HOMEWORK 3 SOLUTIONS

1. Problem 1

From Artin, we may construct $\mathbb{F}_4$ as having the elements $\{0, 1, \alpha, \alpha+1\}$ with characteristic 2 where α is a root of x^2+x+1. Now, in $\mathbb{F}_2[x]$ as per Artin,

$$x^{16} - x = x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$$

We have $x^2+x+1 = (x-\alpha)(x-(\alpha+1))$ in $\mathbb{F}_4[x]$. We now consider the degree 4 polynomials. These split completely in $\mathbb{F}_{16}$ as they divide $x^{16}-x$. The minimal polynomial in $F_4[x]$ of any of the roots β is $(x-\beta)(x-\phi^2(\beta))\cdots(x-\phi^{2n}(\beta))$ where ϕ is the Frobenius function and n is the minimal integer such that $\phi^{2n+2}(\beta) = \beta$. This n is equal to 1 as $\beta \in \mathbb{F}_{16}$, and so satisfies $\phi^4(\beta) = \beta^{16} = \beta$ and does not satisfy this condition for a lower n as this would imply it is an element of a subfield of $\mathbb{F}_{16}$. Then each degree 4 polynomial splits as $(x-\beta)(x-\phi^2(\beta))\cdot(x-\phi(\beta))(x-\phi^3(\beta)) = (x^2-(\beta+\beta^4)x+\beta^5)(x^2-(\beta^2+\beta^8)x+\beta^{10})$ in $F_4[x]$.

Let $\mathbb{F}_{16} = \mathbb{F}_2[\gamma]$ where γ is a root of x^4+x+1 (we may do this by a lecture result). Now γ^3 is a root of $x^4+x^3+x^2+1$ and γ^3+1 is a root of x^4+x^3+1 by direct computation with the modulus. In the case of x^4+x+1, it splits into $x^2+(\gamma+\gamma^4)+\gamma^5 = x^2+x+(\gamma^2+\gamma) = x^2+x+\alpha$ and $x^2+(\gamma^2+\gamma^8)+\gamma^{10} = x^2+x+(\alpha+1)$. We note that we have set $\alpha = \gamma^2+\gamma$, noting our choice is arbitary as both $\gamma^2+\gamma$ and $\gamma^2+\gamma+1$ satisfy $x^2+x+1=0$. Proceeding in a similar manner with the other polynomials by letting β equal γ^3 and γ^3+1, we find

$$\begin{aligned} x^{16} - x = {} & x(x-1)(x-\alpha)(x-(\alpha+1))\cdot \\ & (x^2+\alpha x+1)(x^2+(\alpha+1)x+1)\cdot \\ & (x^2+\alpha x+\alpha)(x^2+(\alpha+1)x+(\alpha+1))\cdot \\ & (x^2+x+\alpha)(x^2+x+(\alpha+1)) \end{aligned}$$

gives the complete factorisation in $\mathbb{F}_4[x]$.

Over $\mathbb{F}_8$

Consider that the degree 2 and degree 4 polynomials split completely in $\mathbb{F}_{2^{12}}$, as they split completely in $\mathbb{F}_{16} \subset \mathbb{F}_{2^{12}}$ as above. Letting a root of the degree 2 polynomial be α, it splits as $(x-\alpha)(x-\phi(\alpha))$ as the degree of the polynomial is 2 and $\phi^n(\alpha)$ for $n \in \mathbb{Z}^+$ are the conjugates of α. Over $\mathbb{F}_8 \subset \mathbb{F}_{2^{12}}$, the minimimal polynomial of α is given by $(x-\alpha)(x-\phi^3(\alpha))\cdots(x-\phi^{3n}(\alpha))$ where n is minimal such that $\phi^{3n+3}(\alpha)=\alpha$. We must have $\phi^2(\alpha)=\alpha$ where $\phi(\alpha)\neq\alpha$ for the factorisation to hold, so $\phi^3(\alpha)=\phi(\alpha), \phi^6(\alpha)=\alpha$, and the minimal polynomial over $\mathbb{F}_8$ is the same.

