(Abstract) Algebra (M7)
Q&A for exam – the sample exam

Georg Loho
g.loho@utwente.nl

April 11, 2023

Final Answer

Each question is worth 3 points. Only a completely correct answer gains points.

What is the discrete logarithm of (3 6)(4 5) with basis (2 1 7)(3 4 6 5) in S_7?

6

---

first approach: multiply (217)(3465) by itself until we get (36)(45)

second approach: look at the length of the cycles

$3n = 4m + 2$

(217)(3465)(217)(3465) = (127)(36)(45)
(127)(36)(45)(217)(3465) = (1)(2)(7)(3564)

What is the word of shortest length equivalent to $zxyzxyyx$ in the group with presentation $\langle x, y, z \mid xx, yz, zz, yy \rangle$?

zx

Alternative: yx

$zxyzxyyx \to zxxyyx \to zxxx$

$\to zx$ [$\to yzzx \to yx$]

Alternative

List the generators of the cyclic group generated by $(1\,8\,9\,2)$ in S_9.

$(1892), (1298)$

Cyclic group: $\{ \overset{\text{order } 4}{(1892)}, \overset{2}{(19)(28)}, \overset{4}{(1298)}, \overset{1}{(1)} \}$

$\{ (1892)^k \mid k \in \mathbb{Z} \}$

approaches: compute all powers, theorem about generators of cyclic group, order of permutation is lcm of cycles

Let $\mathcal{F}(T)$ be the free group on $T = \{x, y, z\}$, and let G be the subgroup of the direct product $S_4 \times \mathbb{Z}_3$ generated by $\{((1\,2), 1), ((1\,3), 1), ((1\,2\,3\,4), 2)\}$. Furthermore, we define the group homomorphism $\phi\colon \mathcal{F}(T) \to G$ by setting $\phi(x) = ((1), 0)$, $\phi(y) = ((1\,3), 1)$, $\phi(z) = ((1\,2\,3\,4), 2)$. Which element of $S_4 \times \mathbb{Z}_3$ is $\phi(zyxx)$?

$$((14)(23), 0)$$

$$\phi(zyxx) = \phi(z)\phi(y)\phi(x)\phi(x) \overset{\text{Def}}{=} ((1234),2)((13),1)((1),0)((1),0)$$

homomorphism property

identity

$(\mathbb{Z}_3, +)$

$$= ((1234),2)((13),1) = ((14)(23), 0)$$

What is the inverse of $(4,5)$ in the direct product $\mathbb{Z}_5 \times U(7)$?

$(1, 3)$

$(\mathbb{Z}_5, +)$

$(U(7), \cdot)$

$4 + 1 = 0 \mod 5$

$4 + x = 0 \mod 5$

$5 \cdot y = 1 \mod 7$, $y = 3$

$5 \cdot 1 = 5 \mod 7$

$5 \cdot 2 = 3 \mod 7$

$5 \cdot 3 = 1 \mod 7$

Give the smallest non-negative integer which is a solution to the following system of congruences:

$$x \equiv 5 \pmod{11}$$
$$x \equiv 3 \pmod{5}$$

38

---

approaches:

- guessing
- Euclidean algo / Bezout theorem $11 + (-2) \cdot 5 = 1$
- Write x as solution of the other congruence

Chinese Remainder Theorem

$x = 5z + 3 \Rightarrow 5z + 3 \equiv 5 \mod 11 \Rightarrow 5z \equiv 2 \mod 11$

What is the index of the kernel of the group homomorphism

$$\psi\colon SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}_2)$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a \pmod 2 & b \pmod 2 \\ c \pmod 2 & d \pmod 2 \end{pmatrix}$$

6

---

approach :

- find kernel and then its cosets
- observe that ψ is surjective. So, by Isomorphism Theorem, quotient group is isomorphic to image

cosets $\quad$ $SL_2(\mathbb{Z}_2)$

$\begin{pmatrix}1&0\\0&1\end{pmatrix}$, ~~$\begin{pmatrix}0&0\\0&0\end{pmatrix}$~~, ~~$\begin{pmatrix}1&0\\0&0\end{pmatrix}$~~, $\begin{pmatrix}1&1\\0&1\end{pmatrix}$, ...

