# 110A HW9

Warren Kim

Winter 2024

## Question 1

Let $R$ be a Euclidean domain, and let $a, b \in R$, such that $b \neq 0$, and let $d$ be a greatest common divisor of $a$ and $b$. Show that $d' \in R$ is also a greatest common divisor of $a$ and $b$ if and only if $d'$ is an associate of $d$.
[Hint: Your proof should also work for PIDs.]

### Response

**Proof:** Let $R$ be a Euclidean domain, $a, b \in R$ such that $b \neq 0$, and $d$ be a greatest common divisor of $a$ and $b$.
$(\implies)$ Suppose $d'$ is another greatest common divisor of $a$ and $b$. Then $d' \mid a$ and $d' \mid b$, so $d' \mid d$. Then $d = d'x$ for some $x \in R$. But since $d \mid a$ and $d \mid b$, we have that $d \mid d'$, so $d' = dy$ for some $y \in R$. Then $d = d'x = (dy)x$. Since $d \neq 0$, apply the cancellation property to get $1 = yx$, which shows that $x$ is a unit. This means that $d'$ is an associate of $d$.

$(\impliedby)$ Suppose $d'$ is an associate of $d'$. Then $d = d'x$ for some unit $x \in R$. Since $d$ is a greatest common divisor of $a$ and $b$, we have that $d \mid a$ and $d \mid b$, which can be written as $a = dp$, $b = dq$ for some $p, q \in R$. Then $a = dp = (d'x)p = d'(xp)$ and $b = dq = (d'x)q = d'(xq)$. This shows that $d' \mid a$ and $d' \mid b$. Now suppose that $c \mid a$ and $c \mid b$. Then $c \mid d$, so $d = cq$ but $d = d'x$, so we get that $d'x = cy$ for $y \in R$ but since $x$ is a unit, there exists $x^{-1} \in R$, so $d' = c(yx^{-1})$, so $c \mid d'$. Therefore, $d'$ is another greatest common divisor of $a$ and $b$.

Therefore, $d' \in R$ is also a greatest common divisor of $a$ and $b$ if and only if $d'$ is an associate of $d$.
□

# Question 2

Let $R$ be a Euclidean domain, and let $N$ be a norm. Show that $N' : R \to \mathbb{Z}$ given by $N'(a) = \min_{r \neq 0} N(ar)$ forms a norm. Moreover, show that $N'(a) \leq N'(ab)$ for nonzero $a, b \in R$

## Response

**Proof:** Let $R$ be a Euclidean domain and $N$ a norm. Consider $N' : R \to \mathbb{Z}$ given by $N'(a) = \min_{s \neq 0} N(as)$. Then $N'(0_R) = \min_{s \neq 0} N(0_R) = 0$. Take $a, b \in R$ such that $b \neq 0$. Then $N'(b) = \min_{s \neq 0} N(bs)$. Since $b \neq 0$, $s \neq 0$, and $R$ is an integral domain, we necessarily have that $bs \neq 0$. Since $N$ is a norm, we have that $a = (bs)q' + r$ for $q', r \in \mathbb{Z}$. such that $r = 0$ or $N(r) < N(bs)$. If $r = 0$, then we are done, so suppose not. If $N(r) < N(bs)$, then since $N'(r) = \min_{s \neq 0} N(rs)$, pick $s = 1$. Then $N'(r) = N(r \cdot 1) < N(bs) = N'(b)$. Put $q := sq'$. Then $a = bq + r$ for $q, r \in R$ such that $r = 0$ or $N'(r) < N'(b)$. Therefore, $N' : R \to \mathbb{Z}$ is a norm of $R$.

Let $a, b \in R$ where $a \neq 0$ and $b \neq 0$. Let $x, y \in R$ be nonzero such that $N'(ab) = \min_{r \neq 0} N(abr)$ and $N'(a) = \min_{r \neq 0} N(ar)$. Choose $x, y \in R$ such that $N(abx), N(ay)$ are minimal. Then Then $N'(a) = N(ay) \leq N(abx) = N'(ab)$. □

# Question 3

Let $F$ be a field. Show that the function $N : F \to \mathbb{Z}$ given by $N(a) = 0$ for all $a \in F$ gives a norm on $F$. Conclude that every field is a Euclidean domain.
[we briefly discussed this in class.]

## Response

**Proof:** Let $F$ be a field. Consider $N : F \to \mathbb{Z}$ given by $N(a) = 0$ for all $a \in F$. Then $N(0_F) = 0$. Now take $a, b \in R$ for $b \neq 0$. Then we have that $a = bq + r$. Since $b \neq 0$ and since $F$ is a field, there exists $b^{-1} \in F$, so define $q := ab^{-1}$ to get $a = b(ab^{-1}) + r = a \cdot 1 + r$. This implies that $r = 0$, so we are done. Therefore, $N$ is a norm on $F$. Since we can do this for any field, every field is a Euclidean domain. □

# Question 4

Let $R$ be an integral domain. Suppose $R[x]$ is a principal ideal domain. Show that $R$ must be a field.
[Hint: Think about $(x)$.]

