22.1

$(\mathbb{Z}/11)^\times$:

$\langle 2\rangle = \{2,4,8,5,10,9,7,3,6,1\}$ ✓
$\langle 3\rangle = \{3,9,5,4,1\}$ ×
$\langle 4\rangle = \{4,5,9,3,1\}$ ×
$\langle 5\rangle = \{5,3,4,9,1\}$ ×
$\langle 6\rangle = \{6,3,7,9,10,5,8,4,2,1\}$ ✓
$\langle 7\rangle = \{7,5,2,3,10,4,6,9,8,1\}$ ✓
$\langle 8\rangle = \{8,9,6,4,10,3,2,5,7,1\}$ ✓
$\langle 9\rangle = \{9,4,3,5,1\}$ ×
$\langle 10\rangle = \{10,1\}$ ×

Generators : 2, 6, 7, 8

$(\mathbb{Z}/13)^\times$:

$\langle 2\rangle = \{2,4,8,3,6,12,11,9,5,10,7,1\}$ ✓
$\langle 3\rangle = \{3,9,1\}$
$\langle 4\rangle = \{4,3,12,9,10,1\}$
$\langle 5\rangle = \{5,12,8,1\}$
$\langle 6\rangle = \{6,10,8,9,2,12,7,3,5,4,11,1\}$ ✓
$\langle 7\rangle = \{7,10,5,9,11,12,6,3,8,4,2,1\}$ ✓
$\langle 8\rangle = \{8,12,5,1\}$
$\langle 9\rangle = \{9,3,1\}$
$\langle 10\rangle = \{10,9,12,7,4,1\}$
$\langle 11\rangle = \{11,4,5,3,7,12,2,9,8,10,6,1\}$
$\langle 12\rangle = \{12,1\}$.

Generators : 2, 6, 7, 11

22.2

Let p be prime. Note $|(\mathbb{Z}/p^2)^\times| = \phi(p^2) = p\phi(p) = p(p-1)$.

Since $(\mathbb{Z}/p)^\times$ cyclic, we can choose some $g \in (\mathbb{Z}/p)^\times$ such that $|g| = p-1$. Now, set $a := |g|$ in $(\mathbb{Z}/p^2)^\times$. Note that

$$g^a \equiv 1 \bmod p \quad \text{and} \quad g^{p-1} \equiv 1 \bmod p.$$

Thus $a \in \{p-1, p(p-1)\}$. If $a = p(p-1)$, then $\langle g\rangle = (\mathbb{Z}/p^2)^\times$ and we're done.

Suppose otherwise that $a = p-1$. Then

$$(g+p)^{|g+p|} \equiv 1 \bmod p \equiv (g+p)^{p-1} \bmod p.$$

So $|g+p| \in \{p-1, p(p-1)\}$. Similarly, suppose $|g+p| = p-1$. Then

$$(*)\quad (g+p)^{p-1} = g^{p-1} + \binom{p-1}{1} p g^{p-2} + \cdots + \binom{p-1}{p-2} p^{p-2} g + p^{p-1} \equiv g^{p-1} + (p-1) p g^{p-2} \bmod p^2.$$

But $(p-1)pg^{p-2} \not\equiv p-1 \bmod p^2$ so $(*) \not\equiv 1 \bmod p^2 \Rightarrow |g+p| = p(p-1)$. ∎

22.3

Take $(\mathbb{Z}/8)^\times = \{1,3,5,7\}$. Since $\langle 1\rangle = \{1\}$, $\langle 3\rangle = \{3,1\}$, $\langle 5\rangle = \{5,1\}$, $\langle 7\rangle = \{7,1\}$, $\nexists g \in (\mathbb{Z}/8)^\times$ where $\langle g\rangle = (\mathbb{Z}/8)^\times$.

