

In matrix terms we have

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1393 & 225 \\ 972 & 157 \end{pmatrix}$$

Taking determinants and multiplying by 10 gives

$$13930 \times 157 + 9720 \times (-225) = 10.$$

(ii)

$$\begin{aligned} (33 + 17i) &= (2 + i)(16 - 2i) + (-1 + 5i) \\ (16 - 2i) &= (-3i)(-1 + 5i) + (1 - 5i) \\ (-1 + 5i) &= (-1)(1 - 5i) + 0 \end{aligned}$$

In matrix terms:

$$\begin{pmatrix} 2 + i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -3i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -2 + 7i & 4 - 6i \\ 1 + 3i & -3i \end{pmatrix}.$$

Taking determinants and multiplying by $1 - 5i$ gives

$$(33 + 17i)(-3i) + (16 - 2i)(-4 + 6i) = (-1)^3(1 - 5i).$$

(iii)

$$\begin{aligned} X^6 + X^5 + X^3 + X + 1 &= 1 \cdot (X^6 + X^3 + X) + (X^5 + 1) \\ X^6 + X^3 + X &= X \cdot (X^5 + 1) + X^3 \\ X^5 + 1 &= X^2 \cdot X^3 + 1 \\ X^3 &= X^3 \cdot 1 + 0 \end{aligned}$$

In matrix terms we have

$$\begin{aligned} &\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} X & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} X^2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} X^3 & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} X^6 + X^5 + X^3 + X + 1 & X^3 + X^2 + 1 \\ X^6 + X^3 + X & X^3 + 1 \end{pmatrix}. \end{aligned}$$

Taking determinants solves for x and y .

3. When is $R[X]$ and integral domain?

Solution.

Precisely when R is.

4. (i) Is 0 irreducible?

(ii) Is 0 a prime in an integral domain?

Solution.

- (i) No, $0 = 0 \cdot 0$ and neither factor is a unit.
- (ii) Yes, $0|ab$ means there is a c such that $0c = ab$. In an integral domain this can only happen if $a = 0$ or $b = 0$. Thus $0|a$ or $0|b$ and so 0 is prime. (Note that in high school mathematics, we usually define a prime to be nonzero, however, in higher mathematics zero is allowed to be prime.)

5. Factorize the following polynomials in $\mathbb{Z}_3[X]$ into products of irreducibles

$$X^2 + 1, X^2 + 2, X^2 + 2X - 2, X^3 + X^2 + 1, X^3 + X^2 + X + 1, X^3 - X^2 + 1, X^4 + 1.$$

Solution.

$$X^2 + 1, (X + 1)(X - 1), (X + 1)^2, (X - 1)(X^2 - X - 1), \\ (X + 1)(X^2 + 1), X^3 - X^2 + 1, (X^2 + X - 1)(X^2 - X - 1).$$

6. If $f(X) = X^5 - X + 1 \in \mathbb{Q}[X]$, then show for all $a \in \mathbb{Q}$ that $f(X + a)$ does not satisfy the hypotheses of Eisenstein's Criterion. By showing that $X^5 - X + 1$ is irreducible in $\mathbb{Z}_5[X]$, or otherwise, deduce that $X^5 - X + 1$ is irreducible in $\mathbb{Z}[X]$.

Solution.

If Eisenstein's criterion works for

$$f(X + a) = X^5 + 5ax^4 + 10a^2X^3 + 10a^3X^2 + (5a^4 - 1)X + (a^5 - a + 1)$$

then the greatest common divisor of the coefficients of X^i , $0 \leq i \leq 4$ must be greater than 1. However $\gcd(5a, a^5 - a + 1)$, equals 5 or 1. Since $a^5 - a \equiv 0 \pmod{5}$ for all a , the gcd is 1.

Note that $f(X)$ has no linear factors in $\mathbb{Z}_5[X]$. If it is reducible in $\mathbb{Z}_5[X]$, then there exist $a, b, c, d, e \in \mathbb{Z}_5$ such that

$$X^5 - X + 1 = (X^2 + aX + b)(X^3 + cX^2 + dX + e).$$

By comparing the coefficients of $X^4, X^3, 1$, we see

$$X^5 - X + 1 = (X^2 + aX + b)(X^3 - aX^2 + (a^2 - b)X + b^{-1}) \\ = X^5 + (b^{-1} + a^2 - 2ab)X^2 + (ab^{-1} + a^2b - b^3)X + 1$$

For each $b \neq 0$, there is no solution for a making the coefficient of X^2 equal to 0 and the coefficient of X equal to -1 . Hence $X^5 - X + 1$ is irreducible in $\mathbb{Z}_5[X]$ and *a fortiori* in $\mathbb{Z}[X]$.

7. Under what circumstances can you solve $aX^2 + bX + c = 0$ in \mathbb{Z}_p where p is a prime and $a \neq 0$?

Solution.

The quadratic formula works when $p \neq 2$ and $b^2 - 4ac$ has a square root in \mathbb{Z}_p . If $p = 2$, we can solve the above quadratic equation provided it does not equal $X^2 + X + 1 = 0$.

8. Count the number of irreducible polynomials in $\mathbb{Z}_p[X]$ of the form $X^2 + aX + b$.

Solution.

