Algebra: Chapter 0 - Aluffi

Conan Pickford <pickfordconan@gmail.com>

October 2023

I - Categories

1.3 - Categories

1. Let C be a category. Consider the structure C^{op} with $\mathsf{obj}(\mathsf{C}^{\text{op}}) := \mathsf{obj}(\mathsf{C})$ and for objects A, B of C^{op}, we have that $\text{Hom}_{\mathsf{C}^{\text{op}}}(A, B) := \text{Hom}_{\mathsf{C}}(B, A)$. For objects A, B, C of C and $f \in \text{Hom}_{\mathsf{C}^{\text{op}}}(A, B)$ and $g \in \text{Hom}_{\mathsf{C}^{\text{op}}}(B, C)$, define the composition law $\circ_{\mathsf{C}^{\text{op}}}$ by $g \circ_{\mathsf{C}^{\text{op}}} f := f \circ_{\mathsf{C}} g \in \text{Hom}_{\mathsf{C}}(C, A) = \text{Hom}_{\mathsf{C}^{\text{op}}}(A, C)$. Let A, B, C, D be objects in C^{op}. Let $f \in \text{Hom}_{\mathsf{C}^{\text{op}}}(A, B), g \in \text{Hom}_{\mathsf{C}^{\text{op}}}(B, C)$ and $h \in \text{Hom}_{\mathsf{C}^{\text{op}}}(C, D)$. Then, $(h \circ_{\mathsf{C}^{\text{op}}} g) \circ_{\mathsf{C}^{\text{op}}} f = f \circ_{\mathsf{C}} (g \circ_{\mathsf{C}} h) = (f \circ_{\mathsf{C}} g) \circ_{\mathsf{C}} h = h \circ_{\mathsf{C}^{\text{op}}} (g \circ_{\mathsf{C}^{\text{op}}} f)$ as $\circ_{\mathsf{C}}$ is an associative operation. Hence, $\circ_{\mathsf{C}^{\text{op}}}$ is associative. For each object A of C^{op}, we have that there is an identity morphism $1_A \in \text{Hom}_{\mathsf{C}}(A, A) = \text{Hom}_{\mathsf{C}^{\text{op}}}(A, A)$ as C is a category. Let $f \in \text{Hom}_{\mathsf{C}^{\text{op}}}(A, B)$, we have that $f \circ_{\mathsf{C}^{\text{op}}} 1_A = 1_A \circ_{\mathsf{C}} 1_A = f$ and $1_B \circ_{\mathsf{C}^{\text{op}}} f = f \circ_{\mathsf{C}} 1_B = f$ as $1_A, 1_B$ are the identities under $\circ_{\mathsf{C}}$. Lastly, we have that for all objects A, B, C, D of C^{op}, we have that $\text{Hom}_{\mathsf{C}^{\text{op}}}(A, B)$ and $\text{Hom}_{\mathsf{C}^{\text{op}}}(C, D)$ are disjoint as $\text{Hom}_{\mathsf{C}}(B, A)$ and $\text{Hom}_{\mathsf{C}}(D, C)$ are disjoint as C is a category. It follows that C^{op} is a category.

2. Let A be a finite set such that $|A| = n \in \mathbb{N}$. We have that $\text{Hom}_{\mathsf{Set}}(A, B)$ is the set of all functions from A to B, in which there are $|B|^{|A|}$ of them. Then, $|\text{End}_{\mathsf{Set}}(A)| = |\text{Hom}_{\mathsf{Set}}(A, A)| = |A|^{|A|} = n^n$.

3. Let S be a set and $\sim$ a relation on S such that $\sim$ is reflexive and transitive. Let S be the category with $\mathsf{obj}(\mathsf{S}) = S$ and morphisms as if $a, b \in S$, then $\text{Hom}_{\mathsf{S}}(a, b)$ be the set consisting of $(a, b) \in S \times S$ if $a \sim b$ and let $\text{Hom}(a, b) = \emptyset$ otherwise. Define the compisition law $\circ_{\mathsf{S}}$ by if $f \in \text{Hom}_{\mathsf{S}}(a, b)$ and $g \in \text{Hom}_{\mathsf{S}}(b, c)$, then $g \circ_{\mathsf{S}} f = (a, c) \in \text{Hom}_{\mathsf{S}}(a, c)$. For each object a of S, let $1_a = (a, a)$. Let $f \in \text{Hom}_{\mathsf{S}}(a, b)$, we have that $f \circ_{\mathsf{S}} 1_a = (a, b) \circ_{\mathsf{S}} (a, a) = (a, b) = f$ and $f \circ_{\mathsf{S}} 1_b = (a, b) \circ_{\mathsf{S}} (b, b) = (a, b) = f$. Hence, $(a, a) \in \text{Hom}_{\mathsf{S}}(a, a)$ is the identity morphism on a.

4. As $<$ is not reflexive, we cannot define a category on the set $\mathbb{Z}$ in the style of the previous exercise.

5. Let S be a set and define a relation on $\mathcal{P}(S)$ by $A \sim B$ if and only if $A \subseteq B$. We have that $\sim$ is reflexive and transitive. We define a category on $\mathcal{P}(S)$ in the style of (3).

6.

7. Let C be a category. Let A be an onject in C. Consider the structure C^A where $\mathsf{obj}(\mathsf{C}^A)$ are all morphisms from A to any object of C; thus, an object of C^A is a morphism $f \in \text{Hom}_{\mathsf{C}}(A, Z)$ for some object Z of C. Let f_1, f_2 be objects of C^A, that is, two arrows,

$$\begin{tikzcd}
A \arrow[d, "f_1"'] & A \arrow[d, "f_2"] \\
Z_1 & Z_2
\end{tikzcd}$$

Define morphisms $f_1 \to f_2$ to be commutative diagrams

$$\begin{tikzcd}
& A \arrow[dl, "f_1"'] \arrow[dr, "f_2"] & \\
Z_1 \arrow[rr, "\sigma"'] & & Z_2
\end{tikzcd}$$

That is, morphisms $f \to g$ correspond precisely to those morphisms $\sigma : Z_1 \to Z_2$ in C such that $\sigma f = g$. For $f \in \mathrm{Hom}_{\mathsf{C}^A}(f_1, f_2)$ and $g \in \mathrm{Hom}_{\mathsf{C}^A}(f_2, f_3)$, thats is, the commutative diagrams

$$\begin{tikzcd} & A \arrow[dl, "f_1"'] \arrow[dr, "f_2"] & \\ Z_1 \arrow[rr, "\sigma"'] & & Z_2 \end{tikzcd} \qquad \begin{tikzcd} & A \arrow[dl, "f_2"'] \arrow[dr, "f_3"] & \\ Z_2 \arrow[rr, "\tau"'] & & Z_3 \end{tikzcd}$$

respecitvely, define the composition $\circ_{\mathsf{C}^A}$ by $g \circ_{\mathsf{C}^A} f$ is the commutative diagram

$$\begin{tikzcd} & A \arrow[dl, "f_1"'] \arrow[dr, "f_3"] & \\ Z_1 \arrow[rr, "\sigma\tau"'] & & Z_3 \end{tikzcd}$$

For $f \in \mathrm{Hom}_{\mathsf{C}^A}(f_1, f_2)$, let $1_{f_1} \in \mathrm{Hom}_{\mathsf{C}^A}(f_1, f_1)$ and $1_{f_2} \in \mathrm{Hom}_{\mathsf{C}^A}(f_2, f_2)$ be the commutative diagrams

$$\begin{tikzcd} & A \arrow[dl, "f_1"'] \arrow[dr, "f_1"] & \\ Z_1 \arrow[rr, "1_{Z_1}"'] & & Z_1 \end{tikzcd} \qquad \begin{tikzcd} & A \arrow[dl, "f_2"'] \arrow[dr, "f_2"] & \\ Z_2 \arrow[rr, "1_{Z_2}"'] & & Z_2 \end{tikzcd}$$

respectively. We have that $f \circ_{\mathsf{C}^A} 1_{f_1} = f$ and $1_{f_2} \circ_{\mathsf{C}^A} f = f$. Finally, we also note that associaitvity holds as $\circ_{\mathsf{C}}$ is associative in C. Therefore, C^A is a category.

8. Let Set_∞ be a structure such that $\mathsf{obj}(\mathsf{Set}_\infty)$ are infinite sets and for $A, B \in \mathsf{obj}(\mathsf{Set}_\infty)$, we have that $\mathrm{Hom}_{\mathsf{Set}_\infty}(A, B)$ are the set functions from A to B. Define the composition law $\circ_{\mathsf{Set}_\infty}$ as function composition. Thus, $\circ_{\mathsf{Set}_\infty}$ is an associative operation. For $f \in \mathrm{Hom}_{\mathsf{Set}_\infty}(A, B)$ define 1_A to be the identity function on A. Then, $f \circ_{\mathsf{Set}_\infty} 1_A = f$ and $1_B \circ_{\mathsf{Set}_\infty} f = f$. Therefore, Set_∞ is a category. We have that Set_∞ is a subcategory of Set as $\mathsf{obj}(\mathsf{Set}_\infty) \subseteq \mathsf{obj}(\mathsf{Set})$ and $\mathrm{Hom}_{\mathsf{Set}_\infty}(A, B) \subseteq \mathrm{Hom}_{\mathsf{Set}}(A, B)$ for all objects $A, B \in \mathsf{obj}(\mathsf{Set}_\infty)$. In fact, $\mathrm{Hom}_{\mathsf{Set}_\infty}(A, B) = \mathrm{Hom}_{\mathsf{Set}}(A, B)$ as both are classes of all set functions from A to B. It follows that Set_∞ is a full subcategory of Set.

9.

10.

11.

1.4 - Morphisms

1.

2. Let S be a set and $\sim$ be an equivalence relation on S. Define a category C such that $\mathsf{obj}(\mathsf{C}) = S$ and for objects A, B of C, define $\mathrm{Hom}_{\mathsf{C}}(A, B) = (A, B)$ if $A \sim B$ and $\mathrm{Hom}_{\mathsf{C}}(A, B) = \emptyset$ otherwise. Define the composition law as before. Let $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$. As $\mathrm{Hom}_{\mathsf{C}}(A, B)$ is non-empty, we have that $A \sim B$ and so $B \sim A$ as $\sim$ is symmetric. There then exists a $g \in \mathrm{Hom}_{\mathsf{C}}(B, A)$ where $g = (B, A)$. We have that $gf = (a, a) = 1_A \in \mathrm{End}_{\mathsf{C}}(A)$ and $fg = (b, b) = 1_B \in \mathrm{End}_{\mathsf{C}}(B)$. Therefore, f is an isomorphism. As f was arbitrary, it follows that C is a groupoid.

3. Let A, B be objects of a category C and let $f \in \mathrm{Hom}_{\mathsf{C}}(A, B)$ be a morphism such that f has a right inverse. Thus, there exists a $g \in \mathrm{Hom}_{\mathsf{C}}(B, A)$ such that $fg = 1_B$ where $1_B \in \mathrm{End}_{\mathsf{C}}(B)$ is the identity morphism on B. Let Z be an object of C and $\beta', \beta'' \in \mathrm{Hom}_{\mathsf{C}}(B, Z)$ be morphisms from B to Z such that $\beta' f = \beta'' f$. Then, $\beta' = \beta' 1_B = \beta'(fg) = (\beta' f)g = (\beta'' f)g = \beta''(fg) = \beta'' 1_B = \beta''$. Therefore, $\beta' = \beta''$ and so f is an epimorphism. The converse is not true, however. Let C be a category such that $\mathsf{obj}(\mathsf{C}) = \mathbb{Z}$ and for each pair of objects A, B of C, we have $\mathrm{Hom}_{\mathsf{C}}(A, B) = (A, B) \in \mathbb{Z} \times \mathbb{Z}$ if $A \leq B$ and $\mathrm{Hom}_{\mathsf{C}}(A, B) =$ otherwise. Let $f = (0, 1) \in \mathrm{Hom}_{\mathsf{C}}(0, 1)$. Let Z be an object of C and let $\beta', \beta'' \in \mathrm{Hom}_{\mathsf{C}}(1, Z)$ such that $\beta' \circ f = \beta'' \circ f$. We have that $\mathrm{Hom}_{\mathsf{C}}(1, Z)$ is non-empty and will contain only one element, namely, $(1, Z) \in \mathbb{Z} \times \mathbb{Z}$. Then, $\beta' = \beta'' = (1, Z)$. Therefore, f is an epimorphism. Suppose there exists a $g \in \mathrm{Hom}_{\mathsf{C}}(1, 0)$, then we have that $1 \leq 0$. This is ofcourse ridiculous, hence, g cannot exist. There cannot possibly exist a right inverse of f.

4. Let C be a category. Let $f \in \mathrm{Hom}_{\mathsf{C}}(A, B), g \in \mathrm{Hom}_{\mathsf{C}}(B, C)$ be monomorphisms. Let $gf \in \mathrm{Hom}_{\mathsf{C}}(A, C)$ be their composition. Let Z be an object of C and $\alpha, \alpha' \in \mathrm{Hom}_{\mathsf{C}}(Z, A)$ such that $gf\alpha = gf\alpha'$. We have that $f\alpha, f\alpha' \in \mathrm{Hom}_{\mathsf{C}}(Z, B)$ and since g is a monomorphism, we have that $f\alpha = f\alpha'$. As f is a monomorphism, we have that $\alpha = \alpha'$. Therefore, gf is a monomorphism. Consider the structure C_{mono} where $\mathsf{obj}(\mathsf{C}_{\text{mono}}) = \mathsf{obj}(\mathsf{C})$ and for objects A, B of C_{mono}, let $\mathrm{Hom}_{\mathsf{C}_{\text{mono}}}(A, B)$ be the monomorphisms of $\mathrm{Hom}_{\mathsf{C}}(A, B)$. For $f \in \mathrm{Hom}_{\mathsf{C}_{\text{mono}}}(A, B), g \in \mathrm{Hom}_{\mathsf{C}_{\text{mono}}}(B, C)$, define their composition $g \circ_{\mathsf{C}_{\text{mono}}} f = g \circ_{\mathsf{C}} f \in \mathrm{Hom}_{\mathsf{C}_{\text{mono}}}(A, C)$. We have that $\circ_{\mathsf{C}_{\text{mono}}}$ is associative as $\circ_{\mathsf{C}}$ is associative. For object A of C_{mono}, let $1_A \in \mathrm{End}_{\mathsf{C}_{\text{mono}}}(A)$ be the identity morphism of A in C. We verify that 1_A is a monomorphism. Let Z be an object in C_{mono} and $\alpha, \alpha' \in \mathrm{Hom}_{\mathsf{C}_{\text{mono}}}(Z, A)$ such that $1_A \circ_{\mathsf{C}_{\text{mono}}} \alpha = 1_A \circ_{\mathsf{C}_{\text{mono}}} \alpha'$. Then, $1_A \circ_{\mathsf{C}_{\text{mono}}} \alpha = 1_A \circ_{\mathsf{C}_{\text{mono}}} \alpha' \implies 1_A \circ_{\mathsf{C}} \alpha = 1_A \circ_{\mathsf{C}} \alpha' \implies \alpha = \alpha'$ as $1_A \in \mathrm{End}_{\mathsf{C}}(A)$ is the identity morphism. Hence, 1_A is a monomorphism. Therefore, $1_A \in \mathrm{End}_{\mathsf{C}_{\text{mono}}}(A)$. Let $f \in \mathrm{Hom}_{\mathsf{C}_{\text{mono}}}(A, B)$. Then, $f \circ_{\mathsf{C}_{\text{mono}}} 1_A = f \circ_{\mathsf{C}} 1_A = f$ and $1_B \circ_{\mathsf{C}_{\text{mono}}} f = 1_B \circ_{\mathsf{C}} f = f$. Therefore, the identity morphisms are identities with respect to composition in C_{mono}. It follows that C_{mono} is a category and is a subcategory of C.

5.

1.5 - Universal Properties

1. Let C be a category and C^{op} be its opposite category. Let F be a final object of C. We have that F is an object of C^{op}. Let A be an object of C^{op}. Then, $\mathrm{Hom}_{\mathsf{C}^{\text{op}}}(F, A) = \mathrm{Hom}_{\mathsf{C}}(A, F)$ is singleton as F is final in C. Therefore, F is initial in C^{op}.

2. Let $\emptyset$ be the empty set in the category Set. For all objects A of Set, we have that there is exactly one set function from $\emptyset$ to A, namely, the empty graph. Therefore, $\mathrm{Hom}_{\mathsf{Set}}(\emptyset, A)$ is a singleton for all objects A. Thus, $\emptyset$ is inital in Set. Suppose there exists an object I of Set such that I is non-empty and I is an initial object. As I is an initial object, we have that $\mathrm{Hom}_{\mathsf{Set}}(I, A)$ is singleton for all objects A. However, $\mathrm{Hom}_{\mathsf{Set}}(I, \emptyset)$ is empty as I is non-empty. Hence, I cannot possibly be initial in Set. It follows that $\emptyset$ is the unique initial object of Set.

3. Let C be a category and let F, F' be final objects of C. Let $f \in \mathrm{Hom}_{\mathsf{C}}(F, F')$ and $g \in \mathrm{Hom}_{\mathsf{C}}(F', F)$. We note $f \in \mathrm{Hom}_{\mathsf{C}}(F, F')$ is unique and $g \in \mathrm{Hom}_{\mathsf{C}}(F', F)$ is unique as F, F' are final objects. We have that $gf \in \mathrm{Hom}_{\mathsf{C}}(F, F)$ and $1_F \in \mathrm{Hom}_{\mathsf{C}}(F, F)$, thus, $gf = 1_F$ as F is final and so $\mathrm{Hom}_{\mathsf{C}}(F, F)$ is a singleton. Similarly, $\mathrm{Hom}_{\mathsf{C}}(F', F') \ni fg = 1_{F'}$. It follows that f and g are isomorphisms and F is isomorphic to F'.

4. Let Set^* be the category of pointed sets. Let $f : \{*\} \to S$ be an object of Set^* such that S is singleton. Let $g : \{*\} \to A$ be an object of Set^*. We have that a morphism $f \to g$ would correspond to a set function $\sigma : S \to A$ such that $\sigma f = g$. We have that there exists only one choice of σ, namely, the map $\alpha \mapsto g(*)$ where $\alpha \in S$. Thus, $\mathrm{Hom}_{\mathsf{Set}^*}(f, g)$ is singleton. Similarly, a morphism $g \to f$ corresponds to a set function $\tau : A \to S$ such that $\tau g = f$ and there exists only one possible choice of τ, namely, the constant function. Hence, $\mathrm{Hom}_{\mathsf{Set}^*}(g, f)$ is singleton. We have that f is an initial and final object of Set^*.

5. Let $\sim$ be an equivalence relation defined on a set A. Let C be a category where $\mathsf{obj}(\mathsf{C})$ is the class of set functions $\varphi : A \to Z$ where Z is a set and for $a, a' \in A$, if $a \sim a'$, then $\varphi(a) = \varphi(a')$. For f, g objects of C, let a morphism $f \to g$ correspond to a set function σ such that $\sigma f = g$. Let $\varphi : A \to Z$ be an object of C and let $f : A \to \{*\}$ be an object such that $\{*\}$ is singleton. In the commutative diagram

$$\begin{tikzcd} & A \arrow[dl, "\varphi"'] \arrow[dr, "f"] & \\ Z \arrow[rr, "\sigma"'] & & \{*\} \end{tikzcd}$$

there is only one possibility for $\sigma : Z \to \{*\}$. Therefore, $\mathrm{Hom}_{\mathsf{C}}(\varphi, f)$ is singleton. It follows that f is a final object in C.

6. Let C be the category corresponding to endowing $\mathbb{Z}^+$ with the relation $\sim$ where $a \sim a'$ if $a \mid a'$. Let a, b be objects in C. Let (g_1, g_2) be the object in $\mathsf{C}_{a,b}$ corresponding to the diagram

$$\begin{tikzcd} & a \\ \gcd(a,b) \arrow[ur, "g_1"] \arrow[dr, "g_2"'] & \\ & b \end{tikzcd}$$

Let (f_1, f_2) be an object in $\mathsf{C}_{a,b}$. We have that a morphism $(f_1, f_2) \to (g_1, g_2)$ corresponds to a commutative diagram

$$\begin{tikzcd} & & a \\ c \arrow[r, "\sigma"'] \arrow[urr, bend left, "f_1"] \arrow[drr, bend right, "f_2"'] & \gcd(a,b) \arrow[ur, "g_1"'] \arrow[dr, "g_2"] & \\ & & b \end{tikzcd}$$

As there is a morphism $c \to a$ and a morphism $c \to b$ in C, we have that $c \mid a$ and $c \mid b$. Hence, $c \mid \gcd(a, b)$ by definition. It follows that $\mathrm{Hom}_{\mathsf{C}}(c, \gcd(a, b))$ is non-empty and is then singleton. Therefore, there is a unique σ which makes the above diagram commute. Hence, $\mathrm{Hom}_{\mathsf{C}_{a,b}}((f_1, f_2), (g_1, g_2))$ is singleton and so (g_1, g_2) is a final object of $\mathsf{C}_{a,b}$. Let (h_1, h_2) be the object in $\mathsf{C}^{a,b}$ corresponding to the diagram

$$\begin{tikzcd} & a \arrow[dl, "h_1"'] \\ \mathrm{lcm}(a,b) & \\ & b \arrow[ul, "h_2"] \end{tikzcd}$$

Let (f_1, f_2) be an object in $\mathsf{C}^{a,b}$. We have that a morphism $(f_1, f_2) \to (h_1, h_2)$ corresponds to a commutative diagram

$$\begin{tikzcd} & & a \arrow[dl, "h_1"] \arrow[dll, bend right, "f_1"'] \\ c & \mathrm{lcm}(a,b) \arrow[l, "\tau"] & \\ & & b \arrow[ul, "h_2"'] \arrow[ull, bend left, "f_2"] \end{tikzcd}$$

As there is a morphism $a \to c$ and a morphism $b \to c$ in C, we have that $a \mid c$ and $b \mid c$. Hence, $\mathrm{lcm}(a, b) \mid c$. It follows that $\mathrm{Hom}_{\mathsf{C}}(\mathrm{lcm}(a, b), c)$ is non-empty and is then singleton. Therefore, there is a unique τ which makes the above diagram commute. Hence, $\mathrm{Hom}_{\mathsf{C}^{a,b}}((f_1, f_2), (h_1, h_2))$ is singleton and so (h_1, h_2) is a final object of $\mathsf{C}^{a,b}$. We can conclude that C has products and coproducts.

7.

8.

9.

10.

11.

12. **Not Done** Let $\alpha : A \to C$ and $\beta : B \to C$ be morphisms in Set. Let $A \times_{\alpha,\beta} B$ be the subset of $A \times B$ defined by $A \times_{\alpha,\beta} B = \{(x, y) \mid \alpha(x) = \beta(y)\}$. Let

$$\begin{tikzcd}
& A \arrow[dr, "\alpha"] & \\
Z \arrow[ur, "f"] \arrow[dr, "g"'] & & C \\
& B \arrow[ur, "\beta"'] &
\end{tikzcd}$$

be a morphism in $\mathsf{Set}_{\alpha,\beta}$. We have that the following diagram is commutative as a morphism $(Z, f, g) \to (A \times_{\alpha,\beta} B, \pi_A, \pi_B)$ in $\mathsf{Set}_{\alpha,\beta}$

$$\begin{tikzcd}
& & A \arrow[dr, "\alpha"] & \\
Z \arrow[r, "\sigma"] \arrow[urr, bend left, "f"] \arrow[drr, bend right, "g"'] & A \times_{\alpha,\beta} B \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"'] & & C \\
& & B \arrow[ur, "\beta"'] &
\end{tikzcd}$$

As the diagram is commutative, $f = \pi_A\sigma$ and $g = \pi_B\sigma$, hence, $\sigma(z) = (f(z), g(z))$ for all $z \in Z$. Thus, σ is unique. We also have that σ is well-defined as for each $z \in Z$, we have that $(\alpha f)(z) = (\beta g)(z)$, so $(f(z), g(z)) \in A \times_{\alpha,\beta} B$. It follows that $(A \times_{\alpha,\beta} B, \pi_A, \pi_B)$ is final in $\mathsf{Set}_{\alpha,\beta}$, thus, Set has fibered products. Similarly, let $\alpha : C \to A, \beta : C \to B$ be morphisms in Set. Let $\sim$ be an equivalence relation defined on $A \amalg B$ generated by the set of $(0, \alpha(x)) \sim (1, \beta(x))$ for all $x \in C$. Let

$$\begin{tikzcd}
& A \arrow[dr, "f"] & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & Z \\
& B \arrow[ur, "g"'] &
\end{tikzcd}$$

be a morphism in Set. We have that the following diagram is commutative as a morphism $(A \amalg B/\sim, i_A, i_B) \to (Z, f, g)$

$$\begin{tikzcd}
& A \arrow[dr, "i_A"] \arrow[drr, bend left, "f"] & & \\
C \arrow[ur, "\alpha"] \arrow[dr, "\beta"'] & & A \amalg B/\sim \arrow[r, "\sigma"] & Z \\
& B \arrow[ur, "i_B"'] \arrow[urr, bend right, "g"'] & &
\end{tikzcd}$$

where $i_A : A \to A \amalg B/\sim$ is defined by $i_A(a) = [(0, a)]_\sim$ and $i_A : B \to A \amalg B/\sim$ is defined by $i_B(b) = [(1, b)]_\sim$.

II - Groups, first encounter

2.1 - Definition of Group

1.

2.

3. Let G be a group and $h, g \in G$. We have that $(hg)(g^{-1}h^{-1}) = hgg^{-1}h^{-1} = he_Gh^{-1} = hh^{-1} = e_G$. Therefore, $(hg)^{-1} = g^{-1}h^{-1}$.

4. Let G be a group such that for each $g \in G$, we have that $g^2 = e_G$. Let $x, y \in G$, we have that $x^2 = e_G$ and $y^2 = e_G$. Then, $x^2y^2 = e_G$. We also have that $xy \in G$ and so $xyxy = (xy)^2 = e_G$. Hence, $x^2y^2 = xyxy$. By left and right cancellation, it follows that $xy = yx$. Therefore, G is abelian.

5. Let G be a group such that there exists x, y, z such that $xz = yz$. By right cancellation, we must have that $x = y$. Hence, in a groups multiplication table, every column and every row must contain all the elements of the group exactly once.

6.

7. Let $g \in G$ be an element of finite order and let $N \in \mathbb{Z}$. Suppose that $g^N = e$. By Lemma 1.10, we have that $|g| \mid N$. For the converse, suppose that $|g| \mid N$. Then, $N = k|g|$ for some $k \in \mathbb{N}$. We have that $g^N = g^{k|g|} = (g^{|g|})^k = e^k = e$.

8. Let G be a finite abelian group with exactly one element $f \in G$ of order 2. For each non-trivial g with $g \neq f$, we have that g has a unique inverse in G that is not itself. If g was self inverse, then g has order 2, which is not possible. Hence, $\prod_{g \in G} g = f$.

9. Let G ve a finite group of order n with m elements of order 2. We must have that $n - m - 1$ is even as this number represents the number of elements in G that are not self inverse. As every inverse of $g \in G$ is unique for those $n - m - 1$ elements, we must have that $n - m - 1$ is even as for every g, there is a unique element $g^{-1} \in G$ that is also not of order 2. Hence, $n - m$ is odd. We deduce that if n is even, then, as $n - m$ is odd, we must have that G necessarily contains an element of order 2 as $m \geq 1$.

10.

11. Let G be a group and $g, h \in G$. Suppose g has order n and hgh^{-1} has order m. We have that $(hgh^{-1})^n = hg^nh^{-1} = heh^{-1} = hh^{-1} = e$, hence, n is a multiple of m. We have that $e = (hgh^{-1})^m = hg^mh^{-1} \implies g^m = e$. Thus, m is a multiple of n. It follows that $m = n$. Therefore, $|gh| = |h(gh)h^{-1}| = |hghh^{-1}| = |hge| = |hg|$.

12.

13. Let $G = \mathbb{Z}_8$ and $g = h = [4] \in G$. Note that G is abelian. We have that $|gh| = |[4] + [4]| = |[8]| = |[0]| = 1$, however, $|g| = |h| = |[4]| = 2$. We have $|gh| = 1$ and $\text{lcm}(|g|, |h|) = 2$.

14. Let G be a group and let $g, h \in G$ such that $gh = hg$ and $\gcd(|g|, |h|) = 1$. By Proposition 1.14, we have that $|gh|$ divides $|g||h|$. We have that $e = (gh)^{|gh||h|} = g^{|gh||h|}h^{|gh||h|} = g^{|gh||h|}$. Hence, $|g|$ divides $|gh||h|$. As $\gcd(|g|, |h|) = 1$, we have that $|g|$ divides $|gh|$. Similarly, $e = (gh)^{|gh||g|} = h^{|gh||g|}$ and so $|h|$ divides $|gh|$. It follows that $|g||h|$ divides $|gh|$. Therefore, $|gh| = |g||h|$.

