

# MATH 601 (DUE 9/25)

HIDENORI SHINOHARA

**Exercise.** (Problem 1) Define  $\gamma : \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}[\sqrt{2}]$  by  $\gamma(a + b\sqrt{2}) = a - b\sqrt{2}$ . Show that  $\gamma$  is a ring isomorphism and compute its inverse.

*Proof.* Let  $a + b\sqrt{2}, c + d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$  be given.

$$\begin{aligned}
 \gamma((a + b\sqrt{2}) + (c + d\sqrt{2})) &= \gamma((a + c) + (b + d)\sqrt{2}) \\
 &= (a + c) - (b + d)\sqrt{2} \\
 &= (a - b\sqrt{2}) + (c - d\sqrt{2}) \\
 &= \gamma(a + b\sqrt{2}) + \gamma(c + d\sqrt{2}). \\
 \gamma((a + b\sqrt{2})(c + d\sqrt{2})) &= \gamma((ac + 2bd) + (ad + bc)\sqrt{2}) \\
 &= (ac + 2bd) - (ad + bc)\sqrt{2} \\
 &= (ac + 2(-b)(-d)) + (a(-d) + (-b)c)\sqrt{2} \\
 &= (a - b\sqrt{2})(c - d\sqrt{2}) \\
 &= \gamma(a + b\sqrt{2})\gamma(c + d\sqrt{2}).
 \end{aligned}$$

Moreover,  $\gamma(1) = 1 - 0\sqrt{2} = 1$ . Therefore,  $\gamma$  is a ring homomorphism. For any  $a + b\sqrt{2}$ ,  $\gamma(\gamma(a + b\sqrt{2})) = \gamma(a - b\sqrt{2}) = a + b\sqrt{2}$ . Therefore,  $\gamma$  has an inverse, and the inverse of  $\gamma$  is  $\gamma$ . This implies that  $\gamma$  is bijective.

In conclusion,  $\gamma$  is an isomorphism and its inverse is itself. □

**Exercise.** (Problem 2) Define  $N : \mathbb{Z}[\sqrt{2}] \rightarrow \mathbb{Z}$  by  $N(a + b\sqrt{2}) = (a + b\sqrt{2})\gamma(a + b\sqrt{2})$ . Show that  $N(\alpha\beta) = N(\alpha)N(\beta)$ .

*Proof.* Let  $a + b\sqrt{2}, c + d\sqrt{2}$  be given.

$$\begin{aligned}
 N((a + b\sqrt{2})(c + d\sqrt{2})) &= N((ac + 2bd) + (ad + bc)\sqrt{2}) \\
 &= ((ac + 2bd) + (ad + bc)\sqrt{2})\gamma((ac + 2bd) + (ad + bc)\sqrt{2}) \\
 &= (a + b\sqrt{2})(c + d\sqrt{2})\gamma((a + b\sqrt{2})(c + d\sqrt{2})) \\
 &= (a + b\sqrt{2})(c + d\sqrt{2})\gamma(a + b\sqrt{2})\gamma(c + d\sqrt{2}) \\
 &= (a + b\sqrt{2})\gamma(a + b\sqrt{2})(c + d\sqrt{2})\gamma(c + d\sqrt{2}) \\
 &= N(a + b\sqrt{2})N(c + d\sqrt{2}).
 \end{aligned}$$

□

**Exercise.** (Problem 3) Write  $\mathbb{Z}[\sqrt{2}]^*$  for the group of units in  $\mathbb{Z}[\sqrt{2}]$ . Show that  $\alpha \in \mathbb{Z}[\sqrt{2}]^*$  if and only if  $N(\alpha) = \pm 1$ .

*Proof.* We have  $N(1) = 1 \cdot \gamma(1) = 1$ .

Let  $\alpha$  be a unit and  $\beta$  be the inverse. Then  $N(\alpha\beta) = N(1) = 1$ . Thus  $1 = N(\alpha)N(\beta)$ . Since  $N(\alpha), N(\beta) \in \mathbb{Z}$ ,  $N(\alpha) = \pm 1$ .

On the other hand, suppose that  $N(\alpha) = \pm 1$  for some  $\alpha$ .

- Case 1:  $N(\alpha) = 1$ . Then  $\alpha\gamma(\alpha) = 1$ , so  $\gamma(\alpha)$  is an inverse of  $\alpha$ . Therefore,  $\alpha$  is a unit.
- Case 2:  $N(\alpha) = -1$ . Then  $\alpha\gamma(\alpha) = -1$ , so  $-\gamma(\alpha)$  is an inverse of  $\alpha$ . Therefore,  $\alpha$  is a unit.

In each case,  $\alpha$  is a unit.