$\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $\begin{pmatrix}1&1\\0&1\end{pmatrix}$, $\begin{pmatrix}1&0\\1&1\end{pmatrix}$, $\begin{pmatrix}0&1\\1&1\end{pmatrix}$, $\begin{pmatrix}1&1\\1&0\end{pmatrix}$, $\begin{pmatrix}0&1\\1&0\end{pmatrix}$

linearly independent rows

Iso Theorem $\quad SL_2(\mathbb{Z}) / \ker\Psi \cong SL_2(\mathbb{Z}_2)$

Mark all valid possibilities for which a field of characteristic 3 exists with this order.
Not selecting all the correct options or also wrong options yields **0** points for the question.

1 . . . . ☐
∞ . . . . ☒
9 . . . . ☒
27 . . . . ☒

not 1: because there is $0 \neq 1$
if finite: then order is power of characteristic, so
9 and 27 is fine
infinite: algebraic closure of $\mathbb{Z}_p$ (in this case $\mathbb{Z}_3$)

Mixed Multiple Choice

You can get 3 points per question. For each of the statements write 1 for true and 0 for false. If at least one of the three statements is not correctly recognized as true or false or if the answer is missing, then you get **0** points for the question.

1. There is exaclty 1 abelian groups with 9 elements up to isomorphism. $\mathbb{Z}_3 \times \mathbb{Z}_3 \quad \mathbb{Z}_9$
2. $U(6)$ is isomorphic to $U(10)$. $|\{1,5\}| < |\{1,3,7,9\}|$
3. In a group, each element has a unique inverse.

(a) 0

(b) 0

(c) 1

1. $2+\sqrt{5}$ is an element of $\mathbb{Q}(\sqrt[4]{5})$.
2. It is possible to construct $\sqrt[3]{5}$ with straightedge and compass.
3. There exists a group of order 16 which has a subgroup with 2 elements.

$2+\sqrt{5} = 2+(\sqrt[4]{5})^2$

(a) 1

(b) 0

(c) 1

No, because the degree is 3, not a power of 2

Yes, $\mathbb{Z}_{16}$ with subgroup $\{0,8\}$

1. The function mapping all elements to 2 is a zero divisor in the ring of functions $\{f \mid f : \{1,2,3\} \to \mathbb{Z}_3\}$ with component-wise addition and multiplication
2. There is a ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}$ whose image is $2\mathbb{Z}$. image in this case is $\{0\}$ or $\mathbb{Z}$
3. $\mathbb{R}$ is algebraically closed. x^2+1 has no solution

(a) 0

(b) 0

(c) 0

$\varphi(1)(\varphi(1)-1)=0$

(1) $1 \to 2$, $2 \to 2$, $3 \to 2$ No, it is a unit with inverse $1 \to 2$, $2 \to 2$, $3 \to 2$

(2) $\varphi: \mathbb{Z} \to \mathbb{Z}$, $z \mapsto 2z$ $\quad 2 = \varphi(1) = \varphi(1 \cdot 1) = \varphi(1) \cdot \varphi(1) = 2 \cdot 2 = 4$

Questions With Explanations

Write the answers on exam paper.

(6 points)

Let

$$G = \left\{ \begin{array}{rl} \phi\colon \mathbb{Z}_6 & \to \mathbb{Z}_6 \\ z & \mapsto \alpha z + \beta \end{array} \middle| \alpha \in \{1,5\}, \beta \in \{0,3\} \right\}$$

be a subgroup of the group of bijective functions on $\mathbb{Z}_6$. Prove or disprove that G is commutative.

Note that the group G acts on $\mathbb{Z}_6$. List the orbits of this action.

