MATH 601 (DUE 9/25)

HIDENORI SHINOHARA

Exercise. (Problem 1) Define $\gamma : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}[\sqrt{2}]$ by $\gamma(a + b\sqrt{2}) = a - b\sqrt{2}$. Show that γ 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, γ 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, γ has an inverse, and the inverse of γ is γ. This implies that γ is bijective.

In conclusion, γ is an isomorphism and its inverse is itself. $\square$

Exercise. (Problem 2) Define $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ 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.

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

$\square$

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 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 $u > 1$. □