MATH 601 (DUE 10/2)

HIDENORI SHINOHARA

Contents

1. Factorization in Integral Domains

Exercise. (Problem 1) Let $R = \mathbb{Z}$. Compute the content of the following polynomials in $\mathbb{Q}[x]$. The content is an element of the quotient group, $\mathbb{Q}^*/\mathbb{Z}^* \simeq \mathbb{Q}^*/\{\pm 1\}$.

- $f(x) = 2x^2 - 6x + 28$.
- $g(x) = \frac{2}{3}x^2 - \frac{3}{5}x + \frac{7}{11}$.

Proof.

- By property (i) of the content, $\operatorname{cont}(f(x)) = \gcd(2, -6, 28) = 2$.

- $\mathrm{cont}(g(x)) = 2^{o_2(g(x))}3^{o_3(g(x))}5^{o_5(g(x))}\cdots$.

$$\begin{aligned}
o_2(f(x)) &= \min\{\mathrm{ord}_2(2/3), \mathrm{ord}_2(-3/5), \mathrm{ord}_2(7/11)\}\\
&= \min\{\mathrm{ord}_2(2) - \mathrm{ord}_2(3), \mathrm{ord}_2(-3) - \mathrm{ord}_2(5), \mathrm{ord}_2(7) - \mathrm{ord}_2(11)\}\\
&= \min\{1-0, 0-0, 0-0\}\\
&= 0.\\
o_3(f(x)) &= \min\{\mathrm{ord}_3(2/3), \mathrm{ord}_3(-3/5), \mathrm{ord}_3(7/11)\}\\
&= \min\{\mathrm{ord}_3(2) - \mathrm{ord}_3(3), \mathrm{ord}_3(-3) - \mathrm{ord}_3(5), \mathrm{ord}_3(7) - \mathrm{ord}_3(11)\}\\
&= \min\{0-1, 1-0, 0-0\}\\
&= -1.\\
o_5(f(x)) &= \min\{\mathrm{ord}_5(2/3), \mathrm{ord}_5(-3/5), \mathrm{ord}_5(7/11)\}\\
&= \min\{\mathrm{ord}_5(2) - \mathrm{ord}_5(3), \mathrm{ord}_5(-3) - \mathrm{ord}_5(5), \mathrm{ord}_5(7) - \mathrm{ord}_5(11)\}\\
&= \min\{0-0, 0-1, 0-0\}\\
&= -1.\\
o_7(f(x)) &= \min\{\mathrm{ord}_7(2/3), \mathrm{ord}_7(-3/5), \mathrm{ord}_7(7/11)\}\\
&= \min\{\mathrm{ord}_7(2) - \mathrm{ord}_7(3), \mathrm{ord}_7(-3) - \mathrm{ord}_7(5), \mathrm{ord}_7(7) - \mathrm{ord}_7(11)\}\\
&= \min\{0-0, 0-0, 1-0\}\\
&= 0.\\
o_{11}(f(x)) &= \min\{\mathrm{ord}_{11}(2/3), \mathrm{ord}_{11}(-3/5), \mathrm{ord}_{11}(7/11)\}\\
&= \min\{\mathrm{ord}_{11}(2) - \mathrm{ord}_{11}(3), \mathrm{ord}_{11}(-3) - \mathrm{ord}_{11}(5), \mathrm{ord}_{11}(7) - \mathrm{ord}_{11}(11)\}\\
&= \min\{0-0, 0-0, 0-1\}\\
&= -1.
\end{aligned}$$

Therefore, $\mathrm{cont}(g(x)) = 2^0 3^{-1} 5^{-1} 7^0 11^{-1} = \frac{1}{165}$.

□

Exercise. (Problem 2)

- Prove that if $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$, then $\mathrm{cont}(f(x)) = \gcd(a_0, \cdots, a_n)$.
- For $b \in F^*$, $\mathrm{cont}(b \cdot f(x)) = b \cdot \mathrm{cont}(f(x))$.

Proof.