15. Let G be an abelian group and let $g \in G$ be an element of G with maximal finite order. Let $h \in H$ have finite order and suppose, for contradiction, $|h|$ does not divide $|g|$. There is then a prime p such that $|g| = p^m r$ and $|h| = p^n s$ with r, s coprime to p and $m < n$. We have that the element g^{p^m} has order r and the element h^s has order p^n. As $\gcd(r, p) = 1$, we have that $\gcd(|g^{p^m}|, |h^s|) = 1$. By the previous exercise, $|g^{p^m}h^s| = |g^{p^m}||h^s| = rp^n > rp^m = |g|$, which contradicts the assumption that g has maximal finite order. Therefore, $|h|$ must divide $|g|$.

2.2 - Examples of Groups

1.

2. Let $d \leq n \in \mathbb{N}$. Let $\sigma_d \in S_n$ be a permutation such that $\sigma(i) = i + 1$ for all $i < d$, $\sigma(i) = i$ for all $i > d$ and $\sigma(d) = 1$. We have that $\sigma_d \in S_n$ is of order d.

3. Let $d \in \mathbb{N}$. Let $\sigma_d \in S_{\mathbb{N}}$ be a permutation such that $\sigma(i) = i + 1$ for all $i < d$, $\sigma(i) = i$ for all $i > d$ and $\sigma(d) = 1$. We have that $\sigma_d \in S_n$ is of order d.

4.

5.

6.

7.

8.

9. Let $n \in \mathbb{Z}$ and consider the relation on $\mathbb{Z}$ defined by $a \equiv b \mod n \iff n \mid (b-a)$. We have that $n \mid 0 = a-a$, so $a \equiv a \mod n$. Furthermore, suppose that $n \mid (b-a)$. Then, $b-a = kn$ for some k. Thus, $a-b = -kn$ and so $n \mid (a-b)$. Therefore, $a \equiv b \mod n \iff b \equiv a \mod n$. Finally, suppose that $a \equiv b \mod n$ and $b \equiv c \mod n$. We have that $n \mid (b-a)$ and $n \mid (c-b)$. We have that $b-a = kn$ and $c-b = k'n$ for some $k, k' \in \mathbb{Z}$. We have that $c-a = (b-a)+(c-b) = kn+k'n = (k+k')n$. Therefore, $n \mid c-a$ and $a \equiv c \mod n$. It follows that the relation is an equivalence relation.

10.

11. Let $n = 2k+1 \in \mathbb{Z}$ be an odd integer. We have that $(2k+1)^2 = 4k^2+4k+1 = 4(k^2+k)+1$. Let $k = 2m$ be even. Then, $k^2+k = 4m^2+2m = 2(2m^2+m)$ is divisible by 2. Let $k = 2m+1$ be odd. Then, $k^2+k = (2m+1)^2+(2m+1) = 4m^2+6m+2 = 2(2m^2+3m+1)$ is divisible by 2. Hence, $(2k+1)^2 = 4(k^2+k)+1 = 8z+1$ for some $z \in \mathbb{Z}$. It follows that $(2k+1)^2 \equiv 1 \mod 8$ for all $k \in \mathbb{Z}$.

12. Let a, b, c be non-zero integers such that $a^2+b^2 = 3c^2$. We have that $[a^2]_4 + [b^2]_4 \in \{[0]_4, [1]_4, [2]_4\} \subseteq \mathbb{Z}/4\mathbb{Z}$ as $[n^2]_4 \in \{[0]_4, [1]_4\}$ for any $n \in \mathbb{Z}$. This forces $[3c^2]_4 = [a^2] = [b^2] = [0]_4$ as $[c^2]_4$ can only take $[0]_4$ or $[1]_4$. Hence, $3c^2$ must be divisible by 4. As $\gcd(4,3) = 1$, 4 divides c^2 and so 2 divides c. Similarly, 2 divides a and b. We then have that $a/2, b/2, c/2$ are non-zero integers such that $(a/2)^2 + (b/2)^2 = 3(c/2)^2$. By induction, we have that $(a/2^n, b/2^n, c/2^n)$ are integers solutions for all integers $n > 0$. This contradicts that a, b, c are non-zero integers.

13. Let $m, n \in \mathbb{Z}$ such that $\gcd(m,n) = 1$. By Corollary 2.5, we have that there exists an $a \in \mathbb{Z}$ such that $a[m]_n = [1]_n$. Thus, $am = 1 \mod n$. By definition, $n \mid (am-1)$. Therefore, $am - 1 = bn$ for some $b \in \mathbb{Z}$ and so $am - bn = 1$. Conversely, suppose that $am + bn = 1$ for some $a, b \in \mathbb{Z}$. Suppose, for contradiction, that $k = \gcd(m,n) > 1$. Then, $m = km'$ and $n = kn'$ for integer $n' \neq 1, m' \neq 1$. We have that $1 = am+bn = k(am'+bn')$, which is a contradiction as $k > 1$ and $am' + bn' \in \mathbb{Z}$. It follows that $\gcd(m,n) = 1$.

14. Suppose $x \equiv x' \mod n$ and $y \equiv y' \mod n$. We have that $n \mid (x-x')$ and $n \mid (y-y')$. Then, $x - x' = nk$ and $y - y' = nl$ for some $k, l \in \mathbb{Z}$. We have that $xy - x'y' = xy - xy' + xy' - x'y' = x(y-y') + y'(x-x') = xnl + y'nk = n(xl + y'k)$. Hence, $n \mid (xy - x'y')$. Therefore, $xy = x'y' \mod n$.

15. Let $n > 0$ be an odd integer.

(i) Suppose that $\gcd(m,n) = 1$. Let $k = \gcd(2m+n, 2n)$. Assume $2 \mid k$. We have that $k \mid (2m+n)$ and so $2 \mid n$, which is a contradiction as n is odd. Thus, k is odd. We have that $k \mid 2n$, which is follows that $k \mid n$. Then, $k \mid (2m+n)$ implies that $k \mid m$ as k is odd. Hence, $k \mid \gcd(m,n) = 1$. It follows that $k = 1$.

(ii) Suppose $\gcd(r, 2n) = 1$. Let $k = \gcd(\frac{r+n}{2}, n)$. We have that $k \mid n$ and so $k \mid 2n$ and $2k \mid 2n$. Furthermore, $k \mid \frac{r+n}{2}$ and so $2k \mid r+n$. Thus, $2k \mid r+n-2n = r-n$. Then, $2k \mid (r-n)+(r+n) = 2r$. Hence, $k \mid r$. It follows that $k \mid \gcd(r, 2n) = 1$. Therefore, $k = 1$.

(iii) Define the map $\varphi : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/2n\mathbb{Z})^*$ by $\varphi([m]_n) = [2m+n]_{2n}$. Suppose $[x]_n = [y]_n$. Then, $x = y+kn$ for some $k \in \mathbb{Z}$. Hence, $2x+n = 2y+n+2kn$ and so $[2x+n]_{2n} = [2y+n]_{2n}$. Thus, φ is well-defined. Now, suppose $[2x+n]_{2n} = [2y+n]_{2n}$. Then, $2x+n = 2y+n+2kn$ for some $k \in \mathbb{Z}$. We then have that $x = y+kn$ and so $[x]_n = [y]_n$. Therefore, φ is injective. Finally, let $[x]_{2n} \in (\mathbb{Z}/2n\mathbb{Z})^*$. We have that $\gcd(2n, x) = 1$ and so, by the previous exercise, $\gcd(\frac{n+x}{2}, n) = 1$. Hence, $[\frac{n+x}{2}]_n \in (\mathbb{Z}/n\mathbb{Z})^*$. We have that $\varphi([\frac{n+x}{2}]_n) = [(n+x)+n]_{2n} = [x+2n]_{2n} = [x]_{2n}$. And so φ is surjective. It follows that φ is a bijection.

16. The last digit of $x \in \mathbb{Z}$ corresponds to the least residue of x in $\mathbb{Z}/10\mathbb{Z}$. We have that $1238237 \equiv 7 \mod 10$ and so $1238237^{18238456} \equiv 7^{18238456} \mod 10$. We then have that $7^2 \equiv -1 \mod 10$. Hence, $7^{18238456} = 49^{9119228} \equiv (-1)^{9119228} \mod 10 = 1 \mod 10$. Therefore, the last digit of $1238237^{18238456}$ is 1.

17. Suppose $m \equiv m' \mod n$. We set to prove $\gcd(m, n) = 1 \iff \gcd(m', n) = 1$. As $m \equiv m' \mod n \iff m' \equiv m \mod n$, it suffices to only prove one direction. Suppose that $\gcd(m, n) = 1$. Then, $am + bn = 1$ for some $a, b \in \mathbb{Z}$. As $m \equiv m' \mod n$, we have that $m = m' + kn$ for some $k \in \mathbb{Z}$. Then, $a(m' + kn) + bn = 1$. Hence, $am' + (ak + b)n = 1$. Therefore, $\gcd(m', n) = 1$.

18.

19.

2.3 - The Category Grp

1.

2.

3. Let A, B be abelian groups in Ab. Let Z be an object in Ab and $f : A \to Z, g : B \to Z$ be morphisms in Ab. We have that the following diagram commutes for some $\sigma : A \times B \to Z$ where $i_A : A \to A \times B, i_B : B \to A \times B$ are defined by $i_A(x) = (x, 0_B)$ and $i_B(x) = (0_A, x)$.

$$\begin{tikzcd}
A \arrow[dr, "i_A"] \arrow[drr, bend left, "f"] & & \\
& A \times B \arrow[r, "\sigma"] & Z \\
B \arrow[ur, "i_B"'] \arrow[urr, bend right, "g"'] & &
\end{tikzcd}$$

We have that i_A and i_B are homomorphisms as $i_A(x +_A y) = (x +_A y, 0_B) = (x, 0_B) +_{A\times B} (y, 0_B) = i_A(x) +_{A\times B} i_A(y)$ and $i_B(x' +_B y') = (0_A, x' +_B y') = (0_A, x') +_{A\times B} (0_A, y') = i_B(x') + i_B(y')$ for all $x, y \in A$ and $x', y' \in B$. As the diagram commutes, we have that $f = \sigma i_A$ and $g = \sigma i_B$. We have that $\sigma((a, 0)) = f(a)$ and $\sigma((0, b)) = g(b)$ for $a \in A$ and $b \in B$. As σ is a homomorphism, for $(x, y) \in A \times B$, we have that

$$\begin{aligned}
\sigma((x, y)) &= \sigma((x, 0_B) +_{A\times B} (0_A, y)) \\
&= \sigma((x, 0_B)) +_Z \sigma((0_A, y)) \\
&= f(x) +_Z g(y)
\end{aligned}$$

Let $\sigma : A \times B \to Z$ be defined by $\sigma((a, b)) = f(a) +_Z g(b)$. We have that for $(x, y), (x', y') \in A \times B$,

$$\begin{aligned}
\sigma((x, y) +_{A\times B} (x', y')) &= \sigma((x +_A x', y +_B y')) \\
&= f(x +_A x') +_Z g(y +_B y') \\
&= (f(x) +_Z f(x')) +_Z (g(y) +_Z g(y')) \\
&= f(x) +_Z f(x') +_Z g(y) +_Z g(y') \\
&= f(x) +_Z g(y) +_Z f(x') +_Z g(y') \\
&= (f(x) +_Z g(y)) +_Z (f(x') +_Z g(y')) \\
&= \sigma((x, y)) +_Z \sigma((x', y'))
\end{aligned}$$

Hence, σ is a homomorphism and is unique. Therefore, $A \times B$ with the maps i_A and i_B is the coproduct of A and B in Ab.

4.

5. Suppose that there exists nontrivial groups G, H such that $\mathbb{Q} \cong G \times H$. Let $f : \mathbb{Q} \to G \times H$ be an isomorphism. Let $h \in H$ be a nontrivial element in H. As f is an isomorphism, there exists a nontrivial $p/q \in \mathbb{Q}$ such that $f(p/q) = (0, h) \in G \times H$. Let $\pi_G : G \times H \to G$ be the projection onto G and let $g = \pi_G \circ f$. Then, $g(p/q) = 0$. We have that $qg(p/q) = g(p) = pg(1)$ as g is a homomorphism. The only element in $\mathbb{Q}$ with finite order is 0, hence, $g(1) = 0$. Let $m/n \in \mathbb{Q}$, it follows that $ng(m/n) = g(m) = mg(1) = 0$, and so $g(m/n) = 0$. g is then the zero map, which means $G \times \{0\} \subseteq \ker f$. This is a contradiction as f is an isomorphism. Therefore, $\mathbb{Q}$ cannot be written as the direct product of two nontrivial groups.

6. Suppose S_3 is the coproduct of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$. Define $f : \mathbb{Z}/2\mathbb{Z} \to S_3$ by $f([0]_2) = \text{id}$ and $f([1]_2) = (1\ 2)$. Define $g : \mathbb{Z}/3\mathbb{Z} \to S_3$ by $g([0]_3) = \text{id}$,$g([1]_3) = (1\ 2\ 3)$ and $g([2]_3) = (1\ 3\ 2)$. We have that the following diagram commutes for some homomorphisms σ, i_2, i_3.

$$\begin{tikzcd}
\mathbb{Z}/2\mathbb{Z} \arrow[dr, "i_A"] \arrow[drr, bend left, "f"] & & \\
& \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \arrow[r, "\sigma"] & S_3 \\
\mathbb{Z}/3\mathbb{Z} \arrow[ur, "i_B"] \arrow[urr, bend right, "g"'] & &
\end{tikzcd}$$

We have that

$$\begin{aligned}
(1\ 3) &= (1\ 2\ 3)(1\ 2) \\
&= g([1]_3)f([1]_2) \\
&= \sigma(i_B([1]_3))\sigma(i_A([1]_2)) \\
&= \sigma(i_B([1]_3) + i_A([1]_2)) \\
&= \sigma(i_A([1]_2) + i_B([1]_3)) \\
&= \sigma(i_A([1]_2))\sigma(i_B([1]_3)) \\
&= f([1]_2)g([1]_3) \\
&= (1\ 2)(1\ 2\ 3) \\
&= (2\ 3)
\end{aligned}$$

as $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is abelian. Hence, such a commutative diagram cannot exist. Therefore, S_3 is not the coproduct of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.

7.

8. Let G be a group defined by two generators x, y subject only to the relations $x^2 = 1_G$ and $y^3 = 1_G$. Let Z be an object in Ab and let $f : \mathbb{Z}/2\mathbb{Z} \to Z, g : \mathbb{Z}/3\mathbb{Z} \to Z$ be morphisms. Let $\sigma : G \to Z$ be a homomorphism such that $\sigma(x) = f([1]_2)$ and $\sigma(y) = g([1]_3)$. We have that for any $w \in G$, $\sigma(w) = \sigma(\prod_{i=1}^{k} x_i^{n_i}) = \prod_{i=1}^{k} \sigma(x_i)^{n_i} = \prod_{i=1}^{k} \sigma(x_i)^{n_i}$ where $x_i \in \{x, y\}, n_i \in \mathbb{Z}, k \in \mathbb{N}$ and w is generated by x, y and σ is a homomorphism. We have that each w has a unique output as $\sigma(x_i)$ is uniquely determined by x_i. Hence, σ is unique. We have that the following diagram commutes

$$\begin{tikzcd}
\mathbb{Z}/2\mathbb{Z} \arrow[dr, "i_2"'] \arrow[drr, bend left, "f"] & & \\
& G \arrow[r, "\sigma"] & Z \\
\mathbb{Z}/3\mathbb{Z} \arrow[ur, "i_3"] \arrow[urr, bend right, "g"'] & &
\end{tikzcd}$$

where $i_2([n]_2) = x^n$ and $i_3([n]_3) = y^n$. We have that $f = \sigma i_2$ and $g = \sigma i_3$. We have that $\sigma(x) = f([1]_2)$ and $\sigma(y) = g([1]_3)$. It follows σ in the diagram and G is the coproduct of $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$.

9. Not Done Let A, B be abelian groups and $\alpha : A \to C, \beta : B \to C$ be morphisms in Ab. Let $E = \{(x, y) \in A \times B \mid \alpha(x) = \beta(y)\}$ with a binary operation, $+_E$, inherited from $A \times B$. We note that $+_E$ is an associative and commutative operation as $+_{A\times B}$ is associative and commutative. We have that $(0_A, 0_B) \in E$ as $\alpha(0_A) = 0_C = \beta(0_B)$ as α, β are homomorphisms. Let $(x, y) \in E$. Then, $\alpha(-x) = -\alpha(x) = -\beta(y) = -\beta(-y)$. Hence, $(-x, -y) \in E$. It follows that E is an abelian group. We note that for each $(x, y) \in E$, $(\alpha\circ\pi_A)((x, y)) = \alpha(x) = \beta(y) = (\beta\circ\pi_B)((x, y))$. Let Z be an abelian group and let $f : Z \to A$ and $g : Z \to B$ be morphisms in Ab such that $\alpha f = \beta g$. We have that the following diagram commutes

$$\begin{tikzcd}
 & & A \arrow[dr, "\alpha"] & \\
Z \arrow[rru, bend left, "f"] \arrow[r, "\sigma"] \arrow[rrd, bend right, "g"'] & E \arrow[ur, "\pi_A"] \arrow[dr, "\pi_B"] & & C \\
 & & B \arrow[ur, "\beta"'] &
\end{tikzcd}$$

As the diagram commutes, $f = \pi_A\sigma$ and $g = \pi_B\sigma$, hence, $\sigma(x) = (f(x), g(x))$. By assumption, $\alpha f = \beta g$, thus, $\sigma(x) \in E$ for all $x \in Z$. Hence, σ is well-defined. It follows that fiber products exist in Ab.

2.4 - Group Homomorphisms

1.

2.

3. Suppose that G is a group of order n such that G contains an element $g \in G$ such that g has order n. We verify $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ defined by $\varphi([x]_n) = g^x$ is an isomorphism. We have that for $[x]_n, [y]_n \in \mathbb{Z}/n\mathbb{Z}$, $\varphi([x]_n + [y]_n) = \varphi([x + y]_n) = g^{x+y} = g^x g^y = \varphi([x]_n)\varphi([y]_n)$. Furthermore, suppose $\varphi([x]_n) = \varphi([y]_n)$. Then, $g^x = g^y$ and so $g^{x-y} = 1_G$. We must have that the order of $g \in G$ divides $x - y$ so $n \mid x - y$. Therefore, $[x]_n = [y]_n$. Finally, let $h \in G$. Suppose there did not exist an $[x]_n \in \mathbb{Z}/n\mathbb{Z}$ such that $\varphi([x]_n) = h$. Hence, $g^x = h$ does not hold for any $x \in \mathbb{Z}$. This leads to contradiction as G would not contain n elements as $\langle g\rangle = \{1_G, g, g^2, ..., g^{n-1}\} \subseteq G$. It follows that φ must be an isomorphism. For the converse, suppose that G is a group of order n that is isomorphic to $\mathbb{Z}$. We have that there exists an isomorphism $\psi : \mathbb{Z}/n\mathbb{Z} \to G$. We have that $[1]_n \in \mathbb{Z}/n\mathbb{Z}$ has order n. Then, $\psi([1]_n) \in G$ will also be of order n by Proposition 4.8. Hence, G contains an element of order n.

4.

5. Suppose, for contradiction, there exists an isomorphism $\varphi : (\mathbb{C} - \{0\}, \cdot) \to (\mathbb{R} - \{0\}, \cdot)$. We have that i has order 4 in $(\mathbb{C} - \{0\}, \cdot)$ and so $\varphi(i)$ must have order 4 in $(\mathbb{R} - \{0\}, \cdot)$. There must exist an $x \in (\mathbb{R} - \{0\}, \cdot)$ such that $|x| = 4$. Such an x must be a solution to the equation $x^4 = 1$, however, the only solutions in $\mathbb{R}$ to the equation are 1 and -1, which have order 1 and 2, respectively. As such an x cannot exist, we have a contradiction. Therefore, an isomorphism between $(\mathbb{C} - \{0\}, \cdot)$ and $(\mathbb{R} - \{0\}, \cdot)$ cannot exist.

6.

7. Let G be a group and define $\varphi : G \to G$ by $\varphi(g) = g^{-1}$. Suppose that φ is a homomorphism. Then, for each $x, y \in G$, we have that

$$y^{-1}x^{-1} = (xy)^{-1} = \varphi(xy) = \varphi(x)\varphi(y) = x^{-1}y^{-1}$$

It follows that $xy = yx$. Hence, G is abelian. For the converse, suppose that G is abelian. We have that for each $x, y \in G$,

$$\varphi(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1} = \varphi(x)\varphi(y)$$

Hence, φ is a homomorphism. Now, define $\psi : G \to G$ by $\psi(g) = g^2$. Suppose ψ is a homomorphism. Then, for $x, y \in G$

$$xyxy = (xy)^2 = \psi(xy) = \psi(x)\psi(y) = x^2y^2$$

It follows that $xy = yx$. For the converse, suppose that G is abelian. Then, for $x, y \in G$,

$$\psi(xy) = (xy)^2 = xyxy = xxyy = x^2y^2 = \psi(x)\psi(y)$$

Therefore, ψ is a homomorphism.

8. Let G be a group and $g \in G$. Define $\gamma_g : G \to G$ by $\gamma_g(x) = gxg^{-1}$. Suppose $\gamma_g(x) = \gamma_g(y)$ for some $x, y \in G$. Then, $gxg^{-1} = gyg^{-1}$ and so $x = y$. We also have that for each $x \in G$, $\gamma_g(g^{-1}xg) = g(g^{-1}xg)g^{-1} = gg^{-1}xgg^{-1} = 1x1 = x$. It follows γ_g is bijective. Furthermore, for $x, y \in G$, we have that $\gamma_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \gamma_g(x)\gamma_g(y)$. Hence, γ_g is a homomorphism. Therefore, $\gamma_g(y)$ is an automorphism. Define the function $\psi : G \to \mathrm{Aut}_{\mathsf{Grp}}(G)$ by $\psi(g) = \gamma_g$. For $g, g' \in G$, we have that $\psi(gg')[x] = \gamma_{gg'}[x] = gg'x(gg')^{-1} = gg'xg'^{-1}g = (\gamma_g \circ \gamma_{g'})[x] = (\psi(g) \circ \psi(g'))[x]$. Hence, ψ is a homomorphism. Suppose ψ is trivial. We have that for each $x, g \in G$, $\psi(g)[x] = \mathrm{id}[x]$ and so $gxg^{-1} = x$. It follows that $gx = xg$ and so G is abelian. For the converse, suppose that G is abelian. Then, for each $x, g \in G$, $\psi(g)[x] = \gamma_g(x) = gxg^{-1} = xgg^{-1} = x1 = x$. Hence, ψ is trivial.

9. Let $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$. Let k be the order of $([1]_m, [1]_n) \in \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. Then, $([0]_m, [0]_n) = k([1]_m, [1]_n) = ([k]_m, [k]_n)$. Hence, $m \mid k$ and $n \mid k$. As $\gcd(m, n) = 1$, we have that $mn \mid k$. As $mn([1]_m, [1]_n) = ([mn]_m, [mn]_n) = ([0]_m, [0]_n)$, it follows that $k = mn$. As $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ contains an element of order mn and is also of order mn, $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}/mn\mathbb{Z}$.

10.

11.

12. Suppose $x^3 - 9 = 0$ has a solution, c, in $\mathbb{Z}/31\mathbb{Z}$. We have that $c^3 = 9$ and so $[c]_{31}^3 = [9]_{31}$. Note the order of $[9]_{31}$ in $(\mathbb{Z}/31\mathbb{Z})^*$ is 15. We have that $[1]_{31} = [c]_{31}^{30} = [9]_{31}^{10}$, which contradicts the fact that the order of $[9]_{31}$ is 15. Hence, such a c cannot exist.

13. Let $V = \{1, a, b, c\}$ be the Klein four-group. There are exactly 6 distinct bijection set-functions from V to V that fix 1. Let $f : V \to V$ be such a function. We have that $f(a), f(b), f(c)$ are unqiue by assumption. Then, if $x, y \in V$ such that $x \neq y$ and $x \neq 1, y \neq 1$, we have that $f(xy) = f(x)f(y)$. We also have that $f(x1) = f(x) = f(x)1 = f(x)f(1)$. This suffices to show f is a homomorphism as V is abelian. It follows that each f is an isomorphism and so $\mathrm{Aut}_{\mathsf{Grp}}(V)$ has 6 elements. We have that each $f \in \mathrm{Aut}_{\mathsf{Grp}}(V)$ corresponds to a different permutation on a 3-set and an isomorphism between $\mathrm{Aut}_{\mathsf{Grp}}(V)$ and S_3 is trivial.

14. Let $\varphi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be a homomorphism. For each $[x]_n \in \mathbb{Z}/n\mathbb{Z}$, $\varphi([x]_n) = \varphi(x[1]_n) = x\varphi([1]_n)$. Hence, φ is uniquely determined by where $[1]_n$ is mapped. Suppose $\varphi([1]_n) = [m]_n$ where $\gcd(m, n) = 1$. Let $[x]_n, [y]_n \in \mathbb{Z}/n\mathbb{Z}$ such that $\varphi([x]_n) = \varphi([y]_n)$. Then, $\varphi([x-y]_n) = [0]_n$ and so $(x-y)[m]_n = [0]_n$. We have that $n \mid m(x-y)$. As $\gcd(m, n) = 1$, $n \mid x - y$ and so $[x]_n = [y]_n$. It follows that φ is bijective, hence, an automorphism. Now suppose that $\varphi([1]_n) = [m]_n$ where $\gcd(m, n) > 1$. Assume, for contradiction, that φ is an isomorphism, then, $n = |[1]_n| = |\varphi([1]_n)| = |[m]_n| = \frac{n}{\gcd(m,n)} < n$. Therefore, φ cannot be an isomorphism. It follows that $|\mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/n\mathbb{Z})| = \phi(n)$.

15.

16.

17.

18. Let $\varphi : G \to H$ be an isomorphism in of groups G and H. Suppose G is abelian. Let $h, h' \in H$. As φ is an isomorphism, there are elements $g, g' \in G$ such that $\varphi(g) = h$ and $\varphi(g) = h'$. We have that

$$hh' = \varphi(g)\varphi(g') = \varphi(gg') = \varphi(g'g) = \varphi(g')\varphi(g) = h'h$$

Therefore, H is abelian. For the converse, suppose H is abelian. We have that $\varphi^{-1} : H \to G$ exists and is an isomorphism. With the same argument, we can deduce G is abelian.

2.5 - Free Groups

1. Let A be a set and let $\mathscr{F}^A$ be a category where $\mathsf{obj}(\mathscr{F}^A)$ are pairs (j, G), where G is a group and $j : A \to G$ is a set function from A to G and morphisms $(j_1, G_1) \to (j_2, G_2)$ are commutative diagrams

$$\begin{tikzcd} G_1 \arrow[r, "\varphi"] & G_2 \\ A \arrow[u, "j_1"] \arrow[ur, "j_2"'] & \end{tikzcd}$$

where φ is a group homomophism. Let E be the trivial group and i the identity map. We have that a morphism $(j, G) \to (i, E)$ is the commutative diagram

$$\begin{tikzcd} G \arrow[r, "\varphi"] & E \\ A \arrow[u, "j"] \arrow[ur, "i"'] & \end{tikzcd}$$

We have that φ must be the identity homomorphism as it is a homomorphism to the trivial group. Therefore, $\mathsf{Hom}_{\mathscr{F}^A}((j, G), (i, E))$ is singleton. We have that $\mathscr{F}^A$ has final objects.

2.

3. Let A be a set and $F(A)$ be the free group associated with A. We have that there is a unique homomorphism such that the following diagram commutes

$$\begin{tikzcd} F(A) \arrow[r, "\varphi"] & F(A) \\ A \arrow[u, "j"] \arrow[ur, "i"'] & \end{tikzcd}$$

where i is the inclusion map. Let $x, y \in A$ such that $j(x) = j(y)$. We note that $\varphi \circ j = i$, hence,

$$x = i(x) = (\varphi \circ j)(x) = \varphi(j(x)) = \varphi(j(y)) = (\varphi \circ j)(y) = i(y) = y$$

Therefore, j is injective

4.

