Solutions to the midterm

① First consider isomorphisms of $2\mathbb{Z}$ and $3\mathbb{Z}$ as abelian groups (not rings). The generators of additive groups are ± 2 and ± 3, respectively. So an additive isomorphism $\varphi: (2\mathbb{Z}, +) \to (3\mathbb{Z}, +)$ must send generator to generator and hence $\varphi(2) = \pm 3$. But

$$\varphi(4) = \varphi(2+2) = \pm 6 \neq \varphi(2)\cdot\varphi(2)$$

so such φ would not be multiplicative and a <u>ring</u> isomorphism does not exist.

② By the long division algorithm:

$$x^4 + x^3 + x^2 - x + 1 = (x+2)(x^3 - x^2 + 3x - 7) + 15$$

(and 15 is also the value of $x^4+x^3+x^2-x+1$ at $x=-2$)
We need the values of prime p such that $15 \equiv 0 \pmod p$
These are the prime factors of 15, i.e. $p=3$ and $p=5$

③ If F is the field of quotients then $\mathbb{Z}_5[x] \hookrightarrow F$ is a subring. But $\{1, x, x^2, x^3, \dots\} \subset \mathbb{Z}_5[x]$ is an infinite subset. So $\mathbb{Z}_5[x]$ is infinite and F is infinite as well.

We know that $1+1+1+1+1=0$ in F since this holds in $\mathbb{Z}_5$ and $\mathbb{Z}_5 \subset \mathbb{Z}_5[x] \subset F$. Also $m\cdot 1 = 0$ does not hold in F for $m=1,\dots,4$ since it does not hold in $\mathbb{Z}_5$. So $m=5$ is the characteristic of F.

④ First we check that $g=2$ is a generator.
Since $2^{12} \equiv 1 \pmod{13}$ by Fermat, the multiplicative

Since we check that $g=2$ is a generator.

Since $2^{12} \equiv 1 \pmod{13}$ by Fermat, the multiplicative order of 2 divides 12. If that order were <12 we would have $2^6 \equiv 1$ or $2^4 \equiv 1$. But $2^6 = (2^3)^2 = 6^4 \equiv -1$ and $2^4 = (2^2)^2 = 16 \equiv 3$. Hence $g=2$ is a generator.

This means
$$\begin{aligned} (\mathbb{Z}_{12}, +) &\longrightarrow (\mathbb{Z}_{13}^{\times}, \times) \\ a &\longmapsto 2^a \end{aligned}$$
is a group isomorphism.

Other multiplicative generators of $\mathbb{Z}_{13}^{\times}$ correspond to a which are additive generators of $\mathbb{Z}_{12}$. This happens when $\gcd(a,12)=1$ so $a \in \{1,5,7,11\} \subset \mathbb{Z}_{12}$.

So the set of multiplicative generators is

$$\{2^1, 2^5, 2^7, 2^{11}\} = \{2, 6, 7, 11\} \subset \mathbb{Z}_{13}^{\times}.$$