Problem §1 An integral domain R is an **Euclidean domain** if there is a function $\delta : R \setminus \{0\} \to \{0, 1, \ldots\}$ such that

- if $a, b \in R$ non-zero, then $\delta(a) \leq \delta(ab)$.
- if $a, b \in R$ and $b \neq 0$, then there exist $q, r \in R$ such that $a = bq + r$ and either $r = 0$ or $\delta(r) < \delta(b)$.

Explain why $\mathbb{Z}$ and $F[x]$ are Euclidean domains where F is a field. Prove that any ideal in a Euclidean domain is principal.

Solution: For $\mathbb{Z}$, consider the absolute value function $|\cdot| : \mathbb{Z} \setminus \{0\} \to \{0, 1, \ldots\}$. Clearly, $|\cdot|$ satisfies the two requirements, and so $\mathbb{Z}$ is a Euclidean domain.

For $F[x]$, consider the degree map $\deg : F[x] \setminus \{0\} \to \{0, 1, \ldots\}$. We know that for any two polynomials $f, g \in F[x]$, we have

$$\deg(fg) = \deg(f) + \deg(g) \geq \deg(f);$$

and by Proposition 5.20 (Division Algorithm for polynomials), the second condition follows. Thus $F[x]$ is a Euclidean domain.

Let E be a Euclidean domain, and let I_E be an ideal of E. Let $a \in I_E$ be the value with the smallest $\delta(a)$ (note that a is not unique; multiple such as could exist. For example, in the principal ideal $(x^2 + 2)F[x]$, all polynomials with degree 2 would work for a). We claim that $(a) = aE$ generates I_E.

Let $b \in I_E$ be any element in the ideal. Since E is a Euclidean domain, we have

$$b = aq + r,$$

and either $r = 0$ or $\delta(r) < \delta(a)$. If $r = 0$, b is clearly a multiple of a (and hence $b \in I$), so suppose $r \neq 0$. By the closure of ideals, $r = b - aq \in I_E$; but then $r \in I$, and $\delta(r) < \delta(a)$, a contradiction (since by construction, we assume that a has the smallest delta). Thus r must be 0, and hence for any $b \in I_E$, b is divisible by a. Therefore (a) generates I_E, and so I_E is a principal ideal. Since the choice of a and I_E was arbitrary, this holds for any ideal of E, and so every ideal of E is principal.

Problem §2

(a) Let p be a prime integer and J be the set of polynomials in $\mathbb{Z}[x]$ whose constant terms are divisible by p; show that J is a maximal ideal.

(b) Show that $(x - 1)\mathbb{Z}[x]$ is a prime ideal in $\mathbb{Z}[x]$ that is not maximal.

(c) Find an ideal in $\mathbb{Z} \times \mathbb{Z}$ that is prime, but not maximal.

Solution:

(a) First, we observe that $J = p\mathbb{Z}[x] + x\mathbb{Z}[x]$; in other words, all polynomials in $f \in J$ are of the form

$$f(x) = np + a_1 x + \ldots, \text{ where } n \in \mathbb{Z}.$$

Consider the map $\phi : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}$, given by

$$\phi(f) = \phi(a_0 + a_1 x + \ldots) = a_0 \mod p.$$

In other words, ϕ maps a polynomial $f \in \mathbb{Z}[x]$ into the equivalence class of its constant term, modulo p. ϕ is clearly surjective, since $a_0 \in \mathbb{Z}$, and every $a \in \mathbb{Z}/p\mathbb{Z}$ is also in $\mathbb{Z}$. We observe that $\ker(\phi)$ consists of all polynomials of the form

$$f(x) \in p\mathbb{Z}[x] + x\mathbb{Z}[x];$$

equivalently, $\ker(\phi) = \{\text{all polynomials with constant terms}\} = \{f(x) \mid f(x) \in p\mathbb{Z}[x] + x\mathbb{Z}[x]\} = J$ (intuitively, only the constant term matters, since any of the x^n terms do not affect the result; only

the equivalence class of a_0 matters). By Proposition 3.31(b)iii, since $\phi : \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}$ is surjective and $\ker(\phi) = J$, the map

$$\overline{\phi} : \mathbb{Z}[x]/J \to \mathbb{Z}/p\mathbb{Z}$$

is an isomorphism. Proposition 3.17 additionally tells us that $\mathbb{Z}/p\mathbb{Z}$ is a field; hence $\mathbb{Z}[x]/J \cong \mathbb{Z}/p\mathbb{Z}$ is a field as well. Thus by Proposition 3.40, J is thus a maximal ideal.