For any of the degree 4 polynomials, we again set a root as α and note that the polynomial must split as $(x-\alpha)(x-\phi(\alpha))(x-\phi^2(\alpha))(x-\phi^3(\alpha))$. The minimal polynomial of α over $\mathbb{F}_8$ is $(x-\alpha)(x-\phi^3(\alpha))\cdots(x-\phi^{3n}(\alpha))$ where n is minimal such that $\phi^{3n+3}(\alpha)=\alpha$ as before. Then noting $\phi^4(\alpha)=\alpha$ (and this is minimal), we have $\phi^6(\alpha)=\phi^2(\alpha), \phi^9(\alpha)=\phi(\alpha), \phi^{12}(\alpha)=\alpha$. Then the minimal polynomial is the same over $\mathbb{F}_8$. Thus

$$x^{16}-x = x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$$

gives the complete factorisation in $\mathbb{F}_8[x]$

Let $R \subset S$ be an inclusion of rings. Suppose we have an isomorphism

$$S \cong R[x_1, \ldots, x_n]/I,$$

where $x_1, \ldots, x_n$ are variables and $I \subset R[x_1, \ldots, x_n]$ is an ideal. Such an isomorphism is called a *presentation* of S over R.

Let A be another ring and suppose a ring homomorphism $i\colon R \to A$ is given. A presentation of S over R gives us all the ways of extending i to a ring homomorphism $S \to A$. This is because a ring homomorphism $R[x_1, \ldots, x_n] \to A$ extending i is determined uniquely by the images of $x_1, \ldots, x_n$ and such a homomorphism is well-defined modulo I if and only if it sends I to 0.

2. a

Find a presentation for $\mathbb{Q}[\sqrt[3]{2}]$ over $\mathbb{Q}$. Use it to determine all homomorphisms

$$\mathbb{Q}[\sqrt[3]{2}] \to \mathbb{C}.$$

What are the images of these homomorphisms?

Answer

Firstly note in assignment 1 it was shown $x^3 - 2$ is the minimal rational polynomial with $\sqrt[3]{2}$ as a root. Hence it follows from proposition 15.2.6 that

$$\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[x]/(x^3 - 2)$$

which indicates $\mathbb{Q}[x]/(x^3 - 2)$ is the presentation of $\mathbb{Q}[\sqrt[3]{2}]$ over $\mathbb{Q}$. As the only homomorphism from $\mathbb{Q}$ to $\mathbb{C}$ is the identity homomorphism it follows that for a homomorphism $f : \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{C}$ to exist it must satisfy $f(x)^3 - 2 = 0$. This leads to three possible homomorphisms each defined by how they uniquely act on x

$$f_1 : \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{C} \text{ where } f_1(x) = \sqrt[3]{2} \text{ with image } \mathbb{Q}[\sqrt[3]{2}]$$

$$f_2 : \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{C} \text{ where } f_2(x) = \zeta_3\sqrt[3]{2} \text{ with image } \mathbb{Q}[\zeta_3\sqrt[3]{2}]$$

$$f_3 : \mathbb{Q}[x]/(x^3 - 2) \to \mathbb{C} \text{ where } f_3(x) = \zeta_3^2\sqrt[3]{2} \text{ with image } \mathbb{Q}[\zeta_3^2\sqrt[3]{2}]$$

It is not necessary to know that $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis. You only require the weaker and immediate condition that the set spans, so that

$$\dim_{\mathbf{Q}} \mathbf{Q}[\sqrt{2}, \sqrt{3}] \leq 4.$$

2. b

Do the same for $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ over $\mathbb{Q}$.

