110A HW8

Warren Kim

Winter 2024

Throughout this section, F is a field and $F[x]$ is the ring of polynomials with F coefficients.

Question 1

1. Let $a \in F$. Show that $x - a \in F[x]$ is irreducible.
2. Let $f \in F[x]$, and suppose $\deg(f) = n > 0$. Show that f has at most n roots.

Response

1. Let $a \in F$. Show that $x - a \in F[x]$ is irreducible.

   Proof: Let $a \in F$ and $x - a \in F[x]$. Since $\deg(x-a) = 1$, we have that the only polynomials with degree less than 1 are constant polynomials with degree 0. Take $g \in F[x]$ such that $g \mid (x - a)$. Then $x - a = gh$ for some $h \in F[x]$, so

   $$1 = \deg(x - a) = \deg(gh) = \deg(g) + \deg(h)$$

   and since $g \mid (x - a)$ and $h \mid (x - a)$, $\deg(g) \neq 0$ and $\deg(h) \neq 0$. Since $g \mid (x - a)$, $0 \leq \deg(g) \leq \deg(x - a) = 1$. There are two cases:

   (a) If $\deg(g) = 1$, then h is a unit, so g and $x - a$ are associates.

   (b) If $\deg(g) = 0$, then g is a unit, so h and $x - a$ are associates.

   Therefore, the only factors of $x - a$ are units an associates, so $x - a$ is irreducible. $\square$

2. Let $f \in F[x]$, and suppose $\deg(f) = n > 0$. Show that f has at most n roots.

   Proof: Let $f \in F[x]$ and suppose $\deg(f) = n > 0$. We will induct on $n \in \mathbb{N}$. At $n = 1$, we have that $f = a_0 + a_1 x = 0$ with $a_1 \neq 0$, so f has at most one root. Suppose the base case holds for all $1 \leq k < n$. Then when $k = n$, if f has a root $r \in F$, we can uniquely factor f to get $f = (x - r)g$ for some $g \in F[x]$ where $\deg(g) = n - 1$. Then by the inductive hypothesis, g has at most k roots, so f has at most $n - 1 + 1 = n$ roots since r is a root by assumption. Therefore, this holds for all $n \in \mathbb{N}$. $\square$

Question 2

Let $I \subseteq F[x]$ be an ideal. Show that I is principal.

Response

Proof: Let $I \subseteq F[x]$ be an ideal. If $I = \{0\}$, then we are done since F is a field $\implies$ (0) is principal, so suppose not. Take $f \in I$ to be a nonzero polynomial of least degree, and consider (f). $((f) \subseteq I)$ Since $f \in I$, $fa \in I$ for all $a \in F[x]$, so $(f) \subseteq I$.

$((f) \supseteq I)$ Take $a \in I$. Then we can write $a = fq + r$ for $q, r \in F[x]$ where $0 \leq \deg(r) < \deg(f)$. Then we can rewrite the equation as $r = a - fq$. Because $f \in I$, we have $fq \in I$ since I is an ideal. Then $r = a - fq \in I$ since $a, fq \in I$. Then it must be the case that $\deg(r) = 0$ since otherwise, we have that $\deg(r) = \deg(a - fq) < \deg(f)$ which is a contradiction since f was chosen to be the polynomial with least degree. Therefore, $\deg(r) = 0$ so $a = fq$; i.e. $f \mid a$, so $a \in (f)$. Since a was arbitrary, $I \subseteq (f)$.

Since we showed $(f) \subseteq I$ and $(f) \supseteq I$, we have that $(f) = I$ is principal. $\square$

Question 3

Let R be an integral domain (you can do this with any commutative ring). Show that the relation $a \sim b$ if a and b are associates forms an equivalence relation.

Response

Proof: Note that a, b are associates if $a = bc$ for some $c \in R$. Let R be an integral domain and $a, b, c \in R$. Then

(i) $a \sim a$. Pick $d = 1 \in R$. Then $a = ad = a \cdot 1 = a$; i.e. a and a are associates, so $\sim$ is **reflexive**.

