previous lectures. Its simplest form is

$$a,\, b,\, c \in \mathbb{N} \wedge (a,\, b) = 1 \wedge ab = c^2 \Rightarrow a = a_0^2 \wedge b = b_0^2 \ \text{ with } \ a_0,\, b_0 \in \mathbb{N}\,.$$

Proposition 4. *Let $R_{\mathrm{do}} = \langle R, 0_R, 1_R, +, \cdot\rangle$ be* UFD*, let $a, b, c, d \in R$, let $k \in \mathbb{N}$ with $k \geq 2$ and let $(a, b) = 1_R$. Then the following holds.*

1. *If a divides bc then a divides c.*
2. *If $ab \sim c^k$ then $a \sim a_0^k$ and $b \sim b_0^k$ for some coprime $a_0, b_0 \in R$.*
3. *If c is irreducible and $ab \sim cd^k$, then $\{a, b\} \sim \{ca_0^k, b_0^k\}$ for some coprime $a_0, b_0 \in R$.*

Proof. 1. If $c = 0_R$ then $a \,|\, c$. If $b = 0_R$, then $a \in R^\times$ and again $a \,|\, c$. We assume that $b, c \neq 0_R$. Hence also $a \neq 0_R$ and we write the three elements as (possibly empty) products

$$a = a_1 \cdot \ldots \cdot a_l,\ \ b = b_1 \cdot \ldots \cdot b_m \ \text{ and } \ c = c_1 \cdot \ldots \cdot c_n$$

of irreducibles a_i, b_i and c_i. Here $l, m, n \in \mathbb{N}_0$ and if $l = 0$ then a is a unit, and similarly for m and n. It is easy to see that if $l = 0$ or $n = 0$ then the claim holds. We assume that $l, n \geq 1$. By the assumption $bc = ad$ for some $d \in R^*$. Considering the irreducible factorization of d and using that R_{do} is UFD and $(a, b) = 1_R$, we see that there is an injection $f\colon [l] \to [n]$ such that

$$a_i \sim c_{f(i)} \ \text{ for } \ i \in [l]\,.$$

Hence $a \sim \prod_{i=1}^{l} c_{f(i)}$ and $a \,|\, c$.

2. It is easy to see that the claim holds if $c = 0_R$. Thus we assume that $a, b, c \neq 0_R$ and write them as products of irreducibles a_i, b_i and c_i as in 1. We get the relation

$$\textstyle\prod_{i=1}^{l} a_i \cdot \prod_{i=1}^{m} b_i \sim \prod_{i=1}^{n} c_i^k\,.$$

If $l = 0$ then $a \in \mathbb{R}^\times$ and we have $a = a \cdot 1_R^k$ and $b \sim a^{-1} \cdot c^k$. Similarly if $m = 0$. Thus we assume that $l, m \geq 1$. Since a and b are coprime and R_{do} is UFD, every product of k irreducibles $c_i^k = c_i \cdot \ldots \cdot c_i$ is completely contained (up to the $\sim$ relation) among the a_is or among the b_is, and every a_i and b_i is $\sim$ to some c_i. The claim follows.

3. An exercise for the interested reader. $\square$

Proposition 5. *Let $R_{\mathrm{do}} = \langle R, 0_R, 1_R, +, \cdot\rangle$ be* UFD. *If $a, b, c, d \in R$ and $k \in \mathbb{N}$ with $k \geq 2$ are such that c is irreducible and divides both a and b, but this is not true for c^2 nor for any other irreducible different from c, and $ab \sim d^k$, then*

$$\{a,\, b\} \sim \{ca_0^k,\, c^{k-1}b_0^k\}$$

for some coprime $a_0, b_0 \in R$.

Proof. An exercise for the interested reader. $\square$

Units in Gaussian integers

We find units in the domain $\mathbb{Z}[i]_{\mathrm{do}}$. Recall that

$$\mathbb{Z}[i]_{\mathrm{do}} = \langle \mathbb{Z}[i],\, 0,\, 1,\, +,\, \cdot\rangle\,,$$

is the domain of Gaussian integers.