(b) Let $I = (x-1)\mathbb{Z}[x]$ (the ideal generated by $(x-1)$). Consider the evaluation map at 1:

$$E_1 : \mathbb{Z}[x] \to \mathbb{Z},\ E_1(f(x)) = f(1).$$

The kernel of E_1 is the set of all polynomials with 1 as a root; equivalently,

$$\ker(E_1) = \{f(x) \mid f(x) \in (x-1)a(x),\ a(x) \in \mathbb{Z}[x]\} = (x-1)\mathbb{Z}[x] = I$$

(the ideal $(x-1)\mathbb{Z}[x]$ consists of all polynomials with $(x-1)$ as a factor; in other words, all polynomials that have 1 as a root are in $(x-1)\mathbb{Z}[x] = I$). Clearly, E_1 is surjective as well; for any $a \in \mathbb{Z}$, the polynomial $ax \in \mathbb{Z}[x]$ yields $E_1(ax) = a$. Hence by Proposition 3.31(b)iii, the map

$$\overline{E_1} : \mathbb{Z}[x]/I \to \mathbb{Z}$$

is an isomorphism. But $\mathbb{Z}$ is an integral domain; hence $\mathbb{Z}[x]/I \cong \mathbb{Z}$ is an integral domain as well. Thus by Proposition 3.40, I is a prime ideal. However, I is not maximal, since $\mathbb{Z}$ is not a field (thus by isomorphism, the quotient ring $\mathbb{Z}[x]/I$ is not a field either, and so I is not a maximal ideal).

(c) Let $I = (0,b)\mathbb{Z} \times \mathbb{Z}$ (the ideal generated by $(0,b)$). Consider the map

$$\phi : \mathbb{Z} \times \mathbb{Z},\ \phi(a,b) = a \text{ for } a, b \in \mathbb{Z}.$$

The kernel of ϕ consists of all elements in $\mathbb{Z} \times \mathbb{Z}$ of the form $(0,b)$ (b can be anything, as long as a is 0); equivalently, $\ker(\phi) = I$. Clearly, ϕ is surjective as well; for any $a \in \mathbb{Z}$, the pair $(a,0) \in \mathbb{Z} \times \mathbb{Z}$ yields $\phi(a,0) = a$. Hence by Proposition 3.31(b)iii, the map

$$\overline{\phi} : \mathbb{Z} \times \mathbb{Z}/I \to \mathbb{Z}$$

is an isomorphism. But $\mathbb{Z}$ is an integral domain; hence $\mathbb{Z} \times \mathbb{Z}/I$ is an integral domain as well. Thus by Proposition 3.40, I is a prime ideal. However, I is not maximal, for the same reasons listed above; $\mathbb{Z}$ is not a field, so the quotient ring $\mathbb{Z} \times \mathbb{Z}/I$ is not a field either, and so I is not a maximal ideal.

Problem §3 (5.7)

(a) Let F be a finite field. Prove that

$$\prod_{\alpha \in F^*} \alpha = -1.$$

Let p be a prime, and apply this formula to the field $\mathbb{F}_p$ to deduce Wilson's formula:

$$(p-1)! \equiv -1 (\mod p).$$

(b) As a follow-up, let $m \geq 2$ be an integer that need not be prime. Prove that

$$\prod_{\alpha \in (\mathbb{Z}/m\mathbb{Z})^*} \alpha = \pm 1.$$

Solution:

(a) We begin with one lemma:

Lemma 1. *Any finite field F with more than 2 elements has only two self-inverses: ± 1.*

Proof. Let $a \in F^*$. a is a self-inverse if

$$x^2 = 1 \iff x^2 - 1 = 0 \iff (x+1)(x-1) = 0.$$

Since F is an integral domain (and so has the cancellation property), either $x = 1$ or $x = -1$. Thus $x = \pm 1$ are the only self-inverses in F. [Note: if $F = \mathbb{F}_2$ only has two elements, and $1 = -1$, so $\mathbb{F}_2$ only has one self-inverse]. $\square$

Now, consider $\prod_{\alpha \in F^*}$. For any α where $x^2 \neq 1$, α has a unique inverse β such that $\alpha\beta = \beta\alpha = 1$; this shows that $\beta \in F^*$ as well. Thus, for any non-self-inverse $\alpha \in F^*$, its unique inverse $\beta \in F^*$ as well, so all non-self-inverses cancel out.

