# Algebra Qualifying Exam -Spring 2010

1. Let $f(x) = x^6 + 3$ □ Q[x]. Show that the Galois group of f is $S_3$.

2. (a) Let G be a group of order pqr, where $p<q<r$ are primes. Show that G contains a normal subgroup of index p.
(b) Determine up to isomorphism all groups of order $3 \cdot 7 \cdot 13$.

3. Let R be a commutative Noetherian ring, and let I, J, and K be ideals of R. We say I is irreducible if $I = J \cap K$ ® $I = J$, or $I = K$.
(a) Show that every ideal of R is a finite intersection of irreducible ideals.
(b) Show that every irreducible ideal is primary (An ideal I of R is primary if $R/I \neq 0$, and every zero-divisor in R/I is nilpotent.)

4. Let A be a finite-dimensional algebra ever a field K, such that for every a □ A, $a^7 = a$. Show that A is a direct product (sum?) of fields. Which fields can arise?

5. Let G and H be finitely generated abelian groups such that G $□_Z$ H = 0. Show that G and H are finite and have relatively prime orders.

6. Let S and T be diagonalizable endomorphisms of a finite dimensional complex vector space. If S and T commute show that they are polynomials in each other.

7. What are the prime ideals of Z[x]? What are the maximal ideals? Carefully explain your answers.

# Algebra Spring 2010

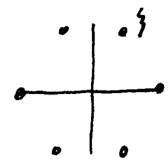
(1) Let $f(X) = X^6 + 3 \in \mathbb{Q}[X]$.

Show the Galois group of $f(x)$ is $S_3$.

---

solution

Let $\xi$ be the primative $6^{th}$ root of unity $\frac{1}{2} + \frac{\sqrt{3}}{2} i$.




Let $\alpha = \sqrt[6]{3}\, i$. The roots of $X^6 + 3$ are $\alpha \xi^n$ $n = 0, 1, \dots, 5$.

Let $F$ be the sylitting field of $f(x)$.
Then $F = \mathbb{Q}(\alpha, \xi)$.

Since $X^6 + 3$ is irred $/ \mathbb{Q}$ by Eisenstein, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. we show $F = \mathbb{Q}(\alpha)$, for which we need to show $\xi \in \mathbb{Q}(\alpha)$.

Indeed, $\alpha^3 = -\sqrt{3}\, i$, so $\xi = \frac{1}{2} - \frac{\alpha^3}{2}$.
Thus, $[F : \mathbb{Q}] = 6$ and $|G| = 6$, where $G$ is the Galois group of $f(X)$.

Let $\boxed{\varphi : \alpha \to \alpha\xi.}$ $\in G.$

Then $\xi = \frac{1}{2} - \frac{\alpha^3}{2} \xrightarrow{\varphi} \frac{1}{2} - \frac{\alpha^3\xi^3}{2} = \frac{1}{2} + \frac{\alpha^3}{2} = \frac{1}{2} - \frac{\sqrt{3}}{2}i = \xi^5.$

$$\boxed{\xi \xrightarrow{\varphi} \xi^5}$$

$\varphi : \alpha \to \alpha\xi \to \alpha\xi\cdot\xi^5 = \alpha \quad \Rightarrow |\varphi| = 2.$

Let $\boxed{\psi : \alpha \longrightarrow \alpha\xi^2}.$

Then $\xi = \frac{1}{2} - \frac{\alpha^3}{2} \xrightarrow{\psi} \frac{1}{2} - \frac{\alpha^3\xi^6}{2} = \frac{1}{2} - \frac{\alpha^3}{2} = \xi.$

$$\boxed{\xi \xrightarrow{\psi} \xi}$$

$\psi : \alpha \to \alpha\xi^2 \to \alpha\xi^4 \to \alpha \quad \Rightarrow |\psi| = 3.$

$\varphi\psi(\alpha) = \varphi(\alpha\xi^2) = \alpha\xi\cdot\xi^{10} = \alpha\xi^5.$

$\psi\varphi(\alpha) = \psi(\alpha\xi) = \alpha\xi^3.$ $\neq$

At this point $G$ is nonabelian $\Rightarrow G \cong S_3.$

Indeed $\psi^2\varphi(\alpha) = \psi^2(\alpha\xi) = \alpha\xi^5 = \varphi\psi(\alpha).$

$\square$

(2) (a) Let $|G| = pqr$ $p<q<r$ primes.

