# Practice Exam 1

1. $(i)$ Find $r \in \mathbb{Z}$ such that $0 \leq r < 7$ and $3^{100} \equiv r \pmod{7}$.

$(ii)$ Let $a, b, n \in \mathbb{Z}$. Suppose that $a$ and $n$ are relatively prime. Prove that the congruence $ax \equiv b \pmod{n}$ has solutions.

2. $(i)$ Write the Cayley table of $D_4$.

$(ii)$ Prove or disprove the following statement: $D_4$ is Abelian.

3. $(i)$ Produce an example of a set $S$ with a binary operation $*$ such that $S$ is closed under $*$.

$(ii)$ Produce an example of an associative binary operation. Produce an example of a non-associative binary operation.

$(iii)$ Produce an example of a commutative binary operation. Produce an example of a non-commutative binary operation.

$(iv)$ Find the inverse element of $5$ in $U(12)$.

4. Let $G$ be a group, and assume that $\forall\, a, b \in G$, $(ab)^2 = a^2b^2$. Prove that $G$ is an Abelian group.

5. $(i)$ List the subgroups of $\mathbb{Z}_{30}$.

$(ii)$ Produce a generator for each subgroup of $\mathbb{Z}_{30}$.

$(iii)$ List all of the elements of $\mathbb{Z}_{30}$ that have an order of $5$.

6. Let $G$ be a group. Prove that the center $Z(G)$ is a subgroup of $G$.

7. Let $n \in \mathbb{Z}^+$. Show that $A_n$ is a subgroup of $S_n$.

## Solutions to Practice Exam 1

$\boxed{1.}$ $(i)$

$$3^{100} \equiv \left(3^2\right)^{50} \equiv 9^{50} \equiv 2^{50} \equiv 2^{48}2^2 \equiv \left(2^3\right)^{16}4 \equiv 8^{16}4 \equiv 1^{16}4 \equiv 4 \pmod 7. \quad (1)$$

$(ii)$ By Bézout's lemma, we know that $\exists\ s, t \in \mathbb{Z}$ such that $as + nt = 1$. Therefore, $abs + nbt = b$. We deduce that $abs - b = n(-bt)$, so $n|abs - b$. This implies that $a(bs) \equiv b \pmod n$, so $x \equiv bs \pmod n$ is the desired solution. $\square$

$\boxed{2.}$ $(i)$ See page 33 of the text.

$(ii)$ $D_4$ is not Abelian, since $VR_{90} = D'$, but $R_{90}V = D$.

$\boxed{3.}$ $(i)$ Possible answers include: $\mathbb{R}$ under addition, $\mathbb{R}$ under multiplication, $\mathbb{Z}$ under multiplication

$(ii)$ Possible associative binary operations include: multiplication of real numbers, matrix multiplication, function composition, addition of integers; possible non-associative binary operations include: subtraction, division, cross products

$(iii)$ Possible commutative binary operations include: multiplication of real numbers, addition of real numbers; possible non-commutative binary operations include: matrix multiplication, function composition, cross products

$(iv)$ $U(12) = \left\{\overline{1}, \overline{5}, \overline{7}, \overline{11}\right\}$. We notice that $\left(\overline{5}\right)\left(\overline{5}\right) = \overline{25} = \overline{1}$, so $\overline{5}$ is the inverse of $\overline{5}$.

$\boxed{4.}$ Let $a, b \in G$. We know that $(ab)^2 = a^2b^2$, so $abab = aabb$. Therefore, by multiplying on the left by $a^{-1}$, $bab = abb$. By multiplying this on the right by $b^{-1}$, this gives us $ba = ab$. Thus, $G$ is Abelian. $\square$

5. $(i)$ The subgroups of $\mathbb{Z}_{30}$ are:

$$\begin{aligned}\left\langle \tfrac{30}{30}\right\rangle &= \mathbb{Z}_{30}\\ \left\langle \tfrac{30}{15}\right\rangle &= \{2,4,6,8,10,12,14,16,18,20,22,24,26,28,0\}\\ \left\langle \tfrac{30}{10}\right\rangle &= \{3,6,9,12,15,18,21,24,27,0\}\\ \left\langle \tfrac{30}{6}\right\rangle &= \{5,10,15,20,25,0\}\\ \left\langle \tfrac{30}{5}\right\rangle &= \{6,12,18,24,0\}\\ \left\langle \tfrac{30}{3}\right\rangle &= \{10,20,0\}\\ \left\langle \tfrac{30}{2}\right\rangle &= \{15,0\}\\ \left\langle \tfrac{30}{1}\right\rangle &= \{0\}\end{aligned} \quad . \tag{2}$$

$(ii)$ The generators are $1$, $2$, $3$, $5$, $6$, $10$, $15$, and $0$.