## Response

**Proof:** Let $R$ be an integral domain and $R[x]$ a principal ideal domain. Consider the principal ideal $(x) \subseteq R[x]$ and a function $f : R[x] \to R$ with $f(p(x)) = p(0)$. Then

- $f(p(x) + q(x)) = p(0) + q(0) = f(p(x)) + f(q(x))$, so $f$ is **closed under addition**.
- $f(p(x) \cdot q(x)) = p(0) \cdot q(0) = f(p(x)) \cdot f(q(x))$, so $f$ is **closed under multiplication**.
- $f(1(x)) = 1$, so $f$ **preserves the multiplicative identity**.

so $f$ is a ring homomorphism. We have that $\ker(f) = \{p(x) : f(p(x)) = 0\} = (x)$, so $\ker(f) = (x)$. To show $\text{Im}(f) = R$, take $a \in R$. Then consider $p \in R$ such that $p(0) = a$. Then $f(p(x)) = p(0) = a \in R$. Therefore, $\text{Im}(f) = R$. Then by the **First Isomorphism Theorem**, we have that $R[x]/(x) \simeq R$.

Note that since $1 \notin (x)$, $(x) \neq R[x]$, so $(x) \subsetneq R[x]$ is a proper ideal. To show that $(x)$ is maximal, consider $(y) \subseteq R[x]$ such that $(y) \supseteq (x)$. If $\deg(y) = 0$, then $y$ is a unit, so $(y) = R[x]$. If $\deg(y) > 0$, then since $x \in (x) \subseteq (y)$, we can write $x = fy$ for some $f \in R[x]$. Then since $\deg(x) = 1$, $\deg(y) \leq \deg(x) = 1$, which means we necessarily have $\deg(y) = 1$. Then $x$ and $y$ are associates, so $(x) = (y)$. Therefore, $(x)$ is maximal, so $R[x]/(x)$ is a field. But since $R[x]/(x) \simeq R$, we have that $R$ is a field. $\square$

# Question 5

Let $R$ be a PID, and let $I \subseteq R$ be a prime ideal. Show that $R/I$ is a PID.

## Response

**Proof:** Let $R$ be a PID and $I \subseteq R$ a prime ideal. Consider $R/I$ and an ideal $J \subseteq R/I$. Consider the projection $\pi : R \to R/I$ given by $a \mapsto a + I$. Then the preimage of $J$ under $\pi$ is given by $\pi^{-1}(J) \supseteq I$. Since $R$ is a PID, $\pi^{-1}(J) = (a)$ for some $a \in R$. By the **Correspondence Theorem**, we have

$$\begin{aligned}
\pi(\pi^{-1}(J)) &= \pi((a)) \\
&= \{\pi(ar) : r \in R\} \\
&= \{(a+I)(r+I) : r + I \in R/I\} \\
&= \{ar + I : r + I \in R/I\} \\
\pi(\pi^{-1}(J)) &= (a + I)
\end{aligned}$$

But $\pi(\pi^{-1}(J)) = J$, so $J = (a + I)$, so J must be principal. Therefore, $R/I$ is a PID. □

# Question 6

Let $R$ be an integral domain. Prove that $R$ is a PID if and only if (i) every ideal of $R$ is finitely generated (i.e., every ideal $I \subseteq R$ can be written $I = (x_1, \cdots x_n)$ for $x_i \in R$) and (ii) whenever $a, b \in R$, the ideal $(a, b)$ is principal.

## Response

**Proof:** Let $R$ be an integral domain.

**( $\Longrightarrow$ )** Suppose $R$ is a PID. Take $x_1, \cdots, x_n \in R$. Then there exists $x \in R$ such that $(x) = (x_1, \cdots, x_n)$, so $(x_1, \cdots, x_n)$ is principal. This satisfies (i). Take $a, b \in R$. Then there exists $d \in R$ such that $(d) = (a, b)$, so $(a, b)$ is principal. This satisfies (ii).

**( $\Longleftarrow$ )** Suppose the following statements hold:

(i) Every ideal of $R$ is finitely generated; that is, every $I \subseteq R$ can be written $I = (x_1 \cdots, x_n)$ for $x_i \in R$.

(ii) Whenever $a, b \in R$, the ideal $(a, b)$ is principal.

We will induct on $n \in \mathbb{N}$. At $n = 2$, take $x_1, x_2 \in R$. Then $(x_1, x_2)$ is principal by (ii), so there exists $d_1 \in R$ such that $(d_1) = (x_1, x_2)$. Assume the base case holds for all $2 \leq k < n$. At $k = n$, take $x_1, \cdots, x_n \in R$. By the inductive hypothesis, $(d_{n-1}) = (x_1, \cdots, x_n)$, so $(d_n) = (d_{n-1}, x_n)$, which is principal by (ii). Therefore, this holds for all $n \in \mathbb{N}$. Since every ideal of $R$ is finitely generated by (i), $R$ is a PID. $\square$

# Question 7

Let $R$ be an integral domain, and let $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideal in $R$. Show their union $\bigcup_j I_j$ is also an ideal.