Answer

It is important to note that $\sqrt{2}+\sqrt{3}$ is a primitive element of $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Trivially $\sqrt{2}+\sqrt{3} \in \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ which indicates $\mathbb{Q}[\sqrt{2}+\sqrt{3}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$. Now consider that Example 15.4.4 indicates the set $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ forms a basis for the vector space $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ over $\mathbb{Q}$, hence $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$ is a degree 4 extension of $\mathbb{Q}$. Examples 15.4.1 and 15.4.4 also provide that $\sqrt{2}+\sqrt{3}$ is a root of the irreducible polynomial $x^4 - 10x^2 + 1$ hence it follows that $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ is a degree 4 extension of $\mathbb{Q}$. Two degree four extensions of $\mathbb{Q}$ cannot be subfields of one another hence it follows that $\mathbb{Q}[\sqrt{2}+\sqrt{3}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{3}]$ implies $\mathbb{Q}[\sqrt{2}+\sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$.

As $\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2}+\sqrt{3}]$ it is equivalent to find a presentation of $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ over $\mathbb{Q}$. Note as stated earlier $x^4 - 10x^2 + 1$ is an irreducible polynomial over $\mathbb{Q}$ with $\sqrt{2}+\sqrt{3}$ as a root of the polynomial. Therefore by proposition 15.2.6 it follows

$$\mathbb{Q}[\sqrt{2}+\sqrt{3}]\mathbb{Q}[x]/(x^4 - 10x^2 + 1)$$

which indicates $\mathbb{Q}[x]/(x^4 - 10x^2 + 1)$ is the presentation of $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$ over $\mathbb{Q}$. As the only homomorphism from $\mathbb{Q}$ to $\mathbb{C}$ is the identity homomorphism it follows that for a homomorphism $f : \mathbb{Q}[x]/(x^4 - 10x^2 + 1) \to \mathbb{C}$ to exist it must satisfy $f(x)^4 - 10f(x)^2 + 1 = 0$. This leads to four possible homomorphisms each defined by how they uniquely act on x. Note example 15.4.3 of the textbook gives all of the roots of the polynomial $x^4 - 10x^2 + 1$ hence the homomorphisms are given by

$$f_1 : \mathbb{Q}[x]/(x^4 - 10x^2 + 1) \to \mathbb{C} \text{ where } f_1(x) = \sqrt{2}+\sqrt{3}$$
with image $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$

$$f_2 : \mathbb{Q}[x]/(x^4 - 10x^2 + 1) \to \mathbb{C} \text{ where } f_2(x) = -\sqrt{2}-\sqrt{3}$$
with image $\mathbb{Q}[\sqrt{2}+\sqrt{3}]$

$$f_3 : \mathbb{Q}[x]/(x^4 - 10x^2 + 1) \to \mathbb{C} \text{ where } f_3(x) = \sqrt{2}-\sqrt{3}$$
with image $\mathbb{Q}[\sqrt{2}-\sqrt{3}]$

$$f_4 : \mathbb{Q}[x]/(x^4 - 10x^2 + 1) \to \mathbb{C} \text{ where } f_3(x) = -\sqrt{2}+\sqrt{3}$$
with image $\mathbb{Q}[\sqrt{2}-\sqrt{3}]$

Here one observes that

$$4 = \dim_{\mathbf{Q}} \mathbf{Q}[\sqrt{2}+\sqrt{3}]$$

$$\leq \dim_{\mathbf{Q}} \mathbf{Q}[\sqrt{2}, \sqrt{3}] \leq 4.$$

0 Need to make clear that the images of $\mathbf{Q}[\sqrt{2}, \sqrt{3}] \to \mathbf{C}$ are all the same field ...

Problem 3.

Let p be a prime number and let $\zeta_p = e^{\frac{2\pi i}{p}}$. ~~Then~~ let $F = \mathbb{Q}[\zeta_p]$. ~~Then~~ consider that ζ_p satisfies the polynomial $x^p - 1$. Which is reducible as

$$x^p - 1 = (x-1)(x^{p-1} + ... + x + 1)$$

~~Then~~ consider $f(x) = x^{p-1} + ... + x + 1$ for $p > 2$ then p is odd and so there are $p-1$ non constant terms so consider $f(x)$ in $\mathbb{F}_2[x]$ then since $p-1$ is even it holds that

$$1^{p-1} + ... + 1 + 1 = 1$$

This argument only shows that

$$x^{p-1} + \cdots + 1$$

has no roots. It does not show that it is irreducible.