$(iii)$ The elements with order $5$ must be elements of $\langle 6\rangle$. We notice that

$$\langle 6\rangle = \langle 12\rangle = \langle 18\rangle = \langle 24\rangle\,, \tag{3}$$

so $6$, $12$, $18$ and $24$ are the elements with order $5$.

6. First, we know that $Z(G) \neq \varnothing$, since $e \in Z(G)$. Let $a, b \in Z(G)$, and let $x \in G$. This means that $ax = xa$ and $bx = xb$.

We claim that $b^{-1}x = xb^{-1}$. First, we know that $bx = xb$, so $bxb^{-1} = x$. Therefore, $xb^{-1} = b^{-1}x$. This establishes the claim.

By the claim, $ab^{-1}x = axb^{-1}$. At the same time, $ax = xa$, so $ab^{-1}x = xab^{-1}$. Thus, $ab^{-1} \in Z(G)$. This shows that $Z(G)$ is a subgroup of $G$. □

7. Let $\sigma, \tau \in A_n$. In that case, $\sigma = \alpha_1\alpha_2...\alpha_r$ for some even $r \in \mathbb{Z}$ and some transpositions $\alpha_1, \alpha_2, ..., \alpha_r \in S_n$. At the same time, $\tau = \beta_1\beta_2...\beta_s$ for some even $s \in \mathbb{Z}$ and some transpositions $\beta_1, \beta_2, ..., \beta_s \in S_n$. Thus, $\sigma\tau = \alpha_1\alpha_2...\alpha_r\beta_1\beta_2...\beta_s$ is a product of $r + s$ transpositions. As $r$ and $s$ are both even, so is $r + s$, and so $\sigma\tau \in A_n$. Since $S_n$ is finite, $A_n$ is also finite, and therefore, this shows that $A_n$ is a subgroup of $S_n$. □

# Practice Exam 2

1. Let $E : \mathbb{Q} \to \mathbb{R}$ such that $\forall\, x, y \in \mathbb{Q}$, $E(x+y) = E(x)E(y)$. Show that $\forall\, x \in \mathbb{Q}$, $E(x) = E(1)^x$.

2. $(a)$ Find all cosets of $\langle 3 \rangle$ in $\mathbb{Z}_{18}$.

$(b)$ Let $K$ be a proper subgroup of $H$, and let $H$ be a proper subgroup of $G$. If $|K| = 7$ and $|G| = 42$, what are the possible orders of $H$?

3. $(a)$ List the elements of order 3 in $\mathbb{Z}_{300}$.

$(b)$ Prove or disprove the following statement: $\mathbb{Z}_{120} \simeq \mathbb{Z}_6 \oplus \mathbb{Z}_{20}$.

4. $(a)$ Let $H \leq S_4$ defined via $H = \{(1), (1,2,3), (1,3,2)\}$. Prove or disprove: $H \triangleleft S_4$.

$(b)$ Let $G$ be a group, and let $H$ be a subgroup of $G$ such that $[G : H] = 2$. Prove that $H \triangleleft G$.

5. List all group homomorphisms $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_6$.

6. Consider the groups $\mathbb{Z}_{81}$, $\mathbb{Z}_{27} \oplus \mathbb{Z}_3$ and $\mathbb{Z}_9 \oplus \mathbb{Z}_9$. List the elements of order 3 of each group. Show that none of these groups are isomorphic.

7. Let $n \in \mathbb{Z}^+$ be even. Define the set $S = \big\{x + n\mathbb{Z} \big| x \text{ is even}\big\}$. Show that $S$ is a subring of $\mathbb{Z}_n$.

8. $(a)$ Produce an example of a ring $R$ and an element $x \in R$ that is a zero divisor. Produce an example of an element $y \in R$ that is a unit.

$(b)$ Let $D$ be an integral domain. Given $a, b \in D$, assume that $a^3 = b^3$ and $a^4 = b^4$. Show that $a = b$.