Hence we are left with only self-inverses; if F only has two elements, then $\prod_{\alpha \in F^*} \alpha = 1 = -1$, so consider F with more than two elements. By the lemma, the only self-inverses are ± 1; thus

$$\prod_{\alpha \in F^*} \alpha = 1 \cdot -1 = -1,$$

as required.

Moreover, for a finite field $\mathbb{F}_p$,

$$\prod_{\alpha \in \mathbb{F}_p^*} \alpha = (p-1)(p-2)\dots(2)(1) = (p-1)! \equiv -1(\mod p),$$

thus proving Wilson's Formula.

(b) For $m = 2$, this is clearly satisfied, so consider all $m > 2$. Consider any $\alpha \in (\mathbb{Z}/m\mathbb{Z})^*$. Like above, any $\alpha \in (\mathbb{Z}/m\mathbb{Z})^*$ has a unique multiplicative inverse $\beta \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $\alpha\beta = \beta\alpha = 1$; moreover, $\beta \in (\mathbb{Z}/m\mathbb{Z})^*$. Thus $\alpha\beta = 1$ for all non-self-inverses, and like before, both are cancelled out in the product.

Thus again we are left with only self-inverses; i.e. all $\alpha \in (\mathbb{Z}/m\mathbb{Z})^*$ that satisfy $\alpha^2 = 1$. Note that if $\alpha^2 \equiv 1(\mod m)$, then

$$(m-\alpha)^2 = m^2 - 2m\alpha - \alpha^2 \equiv -\alpha^2 \equiv -1(\mod m).$$

That is, if α is a self-inverse, then $m - \alpha$ is also a self-inverse; moreover, $m - \alpha \in (\mathbb{Z}/m\mathbb{Z})^*$ (since $0 < m - \alpha < m$, so $m - \alpha \in \mathbb{Z}/m\mathbb{Z}$). Additionally, $m - \alpha \neq \alpha$; otherwise, if $m - \alpha \equiv \alpha$, then $m \equiv 2\alpha \equiv 0(\mod m)$, so $\alpha \equiv 0(\mod m)$. But $\gcd(\alpha, m) = 1$ (recall by Proposition 3.17 that $\alpha \in (\mathbb{Z}/m\mathbb{Z})^*$ if and only if $\gcd(\alpha, m) = 1$), a contradiction.

Consider

$$\alpha(m-\alpha) = \alpha m - \alpha^2 \equiv -\alpha^2 \equiv -1(\mod m).$$

In other words, for every self-inverse $\alpha \in (\mathbb{Z}/m\mathbb{Z})^*$, there exists some $m - \alpha \neq \alpha \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $\alpha(m-\alpha) \equiv -1(\mod m)$. Thus, letting

$$\varphi = \{ \text{ all self-inverses } \alpha \in (\mathbb{Z}/m\mathbb{Z})^* \},$$

we have (since all non-self-inverses cancel out)

$$\prod_{\alpha \in (\mathbb{Z}/m\mathbb{Z})^*} \alpha = \prod_{\alpha \in \varphi} \alpha = (-1)^{\frac{|\varphi|}{2}} = \pm 1.$$

(Note that $|\varphi|$ is even, since every self-inverse $\alpha \in \varphi$ has a distinct and different complement self-inverse $m - \alpha \in \varphi$).

Therefore $\prod_{\alpha \in (\mathbb{Z}/m\mathbb{Z})^*} \alpha = \pm 1$, as required. (It seems that whether the product is 1 or -1 depends on the number of self-inverses are in $\mathbb{Z}/m\mathbb{Z}$; if there are an odd number of self-inverse—complement-self-inverse pairs, then it is -1; otherwise, it is 1. However, I'm not entirely sure how to characterize the number of pairs are in a given $\mathbb{Z}/m\mathbb{Z}$).

Problem §4 (5.15) Let F be a field, and suppose that the polynomial $X^2 + X + 1$ is irreducible in $F[X]$. Let

$$K = F[X]/(X^2 + X + 1)F[X]$$

be the quotient ring, so we know from Theorem 5.26 that K is a field. We will put bars over polynomials to indicate they represent elements in K.

(a) Find a polynomial $p(X) \in F[X]$ of degree at most 1 satisfying

$$\overline{p(X)} = (\overline{X+3}) \cdot (\overline{2X+1}).$$

(b) Find a polynomial $q(X) \in F[X]$ of degree at most 1 satisfying

$$\overline{q(X)} \cdot (\overline{X+1}) = \overline{1}.$$

(c) Find a polynomial $r(X) \in F[X]$ of degree at most 1 satisfying

$$\overline{r(X)}^2 = -\overline{3}.$$

Solution:

(a) First, note that

$$(X+3) \cdot (2X+1) = 2X^2 + 7X + 3 = 5X + 1 + (2X^2 + 2X + 2).$$

Thus $\overline{p(X)} = (\overline{X+3}) \cdot (\overline{2X+1}) = \overline{5X+1}$, so $p(X) = 5X + 1$.

