MTH 4104 Example Sheet VI

Shu SASAKI

VI-1. Write down an equivalence relation on $\{1, 2, 3, 4, 5\}$ with exactly three equivalence classes.

VI-2. Let X be a finite set. For a positive integer n, let X^n denote the set of ordered n-tuples of elements of Z. Prove, by induction, that $|X^n| = |X|^n$.

VI-3. Given two points $p = (x(p), y(p))$ and $q = (x(q), y(q))$ in $\mathbb{R}^2$, the distance between p and q is defined by

$$|p - q| = \sqrt{(x(p) - x(q))^2 + (y(p) - y(q))^2}.$$

Let $\mathcal{R}$ be the relation on $\mathbb{R}^2$ defined such that $p\mathcal{R}q$ if and only if $|p-q|$ is an integer. Is $\mathcal{R}$ reflexive? symmetric? transitive? an equivalence relation? Justify your answer.

VI-4. Let X and Y be any two sets and $f : X \to Y$ be any function. Define a relation $\mathcal{R}$ on X by $x\mathcal{R}y$ if and only if $f(x) = f(y)$. Prove that this is an equivalence relation on X.

VI-5. Let $\mathcal{R}$ be the relation on $\mathbb{R}$ defined by $x\mathcal{R}y$ if and only if $xy \geqslant 0$. (a) Prove that $\mathcal{R}$ is not an equivalence relation. (b) Find a subset X of $\mathbb{R}$ such that the relation $\mathcal{R}$ on X is an equivalence relation.

VI-6. Let X be the set $\{1, 2, 3, 4\}$. (a) How many different relations are there on X? (b) How many different reflexive relations are there on X? (c) How many different symmetric relations are there on X?

VI-7. Write down examples of relations that are (a) not reflexive, not symmetric, and not transitive, (b) reflexive, not symmetric, and not transitive, (c) not reflexive, symmetric, and not transitive, (d) reflexive, symmetric, and not transitive, (e) not reflexive, not symmetric, and transitive, (f) reflexive, not symmetric, and transitive, (g) not reflexive, symmetric, and transitive, (h) reflexive, symmetric and transitive.

VI-8. Write down a partition of $\mathbb{Z}$ into four parts, exactly two of which are infinite.

VI-9. Let $\mathcal{R}$ be the relation on $X = \mathbb{R} - \{0\}$ defined by $x\mathcal{R}y$ if and only if $x = ry$ for some rational number $\mathcal{R}$. (a) Prove that $\mathcal{R}$ is an equivalence relation. (b) Write down the equivalence class of 1. Simplify your description as much as you can. (c) If we define X to be $\mathbb{R}$ instead, would $\mathcal{R}$ define an equivalence relation again?

VI-10. Give two different examples of an equivalence relation on $\mathbb{Z}$ with an infinite number of equivalence classes.

VI-11. Give an example of an equivalence relation with an infinite number of equivalence classes, each of which is infinite.

VI-12. True or false: if X is a set and $\mathcal{R}$ is a relation on X which is not an equivalence relation, then the set of $[x]_{\mathcal{R}} = \{y \in X \,|\, x\mathcal{R}y\}$, where x ranges over X, does not yield a partition of S.

Justify your answer.

VI-13. Let R and S be two equivalence relations on the same set X. Let $\mathcal{R}$ be the relation on X defined by $x\mathcal{R}y$ if and only if xRy and xSy hold simultaneously. Prove that $\mathcal{R}$ is an equivalence relation.

VI-14. An relation $\mathcal{R}$ on a set X is said to be antisymmetric if, for any elements a, b in X, if $a\mathcal{R}b$ and $b\mathcal{R}a$ hold, then $a = b$. (a) Prove that the divisibility relation on the set of positive integers is antisymmetric. (b) Prove that it is not antisymmetric on the set of all integers.

VI-15. Fix an integer a. Can you work what the following look like, knowing $[a]_4$ and $[a]_5$? (a) $[a]_2$. (b) $[a]_3$. (c) $[a]_{20}$.

VI-16. Let r and s be positive integers and a be any integer. (a) Prove that, as sets, $[a]_r \cap [a]_s = [a]_n$ where $n = \operatorname{lcm}(r, s)$. (b) Given the remainders when a is divided by r and by s respectively, is it possible to work out the remainder when it is divided by n? Explain your answer.

VI-17. What is the remainder of 2^{80} when divided by 19, without using a calculator.