Show $G$ has a normal s.g. of index $p$.

(b) Determine groups of order $3\cdot 7\cdot 13$ up to isomorphism.

---

<u>solution to (a)</u>

Let $H$ be a $q$-Sylow s.g. $\Rightarrow |H| = q$.

and let $K$ be a $r$-Sylow s.g. $\Rightarrow |K| = r$.

We show either $H$ or $K$ is normal.

$n_r = 1$ or $pq$ and $n_q = 1$ or $r$ or $pr$.

(margin notes: $p, q, pq, \equiv 1 \pmod r$; $1, p, r, pr, \equiv 1 \pmod q$)

Suppose $n_r = pq$ and $n_q = r$. Then $G$ has at least

$1 + (r-1)pq + r(q-1) = 1 + rpq - pq + r(q-1)$ (*)

elts. $r \geq p+2$ and $q \geq p+1$. So

$pq \overset{?\checkmark}{\leq} r(q-1)$, $r(q-1) \geq (p+2)(q-1)$
$= pq + (2q - p - 2)$

$\Uparrow$

$p+2 \overset{?\checkmark}{\leq} 2q$, $2q \geq 2(p+1) = 2p+2 \geq p+2$.

Either by making an inequality strict or by including the identity in (*)
we see $|G| > pqr$. $\Rightarrow\Leftarrow$ So one of $n_r = 1$ or $n_q = 1$. ✓

Thus $HK$ is a subgroup of index $p$.
Since $p$ is the smallest prime dividing $|G|$, we conclude $HK$ is normal. $\square$.

---

<u>solution to (b)</u> $|G| = 3 \cdot 7 \cdot 13$

Let $P, Q, R$ be 3-Sylow, 7-Sylow, 13-Sylow subgroups, respectively. Then

$$P = \langle x \rangle \cong \mathbb{Z}_3, \quad Q = \langle y \rangle \cong \mathbb{Z}_7, \quad R = \langle z \rangle \cong \mathbb{Z}_{13}$$

all multiplicatively. And $QR$ is normal.
So $G$ is a semidirect product of $P$ and $QR$ whose structure is determined by group homs

$$\mathbb{Z}_3 \longrightarrow \text{Aut}(\mathbb{Z}_7 \times \mathbb{Z}_{13}) \cong \mathbb{Z}_6 \times \mathbb{Z}_{12}.$$

($QR \cong Q \times R$ since $Q$ and $R$ are the unique 7-Sylow and 13-Sylow subgroups in $QR$.)
( $\text{Aut}(G \times H) \cong \text{Aut}\, G \times \text{Aut}\, H$ when $\gcd(|G|, |H|) = 1$.)
Let $\alpha$ be a generator of $\mathbb{Z}_6$; we find $\alpha : y \to y^3$ works; $y \to y^3 \to y^2 \to y^6 \to y^4 \to y^5 \to y$.
And $z \to z^2 \to z^4 \to z^8 \to z^3 \to z^6 \to z^{12} \to \cdots$ implies

$\beta : z \to z^2$ is a generator of $\mathbb{Z}_{12}$.

A group hom $\mathbb{Z}_3 \xrightarrow{\varphi} \mathbb{Z}_6 \times \mathbb{Z}_{12}$ is determined by the image of $x$. Since $|\varphi(x)| \mid |x|$, $x$ is either sent to an elt of order 1 or 3. Conversely, sending $x$ to any such elt determines a well-defined group hom.

There are thus eight possibilities:

$x \mapsto (1,1), (\alpha^2, 1), (\alpha^4, 1),$
$(1, \beta^4), (1, \beta^8), (\alpha^2, \beta^4), (\alpha^2, \beta^8),$
$(\alpha^4, \beta^4), (\alpha^4, \beta^8).$

Each choice yields a presentation for $G$. e.g. $(\alpha^2, \beta^4)$

$$\rightsquigarrow \; G_{(\alpha^2,\beta^4)} \cong \langle x, y, z : x^3 = y^7 = z^{13} = 1, \; xyx^{-1} = y^2, \; xzx^{-1} = z^3, \; yz = zy \rangle$$

All such groups exist by the abstract construction of the semidirect product. See attached at end.

