Introduction to Abstract Algebra II: Homework 3

Due on January 29, 2026 at 23:59

Victor Ostrik 10:00

Hashem A. Damrah
UO ID: 952102243

Exercise 26.1. Describe the field F of quotients of the integral subdomain

$$D = \{n + im \mid n, m \in \mathbb{Z}\},$$

of $\mathbb{C}$. "Describe" means give the elements of $\mathbb{C}$ that make up the field of quotients of D in $\mathbb{C}$. (The elements of D are the Gaussian integers.)

Solution. The elements of the integral subdomain D are the Gaussian integers, which can be expressed as $n+im$ where n and m are integers. The field of quotients of D, denoted as F, consists of all possible fractions formed by elements of D. Therefore, the elements of the field of quotients F can be expressed as:

$$F = \left\{ \frac{a+ib}{c+id} \,\middle|\, a, b, c, d \in \mathbb{Z}, c + id \neq 0 \right\}.$$

To simplify this expression, we can multiply the numerator and denominator by the complex conjugate of the denominator:

$$\frac{a+ib}{c+id} \cdot \frac{c-id}{c-id} = \frac{(a+ib)(c-id)}{c^2+d^2}.$$

Thus, the elements of the field of quotients F can be expressed as:

$$F = \left\{ \frac{p+iq}{r} \,\middle|\, p, q, r \in \mathbb{Z}, r \neq 0 \right\}.$$ □

Exercise 27.6. How many polynomials are there of degree ≤ 2 in $\mathbb{Z}_5[x]$? (Include 0.)

Solution. A polynomial of degree ≤ 2 in $\mathbb{Z}_5[x]$ can be expressed in the form:

$$p(x) = a + bx + cx^2,$$

where a, b, c can take any value from the set $\{0, 1, 2, 3, 4\}$ (the elements of $\mathbb{Z}_5$). Since there are 5 choices for each coefficient a, b, and c, the total number of polynomials of degree ≤ 2 in $\mathbb{Z}_5[x]$ is given by:

$$5 \times 5 \times 5 = 125.$$

Therefore, there are 125 polynomials of degree ≤ 2 in $\mathbb{Z}_5[x]$, including the zero polynomial. □

Exercise 27.10. Let $F = E = \mathbb{Z}_7$ in Theorem 27.4. Compute $\phi_5[(x^3 + 2)(4x^2 + 3)(x^7 + 3x^2 + 1)]$.

Solution. Let $p(x) = x^3 + 2$, $q(x) = 4x^2 + 3$, and $r(x) = x^7 + 3x^2 + 1$. We need to compute $\phi_5[p(x)q(x)r(x)]$. Using the evaluation homomorphism ϕ_5, we evaluate each polynomial at $x = 5$:

$$\begin{aligned}
\phi_5[p(x)] &= p(5) = 5^3 + 2 = 125 + 2 = 127 \equiv 1 \pmod 7, \\
\phi_5[q(x)] &= q(5) = 4(5^2) + 3 = 4(25) + 3 = 100 + 3 = 103 \equiv 5 \pmod 7, \\
\phi_5[r(x)] &= r(5) = 5^7 + 3(5^2) + 1 = 78125 + 75 + 1 = 78201 \equiv 4 \pmod 7.
\end{aligned}$$

Now, we can compute $\phi_5[p(x)q(x)r(x)]$:

$$\phi_5[p(x)q(x)r(x)] = \phi_5[p(x)] \cdot \phi_5[q(x)] \cdot \phi_5[r(x)] \equiv 1 \cdot 5 \cdot 4 \equiv 20 \equiv 6 \pmod 7.$$

Therefore, $\phi_5[(x^3 + 2)(4x^2 + 3)(x^7 + 3x^2 + 1)] \equiv 6 \pmod 7$. □

Exercise 27.14. Find all zeros in the finite field $\mathbb{Z}_5$ of the polynomial $x^5 + 3x^3 + x^2 + 2x$. [Hint: One way is simply to try all candidates!]

Solution. Trying all candidates in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$:

$$\begin{aligned}
x = 0 : 0^5 + 3(0^3) + 0^2 + 2(0) = 0 \equiv 0 \pmod{5},\\
x = 1 : 1^5 + 3(1^3) + 1^2 + 2(1) = 1 + 3 + 1 + 2 = 7 \equiv 2 \pmod{5},\\
x = 2 : 2^5 + 3(2^3) + 2^2 + 2(2) = 32 + 24 + 4 + 4 = 64 \equiv 4 \pmod{5},\\
x = 3 : 3^5 + 3(3^3) + 3^2 + 2(3) = 243 + 81 + 9 + 6 = 339 \equiv 4 \pmod{5},\\
x = 4 : 4^5 + 3(4^3) + 4^2 + 2(4) = 1024 + 192 + 16 + 8 = 1240 \equiv 0 \pmod{5}.
\end{aligned}$$

Therefore, the zeros of the polynomial $x^5 + 3x^3 + x^2 + 2x$ in $\mathbb{Z}_5$ are $x = 0$ and $x = 4$. □

Exercise 27.16. Let $\phi_a : \mathbb{Z}_5[x] \to \mathbb{Z}_5$ be an evaluation homomorphism as in Theorem 27.4. Use Fermat's theorem to evaluate $\phi_3(x^{231} + 3x^{117} - 2x^{53} + 1)$.

