# 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.
- $S^{-1}R$ and $R[1/s]$ are isomorphic because:
  – They are the same set. They both contain all equivalence classes $[(r, s)]$ for $r \in R$ and $s \in S$ with the same equivalence relation.
  – They have the same addition and multiplication.

  What does it look like?

  Let $\pi$ 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 $f, \overline{\pi}$, respectively, such that the following diagram commutes:

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

[1]

$f\left(\sum_0^n r_i x^i\right) = \sum_0^n r_i \left(\frac{1}{s}\right)^i$

"nice" prop??

$R[x] \to S^{-1}R$.

$x \mapsto \frac{1}{s}$

$r \mapsto \frac{r}{1}$.

By Lmm 8(iii) & UMP of Quotient.

Since $\pi$ 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.

□

## 2. Modules

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

*Proof.*

(a) $M = \mathbb{Z}^3 \times \mathbb{Z}/86\mathbb{Z}$.
- (i) $M$ is finitely generated. $(1,0,0,0), (0,1,0,0), \cdots, (0,0,0,1)$.
- (ii) $M$ is finitely presented. $\mathbb{Z}$ Noetherian $\Leftarrow$ fin. gen.
- (iii) 4.
- (iv) Yes.
- (v) Yes.
- (vi) No. $(1,0,0,0) \notin M_{tors}$.

(b) $M = \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$.
- (i) $M$ is not finitely generated.
- (ii) $M$ is not finitely presented.
- (iii) Infinite. $(1,0,\cdots), (0,1,\cdots)$
- (iv) No.
- (v) No. $(0,0,0,a,b,\cdots)$
- (vi) Yes.

(c) $M = \mathbb{Z}[1/p] \subset \mathbb{Q}$.
- (i) $M$ is not finitely generated.
- (ii) $M$ is not finitely presented.
- (iii) 1. $2\mathbb{Z}[\frac{1}{3}]$.
- (iv) No.
- (v) No.
- (vi) No. $0 \leftarrow$ Yes!?

(d) $M = \mathbb{Q}/\mathbb{Z}_{(p)}$.
- (i) $M$ is not finitely generated.
- (ii) $M$ is not finitely presented. $p=3$
- (iii) 1.
- (iv) No.
- (v) No.
- (vi) Yes.

□

## 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 $i : \mathbb{Z} \to \mathbb{Z}[\sqrt{2}]$ be the inclusion and $s = \sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. By the mapping property of polynomials, there exists a ring homomorphism $\phi : \mathbb{Z}[x] \to \mathbb{Z}[\sqrt{2}]$ such that $\phi(\sum_{i=0}^{n} r_i x^i) = \sum_{i=0}^{n} i(r_i)s^i$. In other words, $\phi$ maps $f(x)$ into $f(\sqrt{2})$. For each $a+b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, $\phi(a+bx) = a+b\sqrt{2}$, so $\phi$ is surjective. We claim that $\ker(\phi) = (x^2-2)$.

- Since $\sqrt{2}^2 - 2 = 2 - 2 = 0$, $x^2 - 2 \in \ker(\phi)$. Moreover, $(x^2-2) \subset \ker(\phi)$.
- Let $f(x) \in \ker(\phi)$. Since $\mathbb{Z}[x]$ is a Euclidean domain, $f(x) = q(x)(x^2-2) + ax + b$ for some $q(x) \in \mathbb{Z}[x], a, b \in \mathbb{Z}$. Since $ax + b = f(x) - q(x)(x^2-2)$, $a\sqrt{2} + b = 0$. Since $a, b$ are integers, $a = b = 0$. This implies $f(x) \in (x^2-2)$.

Therefore, $\ker(\phi) = (x^2-2)$. By ~~the first isomorphism theorem(Theorem 16 on P 97, Dummit and Foote)~~ Lmm 8 Comm ring, $\tilde{\phi} : \mathbb{Z}[x]/(x^2-2) \to \mathbb{Z}[\sqrt{2}]$ induced by $\phi$ is an isomorphism.