## Solutions to Practice Exam 2

1. Let $x = \frac{m}{n} \in \mathbb{Q}$. We notice that

$$E(x) = E\left(\frac{m}{n}\right) = E\left(\sum_{k=1}^{m} \frac{1}{n}\right) = \prod_{k=1}^{m} E\left(\frac{1}{n}\right) = E\left(\frac{1}{n}\right)^{m}. \tag{4}$$

Also,

$$E(1) = E\left(\frac{n}{n}\right) = E\left(\frac{1}{n}\right)^{n}. \tag{5}$$

This implies that $E\left(\frac{1}{n}\right) = E(1)^{\frac{1}{n}}$. Thus,

$$E(x) = E\left(\frac{1}{n}\right)^{m} = \left(E(1)^{\frac{1}{n}}\right)^{m} = E(1)^{\frac{m}{n}} = E(1)^{x}. \tag{6}$$

□

2. $(a)$

$$\langle 3 \rangle, \quad 1 + \langle 3 \rangle, \quad 2 + \langle 3 \rangle. \tag{7}$$

$(b)$ Let $|H| = n$. By Lagrange's theorem, $7|n$ and $n|42$. Moreover, $n \neq 7$ and $n \neq 42$. Therefore, $n \in \{14, 21\}$. □

3. $(a)$ $\overline{100}$, $\overline{200}$.

$(b)$ Since $\gcd(6, 20) = 2 \neq 1$, we have that $\mathbb{Z}_{120} \not\approx \mathbb{Z}_6 \oplus \mathbb{Z}_{20}$. □

4. $(a)$ We notice that

$$\begin{array}{l} (1,4)H = \{(1,4), (1,2,3,4), (1,3,2,4)\} \\ H(1,4) = \{(1,4), (1,4,2,3), (1,4,3,2)\} \end{array}. \tag{8}$$

Thus, $H \not\triangleleft S_4$.

$(b)$ Let $x \in G$. If $x \in H$, then $xH = H = Hx$. If $x \notin H$, then $xH \neq H$. At the same time, $Hx \neq H$, so since there exists only one other coset of $H$, $Hx = xH$ must be true. Either way, $H \triangleleft G$. □

$\boxed{5.}$ We know that a group homomorphism $\varphi : \mathbb{Z}_4 \to \mathbb{Z}_6$ is determined by $\varphi\left(\overline{1}\right)$. There exist six possibilities:

$$\begin{array}{lll} \varphi_1\left(\overline{1}\right) = \overline{0} & \varphi_2\left(\overline{1}\right) = \overline{1} & \varphi_3\left(\overline{1}\right) = \overline{2} \\ \varphi_4\left(\overline{1}\right) = \overline{3} & \varphi_5\left(\overline{1}\right) = \overline{4} & \varphi_6\left(\overline{1}\right) = \overline{5}. \end{array} \tag{9}$$

We note that, if $\varphi$ is a homomorphism, then

$$2\varphi\left(\overline{1}\right) = \varphi\left(\overline{2}\right) = \varphi\left(\overline{6}\right) = 6\varphi\left(\overline{1}\right) = \overline{0}. \tag{10}$$

However, the only maps satisfying this condition are $\varphi_1$ and $\varphi_4$. These are the only homomorphisms. $\square$

$\boxed{6.}$ In $\mathbb{Z}_{81}$:

$$\overline{27}, \overline{54}. \tag{11}$$

In $\mathbb{Z}_{27} \oplus \mathbb{Z}_3$:

$$\left(\overline{0}, \overline{1}\right), \left(\overline{0}, \overline{2}\right), \left(\overline{9}, \overline{0}\right), \left(\overline{9}, \overline{1}\right), \left(\overline{9}, \overline{2}\right), \left(\overline{18}, \overline{0}\right), \left(\overline{18}, \overline{1}\right), \left(\overline{18}, \overline{2}\right). \tag{12}$$

In $\mathbb{Z}_9 \oplus \mathbb{Z}_9$:

$$\left(\overline{0}, \overline{3}\right), \left(\overline{0}, \overline{6}\right), \left(\overline{3}, \overline{0}\right), \left(\overline{3}, \overline{3}\right), \left(\overline{3}, \overline{6}\right), \left(\overline{6}, \overline{0}\right), \left(\overline{6}, \overline{3}\right), \left(\overline{6}, \overline{6}\right). \tag{13}$$