22.4

Primes : 2, 3, 5, 7, 11, 13, 17, 19, 23, 29

Recall from 22.5 that $|G| = pq$ is non-abelian $\iff p \mid q-1$ $(p<q)$.

```
primes = [2, 3, 5, 7, 11, 13, 17, 19, 23, 29]
for i, p in enumerate(primes):
    for j in range(i+1, len(primes)):
        q = primes[j]
        # |G|=pq non-abelian iff p | q-1
        if (q-1)%p != 0:
            print(f"{p}x{q} = {p*q}")
```

Abelian groups are of order :

```
3x5 = 15
3x11 = 33
3x17 = 51
3x23 = 69
3x29 = 87
5x7 = 35
5x13 = 65
5x17 = 85
5x19 = 95
5x23 = 115
5x29 = 145
7x11 = 77
7x13 = 91
7x17 = 119
7x19 = 133
7x23 = 161
11x13 = 143
11x17 = 187
11x19 = 209
11x29 = 319
13x17 = 221
13x19 = 247
13x23 = 299
13x29 = 377
17x19 = 323
17x23 = 391
17x29 = 493
19x23 = 437
19x29 = 551
23x29 = 667
```

23.1

Suppose $p < q$ are primes and $p \mid q-1$. (Note that $|GL_2(\mathbb{F}_q)| = q(q-1)^2(q+1)$.)

Define $Q \leq GL_2(\mathbb{F}_q)$ as $Q = \{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{Z}/q \}$, which has order q. Since $p \mid q-1 = |(\mathbb{Z}/q)^\times|$, we have from Cauchy that $\exists b \in (\mathbb{Z}/q)^\times$ with $|b| = p$. Thus we can define $P \leq GL_2(\mathbb{F}_q)$ as $P = \{ \begin{bmatrix} b^n & 0 \\ 0 & 1 \end{bmatrix} : n \in \mathbb{Z}/p \}$, which has order p.

Now, define $\varphi : \mathbb{Z}/p \to \mathbb{Z}/q-1 \cong Aut(\mathbb{Z}/q)$ by $1 \mapsto b \mapsto (x \mapsto bx)$

$$g \mapsto b^g \mapsto (x \mapsto b^g x)$$

and also define $f : \mathbb{Z}/q \times_\varphi \mathbb{Z}/p \to QP$ by $(x,y) \mapsto \begin{bmatrix} b^y & x \\ 0 & 1 \end{bmatrix}$.

Since

$$f(x,y) \cdot f(u,v) = \begin{pmatrix} b^y & x \\ 0 & 1 \end{pmatrix} \begin{pmatrix} b^u & v \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} b^{y+u} & vb^y + x \\ 0 & 1 \end{pmatrix} = f(x + ub^y, y+v) = f((x,y)\cdot(u,v))$$

f is a group homomorphism. Furthermore, $f(x,y) = I_2 \iff x = y = 0$ so f injective.

Finally, $M : \begin{pmatrix} b^y & x \\ 0 & 1 \end{pmatrix} \in Q \times P \to (x,y) \in f^{-1}(M)$ so f surjective. Thus $QP \cong \mathbb{Z}/p \times_\varphi \mathbb{Z}/q$, and since $|\mathbb{Z}/p \times_\varphi \mathbb{Z}/q| = pq$, we're done. ∎

23.2

Note that if $p < q < r$ are prime with G abelian $\forall |G| = pqr$,

① $pq \not\equiv 1 \bmod r$, ② $q \not\equiv 1 \bmod r$, ③ $r \not\equiv 1 \bmod p$, ④ $qr \not\equiv 1 \bmod p$, ⑤ $r \not\equiv 1 \bmod q$, ⑥ $pr \not\equiv 1 \bmod q$.

```python
primes = [3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73]
counter = 0
for i, p in enumerate(primes):
    for j in range(i+1, len(primes)):
        for k in range(j+1, len(primes)):
            q, r = primes[j], primes[k]

            if ((p*q) % r != 1 and
                q % r != 1 and
                r % p != 1 and
                (q*r) % p != 1 and
                r % q != 1 and
                (p*r) % q != 1
                ):
                print(f"{p}, {q}, {r}: {p*q*r}")
                counter += 1

            if counter >= 10: break
        if counter >= 10: break
    if counter >= 10: break
```

```
3, 7, 11: 231
3, 7, 17: 357
3, 7, 23: 483
3, 7, 41: 861
3, 7, 53: 1113
3, 7, 59: 1239
3, 13, 17: 663
3, 13, 23: 897
3, 13, 29: 1131
3, 13, 41: 1599
```

24.1

Let G be a group, $x, y \in G$ elements both commuting with $[x,y] := xyx^{-1}y^{-1}$. To show $(xy)^n = x^n y^n [y,x]^{\frac{n(n-1)}{2}}$ (*) $\forall n \in \mathbb{N}$, we'll proceed by induction on n.