We will solve the second part using the same approach. We will assume that $p$ is a prime. Consider the inclusion $\mathbb{Z}/(p) \hookrightarrow \mathbb{Z}[\sqrt{2}]/(p)$ and the element $\sqrt{2} + (p) \in \mathbb{Z}[\sqrt{2}]/(p)$. Let $\Phi : \mathbb{Z}/(p)[x] \to \mathbb{Z}[\sqrt{2}]/(p)$ be a ring homomorphism associated to the inclusion ~~and element~~. We will examine how $\Phi$ behaves.

$$\begin{aligned}
\Phi\left(\sum_{i=0}^{n}(a_i + (p))x^i\right) &= \sum_{i=0}^{n}(a_i + (p))(\sqrt{2} + (p))^i \\
&= \sum_{i=0}^{n}(a_i + (p))(\sqrt{2}^i + (p)) \\
&= \sum_{i=0}^{n}(a_i\sqrt{2}^i + (p)) \\
&= \left(\sum_{i=0}^{n} a_i\sqrt{2}^i\right) + (p).
\end{aligned}$$

$\mathbb{Z}/(p) \hookrightarrow \mathbb{Z}[\sqrt{2}]/(p)$

$a+(p) \to a+(p)$

$\sqrt{2}+(p) \in \mathbb{Z}[\sqrt{2}]/(p).$

For any $a + b\sqrt{2} + (p) \in \mathbb{Z}[\sqrt{2}]/(p)$, $\Phi((a+(p)) + (b+(p))x) = a + b\sqrt{2} + (p)$, so $\Phi$ is surjective. We claim that $\ker(\Phi) = (x^2-2)$. Here, by $x^2 - 2$, we mean $(1+(p))x^2 - (2+(p))$.

- Since $\sqrt{2}^2 - 2 = 0$, $(x^2-2) \in \ker(\Phi)$.
- Let $f(x) \in \ker(\Phi) \subset \mathbb{Z}/(p)[x]$. Since $p$ is a prime, $\mathbb{Z}/(p)$ is a field. Thus $\mathbb{Z}/(p)[x]$ is a Euclidean domain. Choose $q(x) \in \mathbb{Z}/(p)[x]$ and $a + (p), b + (p) \in \mathbb{Z}/(p)$ such that $f(x) = (x^2-2)q(x) + (\cancel{(a+(p))}\,\bar{a})x + (\cancel{b+(p)}\,\bar{b})$. Then $0 = \Phi(f(x)) = \Phi(x^2-2)\Phi(q(x)) + \Phi((\cancel{a+(p)}\,\bar{a})x + (\cancel{b+(p)}\,\bar{b})) = 0 + \Phi((\cancel{a+(p)}\,\bar{a})x + (\cancel{b+(p)}\,\bar{b}))$. Thus $\Phi((\cancel{a+(p)}\,\bar{a})x + (\cancel{b+(p)}\,\bar{b})) = (\cancel{a+(p)}\,\bar{a})(\sqrt{2}+(p)) + (\cancel{b+(p)}\,\bar{b}) = (a\sqrt{2}+b) + (p)$. Therefore, $a\sqrt{2} + b \in (p)$. Since $a, b \in \mathbb{Z}$, this is possible only if $a = 0$ and $b \in (p)$. In other words, this is possible only if $a + (p) = b + (p) = 0$. Therefore, $f(x) = (x^2-2)q(x) \in (x^2-2)$.

Therefore, $\ker(\Phi) = (x^2-2)$, so the homomorphism $\tilde{\Phi}$ induced by $\Phi$ is an isomorphism from $\mathbb{Z}/(p)[x]/(x^2-2) \to \mathbb{Z}[\sqrt{2}]/(p)$ by ~~the first isomorphism theorem.~~ Lmm 8(iii) $\square$

**Exercise.** (Problem 21) Let $p \in \mathbb{Z}$ be an odd prime. Show that $\mathbb{Z}[\sqrt{2}]/(p)$ is an integral domain if and only if $(x^2-2)$ is an irreducible element of $\mathbb{Z}/(p)[x]$. Show that this occurs if and only if 2 is not a square in $\mathbb{Z}/(p)$.

*Proof.* By Problem 20, $\mathbb{Z}[\sqrt{2}]/(p)$ is isomorphic to $\mathbb{Z}/(p)[x]/(x^2-2)$. Thus it suffices to show that $\mathbb{Z}/(p)[x]/(x^2-2)$ is an integral domain if and only if $x^2-2$ is an irreducible element of $\mathbb{Z}/(p)[x]$. By Corollary 4 on P.300 (Dummit and Foote), since $\mathbb{Z}/(p)$ is a field, $\mathbb{Z}/(p)[x]$ is a UFD. By Proposition 12 on P.286, a nonzero element generates a prime ideal if and only if it is irreducible. By Proposition 13 on P.255, $(x^2-2)$ is a prime ideal if and only if $\mathbb{Z}/(p)[x]/(x^2-2)$ is an integral domain. Therefore, $\mathbb{Z}/(p)[x]/(x^2-2)$ is an integral domain if and only if $x^2-2$ is an irreducible element.