(b) First, observe that

$$\overline{-X^2 - X} = \overline{1},$$

since

$$\overline{-X^2 - X} \equiv \overline{-X^2 - X} + \overline{0} \equiv -X^2 - X + (X^2 + X + 1) \equiv \overline{1}.$$

Thus, if we take $q(X) = -X$ ($-X$ exists in $F[X]$ since $F[X]$ is a ring), then

$$\overline{q(X)}(\overline{X+1}) = \overline{-X^2 - X} = \overline{1}.$$

(c) Observe that

$$-\overline{3} \equiv -\overline{3} + \overline{0} \equiv -\overline{3} + \overline{4X^2 + 4X + 4} \equiv \overline{4X^2 + 4X + 1}.$$

Thus, if we take $r(X) = 2X + 1$, then

$$\overline{r(X)}^2 = (\overline{2X+1})^2 = \overline{4X^2 + 4X + 1} = -\overline{3}.$$

Problem §5 Given a field extension L/K, a K-automorphism of L is an isomorphism $\phi : L \to L$ for which $\phi(a) = a$ for all $a \in K$; that is, ϕ fixes all elements of K. The set of all K-automorphisms of L is called the **Galois group** of L/K, and is denoted by $\mathrm{Gal}_K L$.

(a) Prove that $\mathrm{Gal}_K L$ is in fact a group.

(b) Suppose that $f(x) \in K[x]$ is a polynomial and $\alpha \in L$ is a root. If $\sigma \in \mathrm{Gal}_K L$, show that $\sigma(\alpha)$ is also a root of $f(x)$.

(c) Let $L = \mathbb{Q}(\sqrt{D})$ for some square-free integer D. Write down all elements in $\mathrm{Gal}_{\mathbb{Q}} L$, justifying your reasoning.

Solution:

(a) First, we show closure (to ensure that two K-automorphisms in $\mathrm{Gal}_K L$ is still a K-automorphism in $\mathrm{Gal}_K L$). Let $\phi_1, \phi_2 \in \mathrm{Gal}_K L$. If $a \in K$, then

$$\phi_1 \circ \phi_2(a) = \phi_1(a) = a = \phi_2(a) = \phi_2 \circ \phi_1(a).$$

Moreover, recall that the composition of two isomorphisms is itself an isomorphism. Thus $\phi_1 \circ \phi_2$ is a K-automorphism, and so $\mathrm{Gal}_K L$ is closed.

Associativity naturally follows from the associativity of function composition: for $\phi_1, \phi_2, \phi_3 \in \mathrm{Gal}_K L$, $a \in L$,

$$\phi_1 \circ (\phi_2 \circ \phi_3)(a) = \phi_1 \circ (\phi_2(\phi_3(a))) = \phi_1(\phi_2(\phi_3(a))) = (\phi_1 \circ \phi_2) \circ \phi_3(a).$$

Next, consider $\phi_I : L \to L,\ a \mapsto a$. $\phi_I(a) = a$; moreover, this is clearly an isomorphism. Thus $\phi_I \in \mathrm{Gal}_K L$. For any $\phi \in \mathrm{Gal}_K L$, $a \in L$,

$$\phi \circ \phi_I(a) = \phi(a) = \phi_I \circ \phi(a),$$

and so ϕ_I is the identity element of $\mathrm{Gal}_K L$.

Finally, let $\phi \in \mathrm{Gal}_K L$. For $b \in L \setminus K$, let $b' = \phi(b)$. Note that isomorphism properties force $b' \in L \setminus K$, and b' unique. Define a function

$$\phi' : L \to L,\ a \mapsto a \forall a \in K,\ b' \mapsto b \forall b' \in L \setminus K.$$

In other words, ϕ' maps all $a \in K$ to itself, and for any $b' \in L \setminus K$, ϕ' maps b' to the unique b that satisfies $\phi(b) = b'$ (again, we know the existence and uniqueness of b because ϕ is isomorphic). By definition, we have

$$\phi \circ \phi'(a) = \phi(a) = a = \phi'(a) = \phi \circ \phi'(a)$$

for all $a \in K$, and

$$\phi' \circ \phi(b) = \phi'(b') = b = \phi \circ \phi'(b)$$

for all $b \in L \setminus K$. Thus every $\phi \in \mathrm{Gal}_K L$ has an inverse, and so $\mathrm{Gal}_K L$ is a group.