Irreducibility can be proved via Eisenstein (Artin Theorem 12.4.9, or Lecture March 6 notes, p. 6).

and

$$0^{p-1} + ... + 0 + 1 = 1$$

and so $f(x) = x^{p-1} + ... + x + 1$ is irreducible and $f(\zeta_p) = 0$. ~~Then~~ consider the substitution map

$$\mathbb{Q}[x] \to \mathbb{Q}[\zeta_p]$$

given by the substitution $x \mapsto \zeta_p$. ~~Then~~ the kernel of this map is the ideal $(x^{p-1} + ... + x + 1)$ and so by the first isomorphism theorem we have an isomorphism

$$\varphi : \mathbb{Q}[x]/(x^{p-1} + ... + x + 1) \to \mathbb{Q}[\zeta_p]$$

The presentation φ and the maps ψ_k to be constructed are two completely independent maps. In fact ψ_k is simply an-...

Expand

Therefore we have a presentation of $\mathbb{Q}[\zeta_p]$. ~~Then~~ taking $i : \mathbb{Q} \to \mathbb{Q}[\zeta_p]$ to be the inclusion map of $\mathbb{Q}$ in $\mathbb{Q}[\zeta_p]$, ~~Then~~ we can extend this to a map $\mathbb{Q}[x] \to \mathbb{Q}[\zeta_p]$ by choosing where to send x. To be well defined modulo $(x^{p-1} + ... + x + 1)$, ~~then~~ it must send $(x^{p-1} + ... + x + 1)$ to 0. Therefore x must be sent to a root of $(x^{p-1} + ... + x + 1)$ in $\mathbb{Q}[\zeta_p]$ these are the complex p roots of unity.

$$\zeta_p, \zeta_p^2, ..., \zeta_p^{p-1}$$

Hence we have $p-1$ choices of isomorphisms

$$\psi_k : \mathbb{Q}[x]/(x^{p-1} + ... + x + 1) \to \mathbb{Q}[\zeta_p]$$

and so we have the commutative diagram

$$\begin{tikzcd}
& \mathbb{Q}[x] \arrow[dl] \arrow[d] \arrow[dr] & \\
\mathbb{Q}[\zeta_p] \arrow[rr, bend right] & \mathbb{Q}[x]/(x^{p-1} + ... + x + 1) \arrow[l, "\varphi"] \arrow[r, "\psi_k"] & \mathbb{Q}[\zeta_p]
\end{tikzcd}$$

Masterpiece.

Then we have $p-1$ automorphisms $F \to F$.
We now seek to describe the automorphism group $Aut(F)$. To do this consider the automorphism ϕ_i acquired from sending x to ζ_p^i and the automorphism ϕ_j acquired from sending x to ζ_p^j. Then consider the composition $\phi_i \circ \phi_j$. ~~Then~~ if we begin with ζ_p then this maps to ζ_p^i which then is mapped to by x^i which then maps to ζ_p^{ij} which then corresponds to the automorphism acquired by

Q4

A presentation for k over F is $F[x]/(x^p-2) \cong F[2^{\frac{1}{p}}]$.

Proof: Consider $\phi: F[x] \to F[2^{\frac{1}{p}}]$ which acts as the identity on F and sends x to $2^{\frac{1}{p}}$.

It is a ring homomorphism following the same reason as before.

Then, $\ker(\phi) = \{f(x) \in F[x] \mid f(2^{\frac{1}{p}}) = 0\}$ and $\operatorname{Im}(\phi) = F[2^{\frac{1}{p}}]$.

Claim that $x^p - 2$ is irreducible over F.

It suffices to show that $\deg_F k = p$.

We know that $\mathbb{Q} \subseteq \mathbb{Q}[\zeta_p] \subseteq \mathbb{Q}[\zeta_p, 2^{\frac{1}{p}}]$, $\mathbb{Q} \subseteq \mathbb{Q}[2^{\frac{1}{p}}] \subseteq \mathbb{Q}[\zeta_p, 2^{\frac{1}{p}}]$, $\deg_{\mathbb{Q}}(\zeta_p) = p-1$ and $\deg_{\mathbb{Q}}(2^{\frac{1}{p}}) = p$ by Eisenstein Criteria.