We will show that $\mathbb{Z}[\sqrt{2}]/(p)$ is not an integral domain if and only if 2 is a square in $\mathbb{Z}/(p)$.

- For any $a+(p) \in \mathbb{Z}/(p)$, $(a+\sqrt{2}+(p))(a-\sqrt{2}+(p)) = (a^2-2)+(p)$ in $\mathbb{Z}[\sqrt{2}]/(p)$. If $(a+(p))^2 = 2+(p)$ for some $a+(p) \in \mathbb{Z}/(p)$, then $(a+\sqrt{2}+(p))(a-\sqrt{2}+(p)) = (2-2)+(p) = 0$. Thus $\mathbb{Z}[\sqrt{2}]/(p)$ is not an integral domain.
- Suppose that $\mathbb{Z}[\sqrt{2}]/(p)$ is not an integral domain. Then $x^2-2$ is not irreducible. Since the degree of $x^2-2$ is 2 and every nonzero constant polynomial in $\mathbb{Z}/(p)[x]$ is a unit, $x^2-2$ must have a factor of degree 1. Choose $a, b \in \mathbb{Z}/(p)$ such that $(x+a)(x+b) = x^2-2$. We can assume that the leading coefficients of the factors are 1 because $\mathbb{Z}/(p)$ is a field. This implies $x^2+(a+b)x+ab = x^2-2$. Thus $a+b=0$, so $b=-a$. This implies $\cancel{x^2-2=(x+a)(x-a), \text{ so}}$ $-2=-a^2$. Thus $a^2=2$, so 2 is a square in $\mathbb{Z}/(p)$.

Therefore, $\mathbb{Z}[\sqrt{2}]/(p)$ is an integral domain if and only if 2 is not a square in $\mathbb{Z}/(p)$. ☐

**Exercise.** (Problem 22) Use your answers to 21 and 19 to determine for which of the following values of $p$, $x^2-2y^2=p$ has a solution: $p = 3, 5, 7, 11, 13, 17$.

*Proof.* By Problem 19, $x^2-2y^2=p$ has a solution if and only if $p$ is irreducible in $\mathbb{Z}[\sqrt{2}]$. Since $\mathbb{Z}[\sqrt{2}]$ is a UFD by Problem 14, by Proposition 12 on P.286, $p$ generates a prime ideal if and only if $p$ is irreducible. By Proposition 13 on P.255, $(p)$ is a prime ideal if and only if $\mathbb{Z}[\sqrt{2}]/(p)$ is an integral domain. By Problem 21, 2 is not a square in $\mathbb{Z}/(p)$ if and only if $\mathbb{Z}[\sqrt{2}]/(p)$ is an integral domain.

Therefore, $x^2-2y^2=p$ has a solution if and only if 2 is not a square in $\mathbb{Z}/(p)$.

- (Modulo 3) $2^2 \equiv 1$.
- (Modulo 5) $2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1$.
- (Modulo 7) $2^2 \equiv 4, 3^2 \equiv 2$.
- (Modulo 11) $2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 5, 5^2 \equiv 3, 6^2 \equiv 3, 7^2 \equiv 5, 8^2 \equiv 9, 9^2 \equiv 4, 10^2 \equiv 1$.
- (Modulo 13) $2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 3, 5^2 \equiv 12, 6^2 \equiv 10, 7^2 \equiv 10, 8^2 \equiv 12, 9^2 \equiv 3, 10^2 \equiv 9, 11^2 \equiv 4, 12^2 \equiv 1$.
- (Modulo 17) $2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 16, 5^2 \equiv 8, 6^2 \equiv 2$.

Therefore, $x^2-2y^2=p$ has a solution if $p=7,17$ and it ~~doesn't~~ does not if $p=3,5,11,13$. ☐

## 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 $\phi$ 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, $\deg_y(h_2(x,y)) \geq n$.

element

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. elem. 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 elem 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 $\mathrm{cont}(f(x,y)) = 1$.

$f(a,y) = y \in k[y]$, which is irred. ~~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 $k$.~~

$\square$