- By Proposition 13 of P.287 (Dummit and Foote), $\gcd(up_1^{a_1}\cdots p_n^{a_n}, vp_1^{b_1}\cdots p_n^{b_n}) = p_1^{\min\{a_1,b_1\}}\cdots p_n^{\min\{a_n,b_n\}}$. By mathematical induction, this property holds for greatest common divisors of $n+1$ elements of R. Let $f(x) = \sum_{i=0}^n a_i x^i \in R[x]$ be given. Choose distinct (not equivalent) irreducible elements $p_1, \cdots, p_m \in R$, non-negative integers $a_{i,j}$, and units u_i such that $a_i = u_i p_1^{a_{i,1}}\cdots p_m^{a_{i,m}}$. Since R is a UFD, it is possible to pick such $p_i, a_{i,j}, u_i$. Then $o_{p_j} = \min\{a_{0,j}, \cdots, a_{n,j}\}$ for each j. Thus $\mathrm{cont}(f(x)) = \prod p_j^{o_{p_j}} = \prod p_j^{\min\{a_{0,j},\cdots,a_{n,j}\}} = \gcd(a_0, \cdots, a_n)$
- As discussed below the definition of ord_p in the handout "Factorization in Integral Domains," ord_p is a group homomorphism from a multiplicative group F^* to an additive group $\mathbb{Z}$.

Let $f(x) = \sum_{i=0}^{n} a_i x^i \in R[x], b \in R$ be given. Choose distinct (not equivalent) irreducible elements $p_1, \cdots, p_m \in R$, non-negative integers $a_{i,j}, b_j$, and units u_i, w such that $a_i = u_i p_1^{a_{i,1}} \cdots p_m^{a_{i,m}}$ and $b = w p_1^{b_1} \cdots p_m^{b_m}$. Then $b \cdot f(x) = \sum_{i=0}^{n} (ba_i) x_i$, and $ba_i = (u_i w) p_1^{a_{i,1}+b_1} \cdots p_m^{a_{i,m}+b_m}$. Since ord_p is a group homomorphism for each p, we have that for each i, j, $\mathrm{ord}_{p_j}(ba_i) = \mathrm{ord}_{p_j}(b) + \mathrm{ord}_{p_j}(a_i)$.

$$\begin{aligned} o_{p_j}(b \cdot f(x)) &= \min\{\mathrm{ord}_{p_j}(ba_i) \mid 0 \le i \le n\} \\ &= \min\{\mathrm{ord}_{p_j}(b) + \mathrm{ord}_{p_j}(a_i) \mid 0 \le i \le n\} \\ &= \mathrm{ord}_{p_j}(b) + \min\{\mathrm{ord}_{p_j}(a_i) \mid 0 \le i \le n\} \\ &= \mathrm{ord}_{p_j}(b) + o_{p_j}(f(x)). \end{aligned}$$

Therefore,

$$\begin{aligned} \mathrm{cont}(f(x)) &= \prod_j p_j^{o_{p_j}(b \cdot f(x))} \\ &= \prod_j p_j^{\mathrm{ord}_{p_j}(b) + o_{p_j}(f(x))} \\ &= \prod_j p_j^{\mathrm{ord}_{p_j}(b)} \prod_j p_j^{o_{p_j}(f(x))} \\ &= b \prod_j p_j^{o_{p_j}(f(x))} \\ &= b\,\mathrm{cont}(f(x)). \end{aligned}$$

□

Exercise. (Problem 3) Determine if the given polynomial is an irreducible element of the given integral domain.

- $3x^3 - 15x^2 - 21 \in \mathbb{Z}[x]$.
- $3x^3 - 15x^2 - 21 \in \mathbb{Q}[x]$.

Proof.

- $3x^3 - 15x^2 - 21 = 3(x^3 - 5x^2 - 7)$. Since neither 3 nor $x^3 - 5x^2 - 7$ is a unit, $3x^3 - 15x^2 - 21$ is not irreducible.
- We claim that $f(x) = 3x^3 - 15x^2 - 21 \in \mathbb{Q}[x]$ is irreducible. The content is $\gcd(3, -15, -21) = 3$, so let $f_0(x) = f(x)/3 = x^3 - 5x^2 - 7$. Then $f_0(x)$ is primitive in $\mathbb{Z}[x]$. As discussed in class on 9/27, $f_0(x)$ is irreducible if and only if it has no linear factors. If $mx + n$ is a factor of $f_0(x)$, then $m \mid 1$ and $n \mid -7$. Thus $m \in \{-1, 1\}$ and $n \in \{-1, 1, -7, 7\}$. This implies that it is sufficient to check $x+1, x+7, x-1, x-7$ because the other possibilities can be obtained by multiplying -1.
  - $f(x) = (3x^2 - 18x + 18)(x + 1) - 39$.
  - $f(x) = (3x^2 - 12x - 12)(x - 1) - 33$.
  - $f(x) = (3x^2 - 36x + 252)(x + 7) - 1785$.
  - $f(x) = (3x^2 + 6x + 42)(x - 7) + 273$.