Therefore,  $N(\alpha) = \pm 1$  if and only if  $\alpha$  is a unit. □

**Exercise.** (Problem 4) What does finding the units in  $\mathbb{Z}[\sqrt{2}]$  have to do with solving the equation  $x^2 - 2y^2 = \pm 1$ ?

*Proof.* Let  $(a, b)$  be a solution to the equation. Then  $a^2 - 2b^2 = \pm 1$ , so  $(a + b\sqrt{2})(a - b\sqrt{2}) = \pm 1$ . This implies that  $a \pm b\sqrt{2}$  is a unit in  $\mathbb{Z}[\sqrt{2}]$ .

On the other hand, let  $a + b\sqrt{2}$  be a unit in  $\mathbb{Z}[\sqrt{2}]$ . By Problem 3,  $N(a + b\sqrt{2}) = \pm 1$ . Thus  $\pm 1 = N(a + b\sqrt{2}) = (a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - b^2$ . Hence,  $(a, b)$  is a solution to  $x^2 - 2y^2 = \pm 1$ .

In conclusion, there exists a bijective correspondence between the units in  $\mathbb{Z}[\sqrt{2}]$  and the solutions to  $x^2 - 2y^2 = \pm 1$ . □

**Exercise.** (Problem 5) Show that  $\mathbb{Z}[\sqrt{2}]$  has no smallest positive element.

*Proof.* We have  $0 < \sqrt{2} - 1 < 1$ . Since  $\forall n \in \mathbb{N}$ ,  $(\sqrt{2} - 1)^n \in \mathbb{Z}[\sqrt{2}]$  and  $\lim_{n \rightarrow \infty} (\sqrt{2} - 1)^n = 0$ , there exists no smallest positive element in  $\mathbb{Z}[\sqrt{2}]$ . □

**Exercise.** (Problem 6) Find an element  $u \in \mathbb{Z}[\sqrt{2}]^*$  with  $u > 1$ .

*Proof.*  $(\sqrt{2} + 1)(\sqrt{2} - 1) = 2 - 1 = 1$ . Thus  $u = \sqrt{2} + 1$  is a unit such that  $u > 1$ . □

**Exercise.** (Problem 7) Let  $u \in \mathbb{Z}[\sqrt{2}]^*$  with  $u > 1$ . Write  $u = a + b\sqrt{2}$  with  $a, b \in \mathbb{Z}$ . Show  $a > 0$  and  $b > 0$ .

*Proof.* Since  $u$  is a unit,  $N(u) = \pm 1$  from Problem 3. In other words,  $(a + b\sqrt{2})(a - b\sqrt{2}) = a^2 - 2b^2 = \pm 1$ . Then  $a^2 = \pm 1 + 2b^2 \equiv 1 \pmod{2}$ , so  $a$  is odd. Specifically,  $a \neq 0$ .

- Case 1:  $a < 0$ . Since  $a$  is an integer,  $a \leq -1$ . Since  $u = a + b\sqrt{2} > 1$ ,  $b > 0$ . Since  $b$  is an integer,  $b \geq 1$ . This implies that  $a - b\sqrt{2} \leq -1 - \sqrt{2} < -1$ .

This means  $(a + b\sqrt{2})(a - b\sqrt{2}) < -1$  because  $a + b\sqrt{2} > 1$ . However, this is impossible because  $(a + b\sqrt{2})(a - b\sqrt{2}) = \pm 1$ . This is a contradiction, so  $a$  is not negative.

- Case 2:  $a > 0$  and  $b < 0$ . Since  $a, b$  are integers, this implies  $a \geq 1$  and  $b \leq -1$ . Then  $a - b\sqrt{2} \geq 1 + \sqrt{2} > 2$ . Since  $a + b\sqrt{2} > 1$ , this implies  $(a + b\sqrt{2})(a - b\sqrt{2}) > 1 \cdot 2 = 2$ . This is a contradiction because we have  $(a + b\sqrt{2})(a - b\sqrt{2}) = \pm 1$ .

Therefore, both  $a$  and  $b$  must be positive. □

**Exercise.** (Problem 8) Show that among all  $u$  satisfying the conditions of 7, there is a least element  $u_0$ . What is  $u_0$ ?

*Proof.* Since we know that  $a \geq 1$  and  $b \geq 1$ ,  $1 + \sqrt{2}$  is less than or equal to all such  $u$ . Since  $(1 + \sqrt{2})(\sqrt{2} - 1) = 1$ ,  $1 + \sqrt{2}$  is indeed a unit. Therefore,  $1 + \sqrt{2}$  is the least element in  $\mathbb{Z}[\sqrt{2}]^*$ .  $\square$