There may be duplicates. For instance, $G(\alpha^2, 1) \underset{\text{not obvious}}{\cong} G(\alpha^4, 1)$ by the isomorphism $(x,y,z) \in G_{(\alpha^2,1)} \mapsto$
$\mapsto (x^2, y, z) \in G_{(\alpha^4,1)}$.

It is not clear to me whether there is an algorithm to check duplicates. $\square$

---

(3) $R$ comm Nöth. $I, J, K$ ideals.

$I$ is called <u>irreducible</u> if $I = J \cap K$ implies $I = J$ or $I = K$.

(a) Show every ideal $I$ is a finite intersection of irreducible ideals.

(b) Show every irreducible ideal $I \neq R$ is primary, i.e. $I \neq R$ and every zero divisor in $R/I$ is nilpotent.

---

<u>*solution to (a)*</u>

Let $\mathcal{A}$ be the set of ideals which are <u>not</u> a finite intersection of irreducible ideals.

Suppose $\mathcal{A} \neq \emptyset$. Since $R$ is Nöth, let $I$ be maximal in $\mathcal{A}$. we show $I \notin \mathcal{A}$. $\Rightarrow\Leftarrow$.

[illegible]

Since $I \in \mathcal{A}$, $I$ is <u>not</u> irreducible, so we may choose $J$ and $K$ s.t. $I = J \cap K$ and $I \subsetneq J$, $I \subsetneq K$.
Since $I$ is maximal, $J = J_1 \cap \cdots \cap J_n$ and $K = K_1 \cap \cdots \cap K_m$ are intersections of finitely many irreducible ideals. But then $I = J \cap K = J_1 \cap \cdots \cap J_n \cap K_1 \cap \cdots \cap K_m$. So $\mathcal{A} \not\ni I$. $\Rightarrow\Leftarrow$ so $\mathcal{A} = \emptyset$. $\square$

solution to (b)

Let $I \neq R$. Let $x \notin I$, $y \notin I$, $xy \in I$.

We want to show there is $n$ s.t. $x^n \in I$.

For each $n$ let $\mathrm{Ann}(x^n)$ be the ideal consisting of those $r \in R$ s.t. $rx^n \in I$.

Then $\mathrm{Ann}(x) \subset \mathrm{Ann}(x^2) \subset \cdots$

Since $R$ is Nöth, $\mathrm{Ann}(x^n) = \mathrm{Ann}(x^{n+1})$ for some $n$. We show $I = (I, y) \cap (I, x^n)$ from which it follows $I = (I, x^n)$, i.e. $x^n \in I$.

Let $a + ry = b + sx^n$.

Then $sx^{n+1} = ax + rxy - bx \in I$, i.e. $s \in \mathrm{Ann}(x^{n+1})$.

Since $\mathrm{Ann}(x^{n+1}) = \mathrm{Ann}(x^n)$, we conclude

$sx^n \in I$, hence $b + sx^n \in I$. $\square$

(4) A f.d. alg / field K.

Assume $a^7 = a$ for all $a \in A$.

Show A is a direct product of fields.

Which fields can arise?

---

Solution Assume $A \neq 0$.

Since A is f.d. alg / K

A is right (or left) Artinian.

So the Jacobson radical J consists of nilpotents.

Clearly for any $n$, $a^n = a^d$ for $1 \le d < 7$.

( if $n \geq 7$, then $a^n = a^{n-6}$ )

So the only nilpotent is $0$ : $0 = a^n = a^d \Rightarrow a = a^d a^{7-d} = 0$.

So $J = 0$. Together w/ right (or left) Artinian

this gives A is semisimple.

So $A \cong M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_k)$, $D_i$ division rings.

$n_i = 1$ for all $i$ since A has no nilpotents.

Every elt of $D_i$ is a root of $X^7 - X \in D_i[X]$ which has at most 7 roots. So $D_i$ is finite. So $D_i$ is a finite field, each of whose elts is a root of $X^7 - X$. So $D_i \cong F_7$. Since $D_i$ is an extension of K, K must also be $F_7$. □

(5) $G$ and $H$ f.g. abelian groups.

Assume $G \otimes_{\mathbb{Z}} H = 0$.

Show $G$ and $H$ are finite of relatively prime order.