(b) Suppose $f(x) \in K[x]$ and $\alpha \in L$ is a root of $f(x)$. Note that $f(x)$ can be represented as

$$f(x) = a_0 + a_1 x + \ldots, \text{ where } a_i \in K;$$

thus

$$f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + \ldots = 0.$$

But homomorphisms preserve 0, so

$$f(\alpha) = 0 = \sigma(0) = \sigma(a_0 + a_1\alpha + a_2\alpha^2 + \ldots) = \sigma(a_0) + \sigma(a_1)(\sigma(\alpha)) + \ldots.$$

But every $a_i \in K$, so they remain unchanged by σ:

$$0 = \sigma(f(\alpha)) = \sigma(a_0) + \sigma(a_1)(\sigma(\alpha)) + \ldots = a_0 + a_1\sigma(\alpha) + a_2\sigma(\alpha)^2 + \ldots = f(\sigma(\alpha)).$$

Hence if α is a root of f, then $\sigma(\alpha)$ is also a root.

(c) Any element of $\mathrm{Gal}_{\mathbb{Q}} L$ must be a $\mathbb{Q}$-automorphism; in other words, for any $a + b\sqrt{D} \in L$, if $\phi \in \mathrm{Gal}_{\mathbb{Q}} L$, then

$$\phi(a + b\sqrt{D}) = \phi(a) + \phi(b)\phi(\sqrt{D}) = a + b \cdot \phi(\sqrt{D}) [\text{ since } a, b \in \mathbb{Q}].$$

But since $D \in \mathbb{Z} \subseteq \mathbb{Q}$ and ϕ fixes elements of $\mathbb{Q}$, $D = \phi(D) = \phi(\sqrt{D}^2) = \phi(\sqrt{D})^2$; thus $\phi(\sqrt{D}) = \pm D$. Hence the Galois group $\mathrm{Gal}_{\mathbb{Q}} L$ has two elements: $\phi_1(a + b\sqrt{D}) = a + b\sqrt{D}$ (the identity) and $\phi_2(a + b\sqrt{D}) = a - b\sqrt{D}$.

Problem §6 (5.19) Let F be a finite field with q elements.

(a) Prove that every non-zero element of F is a root of the polynomial $x^{q-1} - 1$.

(b) Prove that every element of F is a root of the polynomial $x^q - x$.

(c) Prove the formula

$$\prod_{\alpha \in F} (x - \alpha) = x^q - x.$$

Solution:

(a) By definition, every non-zero element $a \in F$ has a multiplicative inverse; that is,

$$F^* = F \setminus \{0\}, \text{ and } |F| = q - 1.$$

Let $\alpha \in F^*$, and note that F^* is a group with $q-1$ elements. By Corollary 2.42, the order of α divides the order of F^*; equivalently, if $|\alpha| = n$, then $a - q = kn$ for some $k \in \mathbb{Z}$. Thus

$$\alpha^{q-1} = \alpha^{kn} = (\alpha^n)^k = 1^k = 1.$$

Thus for any non-zero $a \in F$, $a \in F^*$, and so given a polynomial

$$f(x) = x^{q-1} - 1,$$

we have $f(a) = a^{q-1} - 1 = 1 - 1 = 0$. Hence every non-zero $a \in F$ is a root of $f(x) = x^{q-1} - 1$.

(b) Consider $g(x) = xf(x) = x(x^{q-1} - 1) = x^q - x$. From above, any non-zero $\alpha \in F$ is a root of $x^{q-1} - 1$, and so is a root of $g(x)$ as well:

$$g(x) = \alpha^q - \alpha = \alpha(\alpha^{q-1} - 1) = \alpha(1 - 1) = 0.$$

Moreover, clearly $g(0) = 0^q - 0 = 0$. Thus every element in F is a root of $g(x) = x^q - x$.

(c) (b) tells us that $g(x) = x^q - x$ has q distinct roots; specifically, every element of F is a root of $g(x)$. Theorem 5.34 tells us that $g(x)$ has at most $\deg(g) = q$ roots. Thus the elements of F are only **and** all of $g(x)$'s roots. That is, since polynomials uniquely factor into their roots (up to ordering), we have

$$g(x) = x^q - x = \prod_{\alpha \in F} (x - \alpha),$$

as required.