Solution. Using Fermat's Theorem, we know that for any integer a not divisible by a prime p, $a^{p-1} \equiv 1 \pmod{p}$. In this case, we have $p = 5$ and $a = 3$. Therefore, $3^4 \equiv 1 \pmod{5}$. We can reduce the exponents of each term in the polynomial modulo 4:

$$\begin{aligned}
231 &\equiv 3 \pmod{4},\\
117 &\equiv 1 \pmod{4},\\
53 &\equiv 1 \pmod{4}.
\end{aligned}$$

Now, we can evaluate $\phi_3(x^{231} + 3x^{117} - 2x^{53} + 1)$:

$$\begin{aligned}
\phi_3\left(x^{231} + 3x^{117} - 2x^{53} + 1\right) &= 3^{231} + 3\left(3^{117}\right) - 2\left(3^{53}\right) + 1\\
&\equiv 3^3 + 3\left(3^1\right) - 2\left(3^1\right) + 1 \pmod{5}\\
&\equiv 27 + 9 - 6 + 1 \pmod{5}\\
&\equiv 31 \equiv 1 \pmod{5}.
\end{aligned}$$

Therefore, $\phi_3(x^{231} + 3x^{117} - 2x^{53} + 1) \equiv 1 \pmod{5}$. □

Exercise 27.17. Use Fermat's theorem to find all zeros in $\mathbb{Z}_5$ of $2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}$.

Solution. We first check for the zero at $x = 0$ since we can't have 0^0 in Fermat's theorem:

$$2(0^{219}) + 3(0^{74}) + 2(0^{57}) + 3(0^{44}) = 0 \equiv 0 \pmod{5}.$$

Again, picking $p = 5$, we reduce the exponents modulo 4:

$$\begin{aligned}
219 &\equiv 3 \pmod{4},\\
74 &\equiv 2 \pmod{4},\\
57 &\equiv 1 \pmod{4},\\
44 &\equiv 0 \pmod{4}.
\end{aligned}$$

Now, we can evaluate the polynomial $2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}$ for each x in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$:

$$\begin{aligned}
x = 1 : 2(1^3) + 3(1^2) + 2(1^1) + 3(1^0) = 2 + 3 + 2 + 3 = 10 \equiv 0 \pmod{5},\\
x = 2 : 2(2^3) + 3(2^2) + 2(2^1) + 3(2^0) = 16 + 12 + 4 + 3 = 35 \equiv 0 \pmod{5},\\
x = 3 : 2(3^3) + 3(3^2) + 2(3^1) + 3(3^0) = 54 + 27 + 6 + 3 = 90 \equiv 0 \pmod{5},\\
x = 4 : 2(4^3) + 3(4^2) + 2(4^1) + 3(4^0) = 128 + 48 + 8 + 3 = 187 \equiv 2 \pmod{5}.
\end{aligned}$$

Therefore, the zeros of the polynomial $2x^{219} + 3x^{74} + 2x^{57} + 3x^{44}$ in $\mathbb{Z}_5$ are $x = 0, 1, 2, 3$. □

Exercise 27.24. Prove that if D is an integral domain, then $D[x]$ is an integral domain.

Solution. Assume D is an integral domain. We need to show that $D[x]$, the ring of polynomials with coefficients in D, is also an integral domain. Clearly, $D[x]$ is a commutative ring with unity since the addition and multiplication of polynomials are commutative and associative, and there exists a multiplicative identity (the polynomial 1). To prove that $D[x]$ is an integral domain, we need to show that it has no zero divisors. Let $f(x), g(x) \in D[x]$ such that $f(x)g(x) = 0$. We need to show that either $f(x) = 0$ or $g(x) = 0$. Using Einstein's notation, we can write $f(x) = a_i x^i$ and $g(x) = b_j x^j$. The product $f(x)g(x)$ can be written as $a_i b_j x^{i+j}$. Since D is an integral domain, the product of $a_i b_j$ is non-zero unless either $a_i = 0$ or $b_j = 0$. Therefore, if $f(x)g(x) = 0$, it must be that either $f(x) = 0$ or $g(x) = 0$. Thus, $D[x]$ is an integral domain. □

Exercise 27.25. Let D be an integral domain and x an indeterminate.