---

<u>solution</u>

$$G = \mathbb{Z}^n \oplus \bigoplus_{i,j} \mathbb{Z}_{p_i^{n_{ij}}}$$

$$H = \mathbb{Z}^m \oplus \bigoplus_{k,l} \mathbb{Z}_{q_k^{m_{kl}}}$$

From $\frac{R}{I} \otimes_R M \cong \frac{M}{IM}$ for any $R$-module $M$ over a commutative ring $R$, it follows that $R/I \otimes_R R/J \cong R/I+J$. As a consequence, $\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/\gcd(n,m)\mathbb{Z}$.

And $\oplus$, $\otimes$ commute. And $R \otimes_R M \cong M$.

so $G \otimes H \cong \mathbb{Z}^{nm} \oplus \bigoplus_{kl}^{n} \mathbb{Z}_{q_k^{m_{kl}}} \oplus \bigoplus_{ij}^{m} \mathbb{Z}_{p_i^{n_{ij}}}$

$\oplus \bigoplus_{ijkl} \mathbb{Z}_{\gcd(p_i^{n_{ij}}, q_k^{m_{kl}})}$.

First, if $G \otimes H = 0$, then $n = m = 0$.

Hence for all $ijkl$, $\mathbb{Z}_{\gcd(p_i^{n_{ij}}, q_k^{m_{kl}})}$

$= 0$ which only occurs when $\gcd(p_i^{n_{ij}}, q_k^{m_{kl}}) = 1$.

Since $|G| = \prod_{ij} p_i^{n_{ij}}$ and $|H| = \prod_{kl} q_k^{kl}$,

these groups have relatively prime orders.

□

(6) $S$ and $T \in \mathrm{End}(V)$ diagonalizable where $V$ is a f.d. v.s. / $\mathbb{C}$.

If $ST = TS$, show there is $f_T, f_S \in \mathbb{C}[X]$ s.t. $T = f_T(S)$ and $S = f_S(T)$.

---

solution

We must assume in addition that the algebraic multiplicities of all eigenvalues are all 1. Indeed, $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ commutes w/ $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ and since for all $f \in \mathbb{C}[X]$,

$$f\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} f(1) & 0 \\ 0 & f(1) \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}.$$

So we assume $\lambda_1, \dots, \lambda_n$ are distinct eigenvalues of $S$ and $\eta_1, \dots, \eta_n$ are distinct eigenvalues of $T$.

Since $S$ and $T$ commute they are simultaneously diagonalizable. That is, there is an invertible matrix $A$ s.t.

$$ASA^{-1} = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} \ \& \ ATA^{-1} = \begin{pmatrix} \eta_1 & & \\ & \ddots & \\ & & \eta_n \end{pmatrix}.$$

Since the $\lambda_i$ are distinct we may use the Chinese Remainder Theorem on the ring $\mathbb{C}[X]$ to find a polynomial $f_T$ s.t. for all $i$, $f_T(X) \equiv \eta_i \pmod{(X-\lambda_i)}$.

So $f_T(\lambda_i) = \eta_i$ for all $i$. So

$$f_T\begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix} = \begin{pmatrix} f_T(\lambda_1) & & \\ & \ddots & \\ & & f_T(\lambda_n) \end{pmatrix} = \begin{pmatrix} \eta_1 & & \\ & \ddots & \\ & & \eta_n \end{pmatrix}$$

$$\Vert \qquad\qquad\qquad\qquad\qquad\qquad \Vert$$

$$f_T(ASA^{-1}) = Af_T(S)A^{-1}. \qquad\qquad ATA^{-1}$$

And conversely. $\square$.

The harder part is showing these are the *only* primes.

Let $\mathfrak{p} \neq 0 \subset \mathbb{Z}[X]$ be prime. Then $\mathbb{Z} \cap \mathfrak{p}$ is prime, for $ab \in \mathbb{Z} \cap \mathfrak{p}$ implies $a$ and $b$ are in $\mathbb{Z}$, and one of $a$ or $b$ is in $\mathfrak{p}$; so $a$ or $b$ is in $\mathbb{Z} \cap \mathfrak{p}$.

Assume $\mathbb{Z} \cap \mathfrak{p} = \{0\}$.