- Notice $xy = xy$ ✓
- Suppose (*) holds for $n = k \in \mathbb{N}$. Then notice

$$(xy)^{k+1} = (xy)^k (xy) = x^k y^k [y,x]^{\frac{k(k-1)}{2}} xy \qquad \text{(Induction Hypothesis)}$$

$$= x^k y^k xy [y,x]^{\frac{k(k-1)}{2}}$$

Since $yx = yxy^{-1}x^{-1}xy = [y,x]xy = xy[y,x]$, we have that

$$y^k x = xy^k [y,x]^k.$$

Thus

$$\begin{aligned}(xy)^{k+1} &= x^k (y^k x) y [y,x]^{\frac{k(k-1)}{2}} \\ &= x^k x y^k [y,x]^k y [y,x]^{\frac{k(k-1)}{2}} \\ &= x^{k-1} y^{k+1} [y,x]^k [y,x]^{\frac{k(k-1)}{2}} \\ &= x^{k+1} y^{k+1} [y,x]^{\frac{k(k+1)}{2}}.\end{aligned}$$

By the Principle of Mathematical Induction, the proof is complete. ☒

24.2

Note that from Prop 21.12, $G \cong N \rtimes_\varphi H \iff N \trianglelefteq G$, $H \leq G$, $NH = G$, and $N \cap H = \{e\}$.
However, every nontrivial subgroup $S \leq Q_8$ contains -1 since $g^2 = -1 \ \forall g \in Q_8$, $g \neq \pm 1$.
Thus $\nexists N, H \leq Q_8$ with $NH = Q_8$ and $N \cap H = \{e\}$ since $-1 \in N \cap H \ \forall N, H \leq Q_8$ nontrivial. ☒

24.3

Suppose $|G| = 8$ non-abelian. Then $\exists x \in G$ with $|x| = 8$. Then $|x| \in \{2, 4\} \ \forall x \in G$ nontrivial.
However, if $|x| = 2 \ \forall x \in G$ nontrivial, G abelian, so $\exists x \in G$ with $|x| = 4$. ($xy = (xy)^{-1} = y^{-1}x^{-1}$ $\Rightarrow xy(y^{-1}x^{-1}) = e \Rightarrow xy = yx$)
Choose $x \in G$ with $|x| = 4$. Then $\langle x \rangle \trianglelefteq G$.

- Suppose $\exists y \in \frac{G}{\langle x \rangle}$ with $|y| = 4$. Then $|y_i| = 2 \ \forall y_i \in \frac{G}{\langle x \rangle}$. Since $y_i \in G/\langle x \rangle$, $xy_i \notin \langle x \rangle$, so $|xy_i| = 2$ and thus $(xy_i)^2 = 1 \ \forall i$. Thus $G \cong D_8$.
- Suppose $\forall y \in \frac{G}{\langle x \rangle}$ with $|y| = 4$. Then $1 < |\langle x \rangle \cap \langle y \rangle| < 4$ so $x^2 = y^2$ and $|\langle x \rangle \cap \langle y \rangle| = 2$.
  So $xy, yx, x^{-1}y \notin \langle x \rangle \cup \langle y \rangle$ but $|G \setminus (\langle x \rangle \cup \langle y \rangle)| = 2$.
  Also, $xy \neq yx$ so $yx = x^{-1}y$. Then $\varphi : G \cong Q_8$ is defined by $\varphi: \begin{matrix} 1 \mapsto 1 \\ x \mapsto i \end{matrix}$ $\begin{matrix} x^2 \mapsto -1 \\ x^3 \mapsto -1 \end{matrix}$ ...