5. Let H be an abelian group and A be a set. Define

$$H^{\oplus A} = \{\alpha : A \to H \mid \alpha(x) \neq 0_H \text{ for finitely many elements } x \in A\}$$

with the binary operation, $+$, inherited from H^A. We first note $+$ is an associative operation on $H^{\oplus A}$ as H^A is a group. Let $\alpha \in H^{\oplus A}$. Then, $\alpha(x) \neq 0_H$ for finitely many elements $x \in A$. It then follows that $-\alpha(x) \neq 0_H$ for finitely many $x \in A$. Let $i : A \to H$ be a map defined by $i(x) = 0_H$ for all $x \in A$. We have that $i(x) \neq 0_H$ for no $x \in A$. Therefore, $i \in H^{\oplus A}$. Suppose that A is a finite set. Then, if $\alpha : A \to H$ is a set function in H^A, we must have that $\alpha \in H^{\oplus A}$. And so $H^{\oplus A} = H^A$. Now, suppose that A is an infinite set. Let $\alpha, \beta : A \to H$ be elements of $H^{\oplus A}$. Suppose, for contradiction, that $\alpha(x) + \beta(x) \neq 0_H$ for infinitely many $x \in A$. We then have that $\alpha(x) \neq \beta(x)$ for infinitely many $x \in A$. However, $\alpha(x) \neq 0_H$ for finitely many $x \in A$ and $\beta(x) \neq 0_H$ for finitely many $x \in A$. Necessarily, $\alpha(x) = \beta(x)$ for infinitely many $x \in A$. Hence, $\alpha(x) + \beta(x) \neq 0_H$ for finitely many $x \in A$. Therefore, $\alpha + \beta \in H^{\oplus A}$. It follows that $H^{\oplus A}$ is a group.

6.

7.

8. **NOT DONE** Let A, B be sets and let $A \amalg B$ be their coproduct. Denote the free group associated with a set S by $F(S)$. Using the universal property for free groups, there is a $j_A, j_B, j_{A\amalg B}$ such that for any pair of groups G_1, G_2, G_3 and set functions $f : A \to G_1, g : B \to G_2, h : A \amalg B \to G_3$, there exists unique $\varphi_1, \varphi_2, \varphi_3$ such that the following diagrams commute

$$\begin{tikzcd} F(A) \arrow[r, "\varphi_1"] & G_1 \\ A \arrow[u, "j_A"] \arrow[ur, "f"'] & \end{tikzcd} \qquad \begin{tikzcd} F(B) \arrow[r, "\varphi_2"] & G_2 \\ B \arrow[u, "j_B"] \arrow[ur, "g"'] & \end{tikzcd} \qquad \begin{tikzcd} F(A \amalg B) \arrow[r, "\varphi_3"] & G_3 \\ A \amalg B \arrow[u, "j_{A\amalg B}"] \arrow[ur, "h"'] & \end{tikzcd}$$

Using the universal property for coproducts, there are $i_A : A \to A \amalg B, i_B : B \to A \amalg B$ such that for any set Z and pair of set functions $f : A \to Z, g : B \to Z$, there is a unique φ such that the following diagram commutes

$$\begin{tikzcd} A \arrow[dr, "i_A"] \arrow[drr, bend left, "f"] & & \\ & A \amalg B \arrow[r, "\varphi"] & Z \\ B \arrow[ur, "i_B"'] \arrow[urr, bend right, "g"'] & & \end{tikzcd}$$

There then exists unique homomorphisms $i_{F(A)}, i_{F(B)}$ such that the following diagrams commute

$$\begin{tikzcd} F(A) \arrow[rr, "i_{F(A)}"] & & F(A \amalg B) \\ & A \amalg B \arrow[ur, "j_{A\amalg B}"'] & \\ A \arrow[uu, "j_A"] \arrow[ur, "i_A"'] & & \end{tikzcd} \qquad \begin{tikzcd} F(B) \arrow[rr, "i_{F(B)}"] & & F(A \amalg B) \\ & A \amalg B \arrow[ur, "j_{A\amalg B}"'] & \\ B \arrow[uu, "j_B"] \arrow[ur, "i_B"'] & & \end{tikzcd}$$

We then have that the following diagram commutes

$$\begin{tikzcd} A \arrow[rr, "j_A"'] \arrow[dr, "i_A"'] & & F(A) \arrow[dr, "i_{F(A)}"] & \\ & A \amalg B \arrow[rr, "j_{A\amalg B}"] & & F(A \amalg B) \\ B \arrow[rr, "j_B"] \arrow[ur, "i_B"] & & F(B) \arrow[ur, "i_{F(B)}"'] & \end{tikzcd}$$

Let G be a group and $f : F(A) \to G, g : F(B) \to G$ be homomorphisms.

$$\begin{tikzcd} A \arrow[rr, "j_A"'] \arrow[dr, "i_A"'] & & F(A) \arrow[dr, "i_{F(A)}"] \arrow[drr, bend left, "f"] & & \\ & A \amalg B \arrow[rr, "j_{A\amalg B}"] & & F(A \amalg B) \arrow[r, "\psi"] & G \\ B \arrow[rr, "j_B"] \arrow[ur, "i_B"] & & F(B) \arrow[ur, "i_{F(B)}"'] \arrow[urr, bend right, "g"'] & & \end{tikzcd}$$

9.

10. Let A be a set and let $F = F^{\mathrm{ab}}(A)$. Define an equivalence relation on F by setting $f \sim f'$ if and only if $f - f' = 2g$ for some $g \in F$. By Proposition 5.6, we have that $F \cong \mathbb{Z}^{\oplus A}$. Let $\mathbf{x}, \mathbf{y} \in F$. We have that

$\mathbf{x} = \sum_{a \in A} m_a j_a, \mathbf{y} = \sum_{a \in A} n_a j_a$ where $m_a, n_a \in \mathbb{Z}$ and is non-zero for finite $a \in A$ and $j_a(x) = 1$ where $x = a$ and $j_a(x) = 0$ otherwise. Then,

$$\begin{aligned}
\mathbf{x} \sim \mathbf{y} &\iff \exists g \in F,\ \mathbf{x} - \mathbf{y} = 2g \\
&\iff \forall a \in A, \exists k_a \in \mathbb{Z},\ \sum_{a \in A} m_a j_a - \sum_{a \in A} n_a j_a = 2 \sum_{a \in A} k_a j_a \\
&\iff \forall a \in A, \exists k_a \in \mathbb{Z},\ \sum_{a \in A} (m_a - n_a) j_a = 2 \sum_{a \in A} k_a j_a \\
&\iff \forall a \in A,\ 2 \mid (m_a - n_a)
\end{aligned}$$

Let $\mathfrak{C} = \{[\sum_{a \in A} \delta_a j_a]_\sim \mid \delta_a \in \{0,1\}$ and $\delta_a \neq 0$ for finitely many $a \in A\}$. Let $\mathbf{x} \in F$. Then, $\mathbf{x} = \sum_{a \in A} m_a j_a$. Let $\mathbf{x}' = \sum_{a \in A} m'_a j_a$ where m'_a is the least residue of m_a modulo 2. We have $\mathbf{x} \sim \mathbf{x}'$ and $\mathbf{x} \in [\mathbf{x}']_\sim \in \mathfrak{C}$. Let $[\mathbf{x}]_\sim, [\mathbf{y}]_\sim \in \mathfrak{C}$ such that there exists $\mathbf{z} \in [\mathbf{x}]_\sim \cap [\mathbf{y}]_\sim$. Let $\mathbf{x} = \sum_{a \in A} x_a j_a, \mathbf{y} = \sum_{a \in A} y_a j_a$ and $\mathbf{z} = \sum_{a \in A} z_a j_a$. Then, $2 \mid (x_a - z_a)$ and $2 \mid (z_a - y_a)$ and so $2 \mid (x_a - y_a)$. Therefore, $[\mathbf{x}]_\sim = [\mathbf{y}]_\sim$. It follows that $\mathfrak{C}$ is a disjoint partition of F and so $\mathfrak{C} = F/\sim$. It is also clear that $|F/\sim| = 2^{|A|}$ and so $F/\sim$ is finite if and only if A is finite. Now suppose that $F^{\text{ab}}(A) \cong F^{\text{ab}}(B)$ and that A is finite. We then have that $F^{\text{ab}}(A)/\sim$ is finite with $2^{|A|}$ elements. We then have that $F^{\text{ab}}(B)/\sim$ is finite with $2^{|A|}$ elements and so $F^{\text{ab}}(B)$ is finite. We then have that $2^{|A|} = 2^{|B|}$, hence, $|A| = |B|$.

2.6 - Subgroups

1.

2.

3.

4. Let G be a group. Let $\epsilon_g : \mathbb{Z} \to G$ be the exponential map. Suppose g has order n. Define $\varphi : \epsilon_g(\mathbb{Z}) \to \mathbb{Z}/n\mathbb{Z}$ by $\varphi(g^k) = [k]_n$. Suppose $g^k = g^{k'}$. Then, $n \mid k - k'$. We then have that $\varphi(g^k) = [k]_n = [k']_n = \varphi(g^{k'})$. We also have that $\varphi(g^x g^y) = \varphi(g^{x+y}) = [x+y]_n = [x]_n + [y]_n = \varphi(g^x) + \varphi(g^y)$ and for any $[k]_n \in \mathbb{Z}/n\mathbb{Z}$, $\varphi(g^k) = [k]_n$. It follows that φ is an isomorphism. Hence, $\epsilon_g(\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$. Now suppose g has infinite order. Define $\varphi : \epsilon_g(\mathbb{Z}) \to \mathbb{Z}$ by $\varphi(g^k) = k$. We have that φ is an isomorphism and $\epsilon_g(\mathbb{Z}) \cong \mathbb{Z}$.

5. Let $\varphi : G \to G'$ be a homomorphism. Let H be a subgroup of G. Let $x, y \in \varphi(H)$. We have that there are x', y' such that $\varphi(x') = x$ and $\varphi(y') = y$ where $x', y' \in H$. We have that $x'y'^{-1} \in H$ and then $xy^{-1} = \varphi(x')\varphi(y')^{-1} = \varphi(x')\varphi(y'^{-1}) = \varphi(x'y'^{-1}) \in \varphi(H)$. Therefore, $\varphi(H)$ is a subgroup of G'. Let $n > 0$ be an integer. Define $\psi : G \to G$ by $\psi(x) = x^n$. We have that $\text{im } G = \{g^n \mid g \in G\}$ and so $\{g^n \mid g \in G\}$ is a subgroup of G.

6. Let H, H' be subgroups of G. Suppose that $H \subseteq H'$ or $H' \subseteq H$, then $H \cup H' = H$ or $H \cup H' = H'$, which are both subgroups of G in either case. For the converse, suppose that $H \cup H'$ is a subgroup of G. Assume, for contradiction, that H is not contained fully in H' and H' is not contained fully in H. Then, there exists $x \in H - H'$ and $y \in H' - H$. We have that $xy \in H \cup H'$ and so $xy \in H'$ or $xy \in H$. We have that $x^{-1} \in H$ as $x \in H$ and we also have that $y^{-1} \in H'$ as $y \in H'$. If $xy \in H$, then $y = x^{-1}xy \in H$ and if $xy \in H'$, then $x = xyy^{-1} \in H'$. In both cases, we lead to contradiction. It follows that $H \subseteq H'$ or $H' \subseteq H$. Now, let $H_1 \subseteq H_2 \subseteq ...$ be subgroups of a group G. Let $x, y \in H = \bigcup_{i \in \mathbb{N}} H_i$. Then, $x \in H_n$ and $y \in H_m$ for some $n, m \in \mathbb{N}$. Without loss of generality, assume $n \geq m$. Then, $x, y \in H_n$ as $H_m \subseteq H_n$. As H_n is a subgroup of G, we have that $xy^{-1} \in H_n$. Therefore, $xy^{-1} \in H$. We must have that H is a subgroup of G.

7. Let $\gamma_g, \gamma_h \in \text{Inn}(G)$. We have that $(\gamma_g \circ \gamma_h)(x) = \gamma_g(\gamma_h(x)) = \gamma_g(hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh)^{-1} = \gamma_{gh}(x) \in \text{Inn}(G)$. We have that the inverse of γ_g is $\gamma_{g^{-1}}$ as $(\gamma_g \circ \gamma_{g^{-1}})(x) = gg^{-1}xgg^{-1} = x = \text{id}$ and $\gamma_{g^{-1}} \in \text{Inn}(G)$. Then, $\text{Inn}(G)$ is a subgroup of $\text{Aut}(G)$. Suppose that $\text{Inn}(G)$ is cyclic. There then exists an $a \in G$ such that for any $g \in G$ such that $\gamma_g = \gamma_a^n$ for some $n \in \mathbb{N}$. Then, for any $x \in G$, $gxg^{-1} = a^n x a^{-n}$. We then have that $gag^{-1} = a$. We then have that $\gamma_g(x) = \gamma_a^n(x) = a^n x a^{-n} = x = \text{id}$. Therefore, any inner automorphism of G is trivial and so $\text{Inn}(G)$ is trivial. As $\text{Inn}(G)$ is trivial, we have that $\gamma_g = \text{id}$ for all $g \in G$. Let $x, y \in G$. Then, $\gamma_x(y) = y$ and so $xyx^{-1} = y$. Hence, $xy = yx$ and so G is abelian. Suppose G is abelian. Then, for any $g \in G$, we have that $\gamma_g(x) = gxg^{-1} = xgg^{-1} = x = \text{id}$. Then, $\text{Inn}(G)$ is trivial, and thus cyclic. It follows that $\text{Inn}(G)$ is cyclic if and only if $\text{Inn}(G)$ is trivial if and only if G is abelian. Finally, assume $\text{Aut}(G)$ is cyclic. Then, as $\text{Inn}(G)$ is a subgroup of $\text{Aut}(G)$, $\text{Inn}(G)$ is cyclic. Hence, G is abelian.

8. Let G be an abelian group. Suppose that G is finitely generated. Then, $G = \langle A \rangle$ where A is a finite set, $A = \{a_1, ..., a_n\}$ say. Define $\varphi : \mathbb{Z}^{\oplus n} \to G$ by $\varphi(\mathbf{x}) = a_1^{x_1} ... a_n^{x_n}$. We have that φ is surjective as G is generated by A. Let $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^{\oplus n}$. We have that $\varphi(\mathbf{x} + \mathbf{y}) = a_1^{x_1+y_1} ... a_n^{x_n+y_n} = a_1^{x_1} a_1^{y_1} ... a_n^{x_n} a_n^{y_n} = a_1^{x_1} ... a_n^{x_n} a_1^{y_1} ... a_n^{y_n} = \varphi(\mathbf{x})\varphi(\mathbf{y})$. Hence, φ is a homomorphism. Therefore, there exists a surjective homomorphism $\varphi : \mathbb{Z}^{\oplus n} \to G$. For the converse, suppose there exists a surjective homomorphism $\psi : \mathbb{Z}^{\oplus n} \to G$. Let $g \in G$. Then, $g = \psi(\mathbf{x})$ for some $\mathbf{x} \in \mathbb{Z}^{\oplus n}$. As ψ is a homomorphism, we have that $g = \sum_{i=1}^n x_i(\psi \circ j_i)$ where $j_i = (0, ..., 1, ..., 0)$ where 1 is placed in the ith place. We claim G is generated by the set $A = \{\varphi \circ j_i \mid i \in [n]\}$. Trivially, we have $\langle A \rangle$ is a subgroup of G. Let $g \in G$. By before, $g = \sum_{i=1}^n x_i(\psi \circ j_i)$, and so G is contained in $\langle A \rangle$. It follows that G is finitely generated.

9. Let $\langle A \rangle$ be a finitely generated subgroup of the additive group $\mathbb{Q}$. There exists a surjective homomorphism $\varphi : \mathbb{Z}^{\oplus n} \to \langle A \rangle$ for some $n \in \mathbb{N}$ as $\mathbb{Q}$ is abelian, so $\langle A \rangle$ is abelian. For each $a \in \langle A \rangle$, there is an $\mathbf{x} \in \mathbb{Z}^{\oplus n}$ such that $\varphi(\mathbf{x}) = a$. Then, $a = \varphi(\mathbf{x}) = \sum_{i=1}^n x_i \varphi(j_i) = \sum_{i=1}^n x_i \frac{a_i}{b_i}$ where $a_i \in \mathbb{Z}$ and $b_i \in \mathbb{N}$. Then, $a = \frac{k}{b_1 ... b_n}$ for some $k \in \mathbb{Z}$. We have that $a \in \langle g \rangle$ where $g = \frac{1}{b_1 ... b_n}$. Thus, $\langle A \rangle$ is cyclic as a subgroup of a cyclic group. It follows $\mathbb{Q}$ is not finitely generated as $\mathbb{Q}$ is not cyclic.

10.

11.

12. Let $m, n \in \mathbb{Z}$ and $d = \gcd(m, n)$. Let $kd \in d\mathbb{Z}$. We have that $m = m'd$ and $n = n'd$ and $\gcd(m, n) = \gcd(m'd, n'd) = d \gcd(m', n')$, hence, $\gcd(m', n') = 1$. There then exists $x, y \in \mathbb{Z}$ such that $xm' + yn' = 1$ and so $xm + yn = d$. Then, $kd = kxm + kyn \in \langle m, n \rangle$. Let $x \in \langle m, n \rangle$. We have that $x = pm + qn = d(pm' + qn') \in d\mathbb{Z}$ for some $p, q \in \mathbb{Z}$. Therefore, $d\mathbb{Z} = \langle m, n \rangle$.

13.

14.

15. Let $\varphi : G \to G'$ be a group homomorphism such that there exists a group homomorphism $\psi : G' \to G$ with $\psi \circ \varphi = \text{id}_G$. Let $x \in \ker \varphi$. We have that $\varphi(x) = 1_{G'}$. Then, $1_G = \psi(1_{G'}) = \psi(\varphi(x)) = (\psi \circ \varphi)(x) = \text{id}_G(x) = x$. It follows that $\ker \varphi$ is trivial. By Proposition 6.12, φ is a monomorphism.

16.

2.7 - Quotient Groups

1.

2. Define a homomorphism $\varphi : \mathbb{Z}/2\mathbb{Z} \to S_3$ by $\varphi([0]_2) = \text{id}$ and $\varphi([1]_2) = (1\ 2)$. We have that $\varphi(\mathbb{Z}/2\mathbb{Z})$ is not normal in S_3 as $(1\ 3)(1\ 2)(1\ 3)^{-1} = (2\ 3) \notin \varphi(\mathbb{Z}/2\mathbb{Z})$. Hence, the image of a homomorphism is not necessarily normal.

3. Let G be a group and N a subgroup such that $gng^{-1} \in N$ for all $g \in G$ and $n \in N$. Let $g \in G$ and $x \in gNg^{-1}$. Then, $x = gng^{-1}$ for some $n \in N$. By assumption, $x = gng^{-1} \in N$. It follows that $gNg^{-1} \subseteq N$. Let $x \in N$. For all $g \in G$, we have that $x = gg^{-1}xgg^{-1} \in gNg^{-1}$. Then, $N \subseteq gNg^{-1}$ for any $g \in G$. It follows that $gNg^{-1} = N$. Now let $x \in gN$. We have that $x = gn$ for some $n \in N$. As $N = g^{-1}Ng$, we have that $n = g^{-1}n'g$ for some $n' \in N$. Then, $x = gn = gg^{-1}n'g = n'g \in Ng$. Let $y \in Ng$. Then, $y = ng$ for some $n \in N$. As $N = gNg^{-1}$, we have that $n = gn'g^{-1}$ for some $n' \in N$. Hence, $y = ng = gn'g^{-1}g = gn' \in gN$. It follows that $gN = Ng$. Let $n \in N$ and $g \in G$. As $gN = Ng$, we have that $gn = n'g$ for some $n' \in N$. Then, $gng^{-1} = n'gg^{-1} = n' \in N$. It follows that every definition of normal subgroups are equivalent.

4. Let $F = F^{\text{ab}}(A)$ where A is a set. Define a relation $\sim$ on F by $f \sim f'$ if and only if $f - f' = 2g$ for some $g \in F$. Let $x \in F$ and suppose that $f \sim f'$. There then exists a $g \in F$ such that $f - f' = 2g$. We then have that $2g = f - f' = f + 0_F - f' = (f - x) + (x - f')$. Hence, $f + x \sim f' + x$. We have that $\sim$ is compatible with the group structure. By previous exercises, its clear that $F/\sim \cong (\mathbb{Z}/2\mathbb{Z})^{\oplus A}$.

5.

6. Let G be an abelian group. Let $n \in \mathbb{N}$ and define a relation $\sim$ on G by $a \sim b$ if and only if $ab^{-1} = g^n$ for some $g \in G$. For any $a \in G$, we have that $a \sim a$ as $aa^{-1} = 1_G = 1_G^n$. Suppose now $a \sim b$. Then, $ab^{-1} = g^n$ for some $g \in G$. We have that $ba^{-1} = (ab^{-1})^{-1} = (g^n)^{-1} = (g^{-1})^n$. As $g^{-1} \in G$, we have that $b \sim a$. Suppose that $a \sim b$ and $b \sim c$. Then, $ab^{-1} = g^n$ and $bc^{-1} = h^n$ for some $g, h \in G$. Then, $ac^{-1} = ab^{-1}bc^{-1} = g^n h^n = (gh)^n$ as G is abelian. Thus, $a \sim c$. Assume $a \sim b$ and let $x \in G$. Then, $ab^{-1} = g^n$ for some $g \in G$. We have that $g^n = ab^{-1} = axx^{-1}b^{-1} = (ax)(bx)^{-1}$. Therefore, $ax \sim bx$. By Proposition 7.4, the equivalence class of 1_G, $[1_G]_\sim$ is a subgroup of G. We claim $[1_G]_\sim = A = \{g^n \mid g \in G\}$. Let $x \in [1_G]_\sim$. Then, $x = g^n$ for some $g \in G$. Then, $x \in A$. Let $y \in A$. Then, $y = g^n$ for some $g \in G$ and then $y \sim 1_G$. We have that $y \in [1_G]_\sim$. Therefore, $[1_G]_\sim = A$.

7. Let G be a group. Let $n \in \mathbb{N}$ and let $A = \{g \in G \mid |g| = n\}$. Let $H = \langle A \rangle$. Let $\gamma \in \text{Inn}(G)$. As γ is an automorphism, we have that γ preserves order. Let $x \in H$. Then, $x = x_1 ... x_k$ where $x_i \in A$ for each $i \in [k]$. Then, $\gamma(x) = \gamma(x_1 ... x_k) = \gamma(x_1) ... \gamma(x_k) \in H$ as $|\gamma(x_i)| = |x_i| = n$ for each $i \in [k]$. It follows that H is normal.

8. Let H be a subgroup of G and define a relation $\sim_L$ on G by $a \sim_L b$ if and only if $a^{-1}b \in H$. For each $a \in G$, we have that $a \sim_L a$ as $1_G = a^{-1}a \in H$. Suppose $a \sim_L b$. Then, $a^{-1}b \in H$. We then have that $b^{-1}a = (a^{-1}b)^{-1} \in H$. Then, $b \sim_L a$. Finally, suppose that $a \sim_L b$ and $b \sim_L c$. Then, $a^{-1}b, b^{-1}c \in H$. We then have that $a^{-1}c = a^{-1}bb^{-1}c \in H$. Therefore, $\sim_L$ is an equivalence relation. Suppose that $a \sim_L b$ and let $g \in G$. Then, $a^{-1}b \in H$. We then have that $(ga)^{-1}(gb) = a^{-1}g^{-1}gb = a^{-1}b \in H$. Therefore, $ga \sim_L gb$.

9.

10. Let G be a group and $H \subseteq G$ be a subgroup. Suppose H is normal in G. Let $\gamma \in \text{Inn}(G)$. Let $x \in \gamma(H)$. Then, $x = ghg^{-1}$ for some $g \in G$ and $h \in H$. As H is normal, $ghg^{-1} \in H$. Therefore, $\gamma(H) \subseteq H$. For the converse, suppose that $\gamma(H) \subseteq H$ for all $\gamma \in \text{Inn}(G)$. Let $h \in H$ and $g \in G$. Then, $ghg^{-1} = \gamma_g(h) \in H$. Therefore, H is normal.

11. Let G be a group and $[G, G]$ be its commutator. Let $\gamma \in \text{Inn}(G)$. Let $x \in [G, G]$. Then, $x = [x_1, y_1][x_2, y_2]...[x_n, y_n]$ where $x_i, y_i \in G$ for all $i \in [n]$ and $[g, h] = ghg^{-1}h^{-1}$. We have that $\gamma([g, h]) = \gamma(ghg^{-1}h^{-1}) = \gamma(g)\gamma(h)\gamma(g)^{-1}\gamma(h)^{-1} = [\gamma(g), \gamma(h)]$. As γ is a homomorphism, we have that $\gamma(x) = \gamma([x_1, y_1]...[x_n, y_n]) = \gamma([x_1, y_1])...\gamma([x_n, y_n]) = [\gamma(x_1), \gamma(y_1)]...[\gamma(x_n), \gamma(y_n)] \in [G, G]$. We have that $\gamma([G, G]) \subseteq [G, G]$. Therefore, $[G, G]$ is normal. Now, let $x[G, G], y[G, G] \in G/[G, G]$. Then,

$$x[G, G]y[G, G] = xy[G, G] = xy(y^{-1}x^{-1}yx)[G, G] = yx[G, G] = y[G, G]x[G, G]$$

Therefore, $G/[G, G]$ is abelian

12. Let $F = F(A)$ be the free group associated with a set A and let $f : A \to G$ be a set function from the set A to an abelian group G. By the universal property of free groups, there is a unique homomorphism $\psi : F \to G$ such that $\psi \circ j_A = f$ where j_A is the canonical map from A set to its free group. Let $[F, F]$ be the commutator of F and let $x = [a_1, b_1]...[a_n, b_n] \in [F, F]$ where $a_i, b_i \in F$ for all $i \in [n]$. Then,

$$\psi(x) = \psi([a_1, b_1]...[a_n, b_n]) = \psi([a_1, b_1])...\psi([a_n, b_n]) = [\psi(a_1), \psi(b_1)]...[\psi(a_n), \psi(b_n)] = 1_G...1_G = 1_G$$

as G is abelian. Hence, $[F, F] \subseteq \ker \psi$. By Theorem 7.12, there is a unique homomorphism $\varphi : F/[F, F] \to G$ such that the following diagram commutes

$$\begin{tikzcd} A \arrow[d, "j_A"'] \arrow[dr, "f"] & \\ F \arrow[r, "\psi"] \arrow[d, "\pi"'] & G \\ F/[F,F] \arrow[ur, "\varphi"'] & \end{tikzcd}$$

Suppose that $\varphi' : F/[F, F] \to G$ is a homomorphism such that $\varphi' \circ \pi \circ j_A = f$. As $\psi : F \to G$ is the unique homomorphism satisfying $\psi \circ j_A = f$, we must have that $\varphi' \circ \pi = \psi$. We have that $\varphi' \circ \pi = \psi$ and $\varphi' \circ \pi \circ j_A = f$. Hence, φ' also makes the diagram above commute. By uniqueness of φ, we must have that $\varphi = \varphi'$. It follows that φ is the unique homomorphism such that $\varphi \circ \pi \circ j_A = f$ and so the pair $(F/[F, F], \pi \circ j_A)$ satisfies the universal property of the free abelian group of A. Therefore, $F^{\text{ab}} \cong F/[F, F]$.

13.

2.8 - Canonical Decomposition and Lagrange's Theorem

1.

2. Let G be a group and H be a subgroup of index 2. Let the left cosets of H be $\{H, gH\}$ and the right cosets be $\{H, Hg\}$. We must have that $gH = Hg$ as left cosets, aswell as right cosets, form a disjoint partition of G. By a previous exercise, H is normal in G.

3. Let $G = \{g_1, ..., g_n\}$ be a finite group. Let $R = \{g_i g_j g_k^{-1} \in A \mid g_i g_j g_k^{-1} = 1, g_i, g_j, g_k \in G\}$. Clearly, $\langle G \mid R \rangle \cong G$ and so G is finitely presented.

4.

5.

6.

7.

8. Define the homomorphism by $\varphi : \mathrm{GL}_n(\mathbb{R}) \to \mathrm{SL}_n(\mathbb{R})$ by $\varphi(M) = \frac{1}{\det M} M$. We have that φ is clearly surjective with $\ker \varphi = \{aI_n \mid a \in \mathbb{R} - \{0\}\}$ where I_n is the $n \times n$ identity matrix. There is a clear isomorphism between $\ker \varphi$ and $\mathbb{R}^\times$. By the First Isomorphism Theorem, $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \cong \mathbb{R}^\times$.

9.

10.

11. Let G be a group and N be a normal subgroup of G containing the subgroup H of G. Suppose that N is normal in G. Let $xH \in N/H$ and $gH \in G/H$. Then, $(gH)(xH)(g^{-1}H) = gxg^{-1}H \in N/H$ as $gxg^{-1} \in N$ as N is normal in G. For the converse, suppose that N/H is normal in G/H. Let $g \in G$ and $x \in N$. We have that $(gH)(xH)(g^{-1}H) = gxg^{-1}H \in N/H$. Then, $gxg^{-1} \in N$. We have that N is normal in G.