  Since none of them is a factor of $f(x)$, $f_0(x)$ is irreducible. Since 3 is a unit in $\mathbb{Q}[x]$, $f(x) = 3f_0(x)$ is irreducible in $\mathbb{Q}[x]$.

□

Exercise. (Problem 4(i)) The polynomial $f(x) = x^5 + 8x^4 + 7x^3 - 30x^2 + 42x - 36 \in \mathbb{Z}[x]$, reduced modulo 7 and 11 factors as a product of irreducible polynomials as follows:

- $x^5 + 8x^4 + 7x^3 - 30x^2 + 42x - 36 = (x^2 - 3x + 1)(x^3 + 4x^2 + 4x - 1) \in \mathbb{Z}/7\mathbb{Z}[x]$.
- $x^5 + 8x^4 + 7x^3 - 30x^2 + 42x - 36 = (x^2 + 4x + 5)(x^3 + 4x^2 + 8x + 6) \in \mathbb{Z}/11\mathbb{Z}[x]$.

Proof. Suppose $f(x) = (x^2 + ax + b)(x^3 + cx^2 + dx + e)$ for some $a, b, c, d, e \in \mathbb{Z}$. Since the leading coefficient of $f(x)$ is 1, if $f(x)$ is a product of two polynomials, we can assume that their leading coefficients are 1 without loss of generality. If $f(x)$ factors as above, then we can obtain a factorization of $f(x)$ in $\mathbb{Z}/7\mathbb{Z}[x]$ and $\mathbb{Z}/11\mathbb{Z}[x]$ by taking modulo 7 and 11 of each coefficient. We will try to reverse engineer that.

- $a \equiv -3 \pmod 7$ and $a \equiv 4 \pmod{11}$ are satisfied by $a = 4$.
- $b \equiv 1 \pmod 7$ and $b \equiv 5 \pmod{11}$ are satisfied by $b = -6$.
- $c \equiv 4 \pmod 7$ and $c \equiv 4 \pmod{11}$ are satisfied by $c = 4$.
- $d \equiv 4 \pmod 7$ and $d \equiv 8 \pmod{11}$ are satisfied by $d = -3$.
- $c \equiv -1 \pmod 7$ and $c \equiv 6 \pmod{11}$ are satisfied by $c = 6$.

There are other values that satisfy such equations (e.g., $a = 4 + 77 = 81$), but it seems reasonable to start with numbers with small absolute values since each coefficient of $f(x)$ has a relatively small absolute value. It turns out that this set of coefficients indeed gives a factorization of $f(x)$. In other words, $f(x) = (x^2 + 4x - 6)(x^3 + 4x^2 - 3x + 6)$.

We will check if $x^2 + 4x - 6$ and $x^3 + 4x^2 - 3x + 6$ are irreducible.

- $x^2 + 4x - 6$ is irreducible by the Eisenstein irreducibility criterion. Let $P = (2)$. $4 \in P = (2)$ and $6 \in P = (2)$, but $6 \notin P^2$. Thus $x^2 + 4x - 6$ is irreducible.
- Is $x^3 + 4x^2 - 3x + 6$ irreducible? Since the content is 1, this polynomial cannot be factored as a product of a non-unit integer and a polynomial of degree 3. Thus if this polynomial is not irreducible, it must factor as a product of a polynomial of degree 1 and one of degree 2. In other words, $x^3 + 4x^2 - 3x + 6 = (x + a)(x^2 + bx + c)$ for some $a, b, c \in \mathbb{Z}$. We can assume that the leading coefficient of each factor is 1 because the leading coefficient of $x^3 + 4x^2 - 3x + 6$ is 1. Then $ac = 6$, so $a \mid 6$. Thus $a \in \{-1, 1, -2, 2, 3, -3, 6, -6\}$.

