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 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 $N(1) = 1\gamma(1) = 1$.

Let α be a unit and β 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 α.

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

In each case, α is a unit.

Therefore, $N(\alpha) = \pm 1$ if and only if α 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 $\lim_{n\to\infty}(\sqrt{2} - 1)^n = 0$, 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 $\mathbb{Z}[\sqrt{2}]^*$. $\square$

Exercise. (Problem 9) Show that every element of $\mathbb{Z}[\sqrt{2}]^*$ is of the form $\pm u_0^n$, $n \in \mathbb{Z}$.

Proof. Let $u \in \mathbb{Z}[\sqrt{2}]^*$.

- Case 1: $1 < u$. Since $1+\sqrt{2}$ is the least element among all units greater than 1, there must exist an $n \in \mathbb{N}$ such that $(1+\sqrt{2})^n \leq u < (1+\sqrt{2})^{n+1}$. This implies that $1 \leq \frac{u}{(1+\sqrt{2})^n} < 1+\sqrt{2}$. Since u and $1+\sqrt{2}$ are both units, $\frac{u}{(1+\sqrt{2})^n}$ is a unit in $\mathbb{Z}[\sqrt{2}]$ as well. Since $1+\sqrt{2}$ is the least element among all units greater than 1, $u/(1+\sqrt{2})^n = 1$. Therefore, $u = (1+\sqrt{2})^n$.
- Case 2: $u = 1$. Then $u = (1+\sqrt{2})^0$.
- Case 3: $0 < u < 1$. Then $1/u \in \mathbb{Z}[\sqrt{2}]^*$, and $1 < 1/u$. By Case 1, $1/u = (1+\sqrt{2})^n$ for some $n \in \mathbb{Z}$. Therefore, $u = (1+\sqrt{2})^{-n}$.
- Case 4: $-1 < u < 0$. Then $-u \in \mathbb{Z}[\sqrt{2}]^*$ and $0 < -u < 1$. By Case 3, $-u = (1+\sqrt{2})^n$ for some $n \in \mathbb{Z}$. Thus $u = -(1+\sqrt{2})^n$.
- Case 5: $u = -1$. Then $u = -(1+\sqrt{2})^0$.
- Case 6: $u < -1$. Then $-u \in \mathbb{Z}[\sqrt{2}]^*$ and $1 < -u$. By Case 1, $-u = (1+\sqrt{2})^n$ for some $n \in \mathbb{Z}$. Therefore, $u = -(1+\sqrt{2})^n$.

Therefore, u is indeed of the form $\pm(1+\sqrt{2})^n$ with $n \in \mathbb{Z}$. $\square$

Exercise. (Problem 10) Describe all solutions to $x^2 - 2y^2 = 1$.

Proof. We claim that $(x, y) \in \mathbb{Z}^2$ is a solution to $x^2 - 2y^2 = 1$ if and only if $x + y\sqrt{2} = (1+\sqrt{2})^{2n}$ for some $n \in \mathbb{Z}$.

Let $x, y \in \mathbb{Z}$.

- $x^2 - 2y^2 = 1$ if and only if $N(x+\sqrt{2}y) = 1$.
- We showed in Problem 3 that $x + \sqrt{2}y \in \mathbb{Z}[\sqrt{2}]^*$ if and only if $N(x+\sqrt{2}y) = \pm 1$.
- We showed in Problem 9 that every element in $\mathbb{Z}[\sqrt{2}]^*$ is of the form $\pm u_0^n$ for some $n \in \mathbb{Z}$.

Therefore, we will first check which $\pm u_0^n$ satisfies $N(\pm u_0^n) = 1$. We claim that $N(u_0^{2n}) = N(-u_0^{2n}) = 1$ for all $n \in \mathbb{Z}$.

- When $n = 0$, this is clearly true.
- Suppose that $N(u_0^{2n}) = 1$ for some $n \in \mathbb{N}$. Let $x + \sqrt{2}y = u_0^{2n}$ where $x, y \in \mathbb{Z}$. Then $u_0^{2n+2} = (x+\sqrt{2}y)(1+\sqrt{2})^2 = (x+\sqrt{2}y)(3+2\sqrt{2}) = (3x+4y) + (2x+3y)\sqrt{2}$.

$$\begin{aligned}
N(u_0^{2n+2}) &= ((3x+4y) + (2x+3y)\sqrt{2})((3x+4y) - (2x+3y)\sqrt{2}) \\
&= (9x^2 + 24xy + 16y^2) - 2(4x^2 + 12xy + 9y^2) \\
&= x^2 - 2y^2 \\
&= N(u_0^{2n}) = 1.
\end{aligned}$$

By mathematical induction, $N(u_0^{2n}) = 1$ for all $n \in \mathbb{N}$.