(ii) $a \sim b \implies b \sim a$. We have that $a = bd$ for some unit $d \in R$. Since d is a unit, there exists $d^{-1} \in R$. Multiplying both sides by d^{-1}, we get $ad^{-1} = bd \cdot d^{-1} = b$; i.e. b and a are associates, so $\sim$ is **symmetric**.

(iii) $a \sim b, b \sim c \implies a \sim c$. We have that $a = bd$ and $b = ce$ for some units $d, e \in R$. Then $a = bd = (ce)d = c(ed)$. Then since $d, e \in R$ are units, there exist $d^{-1}, e^{-1} \in R$ such that $dd^{-1} = 1$ and $ee^{-1} = 0$. Then $de \cdot e^{-1}d^{-1} = d \cdot 1 \cdot d^{-1} = 1$, so de is a unit. Setting $f := ed$, we get $a = cf$. Therefore, a and c are associates, so $\sim$ is **transitive**.

Since (1) - (3) hold, $\sim$ is an equivalence relation on elements of R. $\square$

Question 4

Let R be an integral domain, and let $p \in R$. Show that p is irreducible if and only if $p = bc$ implies b or c is a unit.

Response

Proof: Let R be an integral domain, and let $p \in R$.
($\Longrightarrow$) Suppose p is irreducible. Let $p = bc$ for some $b, c \in R$. Then $p \mid p = bc$. There are two cases:

Case 1: If b is a unit, then we are done.

Case 2: If b is an associate of p , then c is a unit.

In either case, either b or c is a unit.

($\Longleftarrow$) Suppose "$p = bc$ implies that either b or c is a unit". Let $b \in R$ such that $b \mid p$. Then $p = bc$ for some $c \in R$. Then either b or c is a unit. If b is a unit, then c is an associate of p. If c is a unit, then b is an associate of p. In either case, the only factors of p are units and associates, so p is irreducible. Because we have proved both directions, we have that p is irreducible if and only if $p = bc$ implies b or c is a unit. $\square$

Question 5

Let R be an integral domain, and let $p \in R$. Show that the principal ideal (p) is a prime ideal if and only if p is prime.

Response

Proof: Let R be an integral domain and $p \in R$. Consider the principal ideal $(p) \subseteq R$.
$(\implies)$ Suppose (p) is a prime ideal. Then, whenever $ab \in (p)$ for $a, b \in R$, we have either $a \in (p)$ or $b \in (p)$. Take $a, b \in R$ such that $ab \in (p)$. Then $p \mid ab$ by definition since we can represent $ab = pr$ for some $r \in R$. Since either $a \in (p)$ or $b \in (p)$, we have that $p \mid a$ or $p \mid b$, so p is prime.

$(\impliedby)$ Suppose p is prime; i.e. if $p \mid ab$ for $a, b \in R$, then either $p \mid a$ or $p \mid b$. Then since $p \mid ab$, we can write $ab = pr$ for some $r \in R$, so $pr = ab \in (p)$. Without loss of generality, suppose $p \mid a$. Then $a = pq$ for some $q \in R$, so $pq = a \in (p)$. Since $a, b \in R$ were arbitrary, (p) is a prime ideal. Because we have proven both directions, we have that (p) is a prime ideal if and only if p is prime. $\square$

Question 6

Let R be an integral domain. We denote $S(R) = \{(a,b)|a,b \in R; b \neq 0\}$. Consider the relation $(a,b) \sim (a',b')$ if $ab' = a'b$.

1. Show that the relation $\sim$ forms an equivalence relation on elements of $S(R)$.
2. Suppose $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$. Show that $(ad+bc, bd) \sim (a'd' + b'c', b'd')$

Response

Let R be an integral domain and define $S(R) = \{(a,b) : a,b \in R; b \neq 0\}$. Consider the relation $(a,b) \sim (a',b')$ if $ab' = a'b$.