There are p^2 monic quadratic polynomials and the reducible ones have the form $(X - a)(X - b)$ where $a \neq b$ or $(X - a)^2$. Hence there are $p^2 - p^2(p - 1)/2 - p = (p^2 - p)/2$ irreducible monic quadratic polynomials over \mathbb{Z}_p .

9. If R is an integral domain, show that every prime p is irreducible.

Solution.

If $p = ab$, we must show that a or b are units. Since $p|ab$ and p is prime we have $p|a$ or $p|b$. WLOG suppose that $a = \alpha p$. Then $p = \alpha p b$, or $p(\alpha b - 1) = 0$. Since R is an integral domain and $p \neq 0$, it follows that b is a unit.

10. Show that p is a prime in R if and only if R/pR is an integral domain.

Solution.

$p|ab$ implies $p|a$ or $p|b$ is equivalent to $abR = pR$ implies $aR = pR$ or $bR = pR$.

11. Show that every euclidean domain is a principal ideal domain.

Solution.

Let R be a euclidean domain with euclidean function ϕ . If I is a nonzero ideal of R , then let b be a nonzero element of I with $\phi(b)$ minimal. If $a \in I$, then $a = qb + r$ where either $r = 0$ or $\phi(r) < \phi(b)$. Since I is a (left) ideal, $r = a - qb \in I$, so by the choice of b we must have $r = 0$. Hence $I = Rb$ and so R is a PID.

12. Show that every irreducible in a unique factorization domain is a prime.

Solution.

We showed in 9 that every prime in a domain is irreducible. It suffices to show that every irreducible in a UFD is a prime. This follows quite easily from the definitions of prime and UFD.

13. If R is a PID, and p is an irreducible, show that pR is a maximal ideal of R . Hence deduce that R/pR is a field and p is prime.

Solution.

Let (q) be an ideal, such that $(p) \subseteq (q) \subseteq R$. Then $p = qq'$ and so q or q' is a unit. Hence (q) equals (p) or R , so if R were principal, then (p) would be maximal. The quotient of an integral domain by a maximal ideal is a field. Fields are integral domains and so p is a prime.

***14.** A domain D is called noetherian, after Emmy Noether (1882–1953), if every ascending chain of ideals of D is stationary. (That is, if

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

is a chain of ideals, then there exists an integer N such that $I_n = I_N$ for all $n \geq N$.) Show that if D is noetherian, then every nonzero element of D can be factorized into irreducibles.

Solution.

(Stuart and Tall, p87) Suppose that D is noetherian, but that there exists a nonunit $x \neq 0$ in D which can not be expressed as a product of a finite number of irreducibles. Choose x so that $\langle x \rangle$ is maximal subject to this condition. Then by its definition, this x can not be irreducible, so $x = yz$ where y and z are nonunits. Thus $\langle y \rangle \supseteq \langle x \rangle$. If $\langle y \rangle = \langle x \rangle$, then $x = x_1y$ and $y = y_1x$, so $x = x_1y_1x$ and so $1 = x_1y_1$. Hence x and y are associates (ie. they differ by a unit multiple). This implies that z is a unit – a contradiction. Hence $\langle x \rangle$ is a proper subset of $\langle y \rangle$, and similarly of $\langle z \rangle$. By the maximality of $\langle x \rangle$, it follows that $y = p_1 \cdots p_r$, $z = q_1 \cdots q_s$, where each p_i and q_j is irreducible. Multiplying these together expresses x as a product of irreducibles, a contradiction. Hence the assumption that there exists a nonunit $\neq 0$ which is not a finite product of irreducibles is false, and factorization into irreducibles is always possible.

15. (i) Show that a domain D is noetherian if and only if every ideal of D is finitely generated.

*(ii) Show that every principal ideal domain is a *unique* factorization domain.

Solution.

(i) Suppose that I is an ideal of D which is not finitely generated. Then choose a nonzero element x_1 of I . Since I is not finitely generated, the ideal x_1D is a proper subset of I , so there exists an x_2 in I but not in x_1D . Similarly, the ideal $x_1D + x_2D$ is a proper subset of I , so we may choose $x_3 \in I - (x_1D + x_2D)$, and so on. By construction, the chain of ideals

$$x_1D \subset x_1D + x_2D \subset x_1D + x_2D + x_3D \subset \cdots$$

is not stationary and so D is not noetherian. Conversely, suppose that

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_n \subseteq \cdots$$

is a chain of ideals of D . Let I be the union of all these ideals. Then I is an ideal of D . Since every ideal is finitely generated, there exist $x_1, \dots, x_r \in D$ such that $I = x_1D + \cdots + x_rD$. For each i , there is a smallest integer n_i such that $x_i \in I_{n_i}$. If $N = \max\{n_1, \dots, n_r\}$, then $x_1, \dots, x_r \in I_N$ so $I \subseteq I_N$. Hence for all $n \geq N$, we have $I_n = I_N$. Thus D is noetherian.

(ii) Let D be a PID. Since D is noetherian, factorization into irreducibles is possible in D by 14. To prove uniqueness it suffices to prove that every irreducible is prime. (Think about this!)

Suppose that p is irreducible, then $\langle p \rangle$ is a maximal ideal of D by 13. Suppose that $p|ab$ but $p \nmid a$. Then $\langle p, a \rangle = D$ and since $1 \in \langle p, a \rangle$, we have $1 = cp + da$ for some $c, d \in D$. Multiplying by b gives $b = cpb + dab$ and since $p|ab$, we find $p|(cpb + dab)$, so $p|b$. This shows that p is a prime.