25.1 WTF $S \leq GL_2(\mathbb{Z}/p^2)$, $S \cong \mathbb{Z}/p^2 \rtimes_\varphi \mathbb{Z}/p$, $\varphi : \mathbb{Z}/p \to \mathrm{Aut}(\mathbb{Z}/p^2) \cong \mathbb{Z}/p(p-1)$ non-abelian group of order p^3 w/ no elements of order p

Let $G = \left\{ \begin{bmatrix} n & a \\ 0 & 1 \end{bmatrix} : a \in \mathbb{Z}/p^2, \ n \equiv 1 \bmod p \right\}$.
Notice if $\begin{bmatrix} n & a \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} \in G$, $\begin{bmatrix} n & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} m & b \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} \underbrace{nm}_{\equiv 1 \bmod p^2} & \underbrace{nb+a}_{\equiv a \bmod p^2} \\ 0 & 1 \end{bmatrix}$.

- If $n \equiv m \equiv 1 \bmod p$, $nm \equiv 1 \bmod p$, so G is closed under multiplication.
- Furthermore, $\begin{bmatrix} n & a \\ 0 & 1 \end{bmatrix}\begin{bmatrix} n^{-1} & -n^{-1}a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} nn^{-1} & n(-n^{-1}a)+a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ so G is closed under inverses

Thus G is a subgroup; since $\{n \equiv 1 \bmod p\} \leq (\mathbb{Z}/p^2)^\times$ has p elements, $|G| = p^2 \cdot p = p^3$. Finally, $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ has order p^2. ☒

25.2

Let p be prime, $\varphi_i : \mathbb{Z}/p \to GL_2(F_p)$ be non-trivial homomorphisms for $i = 1, 2$.

Note that φ_i will map $1 \mapsto g$, $|g| = p \Rightarrow g \in P_p$.

Let A represent the matrix $\varphi_1(1)$ and define B similarly with $\varphi_2(1)$. Then either A, B are in the same p-Sylow subgroup or conjugate p-Sylow subgroups. $|P_p| = p$, so

$$B^n = MAM^{-1}$$

for some $n \in (\mathbb{Z}/p)^\times$, $M \in GL_2(F_p)$. Now, define $f : (\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_{\varphi_1} \mathbb{Z}/p \to (\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_{\varphi_2} \mathbb{Z}/p$ by

$$f : (\vec{a}, x) \mapsto (M\vec{a}, nx)$$

for all $\vec{a} \in (\mathbb{Z}/p \times \mathbb{Z}/p)$, $x \in \mathbb{Z}/p$. Thus

$$\begin{aligned} f((\vec{a},x)(\vec{b},y)) &= f((\vec{a} + A^x\vec{b},\ x+y)) \\ &= (M\vec{a} + MA^x\vec{b},\ n(x+y)) \\ &= (M\vec{a} + MA^xM^{-1}M\vec{b},\ n(x+y)) \\ &= (M\vec{a} + B^{nx}M\vec{b},\ n(x+y)) \qquad (B^{nx} = MA^xM^{-1}) \\ &= (M\vec{a}, nx)(M\vec{b}, ny) \\ &= f((\vec{a},x))f((\vec{b},y)) \end{aligned}$$

so f is a homomorphism.

Since M invertible, $\exists n^{-1} \in (\mathbb{Z}/p)^\times$, $g : (\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_{\varphi_2} \mathbb{Z}/p \to (\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_{\varphi_1} \mathbb{Z}/p$ defined by

$$g : (\vec{a}, x) \mapsto (M^{-1}\vec{a}, xn^{-1})$$

is the inverse of f. Thus f bijective, so $(\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_{\varphi_1} \mathbb{Z}/p \cong (\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_{\varphi_2} \mathbb{Z}/p$. ☒

25.3

Let $U_3(F_p)$ be the non-abelian group of order p^3. Consider $N = \left\{ \begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix} : a, b \in \mathbb{Z}/p \right\}$.

Clearly, $I_3 \in N$ and $\begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & c & d \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & a+c & ac+b+d \\ 0 & 1 & a+c \\ 0 & 0 & 1 \end{bmatrix} \in N$ is closed under multiplications.

Furthermore, taking $c = -a$, $d = a^2 - b$ gives inverses. Finally,

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & a & * \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix} \in N$$

so $N \leq U_3(F_p)$. Further, $\begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix}^m = \begin{bmatrix} 1 & ma & ma^2+mb \\ 0 & 1 & ma \\ 0 & 0 & 1 \end{bmatrix}$ $\forall m \in \mathbb{N}$

Since $(a, p) = 1$ $\forall a \in (\mathbb{Z}/p) \setminus \{\bar{0}\}$, $ma \equiv 0 \bmod p \Rightarrow m = p \Rightarrow ma^2 + mb = p(a^2+b) \equiv 0 \bmod p$.