12.

13.

14. Let G be a group of order n. Let $k \in \mathbb{Z}$ such that $\gcd(n,k) = 1$. As $\gcd(n,k) = 1$, there exists $x, y \in \mathbb{Z}$ such that $nx + ky = 1$. For any $g \in G$,

$$g = g^{nx+ky} = g^{nx}g^{ky} = (g^x)^n(g^y)^k = (g^y)^k$$

As $g^y \in G$, we have that there exists some $g' \in G$ such that $g = g'^k$. Therefore, the function $\varphi : G \to G$ given by $\varphi(g) = g^K$ is surjective.

15. Let n, a be positive integers. Let $G = \mathbb{Z}/(a^n - 1)\mathbb{Z}$. We note that the order of G is $\phi(a^n - 1)$. Let $k = \gcd(a^n - 1, a)$. Then, $k \mid a^n - 1$ and $k \mid a$. We have that $k \mid a^n$ as $k \mid a$ and so $k \mid a^n - (a^n - 1) = 1$. It follows $\gcd(a^n - 1, a) = 1$. Hence, $a \in G$. We have that $a^n - 1 \equiv 0 \mod a^n - 1$ and so $a^n \equiv 1 \mod a^n - 1$. We must have that the order of a must divide n. As $a^k < a^n - 1$ for all $k < n$, we must have that the order of a is n. By Lagrange's Theorem, $n = |\langle a \rangle|$ must divide $|G| = \phi(a^n - 1)$. Therefore, $n \mid \phi(a^n - 1)$.

16.

17. Let G be a non-trivial group and let $x \in G$ be a non-trivial element in G. As $|x| > 1$, we must have that $|x| = qm$ for some prime q and some $m \in \mathbb{Z}$. Then, $(x^m)^q = x^{qm} = 1_G$ and so $|x^m| \mid q$. It must follow that $|x^m| = q$ as q is prime and x^m is non-trivial as $|x| = qm$ and $m < qm$. Hence, every non-trivial group contains an element of prime order. We set to prove that if G is an abelian group of order n and p is a prime dividing n, then G contains an element of order p. Let G be an abelian group of order 2. We must have that G contains and element of prime order, hence, G must contain an element of order 2 as 2 is the only prime dividing 2. Let $n \in \mathbb{N}$. Assume for all abelian groups G of order $k < n$, if p is a prime dividing k, then G contains an element of order p. Let G be an abelian group of order n and let p be a prime dividing n. Let $x \in G$ be an element of prime order, q. If $q = p$, then we are done. If $p \neq q$, then consider the group G/H where $H = \langle x \rangle$. We have that $|G/H| = n/q < n$ and $p \mid n/q$, then, there is some $gH \in G/H$ such that $|gH| = p$. We have that $g^pH = (gH)^p = H$ and so $g^p \in H$. As $p \neq q$, we have that $g^p \neq 1_G$ and so $g^p = x^d$ for some $d \in \mathbb{Z}$. We have that $(g^q)^p = g^{pq} = x^{dpq} = 1_G$ and so $|g^q| \mid p$. As g^q is non-trivial, we have that $|g^q| = p$. It follows that G contains an element of order p. By the principle of strong induction, the claim holds.

18. Let G be an abelian group of order $2n$ where n is odd. By the previous exercise, there exists an element of order 2, x say. Suppose there exists a non-trivial element $y \in G$ such that y has order 2 and $x \neq y$. Let $H = \{1_G, x, y, xy\}$. We have that H is a subgroup of G and is of order 4. By Lagrange's Theorem, the order of H must divide the order of G. Hence, $4 \mid 2n$. This is a contradiction as n is odd, hence, such an element y cannot exist. It follows that x is unique.

19.

20. Let G be a finite abelian group of order 1. Then, G is the trivial group and for every d dividing 1 (which is just 1), there is a subgroup of order d, H, of G. Assume for all finite abelian groups of order $k < n$, if $d \mid n$, then G contains a subgroup of order d. Let G be a finite abelian group of order n and let d be a divisor of n. If $d = 1$, then G clearly has a subgroup of order d. Suppose $d > 1$. Then, $d = pm$ for some prime p and $m \in \mathbb{N}$. We have that G contains an element of order p, x say, and so $\langle x \rangle$ is a subgroup of order p. We have that $G/\langle x \rangle$ is a group of order n/p and $d/p \mid n/p$. As $n/p < n$, we have that $G/\langle x \rangle$ contains a subgroup of order d/p, $H/\langle x \rangle$. By the Third Isomorphism Theorem, H is a subgroup of G, and $|H| = |H/\langle x \rangle||\langle x \rangle| = d/p \cdot p = d$ by Lagrange's Theorem. Therefore, G has a subgroup of order d. By the principle of strong induction, if d is a divisor of $|G|$, where G is a finite abelian group, then G contains a subgroup of order d.

21.

22. Let G, G' be groups and let $\varphi : G \to G'$ be a homomorphism. Let L be a group and let $\alpha : G' \to L$ be a homomorphism such that $\alpha \circ \varphi = 0$. Let N be the normal closure of $\operatorname{im} \varphi$ and $\pi : G' \to G'/N$ be the canonical projection. As $\alpha \circ \varphi = 0$, we have that $\operatorname{im} \varphi \subseteq \ker \alpha$. We have that $\ker \alpha$ is a normal subgroup of G' and, by definition, im $\varphi \subseteq N \subseteq \ker \alpha$. By Theorem 7.12, there is a unique ψ such that the following diagram commutes,

$$\begin{tikzcd} G \arrow[r, "\varphi"] \arrow[rr, bend left, "0"] & G' \arrow[r, "\alpha"] \arrow[d, two heads, "\pi"'] & L \\ & G'/N \arrow[ur, "\psi"'] & \end{tikzcd}$$

Therefore, in Grp, coker $\varphi \cong G'/N$

23.

24.

25.

2.9 - Group Actions

1.

2.

3. Let $G = (G, *)$ be a group and define the opposite group of G, $G^\circ = (G, \cdot)$, supported on the same set G, by prescribing $\forall g, h \in G$, $g \cdot h = h * g$. We verify G° is a group. We have that for all $x, y, z \in G^\circ$, $x \cdot (y \cdot z) = (y \cdot z) * x = (z * y) * x = z * (y * x) = (y * x) \cdot z = (x \cdot y) \cdot z$. Let 1_G be the identity element in G. We have that $1_G \in G^\circ$, and for each $x \in G^\circ$, $1_G \cdot x = x * 1_G = x$ and $x \cdot 1_G = 1_G * x = x$. Hence, $1_{G^\circ} = 1_G$. Furthermore, for each $x \in G^\circ$, let $x^{-1} \in G$ be the inverse of $x \in G$. We have that $x \cdot x^{-1} = x^{-1} * x = 1_G = 1_{G^\circ}$. It follows that G° is a group. Let $i : G^\circ \to G$ be the identity map, sending $g \in G^\circ$ to $g \in G$. i is trivially bijective. For all $x, y \in G$, we have that i is a homomorphism if and only if $i(x \cdot y) = i(x) * i(y)$ if and only if $x \cdot y = x * y$ if and only if $y * x = x * y$. Hence, i is an isomorphism if and only if G is abelian. Define $\varphi : G^\circ \to G$ by $\varphi(g) = g^{-1}$. We have that φ is clearly bijective. As well as that,

$$\varphi(x \cdot y) = (x \cdot y)^{-1} = (y * x)^{-1} = x^{-1} * y^{-1} = \varphi(x) * \varphi(y)$$

Hence, φ is an isomorphism. It follows that $G \cong G^\circ$.

4.

5. Let G be a group and let A be the underlying set. Let $\rho : G \times A \to A$ be the action by left multiplication. Suppose there is a $g \in G$ such that for all $a \in A$, $\rho(g, a) = a$. Then, we have that, in G, $ga = a$ for all $a \in A$. It follows from right multiplication, $g = 1_G$. Hence, ρ is free.

6. Let G be a group and let $a \in G$. Let $\rho : G \times A \to A$ be an action of G on a set A. Let $\mathrm{Orb}_G(a)$ be the orbit of $a \in G$ under ρ. Let ρ' be the restriction of ρ to $G \times \mathrm{Orb}_G(a)$. Let $g, h \in \mathrm{Orb}_G(a)$. Then, $g = \rho(g', a)$ and $h = \rho(h', a)$ for some $g', h' \in G$. We have that

$$\rho'(h'g'^{-1}, g) = \rho'(h', \rho'(g'^{-1}, g)) = \rho'(h', \rho'(g'^{-1}, \rho(g', a))) = \rho'(h', \rho'(1_G, \rho(1_G, a))) = \rho'(h', \rho'(1_G, a)) = \rho'(h', a) = h$$

It follows that there exists an $a \in G$ such that $\rho'(a, g) = h$. Therefore, the action ρ' is transitive.

7. Let G be a group and let $a \in G$. Let $\rho : G \times A \to A$ be a left action of G on a set A. Define $\mathrm{Stab}_G(a) = \{g \in G \mid \rho(g, a) = a\}$. Let $g, h \in \mathrm{Stab}_G(a)$. We have that

$$\rho(gh^{-1}, a) = \rho(gh^{-1}, \rho(h, a)) = \rho(gh^{-1}h, a) = \rho(g, a) = a$$

Therefore, $\mathrm{Stab}_G(a)$ is a subgroup of G.

8. Let G be a group. Consider the structure G-Set where $\mathsf{obj}(G\text{-}\mathsf{Set})$ is the class of pairs (ρ, A) where $\rho : G \times A \to A$ is a left action of G on a set A and a morphism $(\rho, A) \to (\rho', A')$ corresponds to a set function $\varphi : A \to A'$ such that the following diagram commutes,

$$\begin{tikzcd} G \times A \arrow[r, "\mathrm{id}_G \times \varphi"] \arrow[d, "\rho"'] & G \times A' \arrow[d, "\rho'"] \\ A \arrow[r, "\varphi"'] & A' \end{tikzcd}$$

i.e for all $g \in G, a \in A$, φ is a set function such that $\varphi(\rho(g,a)) = \rho'(g, \varphi(a))$. Let (ρ, A) be an object of G-Set. We have that there is a $1_{(\rho,A)} \in \mathrm{Hom}((\rho,A),(\rho,A))$, namely, the identity set function $\mathrm{id}_A : A \to A$, as $\mathrm{id}_A(\rho(g,a)) = \rho(g,a) = \rho(g, \mathrm{id}_A(a))$ for all $g \in G, a \in A$. Let $(\rho, A), (\rho', A'), (\rho'', A'')$ be objects in G-Set and f be a morphism $(\rho, A) \to (\rho', A)$ and g be a morphism $(\rho', A) \to (\rho'', A'')$. Let $\varphi : A \to A'$ correspond to f and $\psi : A' \to A''$ correspond to g. Define the composition gf as the set function $\psi \circ \varphi$. We have that

$$(\varphi \circ \psi)(\rho(g,a)) = \varphi(\psi(\rho(g,a))) = \varphi(\rho'(g, \psi(a))) = \rho''(g, \varphi(\psi(a))) = \rho''(g, (\varphi \circ \psi)(a))$$

for all $g \in G, a \in A$. Hence, their composition is G-equivariant. We note this composition is associative as function composition is associative. Let $f \in \mathrm{Hom}(A,B)$, we have that $f 1_A = f$ and $1_B f = f$ as $1_A, 1_B$ are simply identity functions. It follows G-Set is a category.

9. Let $(\rho, A), (\rho', A')$ be objects in the category G-Set. Let $\rho \times \rho' : G \times (A \times A') \to A \times A'$ be a map defined by $(\rho \times \rho')(g, (a, a')) = \rho(g,a) \times \rho'(g, a')$. We have that $(\rho \times \rho')(1_G, (a,a')) = \rho(1_G, a) \times \rho'(1_G, a') = (a, a')$ and

$$(\rho \times \rho')(gh, (a,a')) = \rho(gh, a) \times \rho'(gh, a') = \rho(g, \rho(h,a)) \times \rho'(g, \rho(h,a')) = (\rho \times \rho')(g, (\rho(h,a), \rho(h,a')))$$
$$= (\rho \times \rho')(g, (\rho \times \rho')(h, (a,a')))$$

for all $g, h \in G$ and $(a, a') \in A \times A'$. Hence, $\rho \times \rho'$ is an action, so $(\rho \times \rho', A \times A')$ is an object of G-Set. Let $\pi_A : A \times A' \to A$ be the projection map. We have that

$$\pi_A((\rho \times \rho')(g, (a,a'))) = \pi_A(\rho(g,a) \times \rho'(g,a')) = \rho(g,a) = \rho(g, \pi_A(a,a'))$$

for all $g \in G$ and $(a,a') \in A \times A'$. Therefore, π_A is G-equivariant. Let (σ, Z) be an object in G-Set and f, g be morphisms from (σ, Z) to (ρ, A) and (σ, Z) to (ρ', A'), respectively. We claim there exists a unique morphism φ such that the following diagram commutes,

$$\begin{tikzcd} & & (\rho, A) \\ (\sigma, Z) \arrow[r, "\varphi"] \arrow[urr, bend left, "f"] \arrow[drr, bend right, "g"'] & (\rho \times \rho', A \times A') \arrow[ur, "\pi_A"] \arrow[dr, "\pi_{A'}"'] & \\ & & (\rho', A') \end{tikzcd}$$

We have that $\pi_A \circ \varphi = f$ and $\pi_{A'} \circ \varphi = g$. Then, $\varphi : Z \to A \times A'$ must take form of $f \times g$. Furthermore,

$$\varphi(\sigma(h,a)) = f(\sigma(h,a)) \times g(\sigma(h,a)) = \rho(h, f(a)) \times \rho'(h, g(a)) = (\rho \times \rho')(h, (f(a), g(a))) = (\rho \times \rho')(h, \varphi(a))$$

for all $h \in G$ and $a \in Z$. Hence, φ is G-equivariant. Therefore, φ is a unique morphism that makes the above diagram commute. We conclude that the product of (ρ, A) and (ρ', A') in G-Set exists, and is $(\rho \times \rho', A \times A')$. Next, we show G-Set has coproducts. Let $(\rho, A), (\rho', A')$ be objects in G-Set. Define $\rho \amalg \rho' : G \times A \amalg A' \to A \amalg A'$ by

$$(\rho \amalg \rho')(g, (a, i)) = \begin{cases} (\rho(g,a), 1) & \text{if } i = 1 \\ (\rho'(g,a), 2) & \text{if } i = 2 \end{cases}$$

We have that

$$(\rho \amalg \rho')(1_G, (a, 1)) = (\rho(1_G, a), 1) = (a, 1)$$
$$(\rho \amalg \rho')(1_G, (a', 2)) = (\rho'(1_G, a'), 2) = (a', 2)$$

for all $a \in A$ and $a' \in A'$. Furthermore, for each $g, h \in G$,

$$(\rho \amalg \rho')(gh, (a, 1)) = (\rho(gh, a), 1) = (\rho(g, \rho(h, a)), 1) = (\rho \amalg \rho')(g, (\rho(h, a), 1)) = (\rho \amalg \rho')(g, (\rho \amalg \rho')(h, (a, 1)))$$

$$(\rho \amalg \rho')(gh, (a', 2)) = (\rho'(gh, a'), 2) = (\rho'(g, \rho'(h, a')), 2) = (\rho \amalg \rho')(g, (\rho'(h, a'), 2)) = (\rho \amalg \rho')(g, (\rho \amalg \rho')(h, (a', 2)))$$

Hence, $\rho \amalg \rho'$ is an action, and so $(\rho \amalg \rho', A \amalg A')$ is an object in G-Set. Let $i_A : A \to A \amalg A', i_{A'} : A' \to A \amalg A'$ be the canonical inclusions. We have that

$$i_A(\rho(g, a)) = (\rho(g, a), 1) = (\rho \amalg \rho')(g, (a, 1)) = (\rho \amalg \rho')(g, i_A(a))$$

$$i_{A'}(\rho'(g, a')) = (\rho'(g, a'), 2) = (\rho \amalg \rho')(g, (a', 2)) = (\rho \amalg \rho')(g, i_{A'}(a))$$

Hence, $i_A, i_{A'}$ are G-equivariant. Let (σ, Z) be an object in G-Set and f, g be morphisms to (σ, Z) from (ρ, A) and to (σ, Z) from (ρ', A'), respectively. We claim there exists a unique morphism ψ such that the following diagram commutes,

$$\begin{tikzcd}
& & (\rho, A) \arrow[dl, "i_A"'] \arrow[dll, bend right, "f"'] \\
(\sigma, Z) & (\rho \amalg \rho', A \amalg A') \arrow[l, "\psi"'] & \\
& & (\rho', A') \arrow[ul, "i_{A'}"] \arrow[ull, bend left, "g"]
\end{tikzcd}$$

We have that $\psi \circ i_A = f$ and $\psi \circ i_{A'} = g$. Hence,

$$\psi(a, i) = \begin{cases} f(a) & \text{if } i = 1 \\ g(a) & \text{if } i = 2 \end{cases}$$

We have that

$$\psi((\rho \amalg \rho')(h, (a, 1))) = \psi((\rho(h, a), 1)) = f(\rho(h, a)) = \sigma(h, f(a)) = \sigma(h, \psi(a, 1))$$

$$\psi((\rho \amalg \rho')(h, (a', 2))) = \psi((\rho(h, a'), 2)) = g(\rho(h, a)) = \sigma(h, g(a)) = \sigma(h, \psi(a', 2))$$

for all $h \in G$ and $a \in A, a' \in A'$. Therefore, ψ is G-equivariant. It follows that G-Set has coproducts, and the coproduct of (ρ, A) and (ρ', A') is $(\rho \amalg \rho', A \amalg A')$.

10.

11. Let G be a finite group and let H be a subgroup of index p where p is the smallest prime dividing $|G|$. Let $\rho : G \times G/H \to G/H$ be left multiplication of G on G/H. We have that ρ is an action and induces a homomorphism $\sigma : G \to S_{G/H}$ given $\sigma(g)(aH) = (ga)H$. We have that $G/\ker\sigma$ is isomorphic to a subgroup of $S_{G/H}$ by the First Isomorphism Theorem. Let $x \in \ker\sigma$. Then, $\sigma(x)(aH) = (xa)H = H$ for all $a \in G$. For $a = 1_G$, we deduce that $xH = H$. Hence, $x \in H$. We have that $|G/\ker\sigma|$ must divide $p!$ as $G/\ker\sigma$ is isomorphic to a subgroup of $S_{G/H}$. We must also have that $|G/\ker\sigma|$ must also divide $|G|$ as $|G| = |G/\ker\sigma||\ker\sigma|$. As p is the smallest prime dividing $|G|$, we must have that $|G/\ker\sigma| = p$. Then, $p = |G/\ker\sigma| = [G : \ker\sigma] = [G : H][H : \ker\sigma] = p[H : \ker\sigma]$. Hence, $[H : \ker\sigma] = 1$. As $\ker\sigma \subseteq H$, we must have that $\ker\sigma = H$. As $\ker\sigma$ is normal, H is therefore normal in G.

12. Let G be a finite group and $H \subseteq G$ a subgroup of index n. Let $\rho : G \times G/H \to G/H$ be left multiplication where G/H is the set of left cosets of H in G. We have that ρ is an action and induces a homomorphism $\sigma : G \to S_{G/H}$ given by $\sigma(g)(aH) = (ga)H$. We have that $G/\ker\sigma$ is isomorphic to a subgroup of $S_{G/H}$ by the First Isomorphism Theorem. Let $x \in \ker\sigma$. Then, $\sigma(x)(aH) = (xa)H = H$ for all $a \in G$. For $a = 1_G$, we deduce that $xH = H$. Hence, $x \in H$. We have that $|G/\ker\sigma|$ must divide $n!$ as $G/\ker\sigma$ is isomorphic to a subgroup of $S_{G/H}$. We must also have that $|G/\ker\sigma|$ must also divide $|G|$ as $|G| = |G/\ker\sigma||\ker\sigma|$. Then, $[G : \ker\sigma]$ is a divisor of $|G|$ and $n!$, hence, divides the greatest common divisor of $|G|$ and $n!$. Therefore, there exists a normal subgroup $K \subseteq H$ such that $[G : K] \leq n!$.

13. Let G be a group and let H be a subgroup of G. Let G/H be the set of left cosets of H in G and G/gHg^{-1} be the set of left cosets of gHg^{-1} in G for some $g \in G$. Let $\rho : G \times G/H \to G/H$ and $\rho' : G \times G/gHg^{-1} \to G/gHg^{-1}$ be left multiplication. Define $\varphi : G/H \to G/gHg^{-1}$ by $\varphi(xH) = (xg^{-1})gHg^{-1}$. Suppose that $xH = yH$. We have that

$$\varphi(xH) = (xg^{-1})gHg^{-1} = xHg^{-1} = yHg^{-1} = (yg^{-1})gHg^{-1} = \varphi(yH)$$

Now, suppose that $\varphi(xH) = \varphi(yH)$. Then, $xHg^{-1} = yHg^{-1}$. Hence, $xH = yH$. Let $agHg^{-1} \in G/gHg^{-1}$. Then, $\varphi(agH) = (agg^{-1})gHg^{-1} = agHg^{-1}$. It follows that φ is well-defined and bijective. Finally,

$$\rho'(x, \varphi(aH)) = \rho(x, (ag^{-1})gHg^{-1}) = xaHg^{-1} = xag^{-1}(gHg^{-1}) = \varphi(xaH) = \varphi(\rho(x, aH))$$

for all $x \in G$ and $aH \in G/H$. Therefore, φ is G-equivariant. It follows that $G/H \cong G/gHg^{-1}$ in G-Set.

14.

15.

16.

17. Let G be a group. Consider G as an object in G-Set along with left multiplication. I claim $\mathrm{Aut}_{G\text{-}\mathsf{Set}}(G) = \{\varphi_g(x) = xg \mid g \in G\}$ where $\varphi_g\varphi_h = \varphi_{gh}$. Let $\psi \in \mathrm{Aut}_{G\text{-}\mathsf{Set}}(G)$. We have that ψ is G-equivariant, that is, for each $a, g \in G$, $\psi(ga) = g\psi(a)$. For all $x \in G$, it follows that $\psi(x) = \psi(x1_G) = x\psi(1_G)$. Hence, $\psi = \varphi_g$ for some $g \in G$. Now, let $\varphi_g \in \{\varphi_g = xg \mid g \in G\}$. Its clear that φ_g is bijective. We show φ_g is G-equivariant. For each $x, a \in G$, we have that $\varphi(xa) = (xa)g = x(ag) = x\varphi(a)$. Therefore, φ_g is G-equivariant, and the claim follows. Define $f : G \to \mathrm{Aut}_{G\text{-}\mathsf{Set}}(G)$ by $f(g) = \varphi_g$. f is clearly surjective. Let $h, g \in G$ such that $f(g) = f(h)$. Then, $\varphi_g(x) = \varphi_h(x)$ for each $x \in G$. Hence, $xg = xh$ and so $g = h$. Thus, f is bijective. Finally, we have that for all $g, h \in G$, $f(gh) = \varphi_{gh} = \varphi_g\varphi_h = f(g)f(h)$. Therefore, f is an isomorphism. We have that $\mathrm{Aut}_{G\text{-}\mathsf{Set}} \cong G$.

18.

2.10 - Group Objects In Categories

1.

2.

3.

4.

5.

III - Rings, and Modules

3.1 - Definition of Ring

1. Let R be a ring such that $0_R = 1_R$. Let $x \in R$. Then, $x = x1_R = x0_R = 0_R$. It follows that R is the zero-ring.

2.

3.

4.

5.

6. Let R be a ring where $x, y \in R$ such that $xy = yx$. We first prove the Binomial Theorem, that is,

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

for all $n \in \mathbb{N}$. We see this holds for $n = 1$ easily. Assume

$$(x+y)^k = \sum_{i=0}^{k} \binom{n}{i} x^{n-i} y^i$$

for some $k \in \mathbb{N}$. We have that

$$(x+y)^{k+1} = (x+y)(x+y)^k = (x+y)\sum_{i=0}^{k} \binom{k}{i} x^{k-i} y^i = \sum_{i=0}^{k} \binom{k}{i} x^{n-i} y^i (x+y)$$

$$= \sum_{i=0}^{k} \binom{k}{i} [x^{k+1-i} y^i + x^{k-i} y^{i+1}] = \sum_{i=0}^{k+1} \left[\binom{k}{i-1} + \binom{k}{i}\right] x^{k+1-i} y^i = \sum_{i=0}^{k+1} \binom{k+1}{i} x^{k+1-i} y^i$$

By the principle of mathematical induction, the claim holds. Let R be a ring where $a, b \in R$ are nilpotent and commute. We have that $a^n = 0_R$ and $b^m = 0_R$ for some $n, m \in \mathbb{N}$. We have that

$$(a+b)^{n+m} = \sum_{i=0}^{n+m} \binom{n+m}{i} a^{n+m-i} b^i$$

as a and b commute. For $i < m$, we have that $a^{n+m-i}b^i = a^n a^{m-i} b^i = 0_R$ and for $i \geq m$, $a^{n+m-i}b^i = a^{n+m-i}b^{i-m}b^m = 0_R$. Hence, $(a+b)^{n+m} = 0_R$. It follows that $a+b$ is nilpotent.

7. Let $n \in \mathbb{N}$ and let $[m] \in \mathbb{Z}/n\mathbb{Z}$. Suppose that $[m]$ is nilpotent. There then exists some $q \in \mathbb{N}$ such that $[m]^q = [0]$. Hence, $n \mid m^q$. Let p be a prime dividing n. Then, $p \mid m^q$. As p is prime, $p \mid m$. It follows that m is divisible by each prime divisor of n. For the converse, suppose that $m \in \mathbb{N}$ such that for all p prime dividing n, $p \mid m$. Let $A = \{k \in \mathbb{N} \mid p^k \text{ divides } n \text{ and } p^{k+1} \nmid n, p \text{ prime}\}$. Let $M = \max A$. We have that $n \mid m^M$, hence, $[m]^M = [0]$. Therefore, $[m]$ is nilpotent.

8. Let R be an integral domain and $x \in R$ such that $x^2 = 1_R$. We then have that $x^2 - 1_R = 0_R$ and so $(x - 1_R)(x + 1_R) = 0_R$. As R is an intgeral domain, $x - 1_R = 0_R$ or $x + 1_R = 0$. Hence, $x = 1_R$ or $x_R = -1_R$. Consider the ring $\mathcal{M}_2(\mathbb{R})$. We have that the following matrix is a solution to the equation $x^2 = I$ where the matrix is not I or $-I$:

$$\begin{pmatrix} 2 & 1 \\ -3 & -2 \end{pmatrix}$$

9. Let $u \in R$ be a unit such that u has inverses v and v'. We have that

$$v = v1_R = v(uv') = (vu)v' = 1_R v' = v'$$

Hence, the inverse of u is unique. Let $R^* = \{u \in R \mid u \text{ is a unit in } R\}$ equipped with multiplication induced by R. We note that multiplication is associative as R is a ring. Let $x, y \in R^*$, we have that there exists $x', y' \in R^*$ such that $xx' = x'x = 1_R$ and $yy' = y'y = 1_R$. Then, $(xy)(y'x') = x(yy')x' = x1_R x' = xx' = 1_R$ and $(y'x')(xy) = y'(x'x)y = y'1_R y = y'y = 1_R$. Hence, xy is a unit and R^* is closed under multiplication. We note that $1_R \in R^*$ as $1_R 1_R = 1_R$. Furthermore, for each $x \in R^*$, there is a x' such that $xx' = x'x = 1_R$. We have that x' is an inverse of x and x' is a unit in R. It follows that R^* is a group under multiplication.

10. Let R be a ring and $a \in R$ such that a is a right unit and has atleast two left inverses. Suppose, for contradiction, that there is a non-zero $b \in R$ such that $ab = 0$. As a is a right unit, there is a b' such that $b'a = 1$. We then have that $b = 1b = (b'a)b = b'(ab) = b'0 = 0$, which contradicts the original assumption. Hence, a must be a left-zero divisor. Now let $x, x' \in R$ be left inverses of a such that $x \neq x'$. We have that $x - x' \neq 0$ and $(x - x')a = xa - x'a = 1 - 1 = 0$. Therefore, a is a right zero-divisor.

11.

12.

13.