(i) Describe the units in $D[x]$.

(ii) Find the units in $\mathbb{Z}[x]$.

(iii) Find the units in $\mathbb{Z}_7[x]$.

Solution to (i). The units of $D[x]$ given that D is an integral domain are precisely the constant polynomials whose coefficients are units in D. This is because a polynomial $f(x) \in D[x]$ is a unit if there exists another polynomial $g(x) \in D[x]$ such that $f(x)g(x) = 1$. For this to hold, the degree of $f(x)$ must be zero (i.e., it must be a constant polynomial), and its coefficient must be a unit in D. Therefore, the units in $D[x]$ are exactly the elements of the form u, where u is a unit in D. □

Solution to (ii). The units in $\mathbb{Z}[x]$ are the constant polynomials whose coefficients are units in $\mathbb{Z}$. The only units in $\mathbb{Z}$ are 1 and -1. Therefore, the units in $\mathbb{Z}[x]$ are the constant polynomials 1 and -1. □

Solution to (iii). The units in $\mathbb{Z}_7[x]$ are the constant polynomials whose coefficients are units in $\mathbb{Z}_7$. The units in $\mathbb{Z}_7$ are the non-zero elements $\{1, 2, 3, 4, 5, 6\}$. Therefore, the units in $\mathbb{Z}_7[x]$ are the constant polynomials $1, 2, 3, 4, 5,$ and 6. □

Exercise 27.32. Let $\phi : R_1 \to R_2$ be a ring homomorphism. Show that there is a unique ring homomorphism $\psi : R_1[x] \to R_2[x]$ such that $\psi(a) = \phi(a)$ for any $a \in R_1$ and $\psi(x) = x$.

Solution. To construct the ring homomorphism $\psi : R_1[x] \to R_2[x]$, we define it on the basis elements of $R_1[x]$. Any polynomial $f(x) \in R_1[x]$ can be expressed as $f(x) = a_i x^i$. We define ψ on $f(x)$ as follows:

$$\psi(f(x)) = \psi\left(a_i x^i\right) = \phi(a_i)x^i.$$

We first verify that ψ is a ring homomorphism. For any $f(x), g(x) \in R_1[x]$, we have:

$$\psi(f(x) + g(x)) = \psi\left((a_i + b_i)x^i\right) = \phi(a_i + b_i)x^i = (\phi(a_i) + \phi(b_i))x^i = \psi(f(x)) + \psi(g(x)),$$
$$\psi(f(x)g(x)) = \psi\left(c_k x^k\right) = \phi(c_k)x^k = \left(\phi(a_i)\phi(b_j)\right)x^k = \psi(f(x))\psi(g(x)).$$

Therefore, ψ is a ring homomorphism. Next, we show uniqueness. For any polynomial $f(x) = a_i x^i \in R_1[x]$, we have:

$$\psi'(f(x)) = \psi'\left(a_i x^i\right) = \phi(a_i)x^i = \psi(f(x)).$$

Thus, $\psi' = \psi$, proving the uniqueness of the ring homomorphism ψ. □

Exercise 28.4. Let $f(x) = x^6 + 3x^5 + 4x^2 - 3x + 2$ and $g(x) = x^2 + 2x - 3$ in $\mathbb{Z}_7[x]$. Find $q(x)$ and $r(x)$ as described by the division algorithm so that $f(x) = g(x)q(x) + r(x)$ with $r(x) = 0$ or of degree less than the degree of $g(x)$.

Solution. Using the division algorithm for polynomials in $\mathbb{Z}_7[x]$, we divide $f(x)$ by $g(x)$. Multiplying $g(x)$ by x^4 and subtracting it from $f(x)$, we get:

$$x^5 + 3x^4 + 4x^2 - 3x + 2.$$

Multiplying the remainder by x^3 and subtracting, we get:

$$x^4 + 3x^3 + 4x^2 - 3x + 2.$$

Multiplying $g(x)$ by x^2 and subtracting it from the remainder, we get:

$$x^3 + 7x^2 - 3x + 2.$$

Multiplying $g(x)$ by x and subtracting it from the remainder, we get:

$$5x^2 - 6x + 2.$$

Lastly, multiplying $g(x)$ by 5 and subtracting it from the remainder, we get:

$$-4x + 12 \equiv -4x + 5 \pmod 7.$$

Therefore, the quotient and remainder are:

$$q(x) = x^4 + x^3 + x^2 + x + 5 \quad \text{and} \quad r(x) = -4x + 12 \equiv -4x + 5 \pmod 7.$$ □