Thus $|g| \leq p$ $\forall g \in N$. Since $|N| = p^2$, $N \cong S \in \{\mathbb{Z}/p^2, \mathbb{Z}/p \times \mathbb{Z}/p\}$.

But this holds so $N \cong \mathbb{Z}/p \times \mathbb{Z}/p$.

Now, define

$$H = \left\{ \begin{bmatrix} 1 & c & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} : c \in \mathbb{Z}/p \right\}$$

to be a subgroup of $U_3(F_p)$ of order p. (Thus $H \cong \mathbb{Z}/p$).

Obviously, $H \cap N = \{ I_3 \}$, and

$$\underbrace{\begin{bmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix}}_{\in N} \underbrace{\begin{bmatrix} 1 & c & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}}_{\in H} = \begin{bmatrix} 1 & a+c & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{bmatrix}$$

so $NH = G$. Then Prop 21.12 gives $U_3(F_p) \cong (\mathbb{Z}/p \times \mathbb{Z}/p) \rtimes_\varphi \mathbb{Z}/p$ for some φ. ($\varphi : \mathbb{Z}/p \to \mathrm{Aut}(\mathbb{Z}/p \times \mathbb{Z}/p)$)

If p odd, we have from Ex 25.2 & Prop 25.3 that $G \cong$ the unique group of order p^3 without an element of order p^2. ☑

25.4

Notice $63 = 3^2 \cdot 7$. Thus a group G with $|G| = 63$ has 3-Sylow and 7-Sylow subgroups. Since $n_7 \equiv 1 \bmod 7$ and $n_7 \in \{1, 3, 9\}$, $n_7 = 1$ so $P_7 \trianglelefteq G$.

Also, $n_3 \equiv 1 \bmod 3$ and $n_3 \in \{1, 7\}$. Thus $n_3 = 1$ or $n_3 = 7$.

Note that $|P_3| = 9$, so $P_3 \cong \mathbb{Z}/9$ or $P_3 \cong \mathbb{Z}/3 \times \mathbb{Z}/3$ is abelian.

- If $n_3 = 1$, then $P_3 \trianglelefteq G$ and $G \cong P_3 \times P_7 \cong S \in \{ \mathbb{Z}/7 \times \mathbb{Z}/9, \mathbb{Z}/7 \times \mathbb{Z}/3 \times \mathbb{Z}/3 \}$
- Otherwise, $n_3 = 7$, so $G = P_7 \rtimes_\varphi P_3$, where $\varphi : P_3 \to \mathrm{Aut}(P_7)$ is nontrivial as $P_3 \not\trianglelefteq G$. Since $\mathrm{Aut}(\mathbb{Z}/7) \cong \mathbb{Z}/6$, the image of P_3 under φ is the unique subgroup of $\mathbb{Z}/6$ with order 3.

  Thus $G \cong S \in \{ \mathbb{Z}/7 \rtimes_\varphi \mathbb{Z}/9, \mathbb{Z}/7 \rtimes_\varphi (\mathbb{Z}/3 \times \mathbb{Z}/3) \}$.

25.5

Notice $1225 = 5^2 \cdot 7^2$. Thus a group G with $|G| = 1225$ has 5-Sylow and 7-Sylow subgroups. From Sylow, $n_5 \equiv 1 \bmod 5$ but $n_5 \in \{1, 7, 49\}$. Thus $n_5 = 1$ and thus $P_5 \trianglelefteq G$. Similarly, $n_7 \equiv 1 \bmod 7$ but $n_7 \in \{1, 5, 25\}$, thus $n_7 = 1$ and $P_7 \trianglelefteq G$. Since $|P_5| = 5^2$ and $|P_7| = 7^2$, both P_5 and P_7 are abelian. Moreover, $P_5 P_7 \trianglelefteq G$ and $|P_5 P_7| = |G|$ so $G = P_5 \times P_7$ is abelian. ☑