1. Show that the relation $\sim$ forms an equivalence relation on elements of $S(R)$.

   Proof: Let $a,b,c,d,e,f \in R$. Then

   (i) $(a,b) \sim (a,b)$. By definition, $(a,b) \sim (a,b) \iff ab = ba$. Since integral domains are commutative, this is true, so $\sim$ is **reflexive**.

   (ii) $(a,b) \sim (c,d) \implies (c,d) \sim (a,b)$. By definition, $(a,b) \sim (c,d) \iff ac = bd$. Since equality is symmetric, we have that $bd = ac \iff (c,d) \sim (a,b)$, so $\sim$ is **symmetric**.

   (iii) $(a,b) \sim (c,d), (c,d) \sim (e,f)$. By definition, $(a,b) \sim (c,d) \iff ad = bc$ and $(c,d) \sim (e,f) \iff cf = de$. Then

   $$\begin{aligned} ad &= bc \\ adf &= bcf \\ afd &= bde && cf = de \\ af &= be && \text{cancellation property since } d \neq 0 \end{aligned}$$

   Therefore, $\sim$ is **transitive**.

   Since (1) - (3) hold, $\sim$ is an equivalence relation on elements of $S(R)$. $\square$

2. Suppose $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$. Show that $(ad+bc, bd) \sim (a'd' + b'c', b'd')$

   Proof: Suppose $(a,b) \sim (a',b')$ and $(c,d) \sim (c',d')$. By definition, $ab' = a'b$ and $cd' = c'd$. Note that R is commutative since it is an integral domain. Then

   $$\begin{aligned} ab' &= a'b \\ ab'dd' &= a'bdd' \end{aligned}$$

   and

   $$\begin{aligned} cd' &= c'd \\ cd'bb' &= c'dbb' \end{aligned}$$

So,

$$\begin{aligned}
ab'dd' &= a'bdd' \\
ab'dd' + cd'bb' &= a'bdd' + c'dbb' \\
ad(b'd') + bc(b'd') &= a'd'(bd) + b'c'(bd) \\
(ad+bc)\cdot(b'd') &= (a'd'+b'c')\cdot(bd)
\end{aligned}$$

so $(ad+bc, bd) \sim (a'd'+b'c', b'd')$. $\square$

Question 7

Let F be a field, and consider its field of fractions $Frac(F)$. Show that $F \cong Frac(F)$. [Hint: what can you say about the homomorphism $f : F \to Frac(F)$ given by $f(a) = \frac{a}{1}$?]

Response

Proof: Let F be a field, and consider its field of fractions $Frac(F)$. Define $f : F \to Frac(F)$ given by $a \mapsto \frac{a}{1}$.

1. For any $a, b \in F$, $f(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = f(a) + f(b)$, so f is closed under addition.
2. For any $a, b \in F$, $f(a \cdot b) = \frac{a \cdot b}{1} = \frac{a}{1} \cdot \frac{b}{1} = f(a) \cdot f(b)$, so f is closed under multiplication.
3. $f(1_F) = \frac{1}{1} = 1_{Frac(F)}$, so $1 \in Frac(F)$.

so f is a ring homomorphism. To show that f is injective, note that since F is a field, it has two ideals: (0) and F. Then since $f(1) = \frac{1}{1} = 1 \neq 0$, we have that $1 \notin \ker(f)$, so $\ker(f) = \{0\}$ which implies that f is **injective**. To show that f is surjective, consider an arbitrary $\frac{a}{b} \in Frac(F)$ where $a, b \in F$ and $b \neq 0$. Since F is a field and $b \neq 0$, b is a unit, there exists $b^{-1} \in F$. Then

$$\begin{aligned} a &= a \cdot 1 \\ &= a \cdot (bb^{-1}) \\ a \cdot 1 &= ab^{-1} \cdot b \end{aligned}$$

so $\frac{a}{b} = \frac{ab^{-1}}{1}$. Put $x \in F$ to be $x := ab^{-1}$. Then $f(x) = \frac{ab^{-1}}{1} = \frac{a}{b}$. Since $\frac{a}{b}$ was arbitrary, f is **surjective**. Because f is both injective and surjective, f is a bijection so $F \simeq Frac(F)$. $\square$