1. (1). $G = A_4 \rtimes \mathbb{Z}_2$ find (1234)

identify this action as $\varphi: \mathbb{Z}_2 \longrightarrow Aut(A_4) = S_4$

$\quad\quad\quad\quad\quad\quad\quad\quad z \quad 1 \longmapsto (34)$ so we can write z into (34)

Then $(1234) = [(13)(24)(34)]^{-1}$

(2) Identify $\mathbb{Z}_{17} \rtimes \mathbb{Z}_{16}$

$Aut(\mathbb{Z}_{17}) = \mathbb{Z}_{16}$ and one of prim root of 17 is 3 so let $Aut(\mathbb{Z}_{17}) = \langle a \rangle$ where

$a: \mathbb{Z}_{16} \to \mathbb{Z}_{16}$

$\quad a \; 1 \mapsto a^3$

Consider homomorphism from $\mathbb{Z}_{16}$ to $\mathbb{Z}_{16}$.

$\varphi_1: \mathbb{Z}_{16} \longrightarrow \mathbb{Z}_{16}$ $\quad \langle a, b \mid a^{17} = b^{16} = 1,\ b^{-1}ab = a^3 \rangle$

$\quad a \longmapsto a$

$\varphi_2: \mathbb{Z}_{16} \longmapsto \mathbb{Z}_{16}$ $\quad \langle a, b \mid a^{17} = b^{16} = 1,\ b^{-1}ab = a^9 \rangle$

$\quad a \longmapsto a^2$

$\varphi_3: \mathbb{Z}_{16} \longmapsto \mathbb{Z}_{16}$ $\quad \langle a, b \mid a^{17} = b^{16} = 1,\ b^{-1}ab = a^{13} \rangle$

$\quad a \longmapsto a^4$

$\varphi_4: \mathbb{Z}_{16} \longmapsto \mathbb{Z}_{16}$ $\quad \langle a, b \mid a^{17} = b^{16} = 1,\ b^{-1}ab = a^{-1} \rangle$

$\quad a \longmapsto a^8$

$\varphi_5: \mathbb{Z}_{16} \longmapsto \mathbb{Z}_{16}$

$\quad a \longmapsto a^{16} = 1.$

this is a direct prod $\mathbb{Z}_{17} \times \mathbb{Z}_{16}$

$\langle a, b \mid a^{17} = b^{16} = 1.\ b^{-1}ab = a \rangle$.

(3). Construct $G = \mathbb{Z}_2^3 \rtimes Q_8$ s.t $Z(G) = 1$

Consider $\varphi: Q_8 \longrightarrow Aut(\mathbb{Z}_2^3) = GL_3(\mathbb{F}_2)$

if $\ker\varphi \neq 1$ then $Z(G) \neq 1$

So φ is monomorphism.

$|Aut(\mathbb{Z}_2^3)|$

$= (2^3-1)(2^3-2)(2^3-4)$

$= 7 \times 6 \times 4 = 2^3 \times 3 \times 7$

order 8 subgroup of $Aut(\mathbb{Z}_2^3)$ is Sylow 8-subgroup of $Aut(\mathbb{Z}_2^3)$

No take $P_8 = \left\{ \begin{pmatrix} 1 & x & y \\ & 1 & z \\ & & 1 \end{pmatrix} \middle| \ x, y, z \in \mathbb{F}_2 \right\}$

identify φ as $\varphi(Q_8) \simeq P_8$ then we done.

2. (1). $(\mathbb{Z}, +)$ has no composition series.

Thm (Page 69. Thm 3.7)

If G has composition series then G satisfies ACC and DCC.

We consider DCC

$G = \mathbb{Z} \geq 2\mathbb{Z} \geq 4\mathbb{Z} \cdots\cdots$ we can not find k s.t

$2^k\mathbb{Z} = 2^{k+1}\mathbb{Z}$ so G has no composition series.