Proposition 6. $\mathbb{Z}[i]^{\times} = \{-1, 1, -i, i\}$.

Proof. Consider the map $f\colon \mathbb{Z}[i] \to \mathbb{N}_0$ that is for $\alpha = a + bi \in \mathbb{Z}[i]$ defined by

$$f(\alpha) := \alpha \cdot \overline{\alpha} = (a + bi)(a - bi) = a^2 + b^2\,.$$

Clearly, $f(\alpha\beta) = f(\alpha)f(\beta)$. Each of the four stated elements is a unit. On the other hand, if $\alpha = a + bi$ is a unit then $\alpha\beta = 1$ for some $\beta \in \mathbb{Z}[i]$ and

$$1 = f(1) = f(\alpha\beta) = f(\alpha) \cdot f(\beta) = (a^2 + b^2)f(\beta)\,.$$

Thus $a^2 + b^2 = 1$ (and $f(\beta) = 1$). Hence $a = \pm 1, b = 0$ or $a = 0, b = \pm 1$. Thus $\alpha \in \{-1, 1, -i, i\}$. $\square$

Euclidean domains

We define Euclidean domains. Recall that a linear order $\langle X, \prec\rangle$ is a well ordering if every nonempty subset of X has a minimum element.

Definition 7 (Euclidean domain). *$R_{\mathrm{do}} = \langle R, 0_R, 1_R, +, \cdot\rangle$ is an Euclidean domain iff there exists a well ordering $\langle X, \prec\rangle$ and a map*

$$f\colon R^* = R \setminus \{0_R\} \to X$$

with the property that for every $a, b \in R$ with $b \neq 0_R$ there exist $c, d \in R$ such that

$$a = bc + d \wedge (d = 0_R \vee f(d) \prec f(b))\,.$$

A prominent example of an Euclidean domain is the domain of integers. For it we have $\langle X, \prec\rangle = \langle \mathbb{N}, <\rangle$, with the standard ordering $<$ of natural numbers, and $f(n) = |n|$. We postpone the proof of the next theorem to the next lecture.

Theorem 8. *Every Euclidean domain is* UFD.

$\mathbb{Z}[i]_{\mathrm{do}}$ is Euclidean and hence UFD

Theorem 9. *The domain $\mathbb{Z}[i]_{\mathrm{do}}$ is Euclidean.*

Proof. We again take $\langle X, \prec\rangle = \langle \mathbb{N}, <\rangle$. The required map $f\colon \mathbb{Z}[i] \to \mathbb{N}_0$ is the map used in Proposition 5, $f(\alpha) = \alpha\overline{\alpha}$ (contrary to Definition 6 we allow the value $f(0) = 0$). Let $\alpha \in \mathbb{Z}[i]$ and $\beta \in \mathbb{Z}[i]^*$ be given. We define

$$\frac{\alpha}{\beta} =: u_0 + v_0 i \ \text{ with } \ u_0,\, v_0 \in \mathbb{Q}\,.$$

Let $\gamma := u + vi \in \mathbb{Z}[i]$ where $u, v \in \mathbb{Z}$ are such that

$$|u - u_0|,\ |v - v_0| \le 1/2\,.$$

Finally, $\delta := \alpha - \beta\gamma$. Then $\alpha = \beta\gamma + \delta$ and

$$\begin{aligned} f(\delta) &= f(\beta) \cdot f\big(\tfrac{\alpha}{\beta} - \gamma\big) = f(\beta) \cdot \big((u_0 - u)^2 + (v_0 - v)^2\big) \\ &\le f(\beta)(\tfrac{1}{4} + \tfrac{1}{4}) = \tfrac{f(\beta)}{2} < f(\beta)\,. \end{aligned}$$

□

Thus by Theorem 7 the domain of Gaussian integers $\mathbb{Z}[i]_{\mathrm{do}}$ is UFD and Propositions 4 and 5 hold in it.