Since $\mathbb{Z}_{81}$ has two elements of order $3$ and both $\mathbb{Z}_{27} \oplus \mathbb{Z}_3$ and $\mathbb{Z}_9 \oplus \mathbb{Z}_9$ have eight, we see that $\mathbb{Z}_{81} \not\simeq \mathbb{Z}_{27} \oplus \mathbb{Z}_3$ and $\mathbb{Z}_{81} \not\simeq \mathbb{Z}_9 \oplus \mathbb{Z}_9$. Additionally, $\mathbb{Z}_{27} \oplus \mathbb{Z}_3 \not\simeq \mathbb{Z}_9 \oplus \mathbb{Z}_9$, since $\mathbb{Z}_{27} \oplus \mathbb{Z}_3$ contains an element of order $27$ (namely, $\left(\overline{1}, \overline{0}\right)$), while $\mathbb{Z}_9 \oplus \mathbb{Z}_9$ contains no such element. $\square$

$\boxed{7.}$ We notice first that $S \neq \varnothing$, since $0 + n\mathbb{Z} \in S$. Now, let $x + n\mathbb{Z}, y + n\mathbb{Z} \in S$. In that case, $(x - y) + n\mathbb{Z} \in S$, since if $x$ and $y$ are even, then $x - y$ is also even. Additionally, $xy + n\mathbb{Z} \in S$, since if $x$ is even or $y$ is even, then $xy$ is also even. Thus, $S$ is a subring of $\mathbb{Z}_n$.

$\boxed{8.}$ $(a)$ Consider $M_2(\mathbb{Z})$, and

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad B = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{14}$$

Now $AB \neq 0$, thus $A$ is a zero divisor. The identity matrix $I_2$ is a unit, since $I_2 I_2 = I_2$.

$(b)$ We consider two cases: either $a = 0$ or $a \neq 0$. If $a = 0$, and $a^3 = b^3$, then $b^2 b = b^3 = 0$. This implies that either $b^2 = 0$ or $b = 0$, since $D$ is an integral domain. However, if $b^2 = 0$, then $b = 0$, so either way, $b = 0 = a$.

Consider the case that $a \neq 0$. Since $a^4 = b^4 = b^3 b = a^3 b$, we can write

$$a^3 (a - b) = a^4 - a^3 b = 0. \tag{15}$$

Now, as $a \neq 0$, we know that $a^2 \neq 0$, and so $a^3 \neq 0$. We deduce that $a - b = 0$, and therefore, $a = b$. $\square$

# Practice Exam 3

$\boxed{1.}$ Let $R$ be a commutative ring, and let $I$ and $J$ be ideals of $R$. Prove that $I \cap J$ is an ideal of $R$.

$\boxed{2.}$ Let $\varphi : \mathbb{Z}_n \to \mathbb{Z}_n$ be a ring homomorphism. Show that $\forall\ m \in \mathbb{Z}$, $\varphi(\overline{m}) = m\varphi(\overline{1})$.

$\boxed{3.}$ Let $D$ be an integral domain, and let $f, g \in D[X]$ be nonzero polynomials. Prove that

$$\deg(fg) = \deg f + \deg g. \tag{16}$$

$\boxed{4.}$ Determine which of the following polynomials are irreducible over $\mathbb{Q}$.
$(a)$ $f(X) = X^6 - 5X^5 + 10X^2 + 5X + 5$
$(b)$ $g(X) = X^4 - X + 1$
$(c)$ $h(X) = X^5 + X^4 + X^3 + X^2 + X + 1$.

$\boxed{5.}$ Show that 9 does not factor uniquely as a product of irreducibles in $\mathbb{Z}\left[\sqrt{-8}\right]$.

$\boxed{6.}$ Find the splitting field of $X^4 + 1$ over $\mathbb{Q}$.

$\boxed{7.}$ Find the extension degree of $\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{7}\right)$ over $\mathbb{Q}$.

$\boxed{8.}$ Let $f(X) = X^3 + X^2 + 1 \in \mathbb{Z}_2[X]$. Let $\alpha$ be a root of $f$ in an extension field of $\mathbb{Z}_2$. Find another root of $f$ in the same extension field.

## Solutions to Practice Exam 3

1. First, since $I$ and $J$ are ideals of $R$, we know that $I$ and $J$ are subrings of $R$. This indicates that $0 \in I$ and $0 \in J$. We deduce that $I \cap J \neq \varnothing$.

We claim that $I \cap J$ is an additive subgroup of $R$. Let $a, b \in I \cap J$. We notice that since $a, b \in I$, $a - b \in I$, as $I$ is an ideal. Similarly, since $a, b \in J$, $a - b \in J$. We deduce that $a - b \in I \cap J$. This establishes the claim.