Consider the extension $\mathbb{Q}[X]\mathfrak{p} \subset \mathbb{Q}[X]$. Since $\mathbb{Z} \cap \mathfrak{p} = \{0\}$ this extended ideal is proper and thus is prime and generated over $\mathbb{Q}[X]$ by a monic irreducible polynomial $\tilde{f}(X) \in \mathbb{Q}[X]$ (here we are using that $\mathbb{Q}[X]$ is a PID).

We may take $\tilde{f}(X) \equiv f(X) \in \mathbb{Z}[X]$ (at the cost of being monic, but we may assume primitive) by multiplying through w/ a common denominator.

Since $f(X) \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$ is primitive and irreducible over $\mathbb{Q}[X]$ it is irreducible over $\mathbb{Z}[X]$ (this is the "trivial" direction of Gauss' lemma).

(7) Characterize the prime and maximal ideals in $\mathbb{Z}[x]$.

---

solution

The answer is all primes are of the form $\{0\}$, $(f(X))$ where $f(X) \in \mathbb{Z}[X]$ is irreducible, $(p)$ where $p \in \mathbb{Z}$ is prime, or $(p, f(X))$ where $f(X) \in \mathbb{Z}_p[X]$ is irreducible (i.e. $f(X)$ is irreducible modulo $p$).

Recall $\mathbb{Z}[x]$ is a U.F.D., hence $f(X)$ irreducible implies $(f(X))$ is prime; and if $f(X)$ is irreducible modulo $p$, then $\mathbb{Z}[X]/(p, f(X)) \cong \mathbb{Z}_p[X]/(\overline{f(X)})$ is an I.D. hence $(p, f(X))$ is prime.

So all of the above are primes.

we claim $\mathfrak{p} = \mathbb{Z}[x]f(x)$. First, $f(x) \in \mathfrak{p}$ by degree considerations; indeed, $f(x) \in \mathbb{Q}[x]\mathfrak{p}$ means there is $g(x) \in \mathfrak{p}$ and $\tilde{h}(x) \in \mathbb{Q}[x]$ s.t. $f(x) = \tilde{h}(x)g(x)$, or $N f(x) = \overbrace{h(x)}^{\in \mathbb{Z}[x]} g(x) \in \mathfrak{p}$ for some $N \geq 1$, hence $f(x) \in \mathfrak{p}$ since $\mathfrak{p}$ is prime and $\mathbb{Z} \cap \mathfrak{p} = \{0\}$.

It remains, in this case, to show $\mathfrak{p} \subset \mathbb{Z}[x]f(x)$. If $g(x) \in \mathfrak{p}$, then since $\mathfrak{p} \subset \mathbb{Q}[x]f(x)$ there is $\tilde{h}(x) \in \mathbb{Q}[x]$ s.t. $g(x) = \tilde{h}(x)f(x)$, or $N g(x) = h(x)f(x) \in \overbrace{\mathbb{Z}[x]f(x)}^{\text{prime} \subset \mathbb{Z}[x] \text{ since } f(x) \text{ is irreducible}} \subset \mathfrak{p}$ hence $g(x) \in \mathbb{Z}[x]f(x)$ since $\mathbb{Z} \cap \mathbb{Z}[x]f(x) \subset \mathbb{Z} \cap \mathfrak{p} = \{0\}$.

This establishes $\mathfrak{p} = (f(x))$.

The previous argument is useless when $\mathbb{Z} \cap \mathfrak{p} \neq \{0\}$ since the extension $\mathbb{Q}[x]\mathfrak{p}$ equals the whole ring $\mathbb{Q}[x]$.

So we go in the other direction.

If $\mathbb{Z} \cap \mathfrak{p} \neq \{0\}$, then $\mathbb{Z} \cap \mathfrak{p} = (p)$ where $p \in \mathbb{Z}$ is prime. Let $\pi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]/(p) \cong \mathbb{Z}_p[x]$ be the natural projection. Then $\pi(\mathfrak{p}) \subset \mathbb{Z}_p[x]$ is prime.

Since $\mathbb{Z}_p[x]$ is a PID, the only primes are $\{0\} \in \mathbb{Z}_p[x]$ and $\mathbb{Z}_p[x]\,\tilde{f}(x)$ where $\tilde{f}(x)$ is monic & irreducible over $\mathbb{Z}_p[x]$. If $\pi(\mathfrak{p}) = \{0\}$, then $\mathfrak{p} = \pi^{-1}(\pi(p)) = (p)$. ✓.

