Exam 2018 - Answers

Question 1

a) Remembering that composites should be read from right to left, one finds for example that $f[1] = (1\,8\,9)(1\,7)(4\,5\,6)[1] = (1\,8\,9)(1\,7)[1] = (1\,8\,9)[7] = 7$. Continuing like this, one obtains $f = (1\,7\,8\,9)(4\,5\,6)$.

b) Since the sign of an m-cycle is $(-1)^{m-1}$ and $\mathrm{sign}(f_1 \circ f_2) = \mathrm{sign}(f_1) \cdot \mathrm{sign}(f_2)$, we obtain that $\mathrm{sign}(f) = \mathrm{sign}((1\,7\,8\,9)) \cdot \mathrm{sign}((4\,5\,6)) = (-1)^{4-1} \cdot (-1)^{3-1} = -1$.

c) Since from part a), we know that f is the composition of a 4-cycle and a 3-cycle that are mutually disjoint, we know that the order of f is the least common multiple of 4 and 3. In other words, the order of f is 12. This implies that $f^{121} = f \circ f^{120} = f \circ (f^{12})^{10} = f \circ \mathrm{id} = f = (1\,7\,8\,9)(4\,5\,6)$.

d) We claim that if a subgroup H of $(S_4, \circ)$ contains both $(1\,2)$ and $(1\,2\,3\,4)$, that it is equal to S_4 itself. There are many possible solutions, some requiring more computations than others. Here is one possible solution: since S_4 is generated by 2-cycles, it suffices to show that H contains all the 2-cycles. There are in total six 2-cycles in S_4, namely $(1\,2), (1\,3), (1\,4), (2\,3), (2\,4)$, and $(3\,4)$. Now $(1\,2) = g \in H$ and one idea is to conjugate this with powers of h, since conjugation does not change the cycle type (this was briefly mentioned in Exercise 7 from Chapter 4). Indeed, $(2\,3) = hgh^{-1} \in H$, $(3\,4) = h^2gh^{-2} \in H$, $(1\,4) = h^3gh^{-3} \in H$. Finally, $(1\,3) = g(2\,3)g \in H$ and $(2\,4) = g(1\,4)g \in H$.

Question 2

Note that the notation in this and previous exams is a bit different from that in the 2020 version of the notes. The expression $\mathbb{Z} \mod 5$, can just be replaced by $\mathbb{Z}_5$.

a) Answer: first of all, $\psi(1) = \psi(3 +_5 3) = \psi(3) \circ \psi(3) = (1\,3\,5\,7\,9)(1\,3\,5\,7\,9) = (1\,5\,9\,3\,7)$. Then $\psi(2) = \psi(1 +_5 1) = \psi(1) \circ \psi(1) = (1\,5\,9\,3\,7)(1\,5\,9\,3\,7) = (1\,9\,7\,5\,3)$ and hence $\psi(4) = \psi(2 +_5 2) = \psi(2) \circ \psi(2) = (1\,9\,7\,5\,3)(1\,9\,7\,5\,3) = (1\,7\,3\,9\,5)$. Now the only missing value is $\psi(0)$, since $\psi(3)$ is already given. Since ψ is a group homomorphism, we have $\psi(0) = \mathrm{id}$.

b) The group homomorphism $\psi : \mathbb{Z}_5 \to S_{10}$ is injective, since from part a), we see that $\ker(\psi) = \{0\}$. Also from part a), we can see that $\mathrm{im}(\psi) = \{\mathrm{id}, (1\,5\,9\,3\,7), (1\,9\,7\,5\,3), (1\,3\,5\,7\,9), (1\,7\,3\,9\,5)\}$. This is a subgroup of $(S_{10}, \circ)$, since it is the image of the group homomorphism ψ. If we restrict the codomain of ψ to $\mathrm{im}(\psi)$, we obtain a group homomorphism $\tilde{\psi} : \mathbb{Z}_5 \to \mathrm{im}(\psi)$, which is injective because ψ is, and surjective, since we restricted the codomain to $\mathrm{im}(\psi)$. Hence the groups $(\mathbb{Z}_5, +_5)$ and $(\mathrm{im}(\psi), \circ)$ are isomorphic groups. In particular $(\mathbb{Z}_5, +_5)$ is isomorphic to a subgroup of $(S_{10}, \circ)$.