VI-18. (a) Explain why $[59]_{84}$ has a multiplicative inverse in $\mathbb{Z}_{84}$. (b) Find a non-negative integer $a < 84$ such that $[59]_{84}^{-1} = [a]_{84}$.

VI-19. Find all solutions to the equation $16x + 26 = 2x + 3$ in $\mathbb{F}_{31}$. (Hint: $[14]_{31}^{-1} = [20]_{31}$)

VI-20. Find al solutions to the system of equations $5x + 2y = 6$ and $4x + y = 2$ in $\mathbb{F}_{11}$.

***

VI-21 Let G be the set of rational numbers of the form a/b where a is an even integer and b is an odd (non-zero) integer. Define $*$ on G by $x*y = (x+y)/(1-xy)$. Prove that $(G, *)$ is a group.

VI-22. Let $n \geq 2$ be an integer. (a) Prove that the set $n\mathbb{Z}$ of integers divisible by n is a ring, with usual definitions of addition and multiplication on $\mathbb{Z}$. (b) Prove that $n\mathbb{Z}$ is not a ring with identity.

VI-23. Let X be a non-empty set and S be the set of all subsets of X. Define addition and multiplication on S by: $A + B = (A \cup B) - (A \cap B)$ and $A \times B = A \cap B$. (a) Prove that S is a ring. (b) Is S a ring with identity? a skew field? a commutative ring?

VI-24. Give an example of a ring that is neither commutative nor a ring with identity. Justify your answer.

VI-25. Find the real and imaginary part of $(-3 + 5\sqrt{-1})/(2 - 9\sqrt{-1})$.

VI-26. Solve the linear equation $3(1 - \sqrt{-1})z - 2 = 2z + \sqrt{-1} + 1$.

VI-27. Spell out a proof that $\mathbb{C}$ is a field (by checking all the axioms).

VI-28. If $z = a + b\sqrt{-1}$ is a complex number, its conjugate is defined to be $\overline{z} = a - b\sqrt{-1}$. (a) Prove that if z and τ are complex numbers, then $\overline{z} + \overline{\tau} = \overline{z + \tau}$ and $\overline{z}\overline{\tau} = \overline{z\tau}$. (b) Prove that $\overline{z} - \overline{\tau} = \overline{z - \tau}$ and if τ is non-zero, then $\overline{z}/\overline{\tau} = \overline{z/\tau}$.

VI-29. Define and multiplication on $S = \mathbb{R}^2$ by $(a, b) + (c, d) = (a + c, b + d)$ and $(a, b) \times (c, d) = (ac, ad + bc)$. (a) Name the multiplicative identity in S, and prove (G2) for $(S, \times)$. (b) Prove that if a is non-zero, then (a, b) has a multiplicative inverse in S.

VI-30. Let $S \subset \mathbb{R}^2$ be the set of elements of the form $a + b\tau$, where a and b are real numbers, and τ is a formal symbol subject to the condition $\tau^2 = 2\tau - 2$. Check that $(a + b\tau) + (c + d\tau) = (a + c) + (b + d)\tau$ and $(a + b\tau)(c + d\tau) = (ac - 2bd) + (ad + bc + 2bd)\tau$; and show that S is a field with respect to the addition and multiplication so defined.

VI-31. Prove that $\mathbb{Z}_n$ is a commutative ring with identity.

VI-32. Let F be the set of elements of the form $a + b\tau$, where a and b are elements of $\mathbb{F}_3$ and τ is a formal symbol (Rk: τ plays the role of $[-1]_3$). Define addition and multiplication by: $(a + b\tau) + (c + d\tau) = (a + c) + (b + d)\tau$ and $(a + b\tau)(c + d\tau) = (ac - bd) + (ad + bc)\tau$. (a) How many elements are there in F? (b) Prove (R×+). (c) Name the additive identity 0_G and prove (G2) for $(F, +)$. (d) Prove (G3) for $(F - \{0_G\}, \times)$.

VI-33. Let R be a ring with identity which does not satisfy the condition that the additive identity equals the multiplicative identity. Prove that R has only one element.

VI-34. What kind of a ring R should be for the identity $x^2 - y^2 = (x + y)(x - y)$ holds for every x and y in R.

VI-36. Let R be a ring with identity and a be an element of R satisfying $R^n = 1$ for some positive integer n. Prove that $1 - a$ has multiplicative inverse in R.

***

VI-37. Let F be a skew field, and let f, g be two non-zero polynomials in $F[X]$. Prove that fg is non-zero.