By multiplicative property, we have $p(p-1) \mid \deg_{\mathbb{Q}} \mathbb{Q}[\zeta_p, 2^{\frac{1}{p}}]$ and hence $p(p-1) \leq \deg_{\mathbb{Q}} \mathbb{Q}[\zeta_p, 2^{\frac{1}{p}}]$ since $p \mid \deg_{\mathbb{Q}} \mathbb{Q}[\zeta_p, 2^{\frac{1}{p}}]$, $p-1 \mid \deg_{\mathbb{Q}} \mathbb{Q}[\zeta_p, 2^{\frac{1}{p}}]$, and $(p, p-1) = 1$.

As $2^{\frac{1}{p}}$ satisfies $x^p - 2$ which is irreducible over $\mathbb{Q}$, then $\deg_{\mathbb{Q}[\zeta_p]}(2^{\frac{1}{p}}) \leq p$.

Then, by multiplicative property, we have $\deg_{\mathbb{Q}} \mathbb{Q}[\zeta_p, 2^{\frac{1}{p}}] \leq p(p-1)$

So, $\deg_{\mathbb{Q}} \mathbb{Q}[\zeta_p, 2^{\frac{1}{p}}] = p(p-1)$ and hence $\deg_{\mathbb{Q}[\zeta_p]} \mathbb{Q}[\zeta_p, 2^{\frac{1}{p}}] = p$.

Hence, $x^p - 2$ is irreducible over $\mathbb{Q}[\zeta_p]$.

Then, $\ker(\phi) = (x^p - 2)$ since $F = \mathbb{Q}[\zeta_p]$ is a field and hence $F[x]$ is a ~~principle~~ principal ideal domain by theorem.

By the first isomorphism theorem, we have $F[x]/(x^p-2) \cong F[2^{\frac{1}{p}}] = k$.

- There are $p-1$ homomorphisms from F to $F[2^{\frac{1}{p}}]$: Following the same construction from Q3, as roots of $x^{p-1} + x^{p-2} + \cdots + 1$: $\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1} \in F[2^{\frac{1}{p}}]$, then there are $p-1$ homomorphisms (or by inspection that

$$(2^{1/p}\zeta_p^k)^p = 2$$

for all $k = 0, \dots, p-1$.)

from F to $F[2^{\frac{1}{p}}]$.

- By fundamental theorem of algebra, there are p roots of $x^p - 2$ in $\mathbb{C}$: $2^{\frac{1}{p}}, 2^{\frac{1}{p}}\zeta_p, 2^{\frac{1}{p}}\zeta_p^2, \dots, 2^{\frac{1}{p}}\zeta_p^{p-1}$.

As $2^{\frac{1}{p}}, 2^{\frac{1}{p}}\zeta_p, 2^{\frac{1}{p}}\zeta_p^2, \dots, 2^{\frac{1}{p}}\zeta_p^{p-1} \in K$, then there are p roots of $x^p - 2$ in K: $2^{\frac{1}{p}}, 2^{\frac{1}{p}}\zeta_p, 2^{\frac{1}{p}}\zeta_p^2, \dots, 2^{\frac{1}{p}}\zeta_p^{p-1}$.

So, by mapping property of polynomial ring we have $p(p-1)$ ring homomorphisms $\psi_{k,\ell}$ from $K = F[2^{\frac{1}{p}}] \cong F[x]/(x^p - 2)$ to K with $1 \le k \le p$:

$\psi_{1,\ell}(a_{p-1}x^{p-1} + a_{p-2}x^{p-2} + \dots + a_0) = \varphi_\ell(a_{p-1})(2^{\frac{1}{p}})^{p-1} + \varphi_\ell(a_{p-2})(2^{\frac{1}{p}})^{p-2} + \dots + \varphi_\ell(a_0)$,