Otherwise, $\pi(\mathfrak{p}) = (\tilde{f}(x))$.

If $f(x) \in \mathbb{Z}[x]$ s.t. $\pi(f(x)) = \tilde{f}(x)$, then $f(x) \in \mathfrak{p}$; pick such an $f(x)$. Then $f(x)$ is irreducible over $\mathbb{Z}[x]$, since we may choose $f(x)$ to be monic and so a nontrivial decomposition of $f(x)$ descends to a nontrivial decomposition of $\tilde{f}(x)$.

We claim $\mathfrak{p} = (p, f(x))$. We need to show the inclusion $\subseteq$. Let $g(x) \in \mathfrak{p}$.

Since $\pi(\mathfrak{p}) = \mathbb{Z}_p[X]\tilde{f}(X)$ we may choose $\tilde{h}(X) \in \mathbb{Z}_p[X]$ s.t. $\tilde{g}(X) = \tilde{h}(X)\tilde{f}(X)$.

Hence, $g(X) - h(X)f(X) \in (p)$ where $h(X)$ is any representative of $\tilde{h}(X)$.

So $g(X) \in (p, f(X))$ as desired.

This completes the proof of the classification. Note that the only fact about $\mathbb{Z}$ that was used is its prime ideals are principal and maximal (so that $\mathbb{Z}_p[X]$ is a PID). Hence the classification holds if we replace $\mathbb{Z}$ by any PID $R$. $\square$

## Problem (2) continued

There is a spectacular result in Dummit and Foote, chapter 5, p. 184 which says if $K$ is a cyclic group and $H$ is any group, and if $\rho_1, \rho_2 : K \to Aut(H)$ are two group homomorphisms (where we assume if $K$ is infinite that $\rho_1$ and $\rho_2$ are injective), satisfying $\rho_1(K)$ and $\rho_2(K)$ are conjugate subroups (e.g. if $\rho_1(K) = \rho_2(K)$), then the semidirect products $H \rtimes_{\rho_1} K$ and $H \rtimes_{\rho_2} K$ are <u>isomorphic</u>.

(In the proof one needs to use a lemma that if $a, m, n \in \mathbb{Z}$ s.t. $\gcd(a, m) = 1$ and $m | n$, then there is $a' \in \mathbb{Z}$ s.t. $a \equiv a' \pmod{m}$ and $\gcd(a, n) = 1$, hence there is $b \in \mathbb{Z}$ s.t. $ab \equiv 1 \pmod{n}$.)

Returning to the problem at hand, a consequence if this is that, if we let $G_{mn}$ be the semi direct product associated w/ the group hom $X \mapsto (\alpha^m, \beta^n)$

for the permissible values $m = 0, 2, 4$ & $n = 0, 4, 8$, then

$$G_{20} \cong G_{40}, \quad G_{04} \cong G_{08},$$
$$G_{24} \cong G_{48}, \quad G_{28} \cong G_{44}.$$

! (keep reading!)

Conclusion: $G_{00}, G_{20}, G_{04}, G_{24} \widehat{\cong} G_{28}$

are representatives of the ~~five~~ four! isomorphism classes of groups of order $3 \cdot 7 \cdot 13$.

The claim that these are mutually non-isomorphic is clear, except for possibly $G_{24} \not\cong G_{28}$.

We choose to show instead that $G_{24} \not\cong G_{44}$. Wrong! Suppose there exists an isomorphism $\varphi : G_{24} \longrightarrow G_{44}$. Using that $\alpha : y \mapsto y^3$ and $\beta : z \to z^2$ we realize

$$G_{24} = \langle x, y, z : x^3 = y^7 = z^{13} = 1, \; xy = y^2 x, \; xz = z^3 x, \; yz = zy \rangle,$$

$$G_{44} = \langle x, y, z : x^3 = y^7 = z^{13} = 1, \; xy = y^4 x, \; xz = z^3 x, \; yz = zy \rangle.$$

Let $\tilde{x} = \varphi(x)$, $\tilde{y} = \varphi(y)$, $\tilde{z} = \varphi(z)$.

