MATH 601 (DUE 10/9)

HIDENORI SHINOHARA

Contents

1. Rings of Fractions

Exercise. (Problem 3) Let $T \subset R$ be the subset consisting of all non zero divisors.

- Show that T is a multiplicative set.
- Let $s \in T$ and let $S = \{1, s, s^2, s^3, \cdots\} \subset T$. Show that the following rings are isomorphic: $S^{-1}R$, the subring $R[1/s] \subset T^{-1}R$, and the quotient ring $R[x]/(sx-1)$.

Proof.

- - Let $a, b \in T$. Let $c \in R$ be given. If $(ab)c = 0$, then $a(bc) = 0$. Since a is a non zero divisor, $bc = 0$. Since b is a non zero divisor, $c = 0$. Since R is a commutative ring throughout this handout, there is no need to check the case that $c(ab) = 0$. Thus ab is a non zero divisor, so T is closed under multiplication.
  - $1 \in T$ since $\forall c \in R, c \cdot 1 = 0 \implies c = 0$.

  Therefore, T is indeed a multiplicative set.
- I have some idea, but I don't know how to solve this. There are a few mapping properties that we've covered:
  - The universal mapping property of the quotient. (Proposition 6 on Commutative Rings) Given $\pi : R \to R/I$ and $f : R \to S$ with some nice properties, there exists $\overline{f} : R/I \to S$ such that $\overline{f} \circ \pi = f$.
  - The mapping property of polynomials. (Proposition 1 on Commutative Rings) Given $\phi_0 : R \to S$ and $s \in S$, there exists $\phi : R[x] \to S$.
  - The universal property of rings of fractions. (Proposition (iv) of the Ring of Fractions.) Given $i : R \to S^{-1}R$ and $h : R \to T$ with some nice properties, there exists $\lambda : S^{-1}R \to T$ such that $h = \lambda \circ i$.

  Let π be the canonical map from $R[x]$ into $R[x]/(sx-1)$. Let $f : R[x] \to S^{-1}R$ be the homomorphism associated to the inclusion map $R \to S^{-1}R$ and the element $1/s \in S^{-1}R$. By the mapping property of polynomials, the existence of f is guaranteed.

  By the universal property of the quotient, universal mapping property of the ring of fractions, there exist homomorphisms $\overline{f}, \overline{\pi}$, respectively, such that the following diagram commutes:

$$\begin{tikzcd} R[x] \arrow[r, "\pi"] \arrow[dr, "f"'] & R[x]/(sx-1) \arrow[d, shift left, "\overline{f}"] \\ & S^{-1}R \arrow[u, shift left, "\overline{\pi}"] \end{tikzcd}$$

Since π and f are both surjective, $\overline{f}$ and $\overline{\pi}$ must be surjective in order for the diagram to commute. Then $\overline{f} \circ \overline{\pi} \circ f = \overline{f} \circ \pi = f$. Since f is surjective, this implies that $\overline{f} \circ \overline{\pi} = \mathrm{Id}_{S^{-1}R}$. Similarly, $\overline{\pi} \circ \overline{f} = \mathrm{Id}_{R[x]/(sx-1)}$. Therefore, $\overline{\pi}$ and $\overline{f}$ are the inverse homomorphism of each other, so they are isomorphisms.

What about $R[1/s]$?

□

2. Modules

Exercise. (Problem 1) For each of the $\mathbb{Z}$-modules listed in the handout, answer the questions in the handout.

Proof.

(a) $M = \mathbb{Z}^3 \times \mathbb{Z}/86\mathbb{Z}$.

Solve this problem!

(b) $M = \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$.

Solve this problem!

(c) $M = \mathbb{Z}[1/p] \subset \mathbb{Q}$.

Solve this problem!

(d) $M = \mathbb{Q}/\mathbb{Z}_{(p)}$.

Solve this problem!

□

3. The Quadratic Equation

Exercise. (Problem 20) Construct ring isomorphisms $\mathbb{Z}[x]/(x^2-2) \to \mathbb{Z}[\sqrt{2}]$ and $\mathbb{Z}/(p)[x]/(x^2-2) \to \mathbb{Z}[\sqrt{2}](p)$.

Proof. Let $f : \mathbb{Z}[x]/(x^2-2) \to \mathbb{Z}[\sqrt{2}]$ be defined by $f(p(x) + (x^2-2)) = p(\sqrt{2})$.