16. Show that X is irreducible in $\mathbb{Z}_4[X]$ but is not prime. (Hence $\mathbb{Z}_4[X]$ is not a unique factorization domain.)

Solution.

Now $X|(X+2)^2$ but X does not divide $X+2$, so X is not a prime. Suppose that $X = ab$ for some $a, b \in \mathbb{Z}_4[X]$. If ϕ is the homomorphism $\mathbb{Z}_4[X] \rightarrow \mathbb{Z}_2[X]$, then $\phi(X) = \phi(a)\phi(b)$ and so WLOG $\phi(a) = \phi(1)$ and $\phi(b) = \phi(X)$. Thus $a = 1 + 2\alpha$, $b = X + 2\beta$ for some $\alpha, \beta \in \mathbb{Z}_4[X]$. Hence by exercise 1(iv) a is a unit and so X is irreducible.

17. Show that 3 is irreducible in $\mathbb{Z}[\sqrt{-5}]$, but is not prime. (Hence $\mathbb{Z}[\sqrt{-5}]$ is not a unique factorization domain.)

Solution.

If $x, y \in \mathbb{Z}$, define $N(x + y\sqrt{-5}) = x^2 + 5y^2$, then $N : \mathbb{Z}[\sqrt{-5}] \rightarrow \mathbb{N}$ preserves multiplication. Therefore $x + y\sqrt{-5}$ is a unit iff $x^2 + 5y^2 = 1$ has a solution in \mathbb{Z} , so ± 1 are the only units. Suppose that $3 = \alpha\beta$ where $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ are both nonunits. Then $9 = N(3) = N(\alpha)N(\beta)$ implies $N(\alpha) = N(\beta) = 3$. This is impossible, since $x^2 + 5y^2 = 3$ has no solution for $x, y \in \mathbb{Z}$. Therefore 3 is irreducible. Note that 3 is not prime since $3|(1 + \sqrt{-5})(1 - \sqrt{-5})$ and 3 divides neither $1 + \sqrt{-5}$ nor $1 - \sqrt{-5}$.

18. If R is an integral domain, prove that $\text{char}(R)$ is zero or a prime.

Solution.

Suppose that $\text{char}(R) = ab$, where $1 < a, b < \text{char}(R)$. Then $0 = ab1 = (a1)(b1)$, so $a1 = 0$ or $b1 = 0$. This is a contradiction as $\text{char}(R)$ is the *smallest* positive integer satisfying $\text{char}(R)1 = 0$.

19. Without factorizing, determine whether $f(X) = X^3 + 5X^2 + 3X - 9$ is square-free.

Solution.

Now $Df = 3X^2 + 10X + 3 = (3X + 1)(X + 3)$ and since $f(-3) = 0$, we have $\text{gcd}(f, Df) = X + 3$, so $(X + 3)^2$ divides f .

20. Construct a field of order 9 and find a generator for its multiplicative group.

Solution.

$f(X) = X^2 + 1$ is irreducible, so $\mathbb{Z}_3[X]/(f)$ is a field of order 9. Since $(X + 1)^4 \equiv -1 \pmod{f}$, $(X + 1) + (f)$ has order 8.

21. Factorize the following into a product of irreducibles

- (i) $X^p - X \in \mathbb{Z}_p[X]$,
- (ii) $X^9 - X \in \mathbb{Z}_3[X]$,
- (iii) $X^4 + 1 \in \mathbb{R}[X]$,
- (iv) $X^4 + 1 \in \mathbb{Q}[X]$,
- (v) $X^4 + 1 \in \mathbb{Z}_3[X]$.

Solution.

- (i) $X(X - 1)(X - 2) \cdots (X - (p - 1))$.

- (ii) $X(X-1)(X-2)(X^2+1)(X^2+X-1)(X^2-X-1)$ is the product of all monic irreducibles over \mathbb{Z}_3 of degree dividing 2.
- (iii) Clearly X^4+1 is the product of two irreducible quadratics over \mathbb{R} . Indeed, $(X^2+\sqrt{2}X+1)(X^2-\sqrt{2}X+1)$.
- (iv) $(X+1)^4+1$ is irreducible by Eisenstein's Criterion with $p=2$. Hence X^4+1 is also irreducible.
- (v) $(X^2-X-1)(X^2+X-1)$. Note that even though X^4+1 is irreducible over \mathbb{Z} it can factor over \mathbb{Z}_3 . The converse, however, is false.

22. Find an isomorphism $\mathbb{Z}_3[X]/(X^2+X-1) \rightarrow \mathbb{Z}_3[X]/(X^2-X-1)$.

Solution.

Note that $t = X - 1 + (X^2 - X - 1)$ satisfies the equation $t^2 + t - 1 = 0$. Hence by Theorem 1.6, $aX + b + (X^2 + X - 1) \mapsto a(x - 1) + b + (X^2 - X - 1)$ is a monomorphism. Since the domain and codomain both have order 9, it is an isomorphism.

