Algebraic Structures

Problem sheet

Last update: 18. November 2019

⋆ ⋆ ⋆

Part 1: Groups

Problem 1. Decide whether each of the given sets forms a group with respect to the given operation. If it does, give the identity element and an expression for the inverse of each element. If it does not, give a reason for this. Remember to check whether the relevant set is closed with respect to the given operation. You may assume associativity holds in each case.

∗ (i) $\{1, -1, \mathrm{i}, -\mathrm{i}\}$, multiplication;

(ii) $\mathbb{Q}^\times$ (all nonzero rational numbers), multiplication;

(iii) $10\mathbb{Z}$ (all integers which are multiples of 10), addition;

(iv) $5\mathbb{Z}$ (all integers which are multiples of 5), multiplication;

(v) $\mathrm{Mat}(2, \mathbb{Z})$ (2×2 matrices with integer entries), addition;

(vi) $\mathrm{Mat}(2, \mathbb{Q})$ (2×2 matrices with rational entries), matrix multiplication;

∗ (vii) The set of 2×2 matrices with integer entries and nonzero determinant, matrix multiplication;

(viii) $\mathbb{C}$ (all complex numbers), addition;

(ix) all real-valued functions with domain $\mathbb{R}$, addition (of functions);

(x) a vector space V, addition (of vectors).

Problem 2. Let $(G, \star)$ be a group. Show that the following hold.

(i) $(g \star h)^{-1} = h^{-1} \star g^{-1}$ for all $g, h \in G$;

(ii) for all $g, h, k \in G$

- $g \star h = g \star k$ if and only if $h = k$; "left cancellation law"
- $h \star g = k \star g$ if and only if $h = k$. "right cancellation law"

Problem 3. (An instructive exercise) Let $S = \mathbb{R} \setminus \{-1\}$. For $a, b \in S$ set

$$a \star b := a + b + ab.$$

(i) Show that S is closed with respect to the operation $\star$.

(ii) Show that $(S, \star)$ is a group (you may assume associativity of $+$ and $\cdot$ while showing associativity of $\star$).

(iii) Find the solution of the equation $2 \star x \star 3 = 7$ in S.

Problem 4. Let

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 1 & 5 & 4 \end{pmatrix} \text{ and } \pi := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}$$

be elements of S_6.

(i) Write π and σ as products of disjoint cycles.

(ii) Determine whether σ and π commute.

(iii) Determine σ^{-1}, $\pi \circ \sigma$ and $(\pi \circ \sigma)^{-1}$.

(iv) Give an element of S_6 which commutes with σ.

(v) Express π as product of transpositions.

* **Problem 5.** In S_{12}, let

$$\alpha := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 2 & 4 & 3 & 1 & 7 & 6 & 8 & 9 & 10 & 5 & 12 & 11 \end{pmatrix}.$$

(i) Express α as product of disjoint cycles.

(ii) Express α as product of transpositions.

(iii) Determine whether α is even or odd.

(iv) What is the order of α as an element of S_{12}?

Problem 6. (i) Determine the order of $(123)(45) \in S_5$.

* (ii) Show an example of an element of S_7 that has order 12 and show that no element of S_7 can have order greater than 12.

(iii) Determine the largest order of an element of S_n for each n such that $1 \leqslant n \leqslant 10$.

(iv) Can you formulate a general statement on how to find the largest order for an element of S_n?

Problem 7. (i) Consider the group $(\mathrm{Mat}(2, \mathbb{Z}), +)$ from Problem 1(v). Show that the set of all diagonal matrices forms a subgroup.

(ii) Consider the group $(\mathbb{C}^\times, \cdot)$. Show that the unit circle $\{z \in \mathbb{C} : |z| = 1\}$ forms a subgroup. Can you find a finite non-trivial subgroup of the latter group?

Problem 8. Find all subgroups of the group $(\mathbb{Z}_{16}, +)$. Which elements generate the subgroup of order 8? What elements generate the group $\mathbb{Z}_{16}$?

Problem 9. Show that the group of quaternions Q_8, the additive group $\mathbb{Z}_8$ of the integers modulo 8 and the dihedral group D_4 of order 8 are pairwise non-isomorphic.

Problem 10. (i) Explain why S_7 cannot contain a subgroup of order 11.

(ii) Does S_7 contain any subgroup of order 8? If it does, exhibit one; if it does not, explain why.

(iii) Does S_7 cointain any **cyclic** subgroup of order 8? If it does, exhibit one; if it does not, explain why.

Part 2: Rings and number theory

Problem 11. Consider the set $\mathbb{Z}[\sqrt{2}] := \{a + \sqrt{2}b \mid a, b \in \mathbb{Z}\}$. Show that $(\mathbb{Z}[\sqrt{2}], +, \cdot)$ forms a commutative ring. Is it also an integral domain?

Problem 12. Consider the set of all functions $M(\mathbb{R}) := \{f : \mathbb{R} \to \mathbb{R}\}$. Explain why this set with addition and composition of functions does not form a ring.

Problem 13. Let $2\mathbb{Z}$ denote the set of even integers and define a multiplication

$$m \diamondsuit n := \frac{1}{2} mn.$$

Show that $(2\mathbb{Z}, +, \diamondsuit)$ forms a ring. What is the multiplicative identity (unity) of this ring?