$$
\begin{aligned}
x^3 + 4x^2 - 3x + 6 &= (x^2 + 10x + 57)(x - 6) + 348, \\
x^3 + 4x^2 - 3x + 6 &= (x^2 + 7x + 18)(x - 3) + 60, \\
x^3 + 4x^2 - 3x + 6 &= (x^2 + 6x + 9)(x - 2) + 24, \\
x^3 + 4x^2 - 3x + 6 &= (x^2 + 5x + 2)(x - 1) + 8, \\
x^3 + 4x^2 - 3x + 6 &= (x^2 + 3x - 6)(x + 1) + 12, \\
x^3 + 4x^2 - 3x + 6 &= (x^2 + 2x - 7)(x + 2) + 20, \\
x^3 + 4x^2 - 3x + 6 &= (x^2 + x - 6)(x + 3) + 24, \\
x^3 + 4x^2 - 3x + 6 &= (x^2 - 2x + 9)(x + 6) - 48.
\end{aligned}
$$

  Therefore, $x^3 + 4x^2 - 3x + 6$ is irreducible.

Hence, $f(x)$ is a product of an irreducible polynomial of degree 2 and one of degree 3. □

Exercise. (Problem 4(ii)) Find $i \in 7\mathbb{Z}$ and $j \in 11\mathbb{Z}$ such that $i + j = 1$.

Proof. We will use the Euclid algorithm.

$$\begin{aligned} 11 &= 1 \cdot 7 + 4 \\ 7 &= 1 \cdot 4 + 3 \\ 4 &= 1 \cdot 3 + 1. \end{aligned}$$

Therefore,

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 \\ &= 4 - 1 \cdot (7 - 1 \cdot 4) \\ &= 4 - 1 \cdot 7 + 1 \cdot 4 \\ &= 2 \cdot 4 - 1 \cdot 7 \\ &= 2 \cdot (11 - 1 \cdot 7) - 1 \cdot 7 \\ &= 2 \cdot 11 - 2 \cdot 7 - 1 \cdot 7 \\ &= 2 \cdot 11 - 3 \cdot 7. \end{aligned}$$

Therefore, when $i = 2 \cdot 11 = 22$ and $j = -3 \cdot 7 = -21$, $i + j = 1$. □

Exercise. (Problem 4(iii)) Find $n \in \mathbb{Z}$ with $0 \leq n < 77$ such that $n \equiv 1 \pmod 7$ and $n \equiv 5 \pmod{11}$.

Proof. Since $0 \leq n < 77$ and $n \equiv 5 \pmod{11}$, we know that $n \in \{5, 16, 27, 38, 49, 60, 71\}$. Since $n \equiv 1 \pmod 7$, $7 \mid (n - 1)$.

- $7 \nmid (5 - 1) = 4$.
- $7 \nmid (16 - 1) = 15$.
- $7 \nmid (27 - 1) = 26$.
- $7 \nmid (38 - 1) = 37$.
- $7 \nmid (49 - 1) = 48$.
- $7 \nmid (60 - 1) = 59$.
- $7 \mid (71 - 1) = 70$.

Therefore, $n = 71$. □

Exercise. (Problem 4(iv)) Factor $f(x) \in \mathbb{Z}[x]$ as a product of irreducible polynomials.

Proof. In Problem 4(i), we showed that $f(x) = (x^2 + 4x - 6)(x^3 + 4x^2 - 3x + 6)$ and each of these two polynomials is irreducible in $\mathbb{Z}[x]$. □

2. Rings of Fractions

Exercise. (Problem 1 (iii)) Prove that the natural map $i : R \to S^{-1}R$, which maps r to $\frac{r}{1}$ is an injective ring homomorphism.

Proof.

- Ring homomorphism?
  - For all $r, s \in R$, $i(rs) = \frac{rs}{1} = \frac{r}{1} \cdot \frac{s}{1} = i(r)i(s)$.
  - For all $r, s \in R$, $i(r + s) = \frac{r+s}{1} = \frac{r}{1} + \frac{s}{1} = i(r) + i(s)$.

  Therefore, i is indeed a ring homomorphism.

- Injective? It suffices to check that $\ker(i) = \{1\}$. Let $r \in R$ such that $\ker(r)$ is the multiplicative identity in $S^{-1}R$. By definition, $\ker(r) = \frac{1}{1}$. Thus $\frac{r}{1} = \frac{1}{1}$, so $r \cdot 1 - 1 \cdot 1 = 0$. This means $r = 1$, so $\ker(i) = \{1\}$.