c) We need to show that φ satisfies $\varphi_e = \mathrm{id}$ and that for all $g_1, g_2 \in G$, we have $\varphi_{g_1 \cdot g_2} = \varphi_{g_1} \circ \varphi_{g_2}$. In the first place, using the given definition of φ_g, we see that for any $f \in G$, $\varphi_e[f] = e \cdot f = f = \mathrm{id}[f]$. Hence $\varphi_e = \mathrm{id}$. In the second place, for any $f \in G$, we have $\varphi_{g_1 \cdot g_2}[f] = (g_1 \cdot g_2) \cdot f = g_1 \cdot (g_2 \cdot f) = \varphi_{g_1}[g_2 \cdot f] = \varphi_{g_1}[\varphi_{g_2}[f] = (\varphi_{g_1} \circ \varphi_{g_2})[f]$. Hence $\varphi_{g_1 \cdot g_2} = \varphi_{g_1} \circ \varphi_{g_2}$, which is the last thing we needed to show.

Question 3

a) Since the polynomial $X^3 + X^2 + 1$ has the element $1 \in \mathbb{F}_3$ as root, it is reducible. More precisely, $X - 1$ divides $X^3 + X^2 + 1$, since 1 is a root. Therefore the quotient ring $(\mathbb{F}_3[X]/\langle X^3 + X^2 + 1\rangle, +, \cdot)$ is not a field. Dividing $X^3 + X^2 + 1$ by $X - 1$, one obtains that $X^3 + X^2 + 1 = (X - 1)(X^2 - X - 1) =$

$(X+2)(X^2+2X+2)$. Hence for example $X+2+\langle X^3+X^2+1\rangle$ and $X^2+2X+2+\langle X^3+X^2+1\rangle$ are zero divisors of R, since $X+2+\langle X^3+X^2+1\rangle \neq 0+\langle X^3+X^2+1\rangle$, $X^2+2X+2+\langle X^3+X^2+1\rangle \neq 0+\langle X^3+X^2+1\rangle$, but $(X+2+\langle X^3+X^2+1\rangle)(X^2+2X+2+\langle X^3+X^2+1\rangle) = (X+2)(X^2+2X+2)+\langle X^3+X^2+1\rangle = X^3+X^2+1+\langle X^3+X^2+1\rangle = 0+\langle X^3+X^2+1\rangle$.

b) The element $X^4+2X^2+X+2+\langle X^3+X^2+1\rangle$ is not in standard form. Using division with remainder, one can compute that $X^4+2X^2+X+2 = (X+2)(X^3+X^2+1)+0$. Hence $X^4+2X^2+X+2+\langle X^3+X^2+1\rangle = 0+\langle X^3+X^2+1\rangle$, the zero element of $\mathbb{F}_3[X]/\langle X^3+X^2+1\rangle$. In particular it is not a zero divisor, since these by definition must be nonzero elements.

c) To find the multiplicative inverse, we perform the extended Euclidean algorithm on the polynomials X^3+X^2+1 and $2X^2+2$. Since the coefficients of the polynomials in this question come from $\mathbb{F}_3$, we use that $-1=2$.