- 23.** (i) Prove that $(p-1)!$ is congruent to -1 or 0 modulo p depending on whether or not p is a prime. (This result is known as Wilson's Theorem. Sir John Wilson was an English judge who was neither first to state the theorem nor to prove it. He mentioned it to a Cambridge professor who published it as a conjecture. C.F. Gauss proved the conjecture but never published his proof, subsequently J.L. Lagrange independently proved the conjecture and published his proof.)
- (ii) If p is an odd prime, prove that $(\frac{p-1}{2})!$ is congruent to -1 or 1 modulo p depending on whether p is congruent to 1 or 3 modulo 4 .

Solution.

- (i) True when $p=2$. Suppose p is an odd prime. The only time $x = x^{-1}$ in \mathbb{Z}_p is when $x = 1, -1$. Hence, after cancellation, $(p-1)!$ is equal to -1 in \mathbb{Z}_p .
- (ii) If $x \in \{1, 2, \dots, \frac{p-1}{2}\}$, then $-x \in \{\frac{p+1}{2}, \dots, p-2, p-1\}$. Hence $(p-1)! \equiv (-1)^{\frac{p-1}{2}} (\frac{p-1}{2})!$.

24. If p is an odd rational prime, prove that the numerator of $1 + \frac{1}{2} + \frac{1}{3} \dots \frac{1}{p-1}$ is divisible by p .

Solution.

Now

$$1 + \frac{1}{2} + \frac{1}{3} \dots \frac{1}{p-1} = ((p-1)! + (p-1)!/2 + \dots + (p-2)!) / (p-1)!$$

Since p does not divide the denominator, it suffices to prove that p divides the numerator. We view the equation for the numerator modulo p , and recall that $(p-1)! \equiv -1 \pmod{p}$:

$$- \sum_{x \in \mathbb{F}_p^*} x^{-1} = - \sum_{y \in \mathbb{F}_p^*} y = -1 - 2 - \dots - (p-1) = -p(p-1)/2 = 0.$$

An elementary proof involves rearranging the above sum:

$$\begin{aligned}\sum_{i=1}^{p-1} 1/i &= \sum_{i=1}^{\frac{p-1}{2}} \frac{1}{i} + \frac{1}{p-i} \\ &= \sum_{i=1}^{\frac{p-1}{2}} \frac{p}{i(p-i)}\end{aligned}$$

Since p divides the numerators of these fractions but does not divide the denominators, it follows that the same can be said of the sum.

25. Find all the integral solutions to $158x + 57y = 100$

Solution.

Applying Euclid's algorithm gives;

$$\begin{aligned}158 &= 2 \times 57 + 44 \\ 57 &= 1 \times 44 + 13 \\ 44 &= 3 \times 13 + 5 \\ 13 &= 2 \times 5 + 3 \\ 5 &= 1 \times 3 + 2 \\ 3 &= 1 \times 2 + 1 \\ 2 &= 2 \times 1 + 0\end{aligned}$$

Expressing these data in terms of matrices gives

$$\begin{pmatrix} 158 \\ 57 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

or,

$$\begin{pmatrix} 158 \\ 57 \end{pmatrix} = \begin{pmatrix} 158 & 61 \\ 57 & 22 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Taking determinants gives $158 \times (-22) + 57 \times 61 = 1$. Therefore the general solution to $158x' + 57y' = 1$ is $x' = -22 + 57t, y' = 61 - 158t$. Hence, the general solution to $158x + 57y = 100$ is $x = -2200 + 5700t, y = 6100 - 15800t$.

26. Find a formula for the inverse of a typical nonzero element of $\mathbb{Q}(2^{\frac{1}{3}})$. (Hint: If $2^{\frac{1}{3}} = \theta_1, \theta_2, \theta_3$ are the three roots of $X^3 - 2 = 0$, then $\theta_2 + \theta_3 = -\theta_1, \theta_2\theta_3 = \theta_1^2$ and

$$\Theta = (a + b\theta_1 + c\theta_1^2)(a + b\theta_2 + c\theta_2^2)(a + b\theta_3 + c\theta_3^2)$$

is a nonzero rational.)

Solution.

The polynomial $X^3 - 2$ is irreducible over \mathbb{Q} by Eisenstein's criterion with $p = 2$. Hence $1, \theta_1, \theta_1^2$ is a basis for the vector space $\mathbb{Q}(\theta_1)$ over \mathbb{Q} . Since $a, b, c \in \mathbb{Q}$, so

$\Theta = a^3 + 2b^3 + 4c^3 - 6abc \in \mathbf{Q}$. Furthermore, $\Theta \neq 0$ as it is a product of three nonzero elements in an integral domain. Hence

$$\begin{aligned}(a + b\theta + c\theta^2)^{-1} &= (a + b\theta_2 + c\theta_2^2)(a + b\theta_3 + c\theta_3^2)/(a^3 + 2b^3 + 4c^3 - 6abc) \\ &= ((a^2 - 2bc) + (2c - ab)\theta_1 - ac\theta_1^2)/(a^3 + 2b^3 + 4c^3 - 6abc).\end{aligned}$$

27. (Chinese Remainder Theorem) Find all $x \in \mathbf{Z}$ satisfying:

(i)

$$\begin{aligned}x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \\ x &\equiv -1 \pmod{11}\end{aligned}$$

(ii)

$$\begin{aligned}x &\equiv c_1 \pmod{5} \\ x &\equiv c_2 \pmod{7} \\ x &\equiv c_3 \pmod{11}\end{aligned}$$

Solution.