VI-38. Give a counter example for (G3) for $(G, *) = (\mathbb{R}[X] - \{0\}, \times)$.

VI-39. Given an example of a non-commutative ring R, two polynomials f, g in $R[X]$, and an element γ of R such that $(fg)(\gamma)$ is distinct from $f(\gamma)g(\gamma)$.

VI-40. Let f, g be polynomials in $\mathbb{R}[X]$ with $\deg(g) > 0$. Suppose that $\deg(f) = 8$ and $(X - 1)^3$ divides f. What can be said about the multiplicity of 1 as a root of f?

VI-41. Let f, g be polynomials in $F[X]$ with a field F. (a) Prove that if f divides g, then every root of f is also a root of g. (b) Is the converse true? Justify your answer.

VI-42. Let R be the relation on the polynomial ring $\mathbb{R}[X]$ over $\mathbb{R}$ defined by fRg if and only if $f-g$ is divisible by X^2+1 in $\mathbb{R}[X]$. (a) Prove that R is an equivalence relation. (b) Let F be the set of equivalence classes of R. Define addition and multiplication on F, and prove that they are well-defined. (cc) How is F related to $\mathbb{C}$?

VI-43. Let f be a polynomial in $\mathbb{R}[X]$ and ρ be a real number. Prove that ρ is a root of f of multiplicity at least 2 if and only if ρ is a root of f and the derivative of f with respect to X.

VI-45. (a) Let $f(X) = X^{12} - 1$ and $g(X) = X^5 - 1$ in $\mathbb{R}[X]$. Using the Euclid's algorithm for polynomials, show that $\gcd(f,g) = X-1$ and find polynomials F and G in $\mathbb{R}[X]$ such that $Ff + Gg = X - 1$.

VI-46. Find all complex solutions to the equation $X^8 - 2X^4 + 1 = 0$ in the standard form $a + b\sqrt{-1}$.

VI-47. (a) Write down a general element of $\mathrm{M}_2(\mathrm{M}_2(\mathbb{R}))$. (b) Give the formula for multiplying two elements of $\mathrm{M}_2(\mathrm{M}_2(\mathbb{R}))$. (c) How is $\mathrm{M}_2(\mathrm{M}_2(\mathbb{R}))$ related to $\mathrm{M}_4(\mathbb{R})$.

VI-48. Find a multiplicative inverse of the matrix $\begin{pmatrix} [7]_{13} & [6]_{13} \\ [10]_{13} & [4]_{13} \end{pmatrix}$ within $\mathrm{M}_2(\mathbb{F}_{13})$.

VI-49. Suppose that R is a non-trivial ring with identity. (a) Specify a non-zero 2-by-2 matrix N with coefficients in R such that $N^2 = 0$. (b) Using (a) or otherwise, show that $\mathrm{M}_2(R)$ does not satisfy (G3) in terms of multiplication.

VI-50. Let R be a ring. Let a, b, c, d in R and let $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ and $B = \begin{pmatrix} c & d \\ -d & c \end{pmatrix}$. (a) Calculate AB and $A+B$. (b) Write down a function $f : \mathbb{C} \longrightarrow \mathrm{M}_2(\mathbb{R})$ that satisfies the conditions $f(AB) = f(A)f(B)$ and $f(A+B) = f(A) + f(B)$. (c) Using f and the fact that $\mathrm{M}_2(\mathbb{R})$ is a ring, prove that $\mathbb{C}$ is a field.

VI-51. Let n be a positive integer. Let a and b be integers such that $\gcd(a,n) = 1$. Prove that the function defined by $f(X) = [a]_n X + [b]_n$ is a permutation of the set $\mathbb{Z}_n$.

***

VI-52. Let X and Y be sets and $f : X \longrightarrow Y$ be a function. (a) Prove that there exists a function $p : Y \longrightarrow X$ such that $f \circ p$ is the identity function on Y if and only if f is surjective. (b) Prove that there exists a function $q : Y \longrightarrow X$ such that $q \circ f$ is the identity function on X if and only if f is injective. (c) Prove that if f is bijective, then the p and q from (a) and (b) can be taken to be equal to each other.

VI-53. Let $\mathcal{R}$ be a relation on the set $\{1, \ldots, n\}$. We say that a permutation σ in S_n is a symmetry of $\mathcal{R}$ if it satisfies the conditions: (1) if $x\mathcal{R}y$, then $r\mathcal{R}s$, where $r = \sigma(x)$ and $s = \sigma(y)$, and (2) if $(r,s) \in X \times Y$ and $r\mathcal{R}s$, then there exist $(x,y) \in X \times Y$ such that $x\mathcal{R}y$ and $(r,s) = (\sigma(x), \sigma(y))$.