$$\begin{bmatrix} X^3+X^2+1 & 1 & 0 \\ 2X^2+2 & 0 & 1 \end{bmatrix} \underset{R_1 + X\cdot R_2}{\longrightarrow} \begin{bmatrix} X^2+2X+1 & 1 & X \\ 2X^2+2 & 0 & 1 \end{bmatrix} \underset{R_1 + R_2}{\longrightarrow}$$

$$\begin{bmatrix} 2X & 1 & X+1 \\ 2X^2+2 & 0 & 1 \end{bmatrix} \underset{R_2 \leftrightarrows R_1}{\longrightarrow} \begin{bmatrix} 2X^2+2 & 0 & 1 \\ 2X & 1 & X+1 \end{bmatrix} \underset{R_1 \text{ - } XR_2}{\longrightarrow} \begin{bmatrix} 2 & 2X & 2X^2+2X+1 \\ 2X & 1 & X+1 \end{bmatrix}$$

At this point we can stop the algorithm and conclude that

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

Dividing by 2, which modulo 3 amounts to multiplying by 2, we create a 1 on the left-hand side and obtain:

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

We can now conclude that the multiplicative inverse of $2X^2+2+\langle X^3+X^2+1\rangle$ is equal to $X^2+X+2+\langle X^3+X^2+1\rangle$.

d) First of all note that $\gcd(X^2, X^3+X^2+1)=1$, since X does not divide X^3+X^2+1. Hence $X^2+\langle X^3+X^2+1\rangle$ is a unit. Since $(R,+,\cdot)$ is not a field, we cannot conclude that its multiplicative order of an element divides 3^3-1. Therefore we simply proceed with some trial and error, calculating the standard form of powers of $X^2+\langle X^3+X^2+1\rangle$:

$$(X^2+\langle X^3+X^2+1\rangle)^2 = X^4+\langle X^3+X^2+1\rangle = X^2+2X+1+\langle X^3+X^2+1\rangle.$$

$$(X^2+\langle X^3+X^2+1\rangle)^3 = X^2(X^2+2X+1)+\langle X^3+X^2+1\rangle = 2X+2+\langle X^3+X^2+1\rangle.$$

$$(X^2+\langle X^3+X^2+1\rangle)^4 = X^2(2X+2)+\langle X^3+X^2+1\rangle = 1+\langle X^3+X^2+1\rangle.$$

Hence the multiplicative order of $X^2+\langle X^3+X^2+1\rangle$ is four.

Question 4

a) Since any element in S can uniquely be written in reduced form: $a+bX+cX^2+dX^3+eX^4+\langle X^5+X^2+1\rangle$ with $a,\dots,e\in\mathbb{F}_2$, S contains exactly $2^5=32$ elements.

b) We claim that α is a primitive element. Since $(S,+,\cdot)$ is a finite field with 32 elements, $S^* = S\setminus\{0\}$ and hence the order of any element in S^* divides 31. Since 31 is a prime number, since implies that apart from the one element in S^* any unit has multiplicative order 31. Hence also α has multiplicative order 31, implying that it is a primitive element of S.

c) We have $Y^4 + Y = Y(Y^3 + 1)$. Hence any nonzero root β satisfies $\beta^3 = -1 = 1$. This shows that either $\beta = 1$ or that β has multiplicative order 3. Since in S a unit is either 1 or has multiplicative order 31, see part a), we can conclude that $Y^4 + Y$ has exactly two roots in S, namely 0 and 1.

d) The polynomial $Y^4 + Y \in \mathbb{F}_{2^e}[Y]$ still has the roots 0 and 1 in $\mathbb{F}_{2^e}$. The question is if it has more roots. We know from part b) that these would have to have multiplicative order 3. The key is that since e is even, 3 divides $2^e - 1$. Hence the number of elements of order 3 in S is equal to $\phi(3) = 2$, where ϕ denotes Euler's totient function. Hence the polynomial $Y^4 + Y$ has four roots in $\mathbb{F}_{2^e}$. It is possible to express the elements of order 3 explicitly in terms of a primitive element γ of S. A primitive element has by definition multiplicative order $2^e - 1$. Then the two elements $\gamma^{(2^e-1)/3}$ and $\gamma^{2(2^e-1)/3}$ both have multiplicative order 3.