14. Let R be a ring and $f(x), g(x) \in R[x]$ be non-zero polynomials. We have that $f(x) = \sum_{i\geq 0} a_i x^i$ and $g(x) = \sum_{i\geq 0} b_i x^i$ for some $n, m \in \mathbb{N}$. Then,

$$f(x) + g(x) = \sum_{i\geq 0} (a_i + b_i) x^i$$

WLOG assume $m = \deg(f) \geq \deg(g) = n$. Then, $a_k + b_k = 0$ for all $k > m$. We have that $a_m + b_m$ is 0 or not. Hence, $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$. Furthermore, assume R is an integral domain. We have that

$$f(x)g(x) = \sum_{k\geq 0} \sum_{i+j=k} a_i b_j x^{i+j}$$

We have that for all $k > m + n$, $a_i b_j = 0$ for all i, j such that $i + j = k$. As R is an integral domain, if $a_m b_n = 0$, then $a_m = 0$ or $b_n = 0$. It follows that the coefficient of x^{n+m} is non-zero as f and g are polynomials of degree m and n respectively. Hence, $\deg(fg) = \deg(f) + \deg(m)$.

15. Let R be a ring. Suppose that R is an integral domain. Let $f, g \in R[x]$ such that $fg = 0$. We have that $0 = \deg(fg) = \deg(f) + \deg(g)$. It follows that $\deg(f) = 0$ and $\deg(g) = 0$ as $\deg(p) \geq 0$ for all $p \in R[x]$. We must have that $f(x) = r$ and $g(x) = r'$ for some $r, r' \in R$. Then, $0 = fg = rr'$. As R is an integral domain, $f(x) = r = 0$ or $g(x) = r' = 0$. Therefore, $R[x]$ is an integral domain. For the converse, suppose that $R[x]$ is an integral domain. Let $r, r' \in R$ such that $rr' = 0$. We then have that $f(x) = r \in R[x]$ and $g(x) = r' \in R[x]$ and so $fg = rr' = 0$. As $R[x]$ is an integral domain, $f = 0$ or $g = 0$. It follows that R is an integral domain.

16.

(i) Let R be a ring. Let $f = \sum_{i\geq 0} a_i x^i \in R[\![x]\!]$ be a unit. We have that there exists a $g = \sum_{i\geq 0} b_i x^i \in R[\![x]\!]$ such that $gf = fg = 1 \in R[\![x]\!]$. We that that

$$1 = \sum_{k\geq 0} \sum_{i+j=k} a_i b_j x^k$$

and so $a_0 b_0 = 1$. Therefore, $a_0 \in R$ is a unit. For the converse, let $f = \sum_{i\geq 0} a_i x^i \in R[\![x]\!]$ where a_0 is a unit. Define the sequence b_n where

$$b_n = -a_0^{-1} \left(\sum_{i=0}^{n-1} a_{n-i} b_i \right)$$

and $b_0 = a_0^{-1}$. We have that $\left(\sum_{i\geq 0} a_i x^i\right)\left(\sum_{i\geq 0} b_i x^i\right) = 1$. The inverse of $1 - x$ is then $1 + x + x^2 + x^3 + ...$

(ii) Let R be a ring. Suppose that $R[\![x]\!]$ is an integral domain. Let $r, r' \in R$ be non-zero elements in R such that $rr' = 0$. We have that $f(x) = r$ and $g(x) = r'$ are elements in $R[\![x]\!]$ and we have that $fg = 0$. By assumption, we have that $f = 0$ or $g = 0$. Hence, $r = 0$ or $r' = 0$. Therefore, R is an integral domain. For the converse, suppose that R is an integral domain. Let $f, g \in R[\![x]\!]$ such that $fg = 0$. We have that

$$\sum_{i=0}^{n} a_i b_{n-i} = 0$$

for all $n \geq 0$. Then, $a_0 b_0 = 0$ and so $a_0 = 0$ or $b_0 = 0$. Without loss of generality, assume that $a_0 = 0$ and $b_0 \neq 0$. Then, we have that $a_0 b_1 + a_1 b_0 = a_1 b_0 = 0$. Hence, $a_1 = 0$. Via strong induction, we have that $a_n = 0$ for all $n \in \mathbb{N}$. It follows that $f = 0$. Similiarly, if $b_0 = 0$, then $g = 0$. Therefore, $R[\![x]\!]$ is an integral domain.

17.

3.2 - The Category Ring

1. Let R be a ring and $\mathbf{0}$ the zero-ring. Suppose there exists a homomorphism $\varphi : \mathbf{0} \to R$. Let $0 \in \mathbf{0}$. We have that $\varphi(0) = 1_R$. Then, $1_R = \varphi(0) = \varphi(0+0) = \varphi(0) + \varphi(0) = 1_R + 1_R$. Hence, $1_R = 0_R$. Therefore, R is the zero-ring.

2. Let R and S be rings. Let $\varphi : R \to S$ be a function preserving both additive and multiplicative operations.

(i) Suppose that φ is surjective. We have that there exists an $x \in R$ such that $\varphi(x) = 1_S$. Then,

$$1_S = \varphi(x) = \varphi(x1_R) = \varphi(x)\varphi(1_R) = 1_S\varphi(1_R) = \varphi(1_R)$$

Hence, φ is a ring homomorphism.

(ii) Suppose that $\varphi \neq 0$ and S is an integral domain. We have that $\varphi(1_R) = \varphi(1_R 1_R) = \varphi(1_R)\varphi(1_R)$. Hence, $\varphi(1_R)^2 - \varphi(1_R) = 0_S$. By the distributive law, $\varphi(1_R)(\varphi(1_R) - 1_S) = 0_S$. As S is an integral domain, $\varphi(1_R) = 0_S$ or $\varphi(1_R) = 1_S$. Suppose that $\varphi(1_R) = 0_S$. Let $x \in R$. Then, $\varphi(x) = \varphi(1_R x) = \varphi(1_R)\varphi(x) = 0_S\varphi(x) = 0_S$. This cannot happen as, by assumption, $\varphi \neq 0$. Therefore, $\varphi(1_R) = 1_S$. It follows that φ is a ring homomorphism.

3.

4.

5.

6. Let $\alpha : R \to S$ be a fixed ring homomorphism and let $s \in S$ such that $s\alpha(r) = \alpha(r)s$ for all $r \in R$. Let $\overline{\alpha} : R[x] \to S$ be a ring homomorphism that extends α and sends x to s. Let $f(x) = \sum_{i \geq 0} a_i x^i \in R[x]$. We have that

$$\overline{\alpha}(f(x)) = \overline{\alpha}\left(\sum_{i\geq 0} a_i x^i\right) = \sum_{i \geq 0} \overline{\alpha}(a_i x^i) = \sum_{i\geq 0} \overline{\alpha}(a_i)\overline{\alpha}(x)^i = \sum_{i \geq 0} \alpha(a_i)s^i$$

We note that $\overline{\alpha}(f) = \sum_{i\geq 0} \alpha(a_i)s^i$ fits our criteria and is unique.

7.

8. Let F be a field and S a subring of F. Let $x, y \in S$ such that $xy = 0$. As $x, y \in S$, and S is a subring of F, we have that $x, y \in F$ and $xy = 0$. As F is a field, it is an integral domain, hence, $x = 0$ or $y = 0$. It follows that S is an integral domain.

9.

(i) Let R be a ring and $Z(R) = \{a \in R \mid \forall r \in R, ar = ra\}$ be the centre of R. Let $x, y \in Z(R)$. For each $r \in R$, we have that $(x-y)r = xr - yr = rx - ry = r(x-y)$. Thus, $x - y \in Z(R)$. We also have that $0_R \in Z(R)$ as 0_R commutes with all $r \in R$. We also have that $1_R \in Z(R)$ for the same reason. Furthermore, $r(xy) = (rx)y = (xr)y = x(ry) = x(yr) = (xy)r$. Therefore, $xy \in Z(R)$. It follows that $Z(R)$ is a subring of R.

(ii) Let R be a division ring. Let $x, y \in Z(R)$. Then, $xr = rx$ and $yr = ry$ for all $r \in R$. Thus, $xy = yx$. We have that $Z(R)$ is a commutative ring. Let $x \in Z(R)$. Then, $x \in R$ and so there is a x^{-1} such that $xx^{-1} = x^{-1}x = 1_R$. We have that $xr = rx \implies rx^{-1} = x^{-1}r$ and so $x^{-1} \in Z(R)$. Hence, x is a unit in $Z(R)$. As x was arbitrary, it follows that $Z(R)$ is a division ring. Therefore, $Z(R)$ is a field.

10.

(i) Let R be a ring and let $a \in R$. Let $C(a) = \{r \in R \mid ar = ra\}$. Let $x, y \in C(a)$, then $a(x-y) = ax - ay = xa - ya = (x-y)a$. Hence, $x - y \in C(a)$. We also have that $a1_R = a = 1_R a$ and $a0_R = 0_R = 0_R a$, and so $0_R, 1_R \in C(a)$. Furthermore, $a(xy) = (ax)y = (xa)y = x(ay) = x(ya) = (xy)a$. Thus, $xy \in C(a)$. Therefore, $C(a)$ is a subring of R for all $a \in R$.

(ii) Let $x \in Z(a)$. Then, $xr = rx$ for all $r \in R$. We must have that $x \in C(r)$ for all $r \in R$. Therefore, $x \in \bigcap_{a \in R} C(a)$. Now, let $x \in \bigcap_{a \in R} C(a)$. Hence, $x \in C(a)$ for all $a \in R$. Thus, $xa = ax$ for all $a \in R$ and so $x \in Z(R)$. Therefore,

$$Z(R) = \bigcap_{a \in R} C(a)$$

(iii) Let R be a division ring and let $a \in R$. Let $C(a)$ be the centraliser of a. Let $x \in C(a)$. As R is a division ring, there is an $x^{-1} \in R$ such that $xx^{-1} = x^{-1}x = 1_R$. As $x \in C(a)$, $xa = ax$. Then, $x^{-1}a = ax^{-1}$, which means $x^{-1} \in C(a)$. It follows that $C(a)$ is a division ring.

11. Let R be a division ring consisting of p^2 elements where p is prime. Suppose, for contradiction, R is non-commutative. As R is non-commutative, $Z(R) \neq R$. As $Z(R)$ is a subring of R, 0_R and 1_R are contained in $Z(R)$. We have that $1 < Z(R) < p^2$. The only divisors of p^2 are $1, p$ and p^2, hence, $|Z(R)| = p$ by Lagrange's Theorem. Let $r \in R$ such that $r \notin Z(R)$. We have that $Z(R) \subseteq C(r)$ as $Z(R) = \bigcap_{a \in R} C(a)$. As $C(r)$ is a subring of R, which contains $Z(R)$ and $r \in R$, we must have that $C(r) = R$ by Lagrange's Theorem. Let $x, y \in R$. If $x \in Z(R)$, then $xy = yx$. If $x \notin Z(R)$, then $C(x) = R$ and so $xy = yx$. In both cases, $xy = yx$. Therefore, R is commutative. This is a contradiction. It follows that R is a field.

12.

13. Let R_1, R_2 be rings. Let $R_1 \times R_2$ be their 'componentwise' product. Let S be a ring and $f : R_1 \to S, g : R_2 \to S$ be ring homomorphisms. Let $\varphi : S \to R_1 \times R_2$ be a ring homomorphism such that $f = \pi_{R_1} \circ \varphi$ and $g = \pi_{R_2} \circ \varphi$. We must have that $\varphi = (f, g)$. We verify $\varphi = (f, g)$ is infact a ring homomorphism. Let $x, y \in S$, we have that

$$\varphi(xy) = (f(xy), g(xy)) = (f(x)f(y), g(x)g(y)) = (f(x), g(x))(f(y), g(y)) = \varphi(x)\varphi(y)$$

$$\varphi(x+y) = (f(x+y), g(x+y)) = (f(x) + f(y), g(x) + g(y)) = (f(x), g(x)) + (f(y), g(y)) = \varphi(x) + \varphi(y)$$

$$\varphi(1_S) = (f(1_S), g(1_S)) = (1_{R_1}, 1_{R_2}) = 1_{R_1 \times R_2}$$

Therefore, φ is a ring homomorphism. It follows that $R_1 \times R_2$ satisfies the universal property for the product of R_1 and R_2 in Ring.

14.

15.

16.

17.

18.

19.

3.3 - Ideals and Quotient Rings

1. Let $\varphi : R \to S$ be a ring homomorphism. Let $x, y \in \varphi(R)$. There then exists x', y' such that $\varphi(x') = x$ and $\varphi(y') = y$. We have that $\varphi(x' - y') = \varphi(x') - \varphi(y') = x - y$. Hence, $x - y \in \varphi(R)$. Furthermore, $\varphi(x'y') = \varphi(x')\varphi(y') = xy$. Hence, $xy \in \varphi(R)$. Finally, as φ is a ring homomorphism, $\varphi(1_R) = 1_S$ and so $1_S \in \varphi(R)$. It follows that $\varphi(R)$ is a subring of S. Suppose that $\varphi(R)$ is an ideal of S. By definition, for all $s \in S$ and $x \in \varphi(R)$, we have that $xs \in \varphi(R)$ and $sx \in \varphi(R)$. Setting $x = 1_S$, we have that $s \in \varphi(R)$ for all $s \in S$. It follows that φ is surjective. Suppose that $\ker \varphi$ is a subring of R. We have that $1_R \in \ker \varphi$ and so $\varphi(1_R) = 0_S$. For any $x \in R$, we then have that $\varphi(x) = \varphi(x1_R) = \varphi(x)\varphi(1_R) = \varphi(x)0_S = 0_S$. Hence, φ is the zero map.

2. Let $\varphi : R \to S$ be a ring homomorphism and J an ideal of S. Set $I = \varphi^{-1}(J)$. Let $x, y \in I$. Then, $\varphi(x), \varphi(y) \in J$. As J is an ideal, $\varphi(x) - \varphi(y) \in J$. Hence, $\varphi(x - y) \in J$. We must have that $x - y \in I$. Now, let $r \in R$ and $x \in I$. We have that $\varphi(r) \in S$ and $\varphi(x) \in J$. As J is an ideal, $\varphi(rx) = \varphi(r)\varphi(x) \in J$ and $\varphi(xr) = \varphi(x)\varphi(r) \in J$. It follows that $rx, xr \in I$ and so I is an ideal.

3. Let $\varphi : R \to S$ be a ring homomorphism and let J be an ideal of R

(i) Consider the inclusion map $i : \mathbb{Z} \to \mathbb{Q}$. The inclusion map is a ring homomorphism as $\mathbb{Z}$ is a subring of $\mathbb{Q}$. We have that $\mathbb{Z}$ is an ideal of $\mathbb{Z}$, however, $i(\mathbb{Z}) = \mathbb{Z}$ is not an ideal of $\mathbb{Q}$.

(ii) Assume that φ is surjective. Let $x, y \in \varphi(J)$. We have that there exists $x', y' \in J$ such that $\varphi(x') = x$ and $\varphi(y') = y$. As J is an ideal, $x' - y' \in J$ and so $x - y = \varphi(x') - \varphi(y') = \varphi(x' - y') \in \varphi(J)$. Let $r \in S$ and $x \in \varphi(J)$. As φ is surjective, there is an $r' \in R$ such that $\varphi(r') = r$ and there is an $x' \in J$ such that $\varphi(x') = x$. As J is an ideal, $r'x', x'r' \in J$. Hence, $rx = \varphi(r')\varphi(x') = \varphi(r'x') \in \varphi(J)$ and $xr = \varphi(x')\varphi(r') = \varphi(x'r') \in \varphi(J)$. Therefore, $\varphi(J)$ is an ideal of S.

(iii)

4. Let R be a ring of characteristic n such that every subgroup of $(R, +)$ is an ideal. By definition, $\ker f = n\mathbb{Z}$ where $f : \mathbb{Z} \to R$ is the map defined by $f(x) = x \cdot 1_R$. We have that $f(\mathbb{Z})$ is a subring of R, hence, $1_R \in f(\mathbb{Z})$. By assumption, $f(\mathbb{Z})$ is an ideal of R. $f(\mathbb{Z})$ of R is an ideal that contains 1_R, thus, $f(\mathbb{Z}) = R$. By the first isomorphism theorem, $\mathbb{Z}/n\mathbb{Z} \cong R$.

5.

6.

7. Let R be a ring and let $a \in R$. Let $xa, ya \in Ra$. We have that $xa - ya = (x - y)a \in Ra$ as $x - y \in R$. Let $r \in R$ and $xa \in Ra$. We have that $rxa \in Ra$ as $rx \in R$. Hence, Ra is a left ideal of R. Suppose that a is a right unit. Then, there exists an $a^{-1} \in R$ such that $a^{-1}a = 1_R$. We have that $a = 1_R a \in Ra$. As Ra is a left ideal, we have that $1_R = a^{-1}a \in Ra$. Hence, $R = Ra$. For the converse, suppose that $R = Ra$. Then, $1_R \in R$ can be represented as ra for some $r \in R$. It follows that a is a right unit in R. With a similar argument, we can also show aR is a right ideal of R and $R = aR$ if and only if a is a left unit in R.

8. Let R be a ring. Suppose that R is a division ring. We have that $\{0\}$ is an ideal of R. Let I be a left ideal of R with atleast two elements. Let $x \in I$ such that $x \neq 0_R$. If $x = 1_R$, then $I = R$ and we are done. Suppose $x \neq 1_R$. As R is a division ring, there exists an $x^{-1} \in R$ such that $xx^{-1} = x^{-1}x = 1_R$. As I is a left ideal, $1_R = x^{-1}x \in I$. Hence, $I = R$. With a similar argument, we can also show that every right ideal of R with atleast two elements is equal to R. Therefore, R only contains R and $\{0\}$ as left and right ideals. For the converse, suppose that R only has R and $\{0\}$ as its right and left ideals. Let $x \in R$. By the previous exercise, we have that xR is a right ideal of R. If $x \neq 0_R$, then xR is forced to be R by assumption. Then, by the previous exercise, x is a left unit. Similarly, Rx is a left ideal of R. If $x \neq 0_R$, then Rx is forced to be R. Then, x is a right unit. x is then a unit in R. As x was arbitrary, it follows that R is a division ring.

9.

10. Let $\varphi : k \to R$ be a ring homomorphism where k is a field and R is a non-zero ring. As k is a field, it is a division ring, and so its only ideals are k and $\{0\}$. We have that $\ker\varphi$ is an ideal of k, thus, $\ker\varphi = k$ or $\ker\varphi = \{0\}$. If $\ker\varphi = k$, then φ is the zero map. As φ is a ring homomorphism, $1_R = \varphi(1_k) = 0_R$. Hence, R is the zero-ring, which is not permitted by assumption. This forces $\ker\varphi = \{0\}$. By Proposition 2.4, φ is injective.

11.

12. Let R be a commutative ring and N be set of nilpotent elements of R. Let $x, y \in N$. There exists a $k \in \mathbb{N}$ such that $y^k = 0_R$. We have that $(-y)^k = (-1)^k y^k = (-1)^k 0_R = 0_R$. Hence, $-y \in N$. By a previous exercise, $x - y \in N$. Let $x \in N$ and $r \in R$. There exists a $m \in \mathbb{N}$ such that $x^m = 0_R$. We have that $(rx)^m = r^m x^m = r^m 0_R = 0_R$. Therefore, $rx \in N$. It follows that N is an ideal of R.

13. Let R be a commutative ring and N the nilradical of R. Suppose there exists an $x + N \in R/N$ such that there is a $k \in \mathbb{N}$ such that $(x + N)^k = N$. Then, $x^k + N = N$ and so $x^k \in N$. Hence, x^k is nilpotent in R. There then exists an $m \in \mathbb{N}$ such that $(x^k)^m = 0_R$. Therefore, $x \in N$ as $x^{km} = 0_R$. Hence, $x + N = N$. It follows that the nilradical of R/N is trivial.

14. Let R be an integral domain with $\text{char}R > 0$. Suppose that $\text{char}R = mn$ for $1 < m, n < mn$. Let $f : \mathbb{Z} \to R$ be the ring homomorphism given by $f(x) = x \cdot 1_R$. Then, $0_R = f(mn) = f(m)f(n)$. As R is an integral domain, $f(m) = 0_R$ or $f(n) = 0_R$. In either case, this contradicts $\text{char}R = mn$ as $m, n < mn$. Therefore, $\text{char}R$ cannot be composite. $\text{char}R$ must be prime or 0.

15.

16.

17.

3.4 - Ideals and Quotient Rings: Remarks and Examples

1. Let R be a ring and let $\{I_\alpha\}_{\alpha\in A}$ be a family of ideals in R. Let

$$\sum_{\alpha\in A} I_\alpha = \left\{\sum_{\alpha\in A} r_\alpha \mid r_\alpha \in I_\alpha \text{ and } r_\alpha = 0_R \text{ for all but finitely many } \alpha \in A\right\}$$

Let $x = \sum_{\alpha\in A} r_\alpha, y = \sum_\alpha r'_\alpha$ be elements in $\sum_{\alpha\in A} I_\alpha$. We have that

$$x - y = \sum_{\alpha\in A} r_\alpha - \sum_{\alpha\in A} r'_\alpha = \sum_{\alpha\in A} (r_\alpha - r'_\alpha) \in \sum_{\alpha\in A} I_\alpha$$

as $r_\alpha - r'_\alpha \in I_\alpha$ for all $\alpha \in A$ and $r_\alpha - r'_\alpha = 0_R$ for all but finitely many $\alpha \in A$. Let $s \in R$ and $x = \sum_{\alpha\in A} r_\alpha \in \sum_{\alpha\in A} I_\alpha$. Then,

$$sx = s\left(\sum_{\alpha\in A} r_\alpha\right) = \sum_{\alpha\in A} sr_\alpha \in \sum_{\alpha\in A} I_\alpha$$

$$xs = \left(\sum_{\alpha\in A} r_\alpha\right)s = \sum_{\alpha\in A} sr_\alpha \in \sum_{\alpha\in A} I_\alpha$$

as I_α is an ideal for all $\alpha \in A$ and $sr_\alpha = 0_R, r_\alpha s = 0_R$ for all but finitely many $\alpha \in A$. Therefore, $\sum_{\alpha\in A} I_\alpha$ is an ideal in R. Let J be an ideal of R containing I_α for all $\alpha \in A$. Then, as J is closed under addition, J must contain $\sum_{\alpha\in A} r_\alpha$ where $r_\alpha = 0_R$ for all but finitely many $\alpha \in A$ and $r_\alpha \in I_\alpha$. Hence, $\sum_{\alpha\in A} I_\alpha \subseteq J$. It follows that $\sum_{\alpha\in A} I_\alpha$ is the smallest ideal containing each I_α.

2. Let $\varphi : R \to S$ is a surjective ring homomorphism where R is a Noetherian ring. Let J be an ideal of S. We have that $I = \varphi^{-1}(J)$ is an ideal of R, and since R is Noetherian, I is finitely generated. Hence, $I = (a_1, ..., a_n)$ for some $a_1, ..., a_n \in R$. Let $x \in J$. Then, there exists a $x' \in I$ such that $\varphi(x') = x$. We have that $x' = r_1a_1 + ... + r_na_n$ for some $r_1, ..., r_n \in R$. Then, $x = \varphi(x') = \varphi(r_1x_1 + ... + r_nx_n) = \varphi(r_1)\varphi(x_1) + ... + \varphi(r_n)\varphi(x_n)$. Hence, $J \subseteq (\varphi(x_1), ..., \varphi(x_n))$. Now, let $x \in (\varphi(x_1), ..., \varphi(x_n))$. We have that $x = s_1\varphi(x_1) + ... + s_n\varphi(x_n)$. As φ is surjective, for each s_i, there is an $r_i \in R$ such that $\varphi(r_i) = s_i$. We have that $x = \varphi(r_1x_1 + ... + r_nx_n)$. Note that $r_1x_1 + ... + r_nx_n \in I$, and so $x \in J$. It follows that $J = (\varphi(x_1), ..., \varphi(x_n))$. Therefore, J is finitely generated. It follows that S is Noetherian.

3. Let $(2, x) \in \mathbb{Z}[x]$ be the ideal generated by 2 and x in $\mathbb{Z}[x]$. Suppose that $(2, x) = (f(x))$ for some $f \in \mathbb{Z}[x]$. As $2 \in (2, x)$, we must have that $2 = fg$ for some $g \in \mathbb{Z}[x]$. We have that $\deg(fg) = \deg(2) = 0$ and, as $\mathbb{Z}$ is an integral domain, $\deg(f) + \deg(g) = 0$. It follows that $\deg(f) = \deg(g) = 0$. Hence, $f(x) = a$ and $g(x) = b$ for some $a, b \in \mathbb{Z}$. We have that $2 = fg = ab$. This forces $f = \pm 1$ or $f = \pm 2$. If $f = 1$ or $f = -1$, then $(f) = \mathbb{Z}[x] \neq (2, x)$. If $f = 2$ or $f = -2$, then (f) is the set of all polynomials with even coefficients. Thus, $x \notin (f)$. In both cases, $(f) \neq (2, x)$. It follows that such an f cannot exist. Therefore, $(2, x)$ is not principal in $\mathbb{Z}[x]$.

4. Let k be a field and let I be an ideal of $k[x]$. If $I = (0)$, then I is principal. If $I \neq (0)$, then let $f \in I$ be a non-zero polynomial of minimal degree. Let a be the leading coefficient of f. We have that $g = a^{-1}f$ is a monic polynomial. Let $h \in I$. Then, $h = gp + r$ for some $p, r \in k[x]$ where $\deg r < \deg g$. As $g \in I$, we have that $gp \in I$ and so $r = h - gp \in I$. By minimality of g, r must be the zero polynomial. Hence, $h = gp$. It follows that $I = (g(x))$. Therefore, $k[x]$ is a principal ideal domain.

5. Let I, J be ideal of R, where R is a commutative ring, such that $I + J = (1_R)$. Let $x \in I \cap J$. Then, $x \in I$ and $y \in J$. As $I + J = (1)$, we have that $1_R = i + j$ for some $i \in I$ and $j \in J$. Then, $x = x1_R = x(i + j) = xi + xj = ix + xj$. We have that $ix \in IJ$ and $xj \in IJ$ and so $xi + ix \in IJ$. Hence, $x \in IJ$. Therefore, $I \cap J \subseteq IJ$. It follows that $IJ = I \cap J$.

6. Let R be a commutative ring and I, J be ideals of R such that $I \cap J \neq IJ$. Then, there exists an $x \in I \cap J$ such that $x \notin IJ$. As $x \notin IJ$, $x + IJ$ is not the zero element in R/IJ. As $x \in I \cap J$, we have that $x \in I$ and $x \in J$, hence, $x^2 \in IJ$. Therefore, $(x + IJ)^2 = x^2 + IJ = IJ$. Thus, R/IJ contains nilpotent elements. By taking the contrapositive statement, it follows that if R/IJ is reduced, then $I \cap J = IJ$.

7. Let k be a field and I an ideal of $k[x]$. Suppose that $I = (f(x)) = (g(x))$. Then, $f(x) = P(x)g(x)$ and $g(x) = Q(x)f(x)$. Hence, $f(x) = P(x)Q(x)g(x)$. It follows that $P(x)Q(x) = 1$. We must have that $P(x) = a$ and $Q(x) = a^{-1}$ for $a \in k$. Thus, $f(x) = ag(x)$. It follows that there is a unique monic polynomial that generates I.

8. Let R be a ring and let $f \in R[x]$ be a monic polynomial. Let $g \in R[x]$ be a polynomial of degree $n \geq 0$. Let a_n be the leading coefficient of g. Then, the leading coefficient of fg is $a_n \neq 0$. We have that $\deg(fg) = \deg(f) + \deg(g)$. Let $h \in R[x]$ be a polynomial such that $fh = 0$. We have that $0 = \deg(0) = \deg(fh) = \deg(f) + \deg(h)$. It follows that $\deg(f) = 0$, so $f = 1$ as f is a monic polynomial of degree 0. As $fh = 0$, we must have that $0 = fh = 1h = h$. Hence, h is the zero polynomial. Therefore, f cannot be a left zero divisor. A similar argument can also show that f cannot be a right zero divisor.

9.

10. Let d be a non-square integer. Let $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Z}\}$. We have that for each $x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, $x + y\sqrt{d} + (-x - y\sqrt{d}) = 0$. Let $x_1 + y_1\sqrt{d}, x_2 + y_2\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. We have that

$$(x_1 + y_1\sqrt{d}) + (-x_2 - y_2\sqrt{d}) = (x_1 - x_2) + (y_1 - y_2)\sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

$$(x_1 + y_1\sqrt{d})(x_2 + y_2\sqrt{d}) = x_1x_2 + dy_1y_2 + (x_1y_2 + x_2y_1)\sqrt{d} \in \mathbb{Q}(\sqrt{d})$$

Hence, $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$. Define $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ by $N(x + y\sqrt{d}) = a^2 - b^2d$. For $z = z_1 + z_2\sqrt{d}, w = w_1 + w_2\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, we have that

$$N(zw) = N((z_1 + z_2\sqrt{d})(w_1 + w_2\sqrt{d}) = N(z_1w_1 + dz_2w_2 + (z_1w_2 + z_2w_1)\sqrt{d}) = (z_1w_1 + dz_2w_2)^2 - (z_1w_2 + z_2w_1)^2d$$

$$= (z_1^2w_1^2 + 2z_1w_1z_2w_2 + z_2^2w_2^2d^2) - (z_1^2w_2^2 + 2z_1w_2w_1z_2 + z_2^2w_1^2)d = z_1^2w_1^2 - z_1^2w_2^2d + z_2^2w_2^2d^2 - z_2^2w_1^2d$$
$$= (z_1^2 - z_2^2d)(w_1^2 - w_2^2d) = N(z)N(w)$$

11.