Give the stabilizer subgroup of $3 \in \mathbb{Z}_6$.

Let $\alpha, \gamma \in \{1,5\}$ and $\beta, \delta \in \{0,3\}$.

Then $\gamma(\alpha z + \beta) + \delta = \gamma\alpha z + \gamma\beta + \delta$

and

$\alpha(\gamma z + \delta) + \beta = \alpha\gamma z + \alpha\delta + \beta$

are the two composition of the maps given by the pairs (α, β) and (γ, δ).

We get $\gamma\beta + \delta = \alpha\delta + \beta$ for all possible choices:

We have $\alpha\delta = \delta$ for all $\alpha \in \{1,5\}$ and $\delta \in \{0,3\}$

and $\gamma\beta = \beta$ " $\gamma \in \{1,5\}$ and $\beta \in \{0,3\}$

Therefore, the two functions commute, the group is commutative.

Orbits: $\{0, 3\}$, $\{1, 4, 2, 5\}$

$z+3$ (on $\{0, 3\}$); $1 \xrightarrow{z+3} 4 \xrightarrow{5z+3} 2 \xrightarrow{z+3} 5$

Stabilizer subgroup of 3: $\{z, 5z\}$

$\{(1,0), (5,0)\}$

Check correctness (at least size) with orbit stabilizer theorem

$2 \cdot 2 = 4$

(5 points)

Let $p(x) = x^4 + x^2 + x + 1 \in \mathbb{Z}_2[x]$. Compute the multiplicative inverse of $h(x) = x^3 + x + 1$ in $\mathbb{Z}_2[x]/\langle p(x)\rangle$ and prove that it is indeed an inverse.

$(x^4+x^2+x+1) : (x^3+x+1) = x$ remainder 1

x^4+x^2+x

1

So we get $x \cdot (x^3+x+1) + x^4+x^2+x+1 = 1$

Therefore, we pick $x + \langle x^4+x^2+x+1\rangle \in \mathbb{Z}_2[x]/\langle p(x)\rangle$

Indeed, $(x^3+x+1+\langle p(x)\rangle)(x+\langle p(x)\rangle) =$

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

So it is the inverse.

(5 points)

Consider the ring formed by the set

$$S = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\},$$

a subring of the ring of (2×2)-matrices with entries in $\mathbb{Z}_2$. Let $\phi\colon \mathbb{Z}_2[x] \to S$ be the unique ring homomorphism with

$$\phi(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ and } \phi(x) = \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}.$$

Prove that the kernel of ϕ is not a maximal ideal.

First approach: Realize that the kernel is the ideal $x^2 \mathbb{Z}_2[x]$.
This is not maximal because $x^2 \mathbb{Z}_2[x] \subset x \mathbb{Z}_2[x]$.
Alternatively, x^2 is reducible, so $x^2 \mathbb{Z}_2[x]$ is not maximal.

Second approach: The ring homomorphism is surjective, because
$S = \{\phi(0), \phi(1), \phi(1+x), \phi(x)\}$. Therefore, by Iso Theorem,
$\mathbb{Z}_2[x]/\ker\phi \cong S$. But S has zero divisors, namely
$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. Therefore, it is not a field.
This implies that $\ker\phi$ not a maximal ideal.

(5 points)

Determine the unique monic generator of the smallest ideal I of $\mathbb{Q}[x]$ that contains $p(x) = -x^2 + 2x + 3$ and $q(x) = -x^2 + x + 6$, namely $I = \{p(x)a(x) + q(x)b(x) \mid a(x), b(x) \in \mathbb{Q}[x]\}$, with the Euclidean algorithm.

$(-x^2+2x+3) : (-x^2+x+6) = 1$ remainder $x-3$

$-x^2+x+6$

$x-3$

$(-x^2+x+6) : (x-3) = -x-2$

$-x^2+3x$

$-2x+6$

$-2x+6$

0

The required generator is the gcd, which is just $x-3$ by the computation.