Therefore, i is indeed an injective ring homomorphism. $\square$

Exercise. (Problem 1(iv)) Prove that given a ring homomorphism $h : R \to T$, such that $h(s) \in T^\star$ for every $s \in S$, there exists a unique ring homomorphism $\lambda : S^{-1}R \to T$, such that $h = \lambda \circ i$.

Proof. Suppose such a λ exists. Then for all $r \in R$, $h(r) = (\lambda \circ i)(r) = \lambda(r/1)$. Therefore, $\lambda(r/1) = h(r)$. Let $s \in S$. Then $1_T = \lambda(1/1) = \lambda((s/1) \cdot (1/s)) = \lambda(s/1)\lambda(1/s)$. Therefore, $\lambda(1/s) = \lambda(s/1)^{-1} = h(s)^{-1}$. This implies that $\lambda(r/s) = \lambda(r/1)\lambda(1/s) = h(r)h(s)^{-1}$.

In other words, if such a λ exists, it must map r/s to $h(r)h(s)^{-1}$. This proves the uniqueness. We will show that such a function is indeed well defined and it is a ring homomorphism.

- Well-defined? Since $h(s) \in T^\star$ for each $s \in S$, $h(s)^{-1}$ is well defined. Let $r/s = r'/s' \in S^{-1}R$ be given. Then $rs' = r's$. Since h is a ring homomorphism, $h(r)h(s') = h(r')h(s)$. Therefore, $\lambda(r/s) = h(r)h(s)^{-1} = h(r')h(s')^{-1} = \lambda(r'/s')$.
- Ring homomorphism? Let $r/s, r'/s' \in S^{-1}R$.

$$\begin{aligned}
\lambda(\frac{r}{s} \cdot \frac{r'}{s'}) &= \lambda(\frac{rr'}{ss'}) \\
&= h(rr')h(ss')^{-1} \\
&= h(r)h(r')h(s)^{-1}h(s')^{-1} \\
&= h(r)h(s)^{-1}h(r')h(s')^{-1} \\
&= \lambda(\frac{r}{s})\lambda(\frac{r'}{s'}). \\
\lambda(\frac{r}{s} + \frac{r'}{s'}) &= \lambda(\frac{rs' + r's}{ss'}) \\
&= h(rs' + r's)h(ss')^{-1} \\
&= (h(r)h(s') + h(r')h(s))h(s)^{-1}h(s')^{-1} \\
&= h(r)h(s)^{-1} + h(r')h(s')^{-1} \\
&= \lambda(\frac{r}{s}) + \lambda(\frac{r'}{s'}).
\end{aligned}$$

- Commutes? For any $r \in R$, $\lambda(i(r)) = \lambda(r/1) = h(r)h(1)^{-1} = h(r)$. Therefore, $\lambda \circ i$ is indeed h.

$\square$

3. The Quadratic Equation $x^2 - 2y^2 = n$

Exercise. (Problem 15) Find a solution to $x^2 - 2y^2 = 7$.

Proof. $3^2 - 2 \cdot 1^2 = 9 - 2 = 7$. Thus $(x, y) = (3, 1)$ is a solution to $x^2 - 2y^2 = 7$. $\square$

Exercise. (Problem 16) Is 7 irreducible in $\mathbb{Z}[\sqrt{2}]$? If not, find a factorization into irreducible elements.

Proof. By Problem 3 from the previous assignment, we know that $\alpha \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $N(\alpha) = \pm 1$. We will use this result in this solution.

By Problem 15, we know that $7 = (3+\sqrt{2})(3-\sqrt{2})$. Since $N(3+\sqrt{2}) = N(3-\sqrt{2}) = 7 \neq \pm 1$, 7 can be expressed as a product of two non-unit elements, so 7 is not irreducible.

Suppose $3+\sqrt{2} = (a+b\sqrt{2})(c+d\sqrt{2})$ for some $a, b, c, d \in \mathbb{Z}$. By Problem 2 from the previous assignment, we know that $N(3+\sqrt{2}) = N(a+b\sqrt{2})N(c+d\sqrt{2})$. Since N maps $\mathbb{Z}[\sqrt{2}]$ into integers, exactly one of $N(a+b\sqrt{2})$ and $N(c+d\sqrt{2}$ must be 1 or -1, and the other one is 7 or -7. Therefore, one of $a+b\sqrt{2}$ or $c+d\sqrt{2}$ is a unit, so $3+\sqrt{2}$ is irreducible.