(2). $\mathbb{Z}_6 > \mathbb{Z}_3 > \{e\}$ $\quad \mathbb{Z}_6 > \mathbb{Z}_2 > \{e\}$

(3). $S_3 > \mathbb{Z}_3 > \{e\}$

$S_4 > A_4 > \mathbb{Z}_2 \times \mathbb{Z}_2 > \mathbb{Z}_2 > \{e\}$

$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ $\quad \begin{matrix} 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ & 1 & 0 \\ & 0 & 1 \end{matrix}$

(4). $GL_2(F) \simeq S_3$

$$GL_2(F) > \underset{\langle \left[\begin{smallmatrix} & 1 \\ 1 & 1 \end{smallmatrix}\right] \rangle}{\underset{\text{\rotatebox{90}{$\subseteq$}}}{\mathbb{Z}_3}} > \{e\}$$

3. (1). $S_4 \simeq \langle a, b \mid a^2 = b^3 = e, (ab)^4 = e \rangle = G$

$\varphi: G \longrightarrow S_4$ then

$a \longmapsto (34) \quad b \longmapsto (123)$, $\varphi(ab) = (1234)$

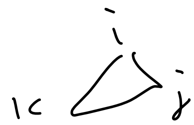
Check φ is an iso.

(2). $A_4 \cong \langle a,b \mid a^2=b^3=e,\ (ab)^3=e\rangle \cong G$.

$$\begin{aligned}\varphi: G &\longrightarrow A_4\\ a &\longmapsto (12)(34)\\ b &\longmapsto (123)\end{aligned}$$ then $\varphi(ab)=(134)$

check φ is an iso.

(3). $Q_8 \cong \langle a,b \mid a^4=b^4=e,\ a^2=b^2,\ b^{-1}ab=a^{-1}\rangle = G$



$$\begin{aligned}\varphi: G &\longrightarrow Q_8\\ a &\longmapsto i\\ b &\longmapsto j\end{aligned}$$ $\varphi(b^{-1}ab) = -jij = -jk = -i = i^{-1}$

check φ is an iso.

4.

$$\begin{tikzcd} & G \\ F \arrow[ur, "\phi"] \arrow[dr, dashed, "\psi"'] & \\ & H \arrow[uu, "\alpha"'] \end{tikzcd}$$

commute. ψ is unique actually

F is a free group, take a basis of F s.t.

$X=\{x_i,\ i\in I\}$

Then $\phi(x_i)\in G$ and α is onto. we have.

$\alpha(h_j)=\phi(x_i)$ for some $h_j\in H$

Construct: $\psi(x_i)=h_j$ then $\alpha(\psi(x_i))=\alpha(h_j)=\phi(x_i)$

only need to show ψ is a group homomorphism

ψ is an extending. see as follows:

Universal property: (definition of free group).

F is a free group with basis X iff: for any group H and any function f $\exists$ unique group homo. γ s.t this diagram commute.

$$\begin{tikzcd} F \arrow[dr, dashed, "\gamma"] & \\ X \arrow[u] \arrow[r, "f"'] & H \end{tikzcd}$$

In our proof we take f as $f: X \longrightarrow H$

$$x_i \longmapsto \psi(X_i)$$

Then γ is an extending of f, so is a group homomorphism.

5. (1). $(I, J) = 1$. prove $IJ = I \cap J$

$IJ \subseteq I \cap J$ is trivial.

$\forall\ a \in I \cap J$, since I, J coprime.

$\exists\ i, j \in I, J$ respectively s.t. $r_1 i + r_2 j = 1$.

then $a = a \cdot 1 = \underset{\substack{\cap \\ IJ}}{a r_1 i} + \underset{\substack{\cap \\ IJ}}{a r_2 j} \in IJ$ thus $IJ = I \cap J$

(2). $I_1, \dots, I_n$ coprime then $I_1 \cap \cdots \cap I_n = I_1 \cdots I_n$.

Observation: $I_1, \dots, I_n$ coprime then

$I_1, \dots, I_{n-1}$ and I_n coprime.

$\Rightarrow I_1 \cdots I_{n-1} \cdot I_n = (I_1 \cdots I_{n-1}) \cap I_n = I_1 \cap I_2 \cdots \cap I_{n-1} \cap I_n$

induction.

check $I_1 \cdots I_{n-1}$ and I_n coprime:

fix $i_n \in I_n$. $\exists\ r_i$ and $r_{j,k}$ s.t.

$$r_1 i_1 + r_{1,n} i_n = 1$$

$$\vdots$$

$$r_{n-1} i_{n-1} + r_{n-1,n} i_n = 1$$

Thus consider

$$\prod r_i i_i \in I_1 \cdots I_{n-1}$$

$$\prod r_i i_i = \prod (1 - r_{i,n} i_n) = 1 + b. \quad b \in I_n$$

i.e. $\exists\ \prod r_i i_i \in I_1 \cdots I_{n-1}$ and $-b \in I_n$ s.t.