Then $|\tilde{x}| = 3$, $|\tilde{y}| = 7$, $|\tilde{z}| = 13$, and $\tilde{x}\tilde{y} = \tilde{y}^2\tilde{x} \in G_{44}$, $\tilde{x}\tilde{z} = \tilde{z}^3\tilde{x} \in G_{44}$, and $\tilde{y}\tilde{z} = \tilde{z}\tilde{y} \in G_{44}$. We show that no such triple $(\tilde{x}, \tilde{y}, \tilde{z})$ exists. together w/ the fact the generic elt is naturally written $z^\alpha y^\beta x^\gamma$ ✓

It follows from $zy = yz \in G_{44}$ (these are the $x, y, z$ generating $G_{44}$) that both the 7-Sylow and the 13-Sylow subgroups (in $G_{44}$) are normal (a fact true for all the $G_{mn}$ for the same reason). The 7-Sylow s.g. is $\{y^\beta : \beta = 0, 1, \ldots, 6\}$ and the 13-Sylow s.g. is $\{z^\alpha : \alpha = 0, 1, \ldots, 12\}$.

We claim if we can show no choice $(\tilde{x}, \tilde{y}, \tilde{z}) = (x^\gamma, y^\beta, z^\alpha)$ works, then we are done. Indeed, note if the relation

$\tilde{x}\tilde{y} = \tilde{y}^2\tilde{x}$ holds in $G_{44}$, then

$(g\tilde{x}g^{-1})(g\tilde{y}g^{-1}) = (g\tilde{y}g^{-1})^2(g\tilde{x}g^{-1})$ $\forall g \in G_{44}$,

and similarly for $\tilde{x}\tilde{z} = \tilde{z}^3\tilde{x}$. Every elt of order 3 is of the form $g^{-1}x^{\gamma}g$.

If $(\tilde{x}, \tilde{y}, \tilde{z}) = (g^{-1}x^{\gamma}g, y^{\beta}, z^{\alpha})$ satisfied the required relations, then by above $(x^{\gamma}, gy^{\beta}g^{-1}, gz^{\alpha}g^{-1}) =$

$= (x^{\gamma}, y^{\beta'}, z^{\alpha'})$ (by normality) would satisfy the relations, which we assumed is false, thus proving the claim.

Hence we have reduced to showing no triple of the form $(\tilde{x}, \tilde{y}, \tilde{z}) = (x^{\gamma}, y^{\beta}, z^{\alpha})$ satisfies the relations, and for this we must calculate. First we find the pairs $(\tilde{x}, \tilde{y}) = (x^{\gamma}, y^{\beta})$ satisfying $\tilde{x}\tilde{y} = \tilde{y}^2\tilde{x}$ using $x^3 = 1$, $y^7 = 1$, and $xy = y^4x$. $(\gamma, \beta) =$ :

$(1,2)$ / $xy^2 \stackrel{?}{=} y^4x$ ✗
$\quad \| $
$y^8x = yx$

$(1,3)$ / $xy^3 \stackrel{?}{=} y^6x$ ✗
$\quad \| $
$y^{12}x = y^5x$

$(1,4)$ / $xy^4 \stackrel{?}{=} y^8x = yx$ ✗
$\quad \| $
$y^{16}x = y^2x$

$(1,5)$ / $xy^5 \stackrel{?}{=} y^{10}x = y^3x$ ✗
$\quad \| $
$y^{20}x = y^6x$

$(1,6)$ / $xy^6 \stackrel{?}{=} y^{12}x = y^5x$ ✗
$\quad \| $
$y^{24}x = y^3x$

$(2,1)$ / $x^2y \stackrel{?}{=} y^2x^2$ ✓
$\quad \| $
$y^{16}x^2 = y^2x^2$

$(2,2)$ / $x^2y^2 \stackrel{?}{=} y^4x^2$ ✓ etc. true for $(2,\beta)$. $\Downarrow$
$\quad \| $
$y^{32}x^2 = (y^2)^2x^2 = y^4x^2$

So we fix $\tilde{x} = x^2$ and we check if any $(z, \alpha)$ satisfies the relation.

And it does! Trivially! The relation $xz = z^3x$ is assumed in both $G_{24}$ & $G_{44}$.

Therefore we have the <u>surprise</u> that, in fact, $G_{24} \cong G_{44}$!! An isomorphism is given by $(x, y, z) \longmapsto (x^2, y, z)$.

$\square$