12.

13.

14.

15. Let $\varphi : R \to S$ be a homomorphism of commutative rings and let I be a prime ideal of S. Let $x, y \in R$ such that $xy \in \varphi^{-1}(I)$. We have that $\varphi(x)\varphi(y) = \varphi(xy) \in I$. By primality of I, $\varphi(x) \in I$ or $\varphi(y) \in I$. Hence, $x \in \varphi^{-1}(I)$ or $y \in \varphi^{-1}(I)$. Therefore, $\varphi^{-1}(I)$ is a prime ideal of R. Let $(0) \subseteq \mathbb{Q}$. As $\mathbb{Q}$ is a field, (0) is a maximal ideal. Let $i : \mathbb{Z} \to \mathbb{Q}$ be the inclusion map. We have that $i^{-1}((0)) = (0) \subseteq \mathbb{Z}$ is not maximal in $\mathbb{Z}$. Therefore, the inverse image of a maximal ideal is not necessarily maximal.

16. Let R be a commutative ring and let P be a prime ideal of R. Suppose that 0 is the only zero-divisor of R contained in P. Let $x, y \in R$ such that $xy = 0$. As $xy = 0 \in P$, we have that $x = 0$ or $y = 0$. By assumption, $x = 0$ or $y = 0$. Therefore, R is an integral domain.

17. Let K be a compact topological space and R the ring of all real-valued functions on K, with addition and multiplication defined pointwise.

(i) For $p \in K$, defined $M_p = \{f \in R \mid f(p) = 0\}$. Define $\varphi : R \to \mathbb{R}$ by $\varphi(f) = f(p)$. We have that M_p is precisely the kernel of this map. For any $r \in \mathbb{R}$, we have that $f : K \to \mathbb{R}$ defined by $f(x) = r$ is continuous, hence, $f \in R$. Thus, φ is surjective. By the first isomorphism theorem, $R/M_p \cong \mathbb{R}$, and so R/M_p is a field. Therefore, M_p is a maximal ideal.

(ii) Let $n > 1$ and let $f_1, ..., f_n \in R$ such that they have no common zeros. Define $g = f_1^2 + ... + f_n^2$. We have that g has no zeros in K and $g \in (f_1, ..., f_n)$, the ideal generated by $f_1, ..., f_n$. As g has no zeros, $1/g \in R$. Thus, $1 = g(1/g) \in (f_1, ..., f_n)$. Therefore, $(1) = (f_1, ..., f_n)$

(iii)

18. Let R be a commutative ring and N be the nilradical of R. Let P be a prime ideal of R. Let $x \in N$. Then, $x^n = 0_R$ for some $n \in \mathbb{N}$. As P is an ideal, $0_R \in P$. Then, $x^{n-1}x \in P$. As P is prime, $x^{n-1} \in P$ or $x \in P$. If $x \in P$, then we are done. If $x^{n-1} \in P$, then $x = x^{2-n}x^{n-1} \in P$ as P is an ideal. Therefore, $N \subseteq P$.

19.

(i) Let R be a commutative ring with prime ideal P. Let I, J be ideals of R such that $IJ \subseteq P$. Without loss of generality, suppose that $J \nsubseteq P$. Then, there is an $x \in J$ such that $x \notin P$. Let $y \in I$. We have that $yx \in IJ \subseteq P$, and so $y \in P$ or $x \in P$. This forces $y \in P$. Therefore, $I \subseteq P$. Now, suppose that $I_1, ..., I_n$ are ideals of R such that $I_1 ... I_n \subseteq P$. Then, $I_k \subseteq P$ or $I_1 ... I_{k-1}I_{k+1} ... I_n \subseteq P$. By repeating this argument, we have that $I_k \subseteq P$ for some k.

(ii) Consider the ideals $I_n = (n)$ of $\mathbb{Z}$. We have that $\bigcap_{n=1}^{\infty} I_n = (0) \subseteq (0)$, however, (0) does not contain any of I_n.

20. Let M be a two-sided ideal in a ring R. Suppose M is maximal. We have that the only ideals containing M are R and M itself. Hence, the only ideals of R/M are R/M and M/M as there are a bijection between ideals containing M and ideals of R/M. It follows R/M is simple. For the converse, suppose that R/M is simple. Again, as there are a bijection between ideals containing M and ideals of R/M, the only ideals containing M are R and M itself, so the maximality of M follows.

21. Let k be an algebraically closed field and let I be an ideal of $k[x]$. Suppose that I is maximal. As k is a field, it is a PID, and so $k[x]$ is a PID. Then, $I = (f(x))$ for some $f \in k[x]$. We note that f is not a constant polynomial, otherwise $I = k[x]$ as k is a field. There then exists an $a \in k$ such that $f(a) = 0_k$ as a is algebraically closed. Hence, $f(x) = g(x)(x-a)$ for some $g \in k[x]$. We have that $f \in (x-a)$ and so $I \subseteq (x-a)$. By maximality, $I = (x-a)$. For the converse, suppose that $I = (x-a)$. By Proposition 4.6, $k[x]/I \cong k$. As k is a field, I is maximal.

22. We have that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{R} \oplus \mathbb{R} \cong \mathbb{C}$ by Proposition 4.6. As $\mathbb{C}$ is a field, (x^2+1) is a maximal ideal.

23.

24. Consider the following chain of ideals of $\mathbb{Z}[x]$

$$(0) \subset (x) \subset (2,x) \subset \mathbb{Z}[x]$$

We have that (x) is a prime ideal as $\mathbb{Z}[x]/(x) \cong \mathbb{Z}$ is an integral domain. Aswell as that, $(2,x)$ is a prime ideal as

$$\mathbb{Z}[x]/(2,x) \cong \frac{\mathbb{Z}[x]/(x)}{(2,x)/(x)} \cong \frac{\mathbb{Z}}{(2)} \cong \mathbb{Z}/2\mathbb{Z}$$

is also an integral domain. Therefore, the Krull dimension of $\mathbb{Z}[x]$ is atleast 2.

3.5 - Modules Over a Ring

1.

2.

3. Let M be a module over a ring R. For all $m \in M$, we have that $0_R \cdot m = (0_R + 0_R) \cdot m = 0_R \cdot m + 0_R \cdot m$. Hence, $0_R \cdot m = 0_M$. Furthermore, $(-1) \cdot m + m = (-1) \cdot m + 1 \cdot m = (-1+1) \cdot m = 0_R \cdot m = 0$. Hence, $(-1) \cdot m = -m$.

4. Let M, N be simple R-modules and let $\varphi : M \to N$ be a homomorphism of R-modules. As M is simple, $\ker \varphi = 0$ or $\ker \varphi = M$. If $\ker \varphi = M$, then immediately $\varphi = 0$. Suppose $\ker \varphi = 0$. As N is simple, $\operatorname{im} \varphi = 0$ or $\operatorname{im} \varphi = N$. If $\operatorname{im} \varphi = 0$, then $\varphi = 0$ immediately. Suppose that $\operatorname{im} \varphi = N$. Then, φ is surjective. Let $x, y \in M$ such that $\varphi(x) = \varphi(y)$. Then, $\varphi(x) - \varphi(y) = 0_N$ and so $\varphi(x-y) = 0_N$. We have that $x - y \in \ker \varphi$ and so $x - y = 0_M$. Hence, $x = y$. Therefore, φ is injective. It follows that φ is bijective and, thus, an isomorphism.

5. Let R be a commutative ring, viewed as a module over itself. Define $\varphi : M \to \operatorname{Hom}_{R\text{-}\mathsf{Mod}}(R, M)$ by $\varphi(m) = \lambda_m$ where $\lambda_m : R \to M$ is defined by $\lambda_m(x) = x \cdot m$. We have that for all $m, n \in M$ and $r \in R$,

$$\varphi(m+n) = \lambda_{m+n} = x \cdot (m+n) = x \cdot m + x \cdot n = \lambda_m + \lambda_n = \varphi(m) + \varphi(n)$$

$$\varphi(r \cdot m) = \lambda_{r \cdot m} = x \cdot (r \cdot m) = (xr) \cdot m = (rx) \cdot m = r(x \cdot m) = r\lambda_m = r\varphi(m)$$

Suppose that $\sigma \in \operatorname{Hom}_{R\text{-}\mathsf{Mod}}(R, M)$. Then, for all $x \in R$, $\sigma(x) = \sigma(x \cdot 1) = x\sigma(1) = \lambda_{\sigma(1)}$. Hence, φ is surjective. Suppose that $\lambda_m, \lambda_n \in \operatorname{Hom}_{R\text{-}\mathsf{Mod}}(R, M)$ such that $\lambda_m = \lambda_n$ for all $x \in R$. By setting $x = 1$, we obtain $m = n$. Hence, φ is injective. It follows that φ is an isomorphism.

6. Let G be an abelian group with the structure of a $\mathbb{Q}$-vector space. We have that the inclusion homomorphism $i : \mathbb{Z} \to \mathbb{Q}$ is an epimorphism. Suppose that there exists homomorphisms $\sigma_1, \sigma_2 : \mathbb{Q} \to \operatorname{End}_{\mathsf{Ab}}(G)$. We have that $(\sigma_1 \circ i)(x) = \sigma_1(x) = \sum_x \sigma_1(1) = \sum_x 1_{\operatorname{End}_{\mathsf{Ab}}(G)}$ and $(\sigma_2 \circ i)(x) = \sigma_2(x) = \sum_x \sigma_2(1) = \sum_x 1_{\operatorname{End}_{\mathsf{Ab}}(G)}$. Hence, $\sigma_1 \circ i = \sigma_2 \circ i$. As i is an epimorphism, $\sigma_1 = \sigma_2$. As a module is determined by such a homomorphism, the $\mathbb{Q}$-vector space structure on G is unique.

7.

8.

9.

10.

11.

12. Let R be a ring and let M, N be R-modules. Let $\varphi : M \to N$ be a homomorphism of modules such that it is bijective as a set function. For $n_1, n_2 \in N$, we have that there exists $m_1, m_2 \in M$ such that $\varphi(m_1) = n_1$ and $\varphi(m_2) = n_2$. We have that $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2) = n_1 + n_2$. Then, $\varphi^{-1}(n_1) + \varphi^{-1}(n_2) = m_1 + m_2 = \varphi^{-1}(n_1 + n_2)$. Furthermore, let $r \in R$ and $n \in N$. Then, there is a unique $m \in M$ such that $\varphi(m) = n$. As φ is a homomorphism, we have that $\varphi(rm) = r \cdot \varphi(m) = r \cdot n$, and so $r\varphi^{-1}(n) = rm = \varphi^{-1}(rn)$. It follows that φ^{-1} is a module homomorphism.

13. Let R be an integral domain, and let $I = (a)$ be a non-zero principal ideal of R. Define $\varphi : R \to I$ by $\varphi(x) = ax$. We have that

$$\varphi(m + n) = a(m + n) = am + an = \varphi(m) + \varphi(n)$$
$$\varphi(rm) = a(rm) = (ar)m = (ra)m = r(am) = r\varphi(m)$$

Hence, φ is an R-module homomorphism. If $\varphi(b) = 0$ for some $b \in R$, then $ab = 0$. As a is assumed non-zero, $b = 0$ as R is an integral domain. Hence, the kernel of the homomorphism is trivial. Let $x \in I$. Then, $x = ax'$ for some $x' \in R$. Hence, φ is surjective. By the first isomorphism theorem, $R \cong I$.

14. Let N, P be submodules of an R-module M. We have that $N + P$ is a subgroup of M. Let $r \in R$ and $x = n + p \in N + P$. Then, $rx = r(n + p) = rn + rp \in N + P$ as $rn \in N$ and $rp \in P$. Hence, $N + P$ is a submodule of M. Furthermore, we have that $N \cap P$ is a submodule of P. Indeed, $N \cap P$ is a subgroup of P and if $r \in R$ and $x \in N \cap P$, then $rx \in N \cap P$ as $rx \in N$ and $rx \in P$ given that N and P are submodules of M. Define the map $\varphi : P \to N + P/N$ by $\varphi(p) = pN$. We have that

$$\varphi(x + y) = (x + y)N = xN + yN = \varphi(x) + \varphi(y)$$
$$\varphi(r \cdot x) = (r \cdot x)N = r \cdot (xN) = r \cdot \varphi(x)$$

Therefore, φ is an R-module homomorphism. Next, we have that

$$\ker\varphi = \{p \in P \mid \varphi(p) = 1_{N+P/N}\} = \{p \in P \mid pN = N\} = \{p \in P \mid p \in N\} = P \cap N$$

Hence, by the first isomorphism theorem, $P/P \cap N \cong (N + P)/N$.

15.

16. Let R be a commutative ring, M an R-module, and let $a \in R$ be a nilpotent element in R. Suppose that $M = 0$. Then, $aM = 0 = M$. For the converse, suppose that $aM = M$. Let $m \in M$. We have that there exists an m' such that $m = am'$. Then, there exists an m'' such that $m = a(am'') = a^2m''$. For each $k \in \mathbb{N}$, there is some $n \in M$ such that $m = a^k n$. As a is nilpotent, it follows that $m = 0$. Therefore, M is the trivial module.

17.

18.

3.6 - Products, Coproducts, etc., In R-Mod

1. Let A be a set and R a ring. Let $\alpha \in R^{\oplus A}$. Then, $\alpha(x) = \sum_{a \in A} \alpha(a) j_a(x)$. Hence, $\alpha(x) \in \langle j_a \mid a \in A \rangle$. We have that $R^{\oplus A} = \langle j_a \mid a \in A \rangle$. Define $j : A \to R^{\oplus A}$ by $j(a) = j_a$. Let $f : A \to M$ be a set function, where M is an R-module, and let $\varphi : R^{\oplus A} \to M$ be an R-module homomorphism such that $\varphi \circ j = f$. For each $a \in A$, we have tht $f(a) = (\varphi \circ j)(a) = \varphi(j_a)$. Hence, for any $\sum_{a \in A} r_a j_a \in R^{\oplus}$, we have that $\varphi(\sum_{a \in A} r_a j_a) = \sum_{a \in A} r_a \varphi(j_a) = \sum_{a \in A} r_a f(a)$. We have that φ is unique. Therefore, $R^{\oplus A}$ satisfies the universal property for the free R-module generated by A. Thus, $R^{\oplus A} \cong F^R(A)$

2.

3. Let R be a ring, M an R-modul, and $p : M \to M$ an R-module homomorphism such that $p^2 = p$. Define $\varphi : M \to \ker p \oplus \operatorname{im} p$ by $\varphi(m) = (m - p(m), p(m))$. We have that $\varphi(m) \in \ker p \oplus \operatorname{im} p$ for all $m \in M$ as $p(m - p(m)) = p(m) - p(p(m)) = p(m) - p(m) = 0$, hence, $m - p(m) \in \ker p$ and $p(m) \in \operatorname{im} p$. Furthermore,

$$\varphi(m+n) = (m+n-p(m+n), p(m+n)) = (m+n-p(m)-p(n), p(m)+p(n)) = (m-p(m), p(m))+(n-p(n), p(n))$$

$$= \varphi(m) + \varphi(n)$$

$$\varphi(r\cdot m) = (r\cdot m-p(r\cdot m), p(r\cdot m)) = (r\cdot m-r\cdot p(m), r\cdot p(m)) = (r\cdot(m-p(m)), r\cdot p(m)) = r\cdot(m-p(m), p(m)) = r\cdot\varphi(m)$$

for all $r \in R$ and $m, n \in M$. Thus, φ is an R-module homomorphism. Next, we have that

$$\ker\varphi = \{m \in M \mid \varphi(m) = 0\} = \{m \in M \mid m - p(m) = 0 \text{ and } p(m) = 0\} = \{m \in M \mid m = 0\} = \{0\}$$

Hence, φ is injective by Proposition 6.2. Let $(x, y) \in \ker p \oplus \operatorname{im} p$. Then, $p(x) = 0$ and there is a $z \in M$ such that $p(z) = y$. We have that

$$\varphi(x + p(z)) = (x + p(z) - p(x + p(z)), p(x + p(z))) = (x + p(z) - p(x) - p(p(z)), p(x) + p(p(z)))$$

$$= (x + p(z) - 0 - p(z), 0 + p(z)) = (x, y)$$

Hence, φ is surjective. We have that φ is a bijective R-module homomorphism. Therefore, $M \cong \ker p \oplus \operatorname{im} p$.

4. Let R be a ring and let $n > 1$. View $R^{\oplus(n-1)}$ as a submodule of $R^{\oplus n}$ via the homomorphism $R^{\oplus(n-1)} \to R^{\oplus n}$ defined by $(r_1, ..., r_{n-1}) \mapsto (r_1, ..., r_{n-1}, 0)$. Define $\varphi : R^{\oplus n} \to R$ by $\varphi(r_1, ..., r_n) = r_1$. We have that φ is a surjective homomorphism and $\ker\varphi \cong R^{\oplus(n-1)}$. Hence, $R^{\oplus n}/R^{\oplus(n-1)} \cong R$ by the first isomorphism theorem.

5.

6. Let R be a commutative ring and let $F = R^{\oplus n}$ be a finitely generated free R-module. Let $\lambda \in \operatorname{Hom}_{R\text{-}\mathsf{Mod}}(F, R)$. Note, for all $\mathbf{x} \in F$, we have that

$$\lambda(\mathbf{x}) = \lambda\left(\sum_{i=1}^{n} x_i j_i\right) = \sum_{i=1}^{n} x_i \lambda(j_i) \tag{$*$}$$

where $j_i = (0, ..., 1, ..., 0)$ where $1 \in R$ is placed in the ith position. Define $\varphi : F \to \operatorname{Hom}_{R\text{-}\mathsf{Mod}}(F, R)$ by sending $\mathbf{r} \in F$ to the homomorphism sending j_i to r_i. φ is clearly surjective by $(*)$. For all $\mathbf{x} \in F$, we have that for all $\mathbf{r}, \mathbf{s} \in F$ and $a \in R$,

$$\varphi(\mathbf{r} + \mathbf{s}) = \sum_{i=1}^{n} x_i(r_i + s_i) = \sum_{i=1}^{n}(x_i r_i + x_i s_i) = \sum_{i=1}^{n} x_i r_i + \sum_{i=1}^{n} x_i s_i = \varphi(\mathbf{r}) + \varphi(\mathbf{s})$$

$$\varphi(a\mathbf{r}) = \sum_{i=1}^{n} x_i a r_i = \sum_{i=1}^{n} a x_i r_i = a\sum_{i=1}^{n} x_i r_i = a\varphi(\mathbf{r})$$

Thus, φ is a homomorphism. Let $\mathbf{r} \in F$ such that $\varphi(\mathbf{r}) = 0$. Then,

$$\varphi(\mathbf{r}) = 0 \implies \forall \mathbf{x} \in F,\ \sum_{i=1}^{n} x_i r_i = 0 \implies \mathbf{r} = 0$$

Thus, φ is injective. It follows that φ is an isomorphism. Therefore, $\operatorname{Hom}_{R\text{-}\mathsf{Mod}}(F, R) \cong F$. View $\mathbb{Q}$ as a $\mathbb{Z}$-module. Let $\psi \in \operatorname{Hom}_{\mathbb{Z}\text{-}\mathsf{Mod}}(\mathbb{Q}, \mathbb{Z})$. We have that $\psi(1) = 2^n\psi(1/2^n)$ for all $n \in \mathbb{N}$. Hence, $2^n \mid \psi(1)$ for all $n \in \mathbb{N}$. Therefore, $\psi(1) = 0$. Let $x \in \mathbb{Q}$. We have that $\psi(x) = x\psi(1) = x0 = 0$. Thus, ψ is the trivial homomorphism. We must have that $\operatorname{Hom}_{\mathbb{Z}\text{-}\mathsf{Mod}}(\mathbb{Q}, \mathbb{Z}) = 0$.

7.

8.

9. Let R be a ring, F a non-zero free R-module, and let $\varphi : M \to N$ be an R-module homomorphism. Suppose that φ is onto. Let $\alpha : F \to N$ be an R-module homomorphism. As F is free, $F \cong R^{\oplus A} = \langle j_a \mid a \in A \rangle$ for some set A. For each $\alpha(a) \in N$, as φ is onto, there is some $m_a \in M$ such that $\varphi(m_a) = \alpha(j_a)$. Define $\beta : F \to M$ by $\beta(\sum_{a\in A} r_a j_a) = \sum_{a\in A} r_a m_a$. We have that β is a well-defined R-module homomorphism such that for all $x \in F$

$$(\varphi \circ \beta)(x) = \varphi(\beta(x)) = \varphi\left(\beta\left(\sum_{a\in A} x_a j_a\right)\right) = \varphi\left(\sum_{a\in A} x_a m_a\right) = \sum_{a\in A} x_a \alpha(j_a) = \alpha\left(\sum_{a\in A} x_a j_a\right) = \alpha(x)$$

For the converse, suppose that for all homomorphisms $\alpha : F \to N$, there exists a $\beta : F \to M$ such that $\alpha = \varphi \circ \beta$. Let $x \in N$. Define $\alpha : F \to N$ sending some j_a to x and sending all other j_a to 0. We have that for some $a \in A$, $x = \alpha(j_a) = (\varphi \circ \beta)(j_a)$, hence, $x \in \text{im } \varphi$. Thus, φ is onto.

10. Let M, N and Z be R-modules and let $\mu : M \to Z, \nu : N \to Z$ be R-module homomorphisms. Let $\varphi : M \oplus N \to Z$ be a map defined by $\varphi((m, n)) = \mu(m) - \nu(n)$. We have that for all $(m, n), (m', n') \in M \oplus N$ and $r \in R$,

$$\begin{aligned}
\varphi((m, n) + (m', n')) &= \varphi((m + m', n + n')) \\
&= \mu(m + m') - \nu(n + n') \\
&= \mu(m) + \mu(m') - \nu(n) - \nu(n') \\
&= \mu(m) - \nu(n) + \mu(m') - \nu(n') \\
&= \varphi((m, n)) + \varphi((m', n'))
\end{aligned}$$

$$\begin{aligned}
\varphi(r(m, n)) &= \varphi((rm, rn)) \\
&= \mu(rm) - \nu(rn) \\
&= r\mu(m) - r\nu(n) \\
&= r(\mu(m) - \nu(n)) \\
&= r\varphi((m, n))
\end{aligned}$$

Hence, φ is an R-module homomorphism. Define

$$M \times_Z N = \ker \varphi = \{(m, n) \in M \oplus N \mid \mu(m) - \nu(n) = 0\} = \{(m, n) \in M \oplus N \mid \mu(m) = \nu(n)\}$$

We note that $M \times_Z N$ is a submodule of $M \oplus N$ as it is a kernel of a homomorphism, hence, an R-module. Let $\pi_M : M \times_Z N \to M$ be the projection map restricted to $M \times_Z N$ and $\pi_N : M \times_Z N \to N$ be the projection map restricted to $M \times_Z N$. We note both are R-module homomorphisms as they are restrictions of R-module homomorphisms to a submodule. Let P be an R-module and $\varphi_M : P \to M, \varphi_N : P \to N$ be R-module homomorphisms such that $\nu\varphi_N = \mu\varphi_M$. Let $(m, n) \in M \times_Z N$. Then, $\nu\pi_N(m, n) = \nu(n) = \mu(m) = \mu\pi_M(m, n)$. Hence, $\nu\pi_N = \mu\pi_M$. We now set to prove there exists a unique R-module homomorphism ψ such that the following diagram commutes,

$$\begin{tikzcd}
P \arrow[dr, "\psi"] \arrow[drr, bend left, "\varphi_N"] \arrow[ddr, bend right, "\varphi_M"'] & & \\
& M \times_Z N \arrow[r, "\pi_N"] \arrow[d, "\pi_M"'] & N \arrow[d, "\nu"] \\
& M \arrow[r, "\mu"'] & Z
\end{tikzcd}$$

We have that $\pi_N\psi = \varphi_N$ and $\pi_M\psi = \varphi_M$. Hence, $\psi = (\varphi_N, \varphi_M)$. We have that ψ is an R-module homomorphism as φ_N, φ_M are R-module homomorphisms. We also note ψ is unique. The claim follows. Therefore, R-Mod has fibered products.

11. Let M, N and Z be R-modules and let $\mu : Z \to M, \nu : Z \to N$ be R-module homomorphisms. Let $I = \langle(\mu(x), -\nu(x)) \mid x \in Z\rangle$ be an ideal of $M \oplus N$ generated by elements of the form $(\mu(x), -\nu(x))$. Define $M \oplus_Z N$ to be the quotient module $(M \oplus N)/I$. Define $i_N : N \to M \oplus_Z N$ by $i_N(n) = (0, n) + I$ and $i_M : M \to M \oplus_Z N$ by $i_M(m) = (m, 0) + I$. Note that for any $x \in Z$,

$$\begin{aligned}
(i_M \circ \mu - i_N \circ \nu)(x) &= i_M(\mu(x)) - i_N(\nu(x)) \\
&= ((\mu(x), 0) + I) - ((0, \nu(x)) + I) \\
&= (\mu(x), 0) - (0, \nu(x)) + I \\
&= (\mu(x), -\nu(x)) + I \\
&= I
\end{aligned}$$

Therefore, $i_M \circ \mu = i_N \circ \nu$. Let P be a R-module and let $\varphi_N : N \to P$ and $\varphi_M : M \to P$ be homomorphisms such that $\varphi_N \circ \nu = \varphi_M \circ \mu$. Suppose the following diagram commutes for some homomorphism $\psi : M \oplus_Z N \to P$,

$$\begin{tikzcd}
P & & \\
& M \oplus_Z N \arrow[ul, "\psi"] & N \arrow[l, "i_N"'] \arrow[ull, bend right, "\varphi_N"'] \\
& M \arrow[u, "i_M"] \arrow[uul, bend left, "\varphi_M"] & Z \arrow[l, "\mu"] \arrow[u, "\nu"']
\end{tikzcd}$$

For all $x \in N$, we have that $\varphi_N = \psi \circ i_N$ so $\varphi_N(x) = \psi((0, x) + I)$. For all $x \in M$, we have that $\varphi_M = \psi \circ i_M$ so $\varphi_M(x) = \psi((x, 0) + I)$. Hence,

$$\begin{aligned}
\psi((m, n) + I) &= \psi((m, 0) + I + (0, n) + I) \\
&= \psi((m, 0) + I) + \psi((0, n) + I) \\
&= \varphi_M(m) + \varphi_N(n)
\end{aligned}$$

ψ is the a unique R-module homomorphism for which the diagram commutes. It follows R-Mod has fibered coproducts.

12.

13. Let M, N be R-modules and let $\varphi : M \to N$ be a surjective homomorphism. Suppose further that M is finitely generated. Then, $M = \langle m_1, ..., m_n \rangle$ for some $m_1, ..., m_n \in M$. Let $x \in N$. As φ is surjective, there is some $x' \in M$ such that $\varphi(x') = x$. We have that $x' = \sum_{i=1}^n r_i m_i$ for some $r_i \in R$. Thus,

$$x = \varphi(x') = \varphi\left(\sum_{i=1}^n r_i m_i\right) = \sum_{i=1}^n r_i \varphi(m_i)$$

Therefore, $x \in \langle \varphi(m_1), ..., \varphi(m_n) \rangle$. It follows that N is finitely generated.

14. Suppose that $(x_1, x_2, ...)$ is finitely generated as a submodule of $\mathbb{Z}[x_1, x_2, ...]$. Then, $(x_1, x_2, ...) = \langle a_1, a_2, ..., a_n \rangle$ for some $a_1, a_2, ..., a_n \in \mathbb{Z}[x_1, x_2, ...]$. We have that each a_i is a finite polynomial, and so, there exists an x_k such that the coefficient of x_k and all x_l for all $l > k$ is 0. There is then a maximum x_N among all a_i, which means that $x_N \notin \langle a_1, a_2, ..., a_n \rangle$. Therefore, $(x_1, x_2, ...)$ cannot be finitely generated.

15.