$\prod r_i i_i - b = 1$ thus $I_1 \cdots I_{n-1}$ and I_n are coprime.

(3). Let I, J, K ideals of R. $IJ \subseteq K$. I, K coprime then $J \subseteq K$

I, K coprime $\Rightarrow \exists\ i, k \in I, K$ respectively

s.t. $i + k = 1$

$\forall\ j \in J$, $\quad j = j \cdot 1 = \underset{\substack{\cap \\ IJ}}{ji} + \underset{\substack{\cap \\ K}}{jk} \in K \quad \Rightarrow J \subseteq K$

(4) $I, J \supseteq K$. $I\ J$ coprime $\Rightarrow IJ \supseteq K$.

$K \subseteq I, J \Rightarrow K \subseteq I \cap J \Rightarrow \underset{I \cap J = IJ}{I, J \text{ coprime}} \Rightarrow K \subseteq IJ$

6. p prime. $n > 1$. $R = \mathbb{Z}/(p^n)$. Prove:

(i). If r not unit then r nil. $R = \{0, 1, \ldots, p^n - 1\}$ as a set.

r unit $\Leftrightarrow \exists\ u, v \in \mathbb{Z}$ s.t. $ur + vp^n = 1$

So r not unit $\iff (r, p^n) \neq 1$

Then $p \mid r$ so $\exists k$ s.t. $r^k = p^n \Rightarrow r$ nil.

(ii). R has only 1 prime ideal.

Claim this ideal is (p)

1° if r is unit. $(r) = (1)$, not prime

2° R is not a integral domain. so (0) not prime.

3° for $r = p^k$, if $k \neq 1$, $\exists$ $a = p$ and $b = p^{k-1}$ s.t.

$ab \in (r)$ but $a \notin (r)$ and $b \notin (r)$

4°. for $r = p$. (r) is prime since.

if $ab \in (p)$. then $p \mid a$ or $p \mid b \Rightarrow a \in (p)$ or $b \in (p)$

(3). If $(p) \underset{\neq}{\trianglelefteq} J \underset{\neq}{\trianglelefteq} R$ then $\exists$ $0 \neq a \in J - (p)$

but $(a, p) = 1 \Rightarrow (a) + (p) = (1) \Rightarrow J = (1)$ $\lightning$

Thus (p) is maximal and R/p is a field.

7. (1). $\varphi : R \to R_1$ ring homo. if $Q \underset{\text{prime}}{\triangleleft} R_1$ then

$P = \varphi^{-1}(Q) \underset{\text{prime}}{\triangleleft} R$.

Let $ab \in P$. $\varphi(ab) = \varphi(a)\varphi(b) \in Q$ since $Q \underset{\text{prime}}{\triangleleft} R_1$

either $\varphi(a)$ or $\varphi(b) \in Q$

$\Rightarrow$ either a or $b \in P \Rightarrow P \underset{\text{prime}}{\trianglelefteq} R$

(2). Is this true for maximal ideal?

no. $\mathbb{Z} \hookrightarrow \mathbb{Q}$

8. (1). if $P \underset{\text{prime}}{\trianglelefteq} R$, $\bigcap_{i=1}^{n} I_i \subseteq P \Rightarrow I_k \subseteq P$ for some k.

if not. pick $a_i \in I_i \setminus P$

$\prod a_i \in \bigcap I_i \subseteq P$ but all $a_i \notin P$ ↯

(2). $I \subseteq \bigcup P_i$ then $I \subseteq P_k$ for some k.

$n=1$ true

Sps $n-1$ true

for n. we can take $P_i \nsubseteq \bigcup_{j \neq i}^{n} P_j$ $(\forall i)$ (if not then its nothing new beyond our induction hypothesis).

then we pick $p_i \in P_i \setminus \bigcup_{j \neq i} P_j$

If $I \nsubseteq P_i$ $(\forall i)$ then pick

$a_i \in I \setminus P_i$

Then $p_2 p_3 \cdots p_n a_1 + p_1 p_3 \cdots p_n a_2 + \cdots + p_1 p_2 \cdots p_{n-1} a_n$

$\in I \setminus \bigcup_{i=1}^{n} P_i$ ↯

(3). prove prime ideal of finite ring is maximal.

Let $P \underset{prime}{\triangleleft} R$

R/p is finite integral domain $\Rightarrow R/p$ is field

$\Rightarrow p \underset{max}{\triangleleft} R$.