There are two methods to solve such problems when the moduli are pairwise relatively coprime. The methods assume different forms for the answer, and the second method has the advantage that it does not perpetuate errors.

- (i) Suppose that $x = x_1 + 5x_2 + (5 \cdot 7)x_3 + (5 \cdot 7 \cdot 11)x_4$.
 From the first congruence, $3 \equiv x_1 + 0 + 0 + 0 \pmod{5}$ so $x_1 = 3$.
 From the second congruence, $2 \equiv 3 + 5x_2 + 0 + 0 \pmod{7}$ so $x_2 = 4$.
 From the third congruence, $-1 \equiv 3 + 20 + 35x_3 + 0 \pmod{11}$ so $x_3 = -1$.
 Hence a typical solution is $x = -12 + 385x_4$.
- (ii) Suppose that $x \equiv (7 \cdot 11)x_1 + (5 \cdot 11)x_2 + (5 \cdot 7)x_3 \pmod{385}$.
 The first congruence gives $c_1 \equiv 77x_1 \pmod{5}$ so $x_1 \equiv 3c_1 \pmod{5}$.
 The second congruence gives $c_2 \equiv 55x_2 \pmod{7}$ so $x_2 \equiv -c_2 \pmod{7}$.
 The third congruence gives $c_3 \equiv 35x_3 \pmod{11}$ so $x_3 \equiv 6c_3 \pmod{11}$.
 Hence a typical solution is $x = 231c_1 - 55c_2 + 210c_3 + 385c_4$.

28. Prove or disprove: $42|(x^7 - x)$ for all $x \in \mathbf{Z}$.

Solution.

$x^7 \equiv x \pmod{7}$ holds for all $x \in \mathbf{Z}$. Since $x^3 \equiv x \pmod{3}$ holds for all $x \in \mathbf{Z}$, so does $x^7 \equiv x \pmod{3}$. Since $x^2 \equiv x \pmod{2}$ holds for all $x \in \mathbf{Z}$, so does $x^7 \equiv x \pmod{2}$. Combining these three results completes the proof.

29. Is the ring $\mathbf{Z}[i]/(2 + 3i)\mathbf{Z}[i]$ a field? Do you recognize this ring?

Solution.

Since $2 + 3i$ is an irreducible in $\mathbf{Z}[i]$, the quotient ring is a field. The Gaussian integer multiples of $2 + 3i$ form a sublattice of $\mathbf{Z}[i]$. The remainder upon division by $2 + 3i$, therefore, can be chosen uniquely to lie in the interior of some basic square,

or on one a specified corner (draw a picture!). There are 13 possibilities for the remainders, so the field is \mathbb{Z}_{13} .

30. Find all integers $x \in \mathbb{Z}$ satisfying

$$\begin{aligned}x &\equiv 1 \text{ or } 2 \pmod{3} \\x &\equiv 2 \text{ or } 4 \pmod{5} \\x &\equiv 2 \text{ or } 4 \pmod{7}.\end{aligned}$$

Hence find all 8 roots of the quadratic $X^2 - 6X + 8 = 0$ in \mathbb{Z}_{105} .

Solution.

Now $X^2 - 6X + 8 = (X - 2)(X - 4)$ so X is congruent to 2 or 4 modulo the primes 3, 5 and 7. Therefore, there are 8 possibilities for X modulo 105. The general solution to

$$\begin{aligned}x &\equiv c_1 \pmod{3} \\x &\equiv c_2 \pmod{5} \\x &\equiv c_3 \pmod{7},\end{aligned}$$

is $x = 70c_1 + 21c_2 + 15c_3 + 105c_4$. We have an isomorphism

$$\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \rightarrow \mathbb{Z}_{105} : (c_1, c_2, c_3) \mapsto 70c_1 + 21c_2 + 15c_3.$$

Under this isomorphism the elements $(2, 2, 2), (2, 2, 4), (2, 4, 2), (2, 4, 4), (4, 2, 2), (4, 2, 4), (4, 4, 2)$ and $(4, 4, 4)$ correspond to 2, 32, 44, 74, 37, 67, 79 and 4.

31. The n^{th} Fermat number F_n is $2^{2^n} + 1$. Fermat proved that $F_0 = 2, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ are all prime and conjectured that F_n is prime for all n . Prove that F_5 is composite by showing that $3^{F_5-1} \not\equiv 1 \pmod{F_5}$.

Solution.

Working modulo $F_5 = 4294967297$ gives the following values of 3^{2^n} for $n = 1, \dots, 32$:
9, 81, 6561, 43046721, 3793201458, 1461798105, 852385491, 547249794, 1194573931, 2171923848, 3995994998, 2840704206, 1980848889, 2331116839, 2121054614, 2259349256, 1861782498, 1513400831, 2897320357, 367100590, 2192730157, 2050943431, 2206192234, 2861695674, 2995335231, 3422723814, 3416557920, 3938027619, 2357699199, 1676826986, 10324303, 3029026160. Hence F_5 is composite. This method does not tell us anything about the factors of F_5 . (In 1732 Euler showed directly that $641|F_5$.)

32. If p is a prime, show that $|\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}| = p$. (Hint: Show that $f(X) = X^{p-1} + \dots + X + 1$ is irreducible over \mathbb{Q} .)

Solution.