- Well defined? $p(\sqrt{2}) \in \mathbb{Q}[\sqrt{2}]$, and if $p(x) + (x^2-2) = q(x) + (x^2-2)$, then $p(x) - q(x) \in (x^2-2)$, so $p(\sqrt{2}) - q(\sqrt{2}) = 0$. Thus $f(p(x) + (x^2-2)) = p(\sqrt{2}) = q(\sqrt{2}) = f(q(x) + (x^2-2))$.

- Ring homomorphism? Let $p(x) + (x^2-2), q(x) + (x^2-2) \in \mathbb{Z}[x]/(x^2-2)$ be given.

$$\begin{aligned} f(p(x) + (x^2-2) + q(x) + (x^2-2)) &= f((p(x)+q(x)) + (x^2-2)) \\ &= p(\sqrt{2}) + q(\sqrt{2}) \\ &= f(p(x) + (x^2-2)) + f(q(x) + (x^2-2)). \\ f((p(x) + (x^2-2))(q(x) + (x^2-2))) &= f((p(x)q(x)) + (x^2-2)) \\ &= p(\sqrt{2})q(\sqrt{2}) \\ &= f(p(x) + (x^2-2))f(q(x) + (x^2-2)). \end{aligned}$$

- Injective? Let $p(x) + (x^2-2)$ be given. Suppose $f(p(x) + (x^2-2)) = 0$. Then $p(\sqrt{2}) = 0$. Since $\mathbb{Z}[x]$ is a Euclidean domain, $p(x) = (x^2-2)q(x) + r(x)$ for some $q(x)$ and $r(x)$ such that $r(x) = ax + b$. Since $r(x) = p(x) - (x^2-2)q(x)$, $r(\sqrt{2}) = 0$. This implies $a\sqrt{2} + b = 0$. Since $a, b \in \mathbb{Z}$, $a = b = 0$. Thus $p(x) \in (x^2-2)$, so $p(x) + (x^2-2) = 0$.
- Surjective? For any $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, $f(a + bx + (x^2-2)) = a + b\sqrt{2}$.

Thus f is a ring isomorphism.

Do the second part.

$\square$

Exercise. (Problem 21)

Exercise. (Problem 22)

4. Factorization in Integral Domains

Exercise. (Problem 5)

- Let k be a field and let $a \in k$. Construct a k-algebra isomorphism, $k[x,y]/(x-a) \to k[y]$. Justify your answer.
- Let $f(x,y) \in k[x,y]$. What is the image of $f(x,y)$ under the above isomorphism?

Proof.

- Let ϕ be defined such that $\phi(f(x,y) + (x-a)) = f(a,y)$.
  - Well-defined? Let $f(x,y) + (x-a) = g(x,y) + (x-a)$. Then $g(x,y) = f(x,y) + h(x,y)(x-a)$.

$$\begin{aligned} \phi(g(x,y) + (x-a)) &= \phi((f(x,y) + h(x,y)(x-a)) + (x-a)) \\ &= f(a,y) + h(a,y)(a-a) \\ &= f(a,y) \\ &= \phi(f(x,y)). \end{aligned}$$

– k-algebra homomorphism? Let $c \in k, f, g \in k[x,y]$ be given.

$$\begin{aligned}
\phi(c(f+(x-a)) &= \phi(cf+(x-a)) \\
&= cf(a,y) \\
&= c\phi(f+(x-a)). \\
\phi((f+g)+(x-a)) &= (f+g)(a,y) \\
&= f(a,y)+g(a,y) \\
&= \phi(f+(x-a))+\phi(g+(x-a)). \\
\phi((fg)+(x-a)) &= (fg)(a,y) \\
&= f(a,y)g(a,y) \\
&= \phi(f+(x-a))\phi(g+(x-a)).
\end{aligned}$$

- $\phi(f(x,y)+(x-a)) = f(a,y)$.

$\square$

Exercise. (Problem 6)

- Give an example of a field k, an element $a \in k$ and a reducible polynomial $f(x,y) \in k[x,y]$ of degree n in y such that $f(a,y) \in k[y]$ is irreducible and has degree n.
- Suppose given a polynomial $f \in k[x,y]$ which when viewed as an element of $k(x)[y]$ has degree n (in y) and content 1. Suppose there is some $a \in k$ such that $f(a,y) \in k[y]$ is irreducible and has degree n. Show that $f(x,y) \in k[x,y]$ is irreducible.
- Give an example of a field k, an element, $a \in k$, and a reducible polynomial $f(x,y) \in k[x,y]$, which when viewed as an element of $k(x)[y]$ has degree n and content 1 such that $f(a,y) \in k[y]$ is irreducible.