Problem 14. Let V be a vector space. Show that the set of all linear transformations $T : V \to V$ with addition and composition forms a ring. What is the unity of this ring? Is this ring commutative?

Problem 15. Describe all units in the following rings. For each unit u give an expression for or compute explicitly its multiplicative inverse.

(i) $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$;

(ii) $\mathbb{Z}_{20}$;

(iii) the ring of linear transformations of a vector space from Problem 14.

Problem 16. Show that the matrix $\begin{pmatrix} 1 & 2 \\ 2 & 4 \end{pmatrix}$ is a zero divisor in $\mathrm{Mat}_{2\times 2}(\mathbb{Z})$.

* **Problem 17.**

(i) Use the Euclidean Algorithm to calculate $\gcd(98, 85)$. Find integers m, n for which

$$1 = 98m + 85n.$$

(ii) Explain why it is impossible to find integers s and t such that

$$50 = 6s + 15t.$$

(iii) Find the (multiplicative) inverse of 14 in $\mathbb{Z}_{33}$.

Problem 18. (i) Use the Euclidean Algorithm to calculate $\gcd(99, 64)$. Find integers m, n for which

$$1 = 99m + 64n.$$

(ii) Find the (multiplicative) inverse of 11 in $\mathbb{Z}_{64}$.

Problem 19. (i) Show that the group of units modulo 8 is not isomorphic to the cyclic group $(\mathbb{Z}_4, +)$.

(ii) How many elements have multiplicative inverse in $\mathbb{Z}_{200}$?

(iii) Compute $3^{1003} \pmod{200}$.

Part 3: Polynomial rings

Problem 20. Use the Euclidean Algorithm to compute the greatest common divisors of the following pairs of polynomials over $\mathbb{Q}$. Also express each greatest common divisor as a linear combination of the two given polynomials.

(i) $x^3 - 3x^2 + 3x - 2$ and $x^2 - 5x + 6$;

(ii) $x^4 + 3x^2 + 2$ and $x^5 - x$;

(iii) $x^3 + x^2 - 2x - 2$ and $x^4 - 2x^3 + 3x^2 - 6x$;

(iv) $x^5 + 4x$ and $x^3 - x$.

Problem 21. Determine the monic associate of:

(i) $2x^3 - x + 1$ in $\mathbb{Q}[x]$;

(ii) $1 + x - \mathrm{i}x^2$ in $\mathbb{C}[x]$;

(iii) $2x^5 - 3x^2 + 1$ in $\mathbb{Z}_7[x]$;

(iv) $2x^5 - 3x^2 + 1$ in $\mathbb{Z}_5[x]$.

Problem 22. Write $x^3 + 3x^2 + 3x + 4 \in \mathbb{Z}_5[x]$ as a product of irreducible polynomials.

Problem 23. Write $x^5 + x^4 + x^2 + 2x \in \mathbb{Z}_3[x]$ as a product of irreducible polynomials.

Problem 24. Prove that $(x - 1)$ divides $f(x) \in \mathbb{Z}_2[x]$ if and only if $f(x)$ has an even number of nonzero coefficients.

Problem 25. Each of the following polynomials can be factored into linear factors in the relevant polynomial ring. Find these factorisations.

(i) $x^4 + 4$ in $\mathbb{Z}_5[x]$;

(ii) $x^3 + 2x^2 + 2x + 1$ in $\mathbb{Z}_7[x]$;

(iii) $2x^3 + 3x^2 - 7x - 5$ in $\mathbb{Z}_{11}[x]$.

Problem 26. Show that $f(x) = x^2 - 8x - 2$ is irreducible over $\mathbb{Q}$. Is $f(x)$ irreducible over $\mathbb{R}$? Over $\mathbb{C}$?

Problem 27. Show that $g(x) = x^2 + 6x + 12$ is irreducible over $\mathbb{Q}$. Is $g(x)$ irreducible over $\mathbb{R}$? Over $\mathbb{C}$?

Problem 28. Determine whether each of the following polynomials in $\mathbb{Z}[x]$ satisfies an Eisenstein criterion for irreducibility over $\mathbb{Q}$.

(i) $x^2 - 12$;

(ii) $8x^3 + 6x^2 - 9x + 24$;

(iii) $4x^{10} - 9x^3 + 24x - 18$;

(iv) $2x^{10} - 25x^3 + 10x^2 - 30$.

∗ **Problem 29.** Determine, with explanation, whether each of the following polynomials is irreducible in $\mathbb{Q}[x]$.

(i) $x^3 + 3x + 2$;

(ii) $x^3 + 4x + 5$;

(iii) $x^4 - 8x^3 + 4x^2 - 6x - 2$.

∗ **Problem 30.** Let F denote the set numbers of the form $a + b\sqrt{2}$ where a and b are rational numbers.

(i) Show that F is closed under multiplication;

(ii) If a and b are rational numbers, show that $(a + b\sqrt{2})(a - b\sqrt{2})$ is a rational number. Deduce that every nonzero element of F has an inverse for multiplication in F.

(iii) Find the multiplicative inverse in F of $1 + \sqrt{2}$.