Now $f(X) = (X^p - 1)/(X - 1)$, so

$$f(X + 1) = ((X + 1)^p - 1)/X = X^{p-1} + \binom{p}{1}X^{p-2} + \dots + \binom{p}{p-1},$$

which is irreducible by Eisenstein's criterion. There is an isomorphism $\mathbb{Q}[X]/(f) \rightarrow \mathbb{Q}(e^{2\pi i/p})$, and so $|\mathbb{Q}(e^{2\pi i/p}) : \mathbb{Q}| = p$.

33. Show that the field $\mathbb{F} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q}\}$ is an infinite dimensional vector space over \mathbb{Q} .

Solution.

For each prime p , $\mathbb{Q}(e^{2\pi i/p})$ is a subfield of \mathbb{F} . Since $|\mathbb{F} : \mathbb{Q}| > p$ for all primes p , we have $|\mathbb{F} : \mathbb{Q}| = \infty$. (A little more work is necessary to show $|\mathbb{F} : \mathbb{Q}| = \aleph_0$.)

34. Show that \mathbb{R} is not an algebraic number field.

Solution.

If \mathbb{R} were a number field, then $|\mathbb{R} : \mathbb{Q}| = n < \infty$. Hence there is a bijection between \mathbb{R} and the vector space \mathbb{Q}^n . Since the latter is countable and \mathbb{R} is not, we must have $|\mathbb{R} : \mathbb{Q}| = \infty$ (or more precisely $|\mathbb{R} : \mathbb{Q}| > \aleph_0$).

***35.** If p_1, \dots, p_n are distinct rational primes, then prove that the set

$$\{1, \sqrt{p_1}, \dots, \sqrt{p_n}, \dots, \sqrt{p_1 \cdots p_n}\}$$

of all 2^n possible products of $\sqrt{p_1}, \dots, \sqrt{p_n}$ is linearly independent over \mathbb{Q} .

Solution.

If \mathbb{F}_n is the field $\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n})$, then it suffices to prove that $|\mathbb{F}_n : \mathbb{Q}| = 2^n$. The proof is easy when $n = 0, 1$. We inductively assume the result is true for n and suppose that

$$\sum a_I \prod_{j \in I} \sqrt{p_j} = \sqrt{p_{n+1}}$$

where $a_I \in \mathbb{Q}$ and I ranges over all possible subsets of $\{1, 2, \dots, n\}$. There must be ≥ 2 coefficients a_I which are nonzero (why?). If a_I and a_J are nonzero, choose an element i of one subset I or J but not the other. Then our linear dependence relation has the form $x\sqrt{p_i} + y = \sqrt{p_{n+1}}$ where x and y are nonzero elements of the field

$$K = \mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_{i-1}}, \sqrt{p_{i+1}}, \dots, \sqrt{p_n}).$$

Squaring gives $x^2 p_i + 2xy\sqrt{p_i} + y^2 = p_{n+1}$ and using our inductive hypothesis on K shows $2xy = 0$. This is a contradiction since x and y were nonzero. Hence our original assumption that $\sqrt{p_{n+1}} \in \mathbb{F}_n$ was false. So

$$|\mathbb{F}_{n+1} : \mathbb{Q}| = |\mathbb{F}_{n+1} : \mathbb{F}_n| \cdot |\mathbb{F}_n : \mathbb{Q}| = 2 \cdot 2^n = 2^{n+1}$$

completing our inductive proof.

36. Find θ such that $\mathbb{Q}(2^{\frac{1}{3}}, i) = \mathbb{Q}(\theta)$.

Solution.

Let $\alpha_1 = 2^{\frac{1}{3}}, \alpha_2 = 2^{\frac{1}{3}}\omega, \alpha_3 = 2^{\frac{1}{3}}\omega^2$ be the $\mathbb{Q}(2^{\frac{1}{3}}, i)$ -conjugates of $2^{\frac{1}{3}}$, where $\omega = e^{2\pi i/3}$. Similarly, let $\beta_1 = i, \beta_2 = -i$ be the $\mathbb{Q}(2^{\frac{1}{3}}, i)$ -conjugates of i . Now $c = 1$ satisfies $\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1$ for $1 \leq i \leq 3, 2 \leq k \leq 2$. Hence $\theta = 2^{\frac{1}{3}} + i$ works.

37. Express $\mathbb{Q}(3^{\frac{1}{2}}, 5^{\frac{1}{3}})$ in the form $\mathbb{Q}(\theta)$.

Solution.

$\theta = 3^{\frac{1}{2}} + 5^{\frac{1}{3}}$ is one possibility.

38. Find all monomorphisms $\mathbb{Q}(7^{\frac{1}{3}}) \rightarrow \mathbb{C}$.

Solution.

By Eisenstein's criterion $X^3 - 7$ is irreducible over \mathbb{Q} and hence is the minimum polynomial of $\alpha = 7^{\frac{1}{3}}$. Thus the monomorphisms $\mathbb{Q}(\alpha) \rightarrow \mathbb{C}$ are $\sigma_i : r(\alpha) \mapsto r(\alpha\omega^i)$, $0 \leq i < 3$, where $\omega = e^{2\pi i/3}$.

39. The Möbius function $\mu : \mathbb{N} \rightarrow \{-1, 0, 1\}$ is defined by

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } a^2 | n \text{ for some } a > 1, \\ (-1)^r & \text{if } n = p_1 p_2 \cdots p_r, \text{ with } p_i \text{ distinct primes.} \end{cases}$$

(i) Prove that μ is multiplicative (ie. $\mu(mn) = \mu(m)\mu(n)$ if $\gcd(m, n) = 1$.)