- Let $n \in \mathbb{N}$. Let $x + y\sqrt{2} = u_0^{2n}$ where $x, y \in \mathbb{Z}$.

$$\begin{aligned}
\frac{1}{u_0^{2n}} &= \frac{1}{x + y\sqrt{2}} \\
&= \frac{x - y\sqrt{2}}{x^2 - 2y^2} \\
&= \frac{x - y\sqrt{2}}{N(x + y\sqrt{2})} \\
&= \frac{x - y\sqrt{2}}{N(u_0^{2n})} \\
&= x - y\sqrt{2}.
\end{aligned}$$

  Since $N(x - y\sqrt{2}) = N(x + y\sqrt{2}) = 1$, $N(u_0^{-2n}) = 1$ for all $n \in \mathbb{N}$.
- Let $k \in \mathbb{Z}$. Let $x + y\sqrt{2} = u_0^{2n}$.

$$\begin{aligned}
N(-u_0^{2n}) &= N(-x - y\sqrt{2}) \\
&= (-x - y\sqrt{2})(-x + y\sqrt{2}) \\
&= (x + y\sqrt{2})(x - y\sqrt{2}) \\
&= N(x + y\sqrt{2}) \\
&= N(u_0^{2n}) = 1.
\end{aligned}$$

Therefore, $N(\pm u_0^{2n}) = 1$ for any sign and $n \in \mathbb{Z}$. We now claim that $N(\pm u_0^{2n+1}) = -1$ for any sign and $n \in \mathbb{Z}$. Let $x + y\sqrt{2} = \pm u_0^{2n}$ for some sign and $n \in \mathbb{Z}$. Then $(x+y\sqrt{2})(1+\sqrt{2}) = (x + 2y) + (x + y)\sqrt{2}$.

$$\begin{aligned}
N((x + y\sqrt{2})(1 + \sqrt{2})) &= N((x + 2y) + (x + y)\sqrt{2}) \\
&= ((x + 2y) + (x + y)\sqrt{2})((x + 2y) - (x + y)\sqrt{2}) \\
&= (x + 2y)^2 - 2(x + y)^2 \\
&= (x^2 + 4xy + 4y^2) - (2x^2 + 4xy + 2y^2) \\
&= -x^2 + 2y^2 \\
&= -(x^2 - 2y^2) \\
&= -N(x + y\sqrt{2}) \\
&= -1.
\end{aligned}$$

Therefore, $N(\pm u_0^{2n+1})$ for any sign and any $n \in \mathbb{Z}$. Hence, $\{(x, y) \in \mathbb{Z}^2 \mid x + \sqrt{2}y \in \{-u_0^{2n}, u_0^{2n} \mid n \in \mathbb{Z}\}\}$ is the set of all solutions to $x^2 - 2y^2 = 1$. $\square$

Exercise. (Problem 11) Construct a group isomorphism $\mathbb{Z}[\sqrt{2}]^* \to \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. By Problem 9, every element in $\mathbb{Z}[\sqrt{2}]^*$ can be represented as $(-1)^a(1+\sqrt{2})^{2k}$ for some $(k, a) \in \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $\phi : \mathbb{Z}[\sqrt{2}]^* \to \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ be defined such that $\phi((-1)^a(1 + \sqrt{2})^{2k}) = (k, a)$.

- Well-defined? Every element in $\mathbb{Z}[\sqrt{2}]^*$ can be expressed unique as $(-1)^a(1+\sqrt{2})^{2k}$ for some $(k,a) \in \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Thus ϕ is well defined.
- Group homomorphism?
$$\begin{aligned}\phi((-1)^a(1+\sqrt{2})^{2k}(-1)^b(1+\sqrt{2})^{2l}) &= \phi((-1)^{a+b}(1+\sqrt{2})^{2(k+l)}) \\ &= (k+l, a+b) \\ &= (k,a)+(l,b) \\ &= \phi((-1)^a(1+\sqrt{2})^{2k})\phi((-1)^b(1+\sqrt{2})^{2l}).\end{aligned}$$
- Injective? $\phi((-1)^a(1+\sqrt{2})^k) = (0,0)$ implies that $k = a = 0$. Therefore, 1 is the only number in the kernel of ϕ. Since the kernel of ϕ only contains the identity element, ϕ is injective.
- Surjective? For any $(k,a) \in \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $(-1)^a(1+\sqrt{2})^{2k} \in \mathbb{Z}[\sqrt{2}]^*$.

Therefore, ϕ is a group isomorphism. □

Exercise. (Problem 12) Show that $\mathbb{Z}[\sqrt{2}]$ is an integral domain.