## Response

**Proof:** Let $R$ be an interal domain and $I_1 \subseteq I_2 \subseteq \cdots$ be a chain of ideals in $R$. Consider $\bigcup_j I_j$.

1. Since $I_1$ is an ideal, $0 \in I_1 \subseteq \bigcup_j I_j$, so the additive identity exists in $\bigcup_j I_j$.
2. Take $a \in I_n, b \in I_m$ and suppose without loss of generality that $n \leq m$. Then we have $a - b \in I_m \subseteq \bigcup_j I_j$, so $\bigcup_j I_j$ is closed under subtraction.
3. Take $a \in I_n$, $r \in R$. Then we have $ra, ar \in I_n \subseteq \bigcup_j I_j$, so $\bigcup_j I_j$ satisfies the absorption property.

Since $\bigcup_j I_j$ satisfies $(1) - (3)$, $\bigcup_j I_j$ is an ideal. □

# Question 8

Let $R$ be a UFD, and let $a, b, c \in R$. Suppose $a|c$ and $b|c$, and that 1 is a greatest common divisor of $a$ and $b$. Show that $ab|c$.

## Response

**Proof:** Let $R$ be a UFD, and let $a, b, c \in R$. Since $a, b \mid c$, we have that $ax = c = by$ for $x, y \in R$. Consider the unique factorizations $a = p_1^{r_1} \cdots p_n^{r_n}$ and $b = p_1^{s_1} \cdots p_m^{s_m}$, where $p_i$ is distinct. Without loss of generality, suppose that $n \leq m$ and that $p_i < p_{i+1}$ for $1 \leq i < m$. Since the greatest common divisor of $a$ and $b$ is 1, they share no irreducible factors, so the exponent at $p_i$ is $\min\{r_i, s_i\} = 0$ for $1 \leq i \leq m$. Express $c$ as its unique factorization $c = p_1^{t_1} \cdots p_m^{t_m}$. Since $a \mid c$, we have that $r_i \leq t_i$ for at least one $1 \leq i \leq n$. Similarly since $b \mid c$, $s_j \leq t_j$ for at least one $1 \leq j \leq m$. Then $ab = p_1^{r_1+s_1} \cdots p_n^{r_n+s_n} \cdot p_{n+1}^{s_{n+1}} \cdots p_m^{s_m}$, where $r_i + s_i = \max\{r_i, s_i\}$ for $1 \leq i \leq n$ and $s_i$ for $n < i \leq m$ since either $r_i = 0$ or $s_i = 0$. Then $ab \mid c$ since for every $p_i$, $\max\{r_i, s_i\} \leq t_i$ for $1 \leq i \leq n$ and $s_i \leq t_i$ for $n < i \leq m$. □

# Question 9

Let $R$ be an integral domain. Show that $R$ is a UFD if and only if $R$ satisfies the ascending chain condition on principal ideals and irreducible elements of $R$ are prime.

## Response

**Proof:** Let $R$ be an integral domain.

$(\implies)$ Let $R$ be a UFD. Consider $(a_1) \subseteq (a_2) \subseteq \cdots$ be an ascending chain of principal ideals in $R$. Then we can write $a_1$ as its unique factorization $a_1 = p_1^{r_1} \cdots p_n^{r_n}$ where $p_i$ is prime. Then $a_n \mid a_1$ so $a_n$ can be written as an associate of $p_1^{s_1} \cdots p_n^{s_n}$ where $0 \leq s_i \leq r_i$. Then for all $m \geq n$, we have that $(a_n) \subseteq (a_m)$. Then $a_m \mid a_n$ or its associates, so we can represent $a_m$ as the unique factorization $a_m = p_1^{t_1} \cdots p_n^{t_n}$ where $0 \leq t_i \leq s_i$ for all $i$. Therefore, $R$ satisfies the ascending chain condition. From class, we showed that if $R$ is a UFD, then $p \in R$ is irreducible if and only if it is prime.

$(\impliedby)$ Suppose $R$ satisfies the ascending chain condition on principal ideals and irreducible elements of $R$ are prime. Then from class, $R$ can be written as a product of irreducibles. To show that it is unique, suppose for the sake of contradiction that $a$ has two different factorizations $a = p_1 \cdots p_n = q_1 \cdots q_m$ where $p_i, q_j$ are irreducible. Then $p_1$ is prime since it is irreducible, so it must divide some $q_j$. Without loss of generality, suppose $p_1 \mid q_1$. Then $p_1, q_1$ are associates so we have that $p_1 \cdots p_n = ap_1q_2 \cdots q_m$ where $a \in R$ is a unit. Since we are over an integral domain, apply the cancellation property to get $p_2 \cdots p_n = aq_2 \cdots q_m$. Without loss of generality, suppose $n \leq m$. Then applying the previous steps iteratively, we are left with $1 = a_1 \cdots a_n q_{n+1} \cdots q_m$. But this implies that $q_{n+1}, \cdots, q_m$ are units, a contradiction. Therefore, $m = n$ so $a$ has a unique factorization. Therefore, $R$ is a UFD.

□