(ii) Prove that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1, \\ 0 & \text{if } n > 1. \end{cases}$$

(iii) (Möbius Inversion Formula) If $g(n) = \sum_{d|n} f(d)$, for every positive integer n , then $f(n) = \sum_{d|n} \mu(d)g(n/d)$.

(iv) Show that the number of irreducible monic polynomials of degree n in $\mathbb{Z}_p[X]$ is $\frac{1}{n} \sum_{d|n} \mu(d)p^{n/d}$.

Solution.

(i) Follows directly from the definition.

(ii) True if $n = 1$. If $n = p^k$, where p is a prime and $k \geq 1$, then the sum equals $1 - 1 = \mu(n)$. If $n = p_1^{k_1} \cdots p_r^{k_r}$, then

$$\sum_{d|n} \mu(d) = \left(\sum_{i_1=1}^{k_1} \mu(p_1^{i_1}) \right) \cdots \left(\sum_{i_r=1}^{k_r} \mu(p_r^{i_r}) \right)$$

which equals zero as each of the factors are zero.

(iii) Substitute for $g(n/d)$, interchange the order of summation and use the above identity.

(iv) Recall that $X^{p^n} - X$ is the product of all the irreducible monic polynomials of degree $d|n$ in $\mathbb{Z}_p[X]$. If $N(d, p)$ is the number of monic irreducible polynomials of degree d in $\mathbb{Z}_p[X]$, then by comparing degrees we have $p^n = \sum_{d|n} dN(d, p)$. Applying Möbius inversion shows that $nN(n, p) = \sum_{d|n} \mu(d)p^{n/d}$.

- 40.** Find all the rational roots of $X^5 - 7X^3 + 6X^2 - 7X + 6$. (Hint: If $\gcd(p, q) = 1$, then prove that p/q is a rational root of the integer polynomial $a_n X^n + \cdots + a_0$ if and only if $p|a_0$ and $q|a_n$.)

Solution.

The possible rational roots are $\pm 1, \pm 2, \pm 3, \pm 6$. Of these only $1, 2, -3$ are roots. Indeed, $X^5 - 7X^3 + 6X^2 - 7X + 6 = (X - 1)(X - 2)(X + 3)(X^2 + 1)$.

- 41.** Which of the following complex numbers are algebraic, and which are algebraic integers?

- | | |
|--|----------------------------|
| (i) $23/41$ | (ii) $e^{2\pi i/17}$ |
| (iii) $e^{\pi i/17}$ | (iv) $\sqrt{6} + \sqrt{8}$ |
| (v) $(1 + \sqrt{5})/2$ | (vi) $(1 + \sqrt{2})/2$ |
| (vii) a root of $X^7 + (\sqrt{2} + \sqrt{3})X^6 - \sqrt[3]{5}X + 42$ | |

Solution.

All of the above are algebraic over \mathbb{Q} .

- | | |
|---|-----------------------------------|
| (i) Not an integer, | (ii) satisfies $X^{17} - 1 = 0$, |
| (iii) satisfies $X^{17} + 1 = 0$, | (iv) integers closed under $+$, |
| (v) satisfies $X^2 - X + 1 = 0$, | |
| (vi) not an integer: $(2X - 1)^2 - 2$ has no monic factors in $\mathbb{Z}[X]$. | |
| (vii) is an integer since the ring of all integers is integrally closed. | |

- 42.** Which of the following polynomials are symmetric? Express each of the symmetric polynomial as a polynomial in the elementary symmetric polynomials.

- | | |
|---|--------------------------------------|
| (i) $X_1^2 + X_2^2 + X_3^2$ where $n = 3$, | (ii) $X_1^3 + X_2^3$ where $n = 2$, |
| (iii) $X_1 X_2^2 + X_2 X_3^2 + X_3 X_1^2$ where $n = 3$, | |
| (iv) $X_1 + X_2^2 + X_3^3$ where $n = 3$. | |

Solution.

Using Newton's theorem gives:

- | | |
|----------------------|---------------------------|
| (i) $s_1^2 - 2s_2$, | (ii) $s_1^3 - 3s_1 s_2$, |
| (iii) not symmetric, | (iv) not symmetric. |

- 43.** Express $X_1^n + X_2^n$ as a polynomial in $s_1 = X_1 + X_2$ and $s_2 = X_1 X_2$ for $n = 1, 2, 3, 4, 5$. Do you see any patterns?

Solution.

$s_1, s_1^2 - 2s_2, s_1^3 - 3s_1 s_2, s_1^4 - 4s_1^2 s_2 + 2s_2^2, s_1^5 - 5s_1^3 s_2 - 5s_1 s_2^2$. The pattern for the coefficients is messy, however, the next question shows how to compute the polynomial using forward substitution.