$\psi_{2,\ell}(a_{p-1}x^{p-1} + a_{p-2}x^{p-2} + \dots + a_0) = \varphi_\ell(a_{p-1})(2^{\frac{1}{p}}\zeta_p)^{p-1} + \varphi_\ell(a_{p-2})(2^{\frac{1}{p}}\zeta_p)^{p-2} + \dots + \varphi_\ell(a_0)$,

$\vdots$

$\psi_{p,\ell}(a_{p-1}x^{p-1} + a_{p-2}x^{p-2} + \dots + a_0) = \varphi_\ell(a_{p-1})(2^{\frac{1}{p}}\zeta_p^{p-1})^{p-1} + \varphi_\ell(a_{p-2})(2^{\frac{1}{p}}\zeta_p^{p-1})^{p-2} + \dots + \varphi_\ell(a_0)$

where $a_i \in F$ with $0 \le i \le p-1$ and $\varphi_\ell : F \to F$ defined as in Q3 with $1 \le \ell \le p-1$.

As $\psi_{k,\ell}|_F = \varphi_\ell$ for all $1 \le k \le p$, $1 \le \ell \le p-1$ and $\varphi_1 = \mathrm{Id}$, then $\psi_{k,\ell}|_F = \mathrm{Id}|_F$ if $\ell = 1$ and hence there are p homomorphisms from K to K restricting to the identity on F.

Q_5

There are $\frac{p^n+1}{2}$ perfect square if p is odd, p^n perfect square if p is even.

There are $\frac{p^n-1}{\gcd(p^n-1,d)}+1$ perfect dth power.

We know that $k^\times$ is a cyclic group, say $k^\times = \{1, g, g^2, \cdots, g^{p^n-2}\}$ where $g \in k^\times$ is a generator of $k^\times$.

Then, the number of elements in k are perfect dth power $=$ the number of distinct elements in $\{1, g^d, (g^d)^2, \cdots, (g^d)^{p^n-2}\} \cup \{0\}$ $= \operatorname{ord}(g^d)+1$ as $0 \notin k^\times$ but 0 is a perfect dth power in k.

Claim that $\operatorname{ord}(g^d) = \frac{\operatorname{ord}(g)}{\gcd(\operatorname{ord}(g), d)} = \frac{p^n-1}{\gcd(p^n-1,d)}$.

First, we have $(g^d)^{\frac{p^n-1}{\gcd(p^n-1,d)}} = g^{p^n-1\left(\frac{d}{\gcd(p^n-1,d)}\right)} = 1$ since $\operatorname{ord}(g) = |k^\times| = p^n-1$ and $\gcd(p^n-1,d) \mid d$.

So, $\operatorname{ord}(g^d) \mid \frac{p^n-1}{\gcd(p^n-1,d)}$ $= \operatorname{ord}(g)/\gcd(\operatorname{ord}(g), d)$

Let $n = \operatorname{ord}(g)$, $n' = \operatorname{ord}(g^d)$, $\lambda = \gcd(n,d)$, $n_0 = \frac{n}{\lambda}$, and $d_0 = \frac{d}{\lambda}$.

Should use a symbol other than n, since n is already used as the exponent for the cardinality p^n. In fact

$$n = \log_p(\operatorname{ord}(g)+1).$$

Then, we have $(n_0, d_0) = 1$. (E.g., by Bezout)

As $1 = a^{dn'} = a^{\lambda d_0 n'}$, then $n \mid \lambda d_0 n'$ and hence $\frac{\lambda d_0 n'}{n} = \frac{d_0 n'}{n_0} \in \mathbb{Z}$.

As $(n_0, d_0) = 1$, then $n_0 \mid n'$ and hence $\frac{\operatorname{ord}(g)}{\gcd(\operatorname{ord}(g), d)} \mid \operatorname{ord}(g^d)$.

So, $\operatorname{ord}(g^d) = \frac{\operatorname{ord}(g)}{\gcd(\operatorname{ord}(g), d)}$ and hence there are $\frac{p^n-1}{\gcd(p^n-1,d)}+1$ perfect dth power.