9. (1). $\mathbb{Z}_{(p)}$

$$\mathbb{Z}_{(p)} = \left\{ \frac{m}{n} \middle| m \in \mathbb{Z}, n \in \mathbb{Z} \setminus (p) \right\}$$

(2). $m \in \mathbb{Z}$ $m \neq 0$ write $m^{-1}\mathbb{Z}$

$$m^{-1}\mathbb{Z} = \left\{ \frac{n}{k} \middle| n \in \mathbb{Z},\ k = m^i,\ i = 0, 1, \cdots \right\}.$$

10. (1). prove $IR_p \triangleleft R_p$

identify R_p with $\left\{ \frac{m}{n} \middle| m \in R, n \in R \setminus p \right\}$.

$IR_p = \left\{ \frac{a}{b} \middle| a \in I, b \in R \setminus p \right\}$.

then $IR_p \triangleleft R_p$ followed by $I \triangleleft R$. (use the disscussion in (2))

(2). $Q \underset{prime}{\triangleleft} R$ then $QR_p \underset{prime}{\triangleleft} R_p$ or $QR_p = (1)$

If $Q \nsubseteq P$, i.e $\exists\ a \in Q,\ a \notin P$

then a invertible in R_p $\Rightarrow R_p = (a) \subseteq Q$

$\Rightarrow Q = (1)$

If $Q \subseteq P$, by (1) $QR_p \triangleleft R_p$

if $\frac{a_1}{b_1}\cdot\frac{a_2}{b_2} \in QR_p \Rightarrow \frac{a_1 a_2}{b_1 b_2} = \frac{c}{d}$ for some $c \in Q$, $d \in R \setminus P$

$\Rightarrow$ for some $x \in R \setminus P$ $x(a_1 a_2 d - b_1 b_2 c) = 0$,

Q prime $\Rightarrow$ $x a_1 a_2 d \in Q \Rightarrow a_1 a_2 \in Q \Rightarrow a_1 \in Q$ or $a_2 \in Q$

$\Rightarrow \frac{a_1}{b_1} \in QR_p$ or $\frac{a_2}{b_2} \in QR_p$ $\square$.

(3). Prove PR_p is unique maximal ideal in R_p.

By 2. if $I \nsubseteq P$, $IR_p = (1)$

if $I \subseteq P$, $IR_p \subseteq PR_p$

and $R_p / PR_p = \text{frac}(R)$ is a field

so PR_p is unique maximal ideal in R_p.

(4). prove.

$$Q \longmapsto Q \cdot R_p$$

$$\left\{ \begin{matrix} I \subseteq P \\ I \triangleleft_{\text{prime}} R \end{matrix} \right\} \underset{1:1}{\rightleftarrows} \left\{ J \triangleleft_{\text{prime}} R_p \right\}$$

by (2) $\rightarrow$ direction is done.

consider $\leftarrow$ let $Q' \triangleleft_{\text{prime}} R_p$

Now take $\pi : R \longrightarrow R_p$ ring homo.

We prove a strengthen proposition:

If $\varphi : R \to S$ be a homomorphism of commutative rings

If $P \underset{\text{prime}}{\trianglelefteq} S$ then either $\varphi^{-1}(P) = R$ or $\varphi^{-1}(P) \underset{\text{prime}}{\trianglelefteq} R$

This is easy. just check.

Remember: Check is trivial work:

Assume $\varphi^{-1}(P) \neq R$ suppose $xy \in \varphi^{-1}(P)$

then $\varphi(xy) = \varphi(x)\varphi(y) \in P$

either $\varphi(x) \in P$ or $\varphi(y) \in P$

either $x \in \varphi^{-1}(P)$ or $y \in \varphi^{-1}(P)$

Thus $\varphi^{-1}(P) \underset{\text{prime}}{\trianglelefteq} R$.

Now take $\pi : R \longrightarrow R_p$

if $Q \underset{\text{prime}}{\trianglelefteq} R_p$, then $\pi^{-1}(Q) = R \cap Q$

if $R \cap Q = R$ then $R \subseteq Q \Rightarrow 1 \in Q \Rightarrow Q = R_p$

$\forall\, Q \underset{\text{prime}}{\trianglelefteq} R_p$

$$IR_p \longleftarrow I$$

thus $Q \longrightarrow \pi^{-1}(Q) = R \cap Q$

is 1:1 correspondence