We claim that $I \cap J$ is an ideal of $R$. Let $a \in I \cap J$, and let $r \in R$. In that case, $a \in I$, so since $I$ is an ideal of $R$, we have that $ra \in I$. Similarly, since $a \in J$ and $J$ is an ideal of $R$, $ra \in J$. Thus, $ra \in I \cap J$. This establishes that $I \cap J$ is an ideal of $R$. $\square$

2. Let $m \in \mathbb{Z}$. We consider two cases: either $m \geq 0$, or $m < 0$.

Consider the case that $m \geq 0$. In that case, $m = \sum_{i=1}^{m} 1$. Therefore, $\overline{m} = \sum_{i=1}^{m} \overline{1}$. Now, since $\varphi$ is a homomorphism,

$$\varphi\left(\overline{m}\right) = \varphi\left(\sum_{i=1}^{m} \overline{1}\right) = \sum_{i=1}^{m} \varphi\left(\overline{1}\right) = m\varphi\left(\overline{1}\right). \tag{17}$$

Consider the case that $m < 0$. In that case, $-m > 0$, so by the first case, $\varphi\left(\overline{-m}\right) = -m\varphi\left(\overline{1}\right)$. Now, we note that $\overline{m} + \overline{-m} = \overline{0}$, so since $\varphi$ is a homomorphism,

$$\varphi\left(\overline{m}\right) - m\varphi\left(\overline{1}\right) = \varphi\left(\overline{m}\right) + \varphi\left(\overline{-m}\right) = \varphi\left(\overline{m} + \overline{-m}\right) = \varphi\left(\overline{0}\right) = \overline{0}. \tag{18}$$

We deduce that $\varphi\left(\overline{m}\right) = m\varphi\left(\overline{1}\right)$. $\square$

3. Define $\deg f = m$ and $\deg g = n$. In that case,

$$\begin{aligned} f(X) &= a_m X^m + a_{m-1} X^{m-1} + \ldots + a_1 X + a_0 \\ g(X) &= b_n X^n + b_{n-1} X^{n-1} + \ldots + b_1 X + b_0 \end{aligned}, \tag{19}$$

for some $a_m \neq 0$ and $b_n \neq 0$. By definition of polynomial multiplication in $D[X]$,

$$f(X)g(X) = \sum_{k=0}^{m+n} c_k X^k, \tag{20}$$

where for each $k \in \{0, 1, 2, ..., m+n\}$,

$$c_k = \sum_{i+j=k} a_i b_j. \tag{21}$$

In particular, the coefficient of $X^{m+n}$ in $f(X)g(X)$ is

$$c_{m+n} = \sum_{i+j=m+n} a_i b_j = a_m b_n. \tag{22}$$

As $D$ is an integral domain and neither $a_m$ nor $b_n$ is 0, we know that $a_m b_n \neq 0$. Therefore, $a_m b_n$ is the leading coefficient of $fg$, and so $\deg(fg) = m + n$. $\square$

$\boxed{4.}$ $(a)$ $f$ is irreducible by Eisenstein's criterion with $p = 5$.

$(b)$ We claim that the polynomial $g$ is irreducible over $\mathbb{Q}$. We consider the polynomial $\overline{g}(X) = X^4 - X + 1 \in \mathbb{Z}_2[X]$. Assume, with the expectation of a contradiction, that $\overline{g}$ is reducible over $\mathbb{Z}_2$. We notice that

$$\begin{matrix} \overline{g}(0) = 1 \\ \overline{g}(1) = 1 \end{matrix}. \tag{23}$$

This shows that $\overline{g}$ has no linear divisor over $\mathbb{Z}_2$. Therefore, $\overline{g}$ factors into quadratic polynomials:

$$\overline{g}(X) = \left(X^2 + bX + c\right)\left(X^2 + eX + f\right) \tag{24}$$

for some $b, c, e, f \in \mathbb{Z}_2$. Ergo,

$$X^4 - X + 1 = X^4 + (e + b) X^3 + (f + be + c) X^2 + (bf + ce) X + ef. \tag{25}$$

This tells us that

$$\begin{aligned} e+b&=0\\ f+be+c&=0\\ bf+ce&=-1=1\\ cf&=1 \end{aligned} \tag{26}$$

Now, if $cf=1$, then $c=f=1$. Thus, the system becomes

$$\begin{aligned} e+b&=0\\ 1+be+1&=0.\\ b+e&=1 \end{aligned} \tag{27}$$

Ergo, $b+e=0$ and $b+e=1$. This contradiction leads us to conclude that our assumption that $\overline{g}$ is reducible is false; $\overline{g}$ is irreducible over $\mathbb{Z}_2$. Thus, $g$ is also irreducible over $\mathbb{Q}$.

