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, $\text{cont}(f(x)) = \gcd(2, -6, 28) = 2$.

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

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

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

□

Exercise. (Problem 2)

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

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 $\operatorname{cont}(f(x)) = \prod p_j^{o_{p_j}} = \prod p_j^{\min\{a_{0,j},\cdots,a_{n,j}\}} = \gcd(a_0, \cdots, a_n)$
-

□

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. $\square$

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, $\beta = \frac{ac+2bd}{c^2-2d^2}\gamma(\alpha)$. $\square$

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 $N(\alpha(1+\sqrt{2})) = N(\alpha)N(1+\sqrt{2}) = (-p)(-1) = p$. $\square$

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 $\mathbb{Z}[\sqrt{2}]$. $\square$