16. Let R be a ring and let M be a simple R-module. Let $x \in M$ such that $x \neq 0$. We have that $\langle x \rangle$ is a submodule of M. As M is simple, $\langle x \rangle = M$ as $\langle x \rangle$ contains $x \neq 0$. Thus, M is cyclic. For the next part, suppose that M is an R-module that is cyclic. We have that $M = \langle x \rangle$ for some $x \in M$. View R as a module over itself and define the R-module homomorphism $\varphi : R \to M$ by $\varphi(r) = rx$. φ is clearly surjective and so $M \cong R/I$, where $I = \ker \varphi$, by the first isomorphism theorem. For the converse, suppose that $M \cong R/I$ for some ideal I of R. We have that $\langle 1 + I \rangle$ is a submodule of R/I. Let $x + I \in R/I$. Then, $x + I = x \cdot (1 + I) \in \langle 1 + I \rangle$. It follows that $R/I = \langle 1 + I \rangle$. Therefore, M is cyclic. Finally, let M be a cyclic module with submodule N. We have that $M \cong R/I$ for some ideal I and so $N \cong S/I$ for some submodule S of R. Then, $M/N \cong (R/I)/(S/I) \cong R/S$. Hence, M/N is cyclic.

17.

(i) Let M be a cyclic R-module so that $M \cong R/I$ for some ideal I, and let N be another R-module. Denote $\{n \in N \mid \forall a \in I, an = 0\}$ by $\mathrm{Ann}_I(N)$. We note this is a submodule of N. Let $\lambda \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R/I, N)$. Then, $\lambda(1+I) \in \mathrm{Ann}_I(N)$ as, for all $a \in I$, we have that $a \cdot \lambda(1+I) = \lambda(a \cdot (1+I)) = \lambda(a+I) = \lambda(I) = 0$. Define $\varphi : \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R/I, N) \to \mathrm{Ann}_I(N)$ by sending $\lambda \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R/I, N)$ to $\lambda(1+I)$. For $\lambda_1, \lambda_2 \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R/I, N)$, we have that $\varphi(\lambda_1 + \lambda_2) = (\lambda_1 + \lambda_2)(1+I) = \lambda_1(1+I) + \lambda_2(1+I) = \varphi(\lambda_1) + \varphi(\lambda_2)$. Additionally, for $r \in R$ and $\lambda \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R/I, N)$, we have that $\varphi(r \cdot \lambda) = (r \cdot \lambda)(1+I) = r \cdot \lambda(1+I) = r \cdot \varphi(\lambda)$. Therefore, φ is an R-module homomorphism. Let $\lambda_1, \lambda_2 \in \mathrm{Hom}_{R\text{-}\mathsf{Mod}}(R/I, N)$ such that $\varphi(\lambda_1) = \varphi(\lambda_2)$. Then, $\varphi(\lambda_1 - \lambda_2) = 0$. Hence, $(\lambda_1 - \lambda_2)(1+I) = 0$. For all $x + I \in R/I$, it follows that $(\lambda_1 - \lambda_2)(x+I) = (\lambda_1 - \lambda_2)(x \cdot (1+I)) = x(\lambda_1 - \lambda_2)(1+I) = x0 = 0$. This forces $\lambda_1 = \lambda_2$ and injectivity of φ follows. Let $n \in \mathrm{Ann}_I(N)$. Define the homomorphism $\sigma : R \to N$ by $\sigma(r) = rn$. Let $i \in I$. Then, $\sigma(i) = in = 0$ as $n \in \mathrm{Ann}_I(N)$. Hence, $I \subseteq \ker \sigma$. By Theorem 5.14, there exists a unique homomorphism $\overline{\sigma} : R/I \to N$ such that $\overline{\sigma}\pi = \sigma$ where $\pi : R \to R/I$ is the canonical projection. We have that $\varphi(\overline{\sigma}) = \overline{\sigma}(1+I) = \overline{\sigma}\pi(1) = \sigma(1) = 1 \cdot n = n$. φ must then be surjective. Therefore, φ is an isomorphism. We conclude $\mathrm{Hom}_{R\text{-}\mathsf{Mod}}(M, N) \cong \mathrm{Ann}_I(N)$.

(ii)

18. Let M be an R-module and N a submodule such that M/N and N are finitely generated. As M/N and N are finitely generated, $M/N = \langle m_1 + N, ..., m_l + N \rangle$ for $m_1, ..., m_l \in M$ for some $l \in \mathbb{N}$ and $N = \langle n_1, ..., n_k \rangle$ for $n_1, ..., n_k \in N$ for some $k \in \mathbb{N}$. Let $x \in M$. We have that

$$x + N = \sum_{i=1}^{l} x_i(m_i + N) = \sum_{i=1}^{l} (x_i m_i + N) = \left(\sum_{i=1}^{l} x_i m_i \right) + N$$

for some $x_1, ..., x_l \in R$. Hence, $x - \sum_{i=1}^{l} x_i m_i \in N$. Thus,

$$x - \sum_{i=1}^{l} x_i m_i = \sum_{j=1}^{k} y_j n_j$$

for some $y_1, ...y_k \in R$. Therefore,

$$x = \sum_{i=1}^{l} x_i m_i + \sum_{j=1}^{k} y_j n_j$$

Hence, $x \in \langle m_1, ..., m_l, n_1, ..., n_k \rangle$. It follows that $M = \langle m_1, ..., m_l, n_1, ..., n_k \rangle$ and so M is finitely generated.

3.7 - Complexes and Homology

1. Let M be an R-module such that

$$\cdots \longrightarrow 0 \xrightarrow{d} M \xrightarrow{d'} 0 \longrightarrow \cdots$$

is exact. As $d : 0 \to M$ is a homomorphism, we must have that $d(0) = 0_M$, hence, d is the trivial homomorphism. As $d' : M \to 0$ is a homomorphism from M to 0, we must have that every element of M must be sent to the zero element, hence, d' is also the trivial homomorphism. We have that $d : M \to 0$ is a map with a left and right inverse, namely d', and is also a homomorphism. Therefore, d is an isomorphism. Thus, $M \cong 0$.

2. Let M, M' be R-modules and $\varphi : M \to M'$ a homomorphism such that

$$\cdots \longrightarrow 0 \longrightarrow M \xrightarrow{\varphi} M' \longrightarrow 0 \longrightarrow \cdots$$

is exact. By exactness, $\ker \varphi = 0$ and $\mathrm{im}\ \varphi = M'$. Hence, φ is a bijection. It follows that φ is an isomorphism, thus, $M \cong M'$.

3. Let $M_\bullet$ be the complex

$$\cdots 0 \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} M' \xrightarrow{\psi'} N \longrightarrow 0 \longrightarrow \cdots$$

Suppose $M_\bullet$ is exact. We have that $\ker \psi' = \text{im } \varphi$ and ψ' is surjective. By the first isomorphism theorem, $N \cong M'/\ker \psi' = M'/\text{im } \varphi \cong \text{coker } \varphi$. Additionally, ψ is injective and $\psi : L \to \ker \varphi$ is a surjective homomorphism as $\text{im } \psi = \ker \varphi$. Therefore, $L \cong \ker \varphi$.

4.

5. Assume that the complex

$$\cdots \longrightarrow L \xrightarrow{\psi} M \xrightarrow{\varphi} N \longrightarrow \cdots$$

is exact with L, N Noetherian. Let M' be a submodule of M. We have that $\varphi(M')$ is a submodule of N and is finitely generated by assumption. Suppose $\varphi(M') = \langle \varphi(x_1), ..., \varphi(x_n) \rangle$ for some $x_1, ..., x_n \in M'$. Let $x \in M'$. Then, $\varphi(x) = \sum_{i=1}^n r_i \varphi(x_i)$ for some $r_1, ..., r_n \in R$. We have that

$$0 = \varphi(x) - \sum_{i=1}^n r_i \varphi(x_i) = \varphi(x) - \varphi\left(\sum_{i=1}^n r_i x_i\right) = \varphi\left(x - \sum_{i=1}^n r_i x_i\right)$$

Thus, $x - \sum_{i=1}^n r_i x_i \in \ker \varphi = \text{im } \psi$ by exactness at M. We have that $\psi^{-1}(M')$ is a submodule of L and is finitely generated as L is Noetherian. Then, $\psi^{-1}(M') = \langle y_1, ..., y_m \rangle$ for some $y_1, ..., y_m \in L$. As $x - \sum_{i=1}^n r_i x_i \in \text{im } \psi$, we have that there is some $y \in \psi^{-1}(M')$ such that $\psi(y) = x - \sum_{i=1}^n r_i x_i \in \ker \varphi = \text{im } \psi$. We then have that

$$x - \sum_{i=1}^n r_i x_i = \psi(y) = \psi\left(\sum_{j=1}^m r_i' y_i\right) = \sum_{j=1}^m r_i' \psi(y_i)$$

for some $r_1', ..., r_m' \in R$. Therefore,

$$x = \sum_{i=1}^n r_i x_i + \sum_{j=1}^m r_i' \psi(y_i)$$

It follows that $M' = \langle x_1, ..., x_n, \psi(y_1), ..., \psi(y_n) \rangle$, hence, M is Noetherian.

6.

7.

(i) Let

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} P \longrightarrow 0$$

be a short exact sequence of R-modules, and let L be an R-module. Define $f : \text{Hom}_{R\text{-Mod}}(P, L) \to \text{Hom}_{R\text{-Mod}}(N, L)$ by $f(\lambda) = \lambda \circ \psi$. We note that ψ is an epimorphism. Let $\lambda \in \ker f$. Then, $\lambda \circ \psi = 0$. As ψ is an epimorphism, we have that $\lambda = 0$. Thus, f is a monomorphism. Define $g : \text{Hom}_{R\text{-Mod}}(N, L) \to \text{Hom}_{R\text{-Mod}}(M, L)$ by $g(\lambda) = \lambda \circ \varphi$. For any $\lambda \in \text{Hom}_{R\text{-Mod}}(P, L)$, we have that $(g \circ f)(\lambda) = g(f(\lambda)) = g(\lambda \circ \psi) = \lambda \circ \psi \circ \varphi = \lambda \circ 0 = 0$. Now, let $\sigma \in \ker g$. Then, $\sigma \circ \varphi = 0$. We have that there exists a unique $\alpha : P \to L$ such that $\sigma = \alpha \circ \psi$. Hence, $\sigma \in \text{im } f$. It follows that the chain complex

$$0 \longrightarrow \text{Hom}_{R\text{-Mod}}(P, L) \xrightarrow{f} \text{Hom}_{R\text{-Mod}}(N, L) \xrightarrow{g} \text{Hom}_{R\text{-Mod}}(M, L)$$

is exact.

(ii)

(iii)

(iv)

8. Let

$$0 \longrightarrow M \xrightarrow{\varphi} N \xrightarrow{\psi} F \longrightarrow 0$$

be a short exact sequence of R-modules with F free. We have that $\psi : N \to F$ is surjective as a set function, hence, by a previous exercise, there exists a homomorphism $\beta : F \to N$ such that $\mathrm{id}_F = \psi \circ \beta$. Therefore, ψ has a right inverse. Note that $M \cong M/0 \cong M/\ker\varphi \cong \text{im }\varphi = \ker\psi$. Hence, by Proposition 7.5, the exact sequence must split.

9.

10. Suppose the following diagram commutes with both rows exact and ν, λ are isomorphisms:

$$\begin{tikzcd}
0 \arrow[r] & L_1 \arrow[r, "\alpha_1"] \arrow[d, "\lambda"] & M_1 \arrow[r, "\beta_1"] \arrow[d, "\mu"] & N_1 \arrow[r] \arrow[d, "\nu"] & 0 \\
0 \arrow[r] & L_0 \arrow[r, "\alpha_0"] & M_0 \arrow[r, "\beta_0"] & N_0 \arrow[r] & 0
\end{tikzcd}$$

As λ, ν are isomorphisms, $\ker\lambda, \ker\nu, \text{coker }\lambda, \text{coker }\nu$ are all trivial. By the snake lemma, there is an exact sequence

$$0 \longrightarrow 0 \longrightarrow \ker\mu \longrightarrow 0 \xrightarrow{\delta} 0 \longrightarrow \text{coker }\mu \longrightarrow 0 \longrightarrow 0$$

where δ is the connecting homomorphism (although in this case it is the trivial homomorphism). By exactness, $\ker\mu \cong 0$ and $\text{coker }\mu \cong 0$. Therefore, μ is an isomorphism.

11. Let

$$0 \longrightarrow M_1 \longrightarrow N \longrightarrow M_2 \longrightarrow 0$$

be an exact sequence of R-modules. Suppose there exists an R-module homomorphism $\varphi : N \to M_1 \oplus M_2$ such that the diagram

$$\begin{tikzcd}
0 \arrow[r] & M_1 \arrow[r] \arrow[d] & N \arrow[r] \arrow[d, "\varphi"] & M_2 \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & M_1 \arrow[r] & M_1 \oplus M_2 \arrow[r] & M_2 \arrow[r] & 0
\end{tikzcd}$$

commutes, where the bottom row is the standard sequence of a direct sum and the morphisms $M_1 \to M_1, M_2 \to M_2$ are the identity maps. By the short five lemma, φ is necessarily an isomorphism. Therefore,

$$0 \longrightarrow M_1 \longrightarrow N \longrightarrow M_2 \longrightarrow 0$$

must split.

12. Suppose that the following is a commutative diagram of R-modules with exact rows, α is an epimorphism, and β, δ are monomorphisms:

$$\begin{tikzcd}
A_1 \arrow[r, "f_1"] \arrow[d, two heads, "\alpha"'] & B_1 \arrow[r, "f_2"] \arrow[d, hook, "\beta"'] & C_1 \arrow[r, "f_3"] \arrow[d, "\gamma"'] & D_1 \arrow[d, hook, "\delta"'] \\
A_0 \arrow[r, "g_1"'] & B_0 \arrow[r, "g_2"'] & C_0 \arrow[r, "g_3"'] & D_0
\end{tikzcd}$$

We prove that γ is a monomorphism. Let $x \in \ker\gamma$. By commutativity of the diagram, $\delta \circ f_3 = g_3 \circ \gamma$, hence, $(\delta \circ f_3)(x) = (g_3 \circ \gamma)(x) = g_3(\gamma(x)) = g_3(0) = 0$. As δ is a monomorphism, $f_3(x) = 0$. Thus, $x \in \ker f_3 = \text{im } f_2$. There then exists a $y \in B_1$ such that $f_2(y) = x$. By commutativity of the diagram, we have that $g_2 \circ \beta = \gamma \circ f_2$. Thus, $(g_2 \circ \beta)(y) = (\gamma \circ f_2)(y) = \gamma(f_2(y)) = \gamma(x) = 0$. We must have that $\beta(y) \in \ker g_2 = \text{im } g_1$. Hence, there is some $z \in A_0$ such that $g_1(z) = \beta(y)$. As α is an epimorphism, there is a $w \in A_1$ such that $\alpha(w) = z$. Therefore, $\beta(y) = g_1(z) = (g_1 \circ \alpha)(w) = (\beta \circ f_1)(w)$ by commutativity of the diagram again. As β is a monomorphism, $y = f_1(w)$. Finally, $x = f_2(y) = (f_2 \circ f_1)(w) = 0$ by exactness at B_1. We deduce $\ker\gamma = 0$, thus making γ a monomorphism.

13. Suppose that the following is a commutative diagram of R-modules with exact rows, ϵ is a monomorphism, and β, δ are epimorphisms:

$$\begin{tikzcd} B_1 \arrow[r, "f_2"] \arrow[d, two heads, "\beta"'] & C_1 \arrow[r, "f_3"] \arrow[d, "\gamma"'] & D_1 \arrow[r, "f_4"] \arrow[d, two heads, "\delta"'] & E_1 \arrow[d, hook, "\epsilon"'] \\ B_0 \arrow[r, "g_2"'] & C_0 \arrow[r, "g_3"'] & D_0 \arrow[r, "g_4"'] & E_0 \end{tikzcd}$$

We prove that γ is an epimorphism. Let $x \in C_0$. As δ is an epimorphism, there exists a $y \in D_1$ such that $\delta(y) = g_3(x)$. By the commutativity of the diagram, $g_4 \circ \delta = \epsilon \circ f_4$. Then, $(\epsilon \circ f_4)(y) = (g_4 \circ \delta)(y) = g_4(\delta(y)) = g_4(g_3(x)) = 0$ due to exactness at D_0. As ϵ is a monomorphism, it follows $f_4(y) = 0$. Hence, $y \in \ker f_4 = \text{im } f_3$ by exactness. There then exists a $z \in C_1$ such that $f_3(z) = y$. Define $x' = x - \gamma(z)$. We have that $g_3(x') = g_3(x - \gamma(z)) = g_3(x) - g_3(\gamma(z)) = g_3(x) - \delta(f_3(z)) = g_3(x) - \delta(y) = g_3(x) - g_3(x) = 0$. Thus, $x - \gamma(z) \in \ker g_3 = \text{im } g_2$ by exactness. There is a $y' \in B_0$ such that $g_2(y') = x'$. As β is an epimorphism, there is a $z' \in B_1$ such that $\beta(z') = y'$. By commutativity of the diagram, $g_2 \circ \beta = \gamma \circ f_2$. Hence, $(\gamma \circ f_2)(z') = (g_2 \circ \beta)(z') = g_2(\beta(z')) = g_2(y') = x'$. Hence, $(\gamma \circ f_2)(z') = x' = x - \gamma(z)$. Therefore, $x = (\gamma \circ f_2)(z') + \gamma(z) = \gamma(f_2(z') + z)$. We conclude that $x \in \text{im } \gamma$. It follows that γ is an epimorphism.

14. Suppose the following diagram commutes with α an epimorphism, ϵ a monomorphism, β, δ isomorphisms and with both rows exact:

$$\begin{tikzcd} A_1 \arrow[r] \arrow[d, two heads, "\alpha"'] & B_1 \arrow[r] \arrow[d, "\beta"'] & C_1 \arrow[r] \arrow[d, "\gamma"'] & D_1 \arrow[r] \arrow[d, "\delta"'] & E_1 \arrow[d, hook, "\epsilon"'] \\ A_0 \arrow[r] & B_0 \arrow[r] & C_0 \arrow[r] & D_0 \arrow[r] & E_0 \end{tikzcd}$$

By using the two versions of the four-lemma, γ is an epimorphism and is a monomorphism. Thus, γ is an isomorphism.

15.

16.

17.

IV - Groups, second encounter

4.1 - The Conjugation Action

1. Let p be a prime integer, and let G be a p group. Let S be a finite set such that $p \nmid |S|$. Suppose that G acts on the set S. Let Z denote the set of fixed points on the action. By Corollary 1.3, $|Z| \equiv |S| \mod p$. Hence, $|Z| \not\equiv 0 \mod p$ by assumption. Therefore, $|Z| \neq 0$. We must have that the action has fixed points.

2. Let D_{2n} be the dihedral group of order n. For $n = 1$ and $n = 2$, D_{2n} has order less than 5, hence, D_{2n} is abelian. Thus, $Z(D_{2n}) = D_{2n}$. Let $n \geq 3$. Note $D_{2n} = \langle x, y \mid x^2 = y^n = 1, yx = xy^{-1} \rangle$. Let $z \in Z(D_{2n})$. Then, $zx = xz$ and $zy = yz$. We have that $z = x^i y^j$ for some i, j aswell as D_{2n} is generated by x, y. Then,

$$zy = yz \implies x^i y^j y = y x^i y^j \implies x^i y^{j+1} = y x^i y^j \implies x^i y = y x^i$$

If $i = 1$, then $xy = yx = xy^{-1}$, hence, $y^2 = 1$, which is not possible. Hence, $i = 0$. Then, $z = y^j$ for some j. Then,

$$zx = xz \implies y^j x = x y^j \implies x y^{-j} = x y^j \implies y^{2j} = 1$$

Hence, $n \mid 2j$. Thus, $j = n/2$ or $j = 0$. We have that $z = 1$ or $z = y^{n/2}$. If n is odd, then $Z(D_{2n}) = \langle y^{n/2} \rangle$ and if n is even, then $Z(D_{2n})$ is trivial.

3. Let S_n be the group of permutations on the set $[n] = \{1, 2, ..., n\}$ with $n \geq 3$. Let $\tau \in S_n$ be a permutation sending l to k where $k \neq l$. Let $m \in [n]$ such that $m \neq l, k$. Let $\sigma \in S_n$ be the permutation solely swapping m and k. We have that $\sigma\tau(l) = \sigma(k) = m$ and $\tau\sigma(l) = \tau(l) = k$. Then, for any non-trivial permutation of S_n, we can find a permutation such that they do not commute. Hence, $Z(S_n)$ is trivial.

4. Let G be a group, and N a subgroup of the center of G, $Z(G)$. Let $x \in N$ and $g \in G$. As N is a subgroup of $Z(G)$, x is an element of $Z(G)$. Hence, $xg = gx$ for all $g \in G$. We have that $gxg^{-1} = xgg^{-1} = x \in N$. Therefore, N is normal in G.

5. Define the homomorphism $\varphi : G \to \mathrm{Inn}(G)$ by $\varphi(g) = \lambda_g$ where $\lambda_g(x) = gxg^{-1}$. Note φ is surjective. We have that

$$\ker\varphi = \{g \in G \mid \lambda_g = \lambda_1\} = \{g \in G \mid \forall x \in G, gxg^{-1} = x\} = \{g \in G \mid \forall x \in G, gx = xg\} = Z(G)$$

By the first isomorphism theorem, $G/Z(G) \cong \mathrm{Inn}(G)$. Let G be a finite group, and assume $G/Z(G)$ is cyclic. We then have that $\mathrm{Inn}(G)$ is cyclic. By a previous exercise, $\mathrm{Inn}(G)$ is cyclic if and only if G is abelian. Hence, G is commutative.

6. Let p, q be prime integers and let G be a group of order pq. Suppose that $Z(G)$ is not trivial. Then, $|Z(G)|$ can either be p, q or pq. If $|Z(G)|$ is either p or q, then $|G/Z(G)|$ is prime, hence, $\mathrm{Inn}(G)$ is cyclic, which makes G abelian. If $Z(G) = G$, then G is abelian straight away. We deduce that a group of order pq is either commutative or has a nontrivial center. Suppose now $p = q$ so that G has order p^2. By Corollary 1.9, G has a nontrivial center being a p-group. Hence, G is commutative.

7. We have that Q_8, the Quarternion group, is a group of order 2^3, however, it is not abelian.

8. Let G be a group of order p^r with p prime. Suppose that G is abelian. Then, with using a previous exercise, G contains elements of order p^k for every $k \leq r$, hence, contains normal subgroups of order p^k for every $k \leq r$. Note that if G is a group of order p, G contains subgroups of order 1 and p, namely, $\{1_G\}$ and G itself, respectively. Let $n \in \mathbb{N}$, and suppose that for every group, G, of order $p^r < p^n$, G contains a normal subgroup of order p^k for every $k \leq r$. Let G be a group of order p^n. If G is abelian, then G contains a subgroup of order p^k for every $k \leq n$. Suppose that G is not abelian. Then, $1 < Z(G) < p^n$ is a normal subgroup of G of order p^k for some $1 \leq k < n$. Under the hypothesis, $Z(G)$ contains a normal subgroup of order p, H say. Then, G/H is a group of order p^{n-1}. Under the hypothesis, G/H contains normal subgroups of order $1, p, p^2, ..., p^{n-1}$. Hence, G contains subgroups of order $1, p, p^2, p^3, ..., p^n$. By the principle of strong mathematical induction, G, being a group of order p^n, contains normal subgroups of order p^k for every $k \leq n$.

9. Let p be a prime number and G a p-group. Let H be a non-trivial normal subgroup of G. Let G act on H via conjugation. Let Z be the set of all fixed points under this action. We have that

$$Z = \{x \in H \mid \forall g \in G, gxg^{-1} = x\} = \{x \in H \mid \forall g \in G, gx = xg\} = Z(G) \cap H$$

By Corollary 1.3, $|Z(G) \cap H| = |Z| \equiv |H| \mod p$. By Lagranges Theorem, $|H| = 0 \mod p$, hence, $|Z(G) \cap H| \equiv 0 \mod p$. As $1_G \in H \cap Z(G)$, $H \cap Z(G) \geq p$.

10. Let G be a group of odd order and let $g \in G$ be a nontrivial element such that g is conjugate to g^{-1}. If $g = g^{-1}$, then $g^2 = 1$, so $2 = |g|$ divides $|G|$, which cannot occur. Suppose that $g \neq g^{-1}$. As $|G|$ is odd, the conjugacy class containing g and g^{-1} must contain some other element $h \in G$. We have that g is conjugate to h, hence, there is some $x \in G$ such that $g = xhx^{-1}$. Thus, $g^{-1} = xh^{-1}x^{-1}$. g^{-1} must be conjuagte to h^{-1}. For every $x \in [g]$, $x^{-1} \in [g]$. Therefore, $|C(g)|$ is even, which cannot happen. We must have that g is the identity element.

11.

12.

13. Let G be a noncommutative group of order 6. Suppose that G does not have an element of order 3. Then, as G is not abelian, it cannot be cyclic, so it cannot have an element of order 6. Hence, every element of G must have order 2 or 1. However, by a previous exercise, G is then abelian. Hence, G must contain an element of order 3. Let y be such an element. As $\langle y \rangle$ has index 2 in G, it must be normal. Let $[y]$ be the conjugacy class of y. We must have that $[y]$ has length 2 or 3 as $y \notin Z(G)$ as $Z(G)$ is trivial. $\langle y \rangle$ is the union of conjugacy classes and it contains 1. $\langle y \rangle$ also must contain $[y]$ as $y \in [y]$. As $[y]$ must have length 2 or 3, it is forced to have length 2 and y^2 is also forced to be an element of $[y]$. Thus, $[y] = \{y, y^2\}$. As y and y^2 are in the same conjugacy class, $y = xy^2x^{-1}$ for some $x \in G$. Then, there is an $x \in G$ such that $yx = xy^2$. We note that $x \neq y, y^2, 1$. Suppose that x has order 3. Then, $\langle x \rangle$ is normal, hence is the union of conjugacy classes. However, it is impossible for $\langle x \rangle$ to be the union of conjugacy classes as $[x]$ must be of length 3 and cannot contain the identity. Thus, a contradiction. x must be of order 2. So far we know that G contains $1, x, y, y^2$. We have that

$$xy = xyy^3 = xy^2y^2 = yxy^2 = y^2x$$

$$xy^2 = yx$$

$$yx = yx$$

$$y^2x = y^2x$$

The other two elements must be y^2x and yx. Note that these two elements cannot possibly equal $1, x, y, y^2$. Hence, x, y generate G. We have that

$$G = \langle x, y \mid x^2 = y^3 = 1, xy = y^2x \rangle$$

Hence, $G \cong S_3$.

14. Let G be a group and assume $[G : Z(G)] = n$ is finite. Let $A \subseteq G$ be a subset of G. We have that $\text{Inn}(G) \cong G/Z(G)$, hence, $|\text{Inn}(G)| = n$. Let $\lambda_g \in \text{Inn}(G)$ be conjugation under g. We have that there exists $g_1, ...g_n \in G$ such that $\lambda_{g_1}, ..., \lambda_{g_n}$ are all distinct and for all $g \in G$, $\lambda_g = \lambda_{g_i}$ for some i. Let $g \in G$, we have that $gAg^{-1} = \lambda_g(A)$. Then, the set of all gAg^{-1} is atmost n as $\text{Inn}(G) = n$.

15. Let G be a group with class formula $60 = 1 + 15 + 20 + 12 + 12$. Let N be a normal subgroup of G. We have that N is the union of the conjugacy classes of its elements. We have that N contains the identity element, and all conjugacy classes are disjoint, hence, $|N| = 1 + ...$ where the rest of the terms are chosen from $\{15, 20, 12\}$ with multiplicty of 12 accounted for. We cannot form any divisors of 60 of this form except 1 and 60. Hence, the only possible normal subgroups of G are 1 and G, which are normal already.

16.

17. Let H be a proper subgroup of a finite group G. By Corollary 1.14, there are atmost $[G : H]$ conjugates of H, each with $|H|$ elements. We note that each conjugate of H contains the identity. Hence,

$$\left| \bigcup_{g \in G} gHg^{-1} \right| \leq [G : H]|H| - [G : H] + 1 = |G| - [G : H] + 1 < |G|$$

as H is a proper subgroup of G. Therefore, G cannot be the union of conjugates of H.

18.

19. Let H be a proper subgroup of a finite group G. By a previous exercise, G is not the union of conjugates of H. Hence, there is some $x \in G$ not contained in any conjugate of H. Then, for all $g \in G$, $ghg^{-1} \neq x$ for any $h \in H$. Hence, for all $g \in G$, $gxg^{-1} \neq h$ for any h. Therefore, $[x]$ is disjoint from H.

20.