$(c)$ We notice that

$$h(X)=\frac{X^6-1}{X-1}, \tag{28}$$

so $h(-1)=0$. This shows that $X+1|h(X)$, and so $h$ is reducible over $\mathbb{Q}$. □

5. We notice that

$$(3)(3)=9=\left(1+\sqrt{-8}\right)\left(1-\sqrt{-8}\right). \tag{29}$$

We claim that 3 is irreducible in $\mathbb{Z}\left[\sqrt{-8}\right]$. Suppose that $3=xy$. In that case, $9=N(3)=N(x)N(y)$. If $N(x)=3$ or $N(y)=3$, then $a^2+8b^2=3$ for some $a,b\in\mathbb{Z}$. As no such $a$ and $b$ exist, we see that one of $N(x)$ and $N(y)$ must be 1. Ergo, one must be a unit, and so 3 is irreducible.

Similarly, since $N\left(1\pm\sqrt{-8}\right)=9$, we see that $1\pm\sqrt{-8}$ are also irreducible. □

6. Let $K$ be the splitting field of $X^4+1$ over $\mathbb{Q}$. We notice that

$$X^4+1=\left(X^2+i\right)\left(X^2-i\right)=\left(X-e^{i\frac{3\pi}{4}}\right)\left(X+e^{i\frac{3\pi}{4}}\right)\left(X-e^{i\frac{\pi}{4}}\right)\left(X+e^{i\frac{\pi}{4}}\right). \tag{30}$$

Now, $e^{i\frac{\pi}{4}} = \frac{1+i}{\sqrt{2}}$ and $e^{i\frac{3\pi}{4}} = \frac{-1+i}{\sqrt{2}}$. We notice that $e^{i\frac{\pi}{4}} - e^{i\frac{3\pi}{4}} = \sqrt{2}$. Therefore, $\sqrt{2} \in K$. Additionally $i = \sqrt{2}e^{i\frac{\pi}{4}} - 1 \in K$, since $K$ is a field. We deduce that the splitting field is $K = \mathbb{Q}\left(\sqrt{2}, i\right)$.

7. By the tower theorem,

$$\left[\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{7}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{7}\right) : \mathbb{Q}\left(\sqrt{3}\right)\right]\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right]. \tag{31}$$

Since $\left\{1, \sqrt{3}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{3}\right)$ over $\mathbb{Q}$, we see that

$$\left[\mathbb{Q}\left(\sqrt{3}\right) : \mathbb{Q}\right] = 2. \tag{32}$$

Since $\left\{1, 7^{\frac{1}{3}}, 7^{\frac{2}{3}}\right\}$ is a basis for $\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{7}\right)$ over $\mathbb{Q}\left(\sqrt{3}\right)$, we see that

$$\left[\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{7}\right) : \mathbb{Q}\left(\sqrt{3}\right)\right] = 3. \tag{33}$$

Therefore,

$$\left[\mathbb{Q}\left(\sqrt{3}, \sqrt[3]{7}\right) : \mathbb{Q}\right] = 6. \tag{34}$$

□

8. Define $K = \mathbb{Z}_2(\alpha)$. As $f(\alpha) = 0$, we know that $\alpha^3 + \alpha^2 + 1 = 0$. Thus, $\alpha^3 = \alpha^2 + 1$, since $\mathrm{char} K = 2$.

We claim that $\alpha^2$ is a root of $f$. We notice

$$f\left(\alpha^2\right) = \alpha^6 + \alpha^4 + 1. \tag{35}$$

We have

$$\alpha^4 = \alpha\left(\alpha^3\right) = \alpha\left(\alpha^2 + 1\right) = \alpha^3 + \alpha = \alpha^2 + \alpha + 1. \tag{36}$$

and

$$\alpha^6 = \left(\alpha^3\right)^2 = \left(\alpha^2 + 1\right)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha^4 + 1 = \alpha^2 + \alpha. \tag{37}$$

Thus,

$$f\left(\alpha^2\right) = \left(\alpha^2 + \alpha\right) + \left(\alpha^2 + \alpha + 1\right) + 1 = 0. \tag{38}$$

Ergo, $\alpha^2$ is a root of $f$. $\square$