- ***44.** Let $p_r(X_1, \dots, X_n) = X_1^r + \cdots + X_n^r$ for $r = 1, 2, \dots$, and let $s_r(X_1, \dots, X_n) = \sum X_{i_1} \cdots X_{i_r}$ be the r th elementary symmetric polynomial. Ignoring temporar-

ily the fact that X_1, \dots, X_n are variables, we define

$$f(t) = \prod_{j=1}^n (1 + tX_j) = 1 + s_1t + s_2t^2 + \dots + s_nt^n$$

(i) Show that $\frac{d}{dt} \log f(t) = \sum_{k=0}^{\infty} (-1)^k p_{k+1} t^k$ and hence deduce that

$$(\dagger) \quad s_1 + 2s_2t + \dots + ns_nt^n = \{p_1 - p_2t + p_3t^2 - \dots\} \{1 + s_1t + \dots + s_nt^n\}$$

(ii) By comparing coefficients of t^k in (\dagger) deduce Newton's identities:

$$\begin{aligned} p_1 &= s_1 \\ p_2 &= s_1p_1 - 2s_2 \\ p_3 &= s_1p_2 - s_2p_1 + 3s_3 \\ &\dots \\ p_{k+1} &= s_1p_k - s_2p_{k-1} + \dots + (-1)^{k-1} s_k p_1 + (-1)^k (k+1)s_{k+1} \\ &\dots \end{aligned}$$

(iii) Use Newton's identities to check your answers in the previous question.

45. A polynomial f is said to be *antisymmetric* or *alternating* if $\pi * f = \text{sign}(\pi)f$, where $\text{sign}(\pi)$ is 1 or -1 depending on whether $\pi \in A_n$ or not.

(i) Show that $\Delta = \prod_{i < j} (X_i - X_j)$ is antisymmetric.

(ii) Let $f \in \mathbf{Q}[X_1, \dots, X_n]$ be antisymmetric. Show that $f = \Delta g$, where g is symmetric.

Solution.

(i) Let

$$\delta = \begin{vmatrix} 1 & 1 & \dots & 1 \\ X_1 & X_2 & \dots & X_n \\ \vdots & \vdots & \dots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \dots & X_n^{n-1} \end{vmatrix}.$$

Now δ is a polynomial in X_i with coefficients in the field

$$\mathbf{Q}(X_1, \dots, X_{i-1}, X_{i+1}, \dots, X_n)$$

If $X_i = X_j$, this polynomial is zero and hence it is divisible by $X_i - X_j$, $1 \leq i < j \leq n$. As these linear factors are coprime their product, δ , divides Δ . Comparing the coefficient of $X_1 X_2^2 \dots X_n^n$ shows that $\delta = \Delta$. Hence interchanging two variables X_i and X_j in Δ , is the same as interchanging the i th and j th columns of the Vandermonde determinant δ . Thus Δ is antisymmetric.

(ii) Consider f as a polynomial in X_i as above. Since f is antisymmetric $X_i = X_j$, $1 \leq i < j \leq n$, are roots of f and so $X_i - X_j$ are factors. Hence Δ divides f and f/Δ is symmetric.

46. Compute integral bases and discriminants for

- | | |
|--|---|
| (i) $\mathbf{Q}(\sqrt{3})$ | (ii) $\mathbf{Q}(\sqrt{-3})$ |
| (iii) $\mathbf{Q}(\sqrt{d})$ where $d \equiv 3 \pmod{4}$ | (iv) $\mathbf{Q}(\sqrt{d})$ where $d \equiv 1 \pmod{4}$ |
| *(v) $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ | (vi) $\mathbf{Q}(\sqrt{2}, i)$ |
| *(vii) $\mathbf{Q}(\sqrt[3]{2})$ | (viii) $\mathbf{Q}(\sqrt[4]{2})$ |

Solution.

- | | |
|--|--|
| (i) $\{1, \sqrt{3}\}$ and 12 | (ii) $\{1, \frac{1+\sqrt{-3}}{2}\}$ and -3 |
| (iii) $\{1, \sqrt{d}\}$ and $4d$ | (iv) $\{1, \frac{1+\sqrt{d}}{2}\}$ and d |
| (v) | |
| (vi) Let $\zeta = (1+i)/\sqrt{2}$, then $\zeta^2 = i$ so ζ is a primitive 8th root of 1. Furthermore, $\mathbf{Q}(\sqrt{2}, i) = \mathbf{Q}(\zeta)$ and so the ring of integers is $\mathbf{Z}[\zeta]$ and an integral basis is $1, \zeta, \zeta^2, \zeta^3$. (Note that $m_\zeta(X) = X^4 + 1$.) | |

47. If $\alpha_1, \dots, \alpha_n$ are \mathbf{Q} -linearly independent algebraic integers in $\mathbf{Q}(\theta)$, and if

$$\Delta[\alpha_1, \dots, \alpha_n] = d$$

where d is the discriminant of $\mathbf{Q}(\theta)$, show that $\{\alpha_1, \dots, \alpha_n\}$ is an integral basis for $\mathbf{Q}(\theta)$.

- 48.** Prove that $\mathbf{Z}[\sqrt{-2}]$ is a Euclidean domain with Euclidean function $a + b\sqrt{-2} \mapsto a^2 + 2b^2$.
- 49.** Prove that the only rational integer solutions to $y^2 + 2 = x^3$ are $y = \pm 5$ and $x = 3$.
- 50.** Prove that the only rational integer solutions to $x^2 + y^2 = z^2$ have the form $x = a^2 - b^2, y = 2ab, z = a^2 + b^2$ or $x = 2ab, y = a^2 - b^2, z = a^2 + b^2$ where a and b are rational integers of different parity.