Prove the following: (a) The identity permutation is a symmetry of $\mathcal{R}$. (b) If σ is a symmetry of $\mathcal{R}$, then so is σ^{-1}. (c) If σ and τ are symmetries of $\mathcal{R}$, then so is $\sigma \circ \tau$.

VI-54. (a) Convert a permutation $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 1 & 7 & 2 & 3 & 9 & 5 & 8 & 3 \end{pmatrix}$ of S_9 into the cycle form.(b) Convert $(1\,10\,4\,6)(5\,8)(7\,9\,3)$ into the 2-by-10 matrix form.

VI-55. (a) Let σ be a permutation that is a single cycle of length n. Prove that if n is odd, then $\sigma \circ \sigma$ is also a single cycle of length n; and if n is even, then $\sigma \circ \sigma$ decomposes into two disjoint cycles of length $n/2$. (b) Let τ be a permutation in S_n. Describe a method to determine if there exists a permutation σ in S_n such that $\sigma \circ \sigma = \tau$.

VI-56. Let S be the square in the plane $\mathbb{R}^2$ with vertices $(1,1)$, $(1,-1)$, $(-1,1)$ and $(-1,-1)$. Let G be the set of linear transformations $f : \mathbb{R}^2 \to \mathbb{R}^2$ such that $f(S) = S$– these transformations are called the *symmetries* of S. (a) Write out all the elements of G. (b) Prove that G is a group under the composition.

VI-57. Let $(G, *_G)$ and $(\Gamma, *_\Gamma)$ be two groups. Define $*_{G\times\Gamma}$ on the set $G \times \Gamma$ of ordered pairs $g = (g_G, g_\Gamma)$ with g_G in G and g_Γ in Γ, by $g *_{G\times\Gamma} \gamma = (g_G *_G \gamma_G, g_\Gamma \times_\Gamma \gamma_\Gamma)$. Prove that $(G \times \Gamma, *_{G\times\Gamma})$ is a group.

VI-58. A group G contains five elements $\{\gamma_\tau\}$, where $1 \leqslant \tau \leqslant 5$, none of which is the identity element, satisfying the conditions $\gamma_{[\tau]}\gamma_{[\tau-1]} = \gamma_{[\tau+1]}$, where by $[\tau]$ we mean the unique integer $1 \leqslant [\tau] \leqslant 5$ congruent to τ mod 5. Compute the order of γ_2.

VI-59. List all elements of the multiplicative group $\mathbb{Z}_{15}^\times$. Calculate the order of each element.

VI-60. Write down a Cayley table for the group $\mathrm{GL}_2(\mathbb{F}_2)$ of units in $\mathrm{M}_2(\mathbb{F}_2)$.

VI-61. (a) Let r be a non-negative integer. Prove that $2^{r+6s} \equiv 2^r$ mod 9 for every positive integer s. (b) Using (a), show that the function $f : \mathbb{Z}_6 \to \mathbb{Z}_9^\times$ which sends $[r]_6$ to $[2^r]_9$ is well-defined. (c) Calculate $f([0]_6)$,$f([1]_6)$,$f([2]_6)$,$f([3]_6)$,$f([4]_6)$,$f([5]_6)$. (d) Prove that f is bijective. (e) Prove that $f(a+b) = f(a)f(b)$ for all a, b in $\mathbb{Z}_6$.

VI-62. Let G be the set $\{q^2 \,|\, q \in \mathbb{Q}^\times\}$. Prove that G is a subgroup of the multiplicative group $\mathbb{Q}^\times$.

VI-63. (a) Let g and γ be the element of a group G. Prove that if $g\gamma = \gamma g$, then $g^{-1}\gamma = \gamma g^{-1}$. (b) Let G be a group and γ be its element. Let C be the set $\{g \in G \,|\, g\gamma = \gamma g\}$. Describe C in words. (c) Prove that C is a subgroup of G.

VI-64. Let S be the set of all complex numbers of modulus 1. Prove that S is a subgroup of the multiplicative group $\mathbb{C}^\times$.

VI-65. (a) Let $(G, *)$ be any abelian group. Define a multiplication operation on G by $a \times b = 0$ for all a, b in G. Prove that $(G, *, \times)$ is a ring. (b) Prove that $\mathrm{M}_n(G)$ is commutative for every n.