Proof.

- Let $k = \mathbb{Q}, a = 1, f(x,y) = xy$. Then the degree of $f(x,y)$ in y is 1. $f(x,y) = xy \in k[x,y]$ is reducible since x and y are not units in $k[x,y]$. However, $f(a,y) = 1y = y$ is irreducible in $k[y]$.
- Choose $f_1, \cdots, f_n \in k[x]$ such that $f(x,y) = f_n(x)y^n + \cdots + f_1(x)y^1 + f_0(x)$. Then $f(a,y) = f_n(a)y^n + \cdots + f_1(a)y^1 + f_0(a)$. Let $h_1(x,y), h_2(x,y) \in k[x]$ be given such that $f(x,y) = h_1(x,y)h_2(x,y)$. Then $f(a,y) = h_1(a,y)h_2(a,y)$. Then $h_1(a,y)$ or $h_2(a,y)$ is a unit in $k[y]$ since $f(a,y)$ is irreducible in $k[y]$. Without loss of generality, we will assume $h_1(a,y)$ is a unit in $k[y]$.

  It is given that $\deg_y(f(a,y))$, the degree of $f(a,y)$ in y, is n. Thus $\deg_y(h_1(a,y)) + \deg_y(h_2(a,y)) = n$. Since $\deg_y(h_1(a,y)) = 0$, $\deg_y(h_2(a,y)) = n$. Therefore, $\deg_y(h_2(x,y)) \geq n$.

  On the other hand, $\deg_y(f(x,y)) = \deg_y(h_1(x,y)) + \deg_y(h_2(x,y))$, so $\deg_y(h_2(x,y)) \leq n$. Thus $\deg_y(h_2(x,y)) = n$. Let $g_1(x), \cdots, g_n(x) \in k[x]$ such that $h_2(x,y) = g_n(x)y^n + \cdots + g_1(x)y^1 + g_0(x)$. Then $f(x,y) = h_1(x,y)h_2(x,y) = (h_1(x,y)g_n(x))y^n + \cdots + (h_1(x,y)g_1(x))y^1 + h_1(x,y)g_0(x)$.

  Since $\deg_y(h_2(x,y)) = n$, $\deg_y(h_1(x,y)) = 0$. Thus, $h_1(x,y) \in k[x]$, so $h_1(x,y)g_i(x) \in k[x]$ for each i. Therefore, $h_1(x,y)g_i(x) = f_i(x)$ for each i.

  Let $p \in k[x]$ be an irreducible. If $p \mid h_1(x,y)$, then $p \mid f_i(x) = h_1(x,y)g_i(x)$ for each i, so $\mathrm{ord}_p(f_i) \geq 1$ for each i. Therefore, $o_p(f(x,y)) \geq 1$, and thus $p \mid \mathrm{cont}(f(x,y))$.

However, since $\mathrm{cont}(f(x,y)) = 1$, $p \nmid h_1(x,y)$. Thus $h_1(x,y)$ is a unit in $k[x]$ since it cannot be divided by any irreducibles. Since $h_1(x,y)$ is a unit in $k[x]$ and $k[y]$, it must consist only of a constant term, which is a unit in k. Hence, $h_1(x,y)$ is a unit in $k[x,y]$.

We have shown that for any $h_1(x,y), h_2(x,y) \in k[x,y]$, $h_1h_2 = f$ implies one of h_1 or h_2 is a unit. Therefore, $f(x,y)$ is an irreducible in $k[x,y]$.

- Let $k = \mathbb{Q}, a = 1, f(x,y) = (x-1)y^2 + y$. Then $f(x,y)$, which when viewed as an element of $k(x)[y]$ has degree 1.
  - The coefficient of y is 1, and $\mathrm{ord}_p(1) = 0$ for any p because $1 \in k[x]^*$.
  - The coefficient of y^2, when $f(x,y)$ is viewed as an element of $k(x)[y]$ is $x-1$. Thus for any irreducible element $p \in k[x]$, $\mathrm{ord}_p(x-1) \geq 0$.

  Therefore, $o_p(f(x)) = 0$ for any irreducible element $p \in k[x]$. Thus $\mathrm{cont}(f(x,y)) = 1$.

  $f(a,y) = y \in k[y]$. This is irreducible because if $f_1f_2 = y$ for some $f_1, f_2 \in k[y]$, then $\deg(f_1) + \deg(f_2) = 1$ implies that one of f_1 or f_2 is a unit in k.

$\square$