Similarly, if $3-\sqrt{2} = (a'+b'\sqrt{2})(c'+d'\sqrt{2})$, then $7 = N(3-\sqrt{2}) = N(a'+b'\sqrt{2})N(c'+d'\sqrt{2})$. Therefore, one of $a'+b'\sqrt{2}$ or $c'+d'\sqrt{2}$ is a unit, so $3-\sqrt{2}$ is irreducible. □

Exercise. (Problem 17) Let $p \in \mathbb{Z} \setminus \{0\}$ and suppose $\alpha\beta = p$ in $\mathbb{Z}[\sqrt{2}]$. Show that $\beta = c\gamma(\alpha)$ with $c \in \mathbb{Q}$.

Proof. Choose $a, b, c, d \in \mathbb{Z}$ such that $a+b\sqrt{2} = \beta, c+d\sqrt{2} = \alpha$. Since $\alpha\beta = p \neq 0$, $\alpha \neq 0$. This implies at least one of c or d is nonzero. Therefore, $\gamma(\alpha) = c - d\sqrt{2} \neq 0$.

We have $\alpha\beta = (ac+2bd) + \sqrt{2}(ad+bc)$. Since $\alpha\beta \in \mathbb{Z}$, $ad+bc = 0$.

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

Therefore, $\frac{\beta}{\gamma(\alpha)} = \frac{ac+2bd}{c^2-2d^2} \in \mathbb{Q}$. In other words, $\beta = \frac{ac+2bd}{c^2-2d^2}\gamma(\alpha)$. □

Exercise. (Problem 18) Let $p \in \mathbb{Z}$ be an odd prime. Show that $p = N(\alpha)$ for some $\alpha \in \mathbb{Z}[\sqrt{2}]$ if and only if p is not irreducible as an element of $\mathbb{Z}[\sqrt{2}]$.

Proof. By Problem 3 from the previous assignment, we know that $\alpha \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $N(\alpha) = \pm 1$. We will use this result in this solution.

Suppose $p = N(\alpha)$ for some $\alpha \in \mathbb{Z}[\sqrt{2}]$. Since $N(\alpha) = \alpha\gamma(\alpha)$, p can be written as a product of α and $\gamma(\alpha)$.

- $N(\alpha) = p \neq \pm 1$, so α is not a unit.
- Since $N(\gamma(\alpha)) = \gamma(\alpha)\gamma(\gamma(\alpha)) = \gamma(\alpha)\alpha = N(\alpha) = p \neq \pm 1$, $\gamma(\alpha)$ is not a unit.

Therefore, p is a product of two non-unit elements $\alpha, \gamma(\alpha)$, so p is not irreducible.

On the other hand, suppose that p is not irreducible as an element of $\mathbb{Z}[\sqrt{2}]$. Then $p = \alpha\beta$ where $\alpha, \beta \in \mathbb{Z}[\sqrt{2}]$ are non-unit elements. Then $N(p) = N(\alpha)N(\beta)$.

- $N(p) = p^2$ because p is an integer.
- $N(\alpha) \neq \pm 1$ because α is not a unit.
- $N(\beta) \neq \pm 1$ because β is not a unit.

Since $N(\alpha), N(\beta)$ are both integers, $N(\alpha) = N(\beta) = p$ or $N(\alpha) = N(\beta) = -p$. If $N(\alpha) = p$, then we are done. If $N(\alpha) = -p$, then $N(\alpha(1+\sqrt{2})) = N(\alpha)N(1+\sqrt{2}) = (-p)(-1) = p$. □

Exercise. (Problem 19) Let $p \in \mathbb{Z}$ be an odd prime. Show that $x^2 - 2y^2 = p$ has a solution if and only if p is not irreducible in $\mathbb{Z}[\sqrt{2}]$.

Proof. Let an odd prime p be given. There exists an $\alpha \in \mathbb{Z}[\sqrt{2}]$ such that $p = N(\alpha)$ if and only if there exist $x, y \in \mathbb{Z}$ such that $p = x^2 - 2y^2$ because $N(x + \sqrt{2}y) = x^2 - 2y^2$. By combining this with the results of Problem 18, we have $x^2 - 2y^2 = p$ has a solution if and only if p is not irreducible in $\mathbb{Z}[\sqrt{2}]$. $\square$