Proof. $\mathbb{Z}[\sqrt{2}]$ is a commutative ring because multiplication of real numbers is commutative. Moreover, $\mathbb{Z}[\sqrt{2}] \subset \mathbb{R}$ where $\mathbb{R}$ is a field. Thus $\mathbb{Z}[\sqrt{2}]$ has no zero divisors. Therefore, $\mathbb{Z}[\sqrt{2}]$ is an integral domain. □

Exercise. (Problem 13) Define $\sigma : \mathbb{Z}[\sqrt{2}] \setminus \{0\} \to \{0,1,2,\cdots,\}$ by $\sigma(\alpha) = |N(\alpha)|$. Show that $(\mathbb{Z}[\sqrt{2}], \sigma)$ is a Euclidean domain.

Proof. Let $a+b\sqrt{2}, c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ be given such that $c+d\sqrt{2} \neq 0$. Consider
$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2}.$$

Let $p, q \in \mathbb{Z}$ be chosen such that
$$\left|\frac{ac-2bd}{c^2-2d^2} - p\right| \leq \frac{1}{2}, \left|\frac{bc-ad}{c^2-2d^2} - q\right| \leq \frac{1}{2}.$$

Such p, q are guaranteed to exist. Let $\alpha + \beta\sqrt{2}$ denote $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} - (p+q\sqrt{2})$. Then $|\alpha| \leq 1/2, |\beta| \leq 1/2$.

Let $\epsilon = (a+b\sqrt{2}) - (c+d\sqrt{2})(p+q\sqrt{2})$. If $\epsilon = 0$, we are done. Suppose otherwise. Then we have $a+b\sqrt{2} = (c+d\sqrt{2})(p+q\sqrt{2}) + \epsilon$.

$$\begin{aligned}\epsilon &= (a+b\sqrt{2}) - (c+d\sqrt{2})(p+q\sqrt{2}) \\ &= (c+d\sqrt{2})(\frac{a+b\sqrt{2}}{c+d\sqrt{2}} - (p+q\sqrt{2})) \\ &= (c+d\sqrt{2})(\alpha+\beta\sqrt{2}) \\ &= (\alpha c + 2\beta d) + (c\beta + \alpha d)\sqrt{2}.\end{aligned}$$

This implies that

$$\begin{aligned}
N(\epsilon) &= (\alpha c + 2\beta d)^2 - 2(c\beta + \alpha d)^2 \\
&= (\alpha^2 c^2 + 2\alpha\beta cd + 4\beta^2 d^2) - 2(c^2\beta^2 + 2\alpha\beta cd + \alpha^2 d^2) \\
&= \alpha^2(c^2 - 2d^2) - 2\beta^2(c^2 - 2d^2) \\
&= (c^2 - 2d^2)(\alpha^2 - 2\beta^2) \\
&= (\alpha^2 - 2\beta^2)N(c + d\sqrt{2}).
\end{aligned}$$

Therefore, $\sigma(\epsilon) = |\alpha^2 - 2\beta^2|\sigma(c + d\sqrt{2})$. Since $|\alpha^2 - 2\beta^2| \leq |\alpha|^2 + 2|\beta|^2 \leq 1/4 + 2 \cdot 1/4 = 3/4$, $\sigma(\epsilon) < \sigma(c + d\sqrt{2})$. □

Exercise. (Problem 14) Conclude that $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain and a unique factorization domain.

Proof. In class, we proved that every principal ideal domain is a unique factorization domain. Therefore, it suffices to show that $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain. Let I be an ideal of $\mathbb{Z}[\sqrt{2}]$. If $I = (0)$, we are done. Suppose otherwise. Let $S = \{|N(\alpha)| \mid \alpha \in I, \alpha \neq 0\}$. Since S is a nonempty set of positive integers, there exists a minimum value m. Let $\beta \in I$ be an element such that $|N(\beta)| = m$. We claim that $I = (\beta)$.

Suppose otherwise. Let $\alpha \in I \setminus (\beta)$. By Problem 13, there exist $\delta, \epsilon \in \mathbb{Z}[\sqrt{2}]$ such that $\alpha = \beta\delta + \epsilon$ with $|N(\epsilon)| < |N(\beta)|$. ϵ cannot be 0 because $\alpha \notin (\beta)$. Since I is an ideal, $\beta\delta \in I$. This implies that $\epsilon = \alpha - \beta\delta \in I$. However, this is a contradiction because β was chosen because $|N(\beta)| \leq |N(\beta')|$ for all $\beta' \in I$. Therefore, $I = (\beta)$, and thus $\mathbb{Z}[\sqrt{2}]$ is a principal ideal domain and a unique factorization domain. □