21. Let H, K be subgroup of a group G with $H \subseteq N_G(K)$. Let $\lambda_h : K \to K$ be conjugation by h. Note $\lambda_h(K) = hKh^{-1} = K$ as $h \in H \subseteq N_G(K)$. Define $\gamma : H \to \mathrm{Aut}_{\mathsf{Grp}}(K)$ by $\gamma(h) = \lambda_h$. Let $x, y \in K$. We have that $\gamma(xy) = \lambda_{xy} = \lambda_x \circ \lambda_y = \gamma(x)\gamma(y)$. Hence, γ is a group homomorphism. Furthermore,

$$\ker\gamma = \{h \in H \mid \lambda_h = \lambda_1\} = \{h \in H \mid \forall x \in K, hxh^{-1} = x\} = \{h \in H \mid \forall x \in K, hx = xh\} = H \cap Z_G(K)$$

22. Let G be a finite group, and let H be a cylic subgroup of G of order p where p is the smallest prime dividing the order of G. Suppose further H is normal in G. We note that $\mathrm{Aut}_{\mathsf{Grp}}(H) \cong \mathrm{Aut}_{\mathsf{Grp}}(\mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/(p-1)\mathbb{Z}$. By the previous exercise, there is a homomorphism $\gamma : G \to \mathbb{Z}/(p-1)\mathbb{Z}$ with kernel $Z_G(H)$. Let $x \in G$ be a non-trivial element. Then, the order of x is greater than or equal to p as p is the smallest prime dividing G. As γ is a homomorphism, the order of $\gamma(x) \in \mathbb{Z}/(p-1)\mathbb{Z}$ must divide the order of x. Every element in $\mathbb{Z}/(p-1)\mathbb{Z}$ has order less than or equal to $p-1$, hence, the order of $\gamma(x)$ must be 1. Therefore, γ is the trivial morphism. Hence, $\ker\gamma = G$. It follows that $Z_G(H) = G$. For all $h \in H$ and $g \in G$, $ghg^{-1} = h$. Then, H is a subgroup of $Z(G)$.

4.2 - The Sylow Theorems

1. With notation given in the proof of the Cauchy's Theorem, we have that $|Z| \equiv 0 \mod p$. Hence, there are kp fixed elements. For every element of order p, the generated subgroup contains $p-1$ generators. Let N be the number of subgroups of order p. We have that $kp = |\{1_G\} \cup \{x_1, ..., x_1^{p-1}\} \cup ... \cup \{x_m, ..., x_m^{p-1}\}| = 1 + N(p-1)$. Hence, $kp = 1 + Np - N$ so $N = 1 + Np - kp$. Therefore, $N \equiv 1 \mod p$.

2.

(i) Let G be a group and suppose that H is a characteristic subgroup of G. We have that $\varphi_g : G \to G$ defined by conjugation by $g \in G$ is an automorphism of G. Hence, for any $g \in G$, $gHg^{-1} = \varphi_g(H) \subseteq H$. Therefore, H is normal.

(ii) Let $H \subseteq K \subseteq G$ such that H is characteristic in K and K is normal in G. Let $g \in G$. As K is normal in G, $gKg^{-1} \subseteq K$. Define $\varphi_g : K \to K$ to be conjugation by $g \in G$. As H is characteristic in K, $gHg^{-1} = \varphi_g(H) \subseteq H$. Therefore, H is normal in G.

(iii) Let G, K be groups such that G contains a single subgroup H isomorphic to K. For any $g \in G$, gHg^{-1} is isomorphic to H via conjugation by g, and is also a subgroup of G. By assumption, we must have that $H = gHg^{-1}$ for all $g \in G$. Therefore, H is normal in G.

(iv) Let K be a normal subgroup of a finite group G such that $|K|$ and $|G/K|$ are relatively prime. Let $\varphi \in \mathrm{Aut}_{\mathsf{Grp}}(G)$ and let $x \in \varphi(K)$. Let $\pi : G \to G/K$ be the natural projection. We have that the order of $\pi(x)$ must divide the order of G/K, and we also must have that the order of $\pi(x)$ divides the order of x. As $x \in \varphi(K)$, there is a $y \in K$ such that $\varphi(y) = x$. Then, the order of x divides the order of y, which divides the order of K by Lagranges Theorem. Thus, $\pi(x)$ divides both $|K|$ and $|G/K|$. As $|K|$ and $|G/K|$ are relatively prime, $\pi(x)$ must be 1. Hence, $\pi(x) = 1$ for all $x \in \varphi(K)$. We must have that $xK = K$ for all $x \in \varphi(K)$, hence, $x \in K$ for all $x \in \varphi(K)$. We conclude $\varphi(K) \subseteq K$, and K is characteristic.

3. Let G be a nonzero finite abelian group. Suppose that $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p. By Lagranges Theorem, the only possible orders of subgroups of G are 1 and p, both corresponding to the trivial subgroups. Hence, G is simple. For the converse, suppose that G is simple. Let $x \in G$ be a non-trivial element of G. We have that $\langle x \rangle$ is a subgroup of G, and as G is abelian, $\langle x \rangle$ is normal, thus, $\langle x \rangle = G$. Assume, for contradiction, $|G| = mn$ where $m, n > 1$. Let $x \in G$. We have that $1 = x^{|G|} = x^{mn} = (x^m)^n$. Hence, $|x^m|$ divides n. Hence, x^m has order strictly less than mn. Thus, $|G|$ cannot be composite. As $|G|$ is prime and is abelian, $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p.

4. Let G be a simple group and let $\varphi : G \to H$ be a surjective homomorphism. As G is simple, $\ker\varphi = \{1_G\}$ or $\ker\varphi = G$. If $\ker\varphi = \{1_G\}$, then, φ is an isomorphism, hence, $H \cong G$. If $\ker\varphi = G$, then φ is the trivial homomorphism. As φ is surjective, $H \cong 0$. Therefore, $H \cong 0$ or $H \cong G$.

5. Let G be a simple group and let $\varphi : G \to H$ be a nontrivial group homomorphism. We have that $\ker\varphi$ is a normal subgroup of G. As G is simple, $\ker\varphi = 1$ or $\ker\varphi = G$. As φ is nontrivial, $\ker\varphi = 1$. Therefore, φ is injective.

6. Let p be a prime, and let G be a group such that $|G| = p^n$ with $n \geq 2$. Suppose G is abelian. By Cauchy's Theorem, this is an $x \in G$ with order p. Hence, $\langle x \rangle$ is a subgroup of G of order p. As G is abelian, $\langle x \rangle$ is normal. It follows that G is not simple. Suppose now G is noncommutative. We have that $Z(G) \neq G$. As G is a p-group, $Z(G)$ is non-trivial. Thus, $1 < |Z(G)| < p^n$. As $Z(G)$ is normal in G, G is not simple. We conclude that groups of order p^n are not simple.

7. We first note that if G is a finite group such that $|G| = mp$ with $1 < m < p$, then G is not simple by Example 2.4. Then, groups of order $6 = 2 \cdot 3, 10 = 2 \cdot 5, 14 = 2 \cdot 7, 15 = 3 \cdot 5, 20 = 4 \cdot 5, 21 = 3 \cdot 7, 22 = 2 \cdot 11, 26 = 2 \cdot 13, 28 = 4 \cdot 7, 33 = 3 \cdot 11, 34 = 2 \cdot 17, 35 = 5 \cdot 7, 38 = 2 \cdot 19, 42 = 6 \cdot 7, 44 = 4 \cdot 11, 46 = 2 \cdot 23, 51 = 3 \cdot 17, 52 = 4 \cdot 13, 55 = 5 \cdot 11, 57 = 3 \cdot 19, 58 = 2 \cdot 29$ are not simple.

8. Let G be a finite group, and let p be a prime integer. Let N be the intersection of all p-Sylow subgroups of G. Let P be some p-Sylow subgroup of G. Then, by the second Sylow theorem, every p-Sylow subgroup of G is of the form gPg^{-1} for some $g \in G$. We also have that for all $g \in G$, gPg^{-1} is a p-Sylow subgroup of G. Hence, $N = \bigcap_{g\in G} gPg^{-1}$. Let $x \in G$. We have that

$$xNx^{-1} = x\left(\bigcap_{g\in G} gPg^{-1}\right)x^{-1} = \bigcap_{g\in G} xgPg^{-1}x^{-1} = \bigcap_{g\in G} (xg)P(xg)^{-1} = N$$

Therefore, N is normal in G.

9. Let P be a p-Sylow subgroup of a finite group G, and let $H \subseteq G$ be a p-subgroup of G. Assume that $H \subseteq N_G(P)$. As P is normal in $N_G(P)$, hence, PH is a subgroup of $N_G(P)$. We have that $|PH||P \cap H| = |H||P|$. As H is a p-group, $H \cap P$ must also be a p-group by Lagranges Theorem. As $H, P, H \cap P$ all have order of a power of p, PH has order of a power of p. Hence, PH is a p-subgroup of $N_G(P)$. We then have that $PH = P$ as P is a maximal p-subgroup of G. Therefore, $H \subseteq PH = P$.

10. Let P be a p-Sylow subgroup of a finite group G, and act P by conjugation on the set of all p-subgroups of G. If P' is a fixed point of this action, then for all $g \in P$, $gP'g^{-1} = P'$. Thus, $P \subseteq N_G(P')$. By the previous exercise, $P \subseteq P'$. As P is a p-Sylow subgroup and P' is a p-group, we must have that $P = P'$. Therefore, P is the unique fixed point of this action.

11. Let p be a prime integer, and let G be a finite group of order $|G| = p^r m$. Assume p does not divide m. Let P be a p-Sylow subgroup of G. Act P by conjugation on the set of all p-Sylow subgroups of G. Let n_p be the number of p-Sylow subgroups of G. Then, by the previous exercise, $n_p \cong 1 \mod p$ as the set of fixed points contains a singular element. We have that $[G : P] = m$, and by Corollary 1.14, the number of subgroups conjugate to P (i.e the number of p-Sylow subgroups, n_p, by Sylow II) is finite and divides m. We conclude Sylow III holds.

12. Let P be a p-Sylow subgroup of a finite group G, and let $H \subseteq G$ be a subgroup containing the normaliser $N_G(P)$. Act P on the set G/H of left cosets of H in G by $(g, xH) \mapsto (gxg^{-1})H$. Let xH be a fixed point of this action. We have that

$$\forall g \in P, (gxg^{-1})H = xH \iff \forall g \in P, gxg^{-1}x^{-1} = 1 \iff \forall g \in P, gx = xg \iff x \in Z_G(P)$$

Then, $x \in Z_G(P) \subseteq N_G(P) \subseteq H$. Therefore, $xH = H$. We must have that the set of fixed points of this action contains a singular element. Hence, $[G : H] = |G/H| \equiv 1 \mod p$.

13. Let P be a p-Sylow subgroup of a finite group G.

(i) Suppose that P is normal. Let $\varphi \in \mathrm{Aut}_{\mathsf{Grp}}(G)$. Then, $\varphi(P)$ is a subgroup of G, and is also a p-group. By Sylow III, $\varphi(P) \subseteq gPg^{-1}$ for some $g \in G$. As P is normal, it follows that $\varphi(P) \subseteq P$. Therefore, P is characteristic.

(ii) Let H be a subgroup containing P, and assume P is normal in H and H is normal in G. As P is a normal p-Sylow subgroup of H, it is then characteristic. By a previous exercise, P is normal in G.

(iii) We have that P is a subgroup of $N_G(P)$ is a subgroup of $N_G(N_G(P))$. We have that P is normal in $N_G(P)$ and $N_G(P)$ is normal in $N_G(N_G(P))$. Hence, P is normal in $N_G(N_G(P))$. As $N_G(P)$ is the largest subgroup of G such that P is normal in that subgroup, $N_G(N_G(P))$ is a subgroup of $N_G(P)$. Therefore, $N_G(N_G(P)) = N_G(P)$.

14. By Claim 2.12, if G is a group of order $18 = 2 \cdot 3^2, 50 = 2 \cdot 5^2, 54 = 2 \cdot 3^3$, then G is not simple. We also have that $40 = 5 \cdot 2^3$ and $45 = 5 \cdot 3^2$. As $\gcd(2,5) = \gcd(3,5) = 1$, and the only divisors d of 5 such that $d \equiv 1 \mod p$ is 1, a group of order 40 or 45 is not simple.

15.

16.

17.

18.

19.

20. Let G be a simple group of order 168. Note that $168 = 2^3 \cdot 3 \cdot 7$. By Sylow I, there exists cyclic subgroups of order 7 in G. By Sylow III, if n_7 is the number of cyclic subgroups of order 7, then $n_7 \mid 2^3 \cdot 3$ and $n_7 \equiv 1 \mod 7$. Then, $n_7 \in \{1, 8\}$. As G is normal, $n_7 \neq 1$. Thus, $n_7 = 8$. As 7 is prime, G then has $8(7-1) = 48$ elements of order 7.

21. Let G be a group of order pqr such that p, q, r are prime and $p < q < r$. By Sylow I, G must contain subgroups of order p, q and r. Let n_p, n_q, n_r be the number of such subgroups in G respectively. As p, q, r are prime, any two Sylow subgroup must intersect trivially. We have that the number of distinct elements of G that are an element of a Sylow subgroup is given by

$$N = 1 + (p-1)n_p + (q-1)n_q + (r-1)n_r$$

By Sylow III, $n_p \mid qr, n_q \mid pr, n_r \mid pq$ and $n_p \equiv 1 \mod p, n_q \equiv 1 \mod q, n_r \equiv 1 \mod r$. As $n_r \equiv 1 \mod r$ and $n \mid pq$ with $p, q < r$, n_r can only possibly be pq or 1. Suppose that $n_r = pq$. As $n_q \mid pr$ and $n_q \equiv 1 \mod q$, n_q can only be $1, r, pr$. Suppose, that $n_r \geq pq, n_q \geq r, n_p \geq q$. Then,

$$N \geq 1 + (p-1)q + (q-1)r + (r-1)pq = pqr + qr - q - r + 1 > pqr = |G|$$

This is not possible, hence, atleast one of n_p, n_q, n_r is equal to one. This implies the normality of a nontrivial group in G. Hence, G is not simple.

22. Let G be a finite noncommutative group of order n, and let p be a prime divisor. Assume that the only divisor of n that is congruent to $1 \mod p$ is 1. By Sylow I, G contains a p-Sylow subgroup. by Sylow III, the number of p-Sylow subgroups is congruent to $1 \mod p$ and divides n. By assumption, there is only a singular p-Sylow subgroup of G. If G is a not a p-group, then this unique Sylow subgroup is not trivial or the group itself. Hence, G is abelian. If G is a p-group, then G has a nontrivial centre, and since G is noncommutative, G is not simple. Therefore, G is not simple.

23. Let n_p denote the number of p-Sylow subgroups of a group G. Suppose that G is simple. Let p be a prime divisor of G. As G is simple, $n_p > 1$ by Sylow II. Act G on the set of p-Sylow subgroups of G via conjugation. This induces a homomorphism $\varphi : G \to S_{n_p}$. We have that $G/\ker\varphi \cong \varphi(G)$. If $\ker\varphi = 1$, then $|G|$ divides $|S_{n_p}| = n_p!$. If $\ker\varphi = G$, then a p-Sylow subgroup is normal, which contradicts simplicity of G. We conclude that $|G|$ divides $n_p!$ for all prime divisors p of G.

24. NOT FINISHED First note that there are no noncommutative groups of order p, p^2 where p prime. Then, we look at groups of order

$$6, 8, 10, 12, 14, 15, 16, 18, 20, 21, 22, 24, 26, 27, 28, 30, 32, 33, 34, 35, 36, 38, 39, 40, 42,$$

$$44, 45, 46, 48, 50, 51, 52, 54, 55, 56, 57, 58, 62, 63, 64, 65, 66, 68, 69, 70, 72, 74, 75, 76, 77,$$

$$78, 80, 81, 82, 84, 85, 86, 87, 88, 90, 91, 92, 93, 94, 95, 96, 98, 99, 100, 102, 104, 105, 106,$$

$$108, 110, 111, 112, 114, 115, 116, 117, 118, 119, 120, 122, 123, 124, 125, 126, 128, 129, 130, 132, 133,$$

$$134, 135, 136, 138, 140, 141, 142, 143, 144, 145, 146, 147, 148, 150, 152, 153, 154, 155, 156, 158,$$

$$159, 160, 161, 162, 164, 165, 166$$

We now remove groups of order mp with $1 < m < p$ with p prime.

$$8, 12, 16, 18, 24, 27, 30, 32, 36, 40, 45, 48, 50, 54, 56, 63, 70, 72, 75, 80, 81, 84, 90, 96, 98, 100, 105,$$

$$108, 112, 120, 125, 126, 128, 132, 135, 140, 144, 147, 150, 154, 160, 162, 165$$

Now remove p-groups with order greater than p^2

$$12, 18, 24, 30, 36, 40, 45, 48, 50, 54, 56, 63, 70, 72, 75, 80, 84, 90, 96, 98, 100, 105,$$

$$108, 112, 120, 126, 132, 135, 140, 144, 147, 150, 154, 160, 162, 165$$

Remove groups of order mp^r with $1 < m < p$

$$12, 24, 30, 36, 40, 45, 48, 56, 63, 70, 72, 80, 84, 90, 96, 105,$$

$$108, 112, 120, 126, 132, 135, 140, 144, 150, 154, 160, 165$$

We now remove $40, 45$ by a previous exercise

$$12, 24, 30, 36, 48, 56, 63, 70, 72, 80, 84, 90, 96, 105,$$

$$108, 112, 120, 126, 132, 135, 140, 144, 150, 154, 160, 165$$

Remove groups of order pqr with p, q, r prime and $p < q < r$

$$12, 24, 36, 48, 56, 63, 72, 80, 84, 90, 96,$$

$$108, 112, 120, 126, 132, 135, 140, 144, 150, 160$$

From the text, there are no simple groups of order $12, 24$

$$36, 48, 56, 63, 72, 80, 84, 90, 96,$$

$$108, 112, 120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a group of order p^2q^2 with $p < q$ and p, q prime. We have that $n_q \equiv 1 \mod q$ and $n_q \mid p^2$. As $p < q$, we must have that $n_q \in \{1, p^2\}$. Suppose that $n_q = p^2$. Then, $p^2 \equiv 1 \mod q$ and so $q \mid p^2 - 1$. As q is prime, $q \mid p - 1$ or $q \mid p + 1$. As $p < q$, $q \mid p + 1$, and $q = p + 1$. Hence, $q = 3$ and $p = 2$. If G is simple, then it must be of order 36. Let H be a group of order 36. We have that $n_3 \equiv 1 \mod 3$ and $n_3 \mid 4$. Then, $n_3 \in \{1, 4\}$. Suppose $n_3 = 4$. We have that $4! = 24$, but 36 does not divide 24. H cannot be simple. Therefore, groups of order p^2q^2 are not simple. We remove these

$$48, 56, 63, 72, 80, 84, 90, 96,$$

$$108, 112, 120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a group of order $2^n \cdot 3$. We have that $n_2 \equiv 1 \mod 2$ and $n_2 \mid 3$. Hence, $n_2 \in \{1, 3\}$. If $n_2 = 3$, then $n_2! = 6$. $|G|$ divides 6 when $n = 1$. If G is of order 6, then G is not simple. Therefore, there are no simple groups of order $2^n \cdot 3$. We remove these

$$56, 63, 72, 80, 84, 90,$$

$$108, 112, 120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a group of order $56 = 2^3 \cdot 7$. Then, $n_7 \mid 8$ and $n_7 \equiv 1 \mod 7$. Then, $n_7 \in \{1, 8\}$. Suppose that $n_7 = 8$. Then, there are 48 elements of order 7. The remaining 8 elements must form a unique 2-Sylow subgroup of G. Hence, G is not simple. Remove the group of order 56.

$$63, 72, 80, 84, 90, 108, 112, 120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a group of order $63 = 3^2 \cdot 7$. We have that $n_7 \mid 9$ and $n_7 \equiv 1 \mod 7$ and $n_7 \mid 9$. Therefore, $n_7 = 1$. A group of 63 cannot be simple.

$$72, 80, 84, 90, 108, 112, 120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a group of order $72 = 2^3 \cdot 3^2$. We have that $n_3 \equiv 1 \mod 3$ and $n_3 \mid 8$. Hence, $n_3 \in \{1, 4\}$. Suppose that $n_3 = 4$. Then, G does not divide $n_3!$, and so G is not simple. We remove 72

$$80, 84, 90, 108, 112, 120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a group of order $80 = 2^4 \cdot 5$. We have $n_2 \equiv 1 \mod 2$ and $n_2 \mid 5$. Then, $n_2 \in \{1, 5\}$. If $n_2 = 5$, then $n_2! = 120$, and $|G|$ does not divide 120. Hence, G is not simple.

$$84, 90, 108, 112, 120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a group of order $84 = 2^2 \cdot 3 \cdot 7$. We have $n_7 \equiv 1 \mod 7$ and $n_7 \mid 12$. We must have that $n_7 = 1$. Therefore, G is not simple.

$$90, 108, 112, 120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a noncommutative simple group of order $90 = 2 \cdot 3^2 \cdot 5$. We have that $n_3 \equiv 1 \mod 3$ and $n_3 \mid 10$. Then, $n_3 \in \{1, 10\}$. Additionally, $n_5 \equiv 1 \mod 5$ and $n_5 \mid 18$. Then, $n_5 \in \{1, 6\}$. As G is simple, $n_5 = 6$ and $n_3 = 10$. Let $\{P_1, ..., P_{10}\}$ be the set of 3-Sylow subgroups of G. Suppose $P_i \cap P_j = 1$ for all $i \neq j$. Then, $|P_1 \cup ... \cup P_{10}| = 81$. We also have that the set of 5-Sylow subgroups intersect trivially, hence, there are 24 elements of order 5. Therefore, G has more than 105 elements, which is a contradiction. There must exist P_i, P_j with $i \neq j$ such that $|P_i \cap P_j| = 3$. Note that $P_i, P_j, P_iP_j \subseteq N_G(P_i \cap P_j) = N$. As $P_i \subseteq N$, $|N|$ must be a multiple of 9. Note that $|P_iP_j| = |P_i||P_j|/|P_i \cap P_j| = 27$. Hence, $|N|$ must be greater than 27. As N is a subgroup of G, $|N|$ must also divide 90. Therefore, $|N| \in \{45, 90\}$. If $|N| = 45$, then N has index 2, which implies N is a nontrivial normal subgroup of G. If $|N| = 90$, then $P_i \cap P_j$ is normal in G. Both cases lead to contradiction, thus, G cannot be simple.

$$108, 112, 120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a noncommutative group of order $108 = 2^2 \cdot 3^3$. We have that $n_3 \equiv 1 \mod 3$ and $n_3 \mid 4$. Hence, $n_3 \in \{1, 4\}$. If $n_3 = 4$, then 108 does not divide $n_3!$. Thus, G cannot be simple.

$$112, 120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a noncommutative simple group of order $112 = 2^4 \cdot 7$. Then, $n_7 \equiv 1 \mod 7$ and $n_7 \mid 16$. Hence, $n_7 \in \{1, 8\}$. Additionally, $n_2 \equiv 1 \mod 2$ and $n_2 \mid 7$. Hence, $n_2 \in \{1, 7\}$. As G is simple, $n_2 = 7$ and $n_7 = 8$. Let $\{P_1, ..., P_7\}$ be the set of 2-Sylow subgroups of G. Suppose that for all i, j, $P_i \cap P_j = 1$. As each P_i is unique and intersects trivially with a different 2-Sylow subgroup, the set of P_i's contribute to $7 \cdot 15 = 105$ nontrivial elements. We have that the 7-Sylow subgroups are cyclic and intersect with eachother trivially. Hence, there subgroups contribute to $6 \cdot 8 = 48$ nontrivial elements of G. Thus, G has atleast 153 elements, which is a clear contradiction. Hence, there is P_i, P_j with $i \neq j$ such that $|P_i \cap P_j| \in \{2, 4, 8\}$. If $|P_i \cap P_j| = 2$, then $|P_iP_j| = |P_i||P_j|/2 = 128$, which cannot occur. If $|P_i \cap P_j| = 4$, then $|P_iP_j| = 64$. Let $N = N_G(P_i \cap P_j)$. Note $P_i, P_iP_j \subseteq N$. As $P_iP_j \subseteq N$, $|N| \geq 64$. Therefore, $N = G$. Hence, $P_i \cap P_j$ is normal in G, which cannot happen. Then, $|P_i \cap P_j| = 8$, which means $|P_iP_j| = 32$. We have that $|N| \geq 32$. As P_i is a subgroup of N, $16 \mid |N|$. As N is a subgroup of G, we have that $|N| \mid 112$. It follows that $|N| = 112$, hence, $P_i \cap P_j$ is normal in G, which is another contradiction. We conclude that there is no noncommutative simple group of order 112.

$$120, 126, 132, 135, 140, 144, 150, 160$$

Let G be a noncommutative group of order $135 = 3^3 \cdot 7$. By Sylow III, $n_7 \equiv 1 \mod 7$ and $n_7 \mid 27$. Then, $n_7 = 1$. Therefore, G is simple.

$$120, 126, 132, 140, 144, 150, 160$$

Let G be a noncommutative group of order $126 = 2 \cdot 3^2 \cdot 7$. We have that $n_7 \equiv 1 \mod 7$ and $n_7 \mid 18$. Then, $n_7 = 1$. Hence, G cannot be simple.

$$120, 132, 140, 144, 150, 160$$

Let G be a simple noncommutative group of order $132 = 2^2 \cdot 3 \cdot 11$. We have that $n_2 \equiv 1 \mod 2$ and $n_2 \mid 33$. Hence, $n_2 \in \{1, 3, 11, 33\}$. Additionally, $n_3 \equiv 1 \mod 3$ and $n_3 \mid 44$, hence, $n_3 \in \{1, 4, 22\}$. Lastly, $n_{11} \equiv 12$ and $n_{11} \equiv 1 \mod 11$. Hence, $n_{11} \in \{1, 12\}$. As G is simple and $132 \geq 5!$, $n_2 \in \{11, 33\}, n_3 = 22, n_{11} = 12$. We have that the number of elements in G of order 3 is $22(3-1) = 44$. The number of elements in G of order 11 is $12(11-1) = 120$. Hence, G contains atleast 164 elements. This is a contradiction. G cannot be simple.

$$120, 140, 144, 150, 160$$

Let G be a noncommutative group of order $140 = 2^2 \cdot 5 \cdot 7$. Then, $n_5 \equiv 1 \mod 5$ and $n_5 \mid 28$. Then, $n_5 = 1$. G cannot possible simple.

$$120, 144, 150, 160$$

Let G be a noncommutative group of order $150 = 2 \cdot 3 \cdot 5^2$. Then, $n_5 \equiv 1 \mod 5$ and $n_5 \mid 6$. Then, $n_5 \in \{1, 6\}$. We have that 150 does not divide 6!, hence, G cannot be simple.

$$120, 144, 160$$

Let G be a noncommutative group of order $160 = 2^5 \cdot 5$. We have that $n_2 \equiv 1 \mod 2$ and $n_2 \mid 5$. Hence, $n_2 \in \{1, 5\}$. As 160 does not divide 1! or 5!, G cannot be simple.

$$120, 144$$

25.

4.3 - Composition Series and Solvability

1. Let $n \in \mathbb{Z}$. We have that

$$\mathbb{Z} \supset 2^{n-1}\mathbb{Z} \supset 2^{n-2}\mathbb{Z} \supset ... \supset 2\mathbb{Z} \supset \{1\}$$

is a normal series of length n as $\mathbb{Z}$ is abelian. Therefore, $\ell(G)$ is not finite.

2.

3. Note that $\mathbb{Z}/2\mathbb{Z}$ is simple, hence, it has composition series $\mathbb{Z}/2\mathbb{Z} \supset \{[0]_2\}$. Thus, groups of order 2 have composition series. Suppose that for all groups of order less than n, it has a composition series. Let G be a group of order n. If G is simple, then we are done and G has a composition series. If G has normal subgroups, let N be a maximal normal subgroup of G. We note that G/N is simple by the Correspondance Theorem, hence, has a composition series. N is a group of order less than n by Lagranges Theorem, hence, by assumption N has a composition series. By Proposition 3.4, G has a composition series. By the Principle of Strong Induction, all finite groups have a composition series. Note that $\mathbb{Z}$ does not have a composition series. Suppose that there exists a composition series of $\mathbb{Z}$,

$$\mathbb{Z} = d_0\mathbb{Z} \supset d_1\mathbb{Z} \supset ... \supset d_n\mathbb{Z} = \{[0]_1\}$$

Then, $d_i\mathbb{Z}/d_{i+1}\mathbb{Z} \cong \mathbb{Z}/(d_{i+1}/d_i)\mathbb{Z}$ is simple for all i. Hence, $d_{i+1}/d_i = p_i$ for some prime p_i for all i. We have that

$$\prod_{i=0}^{n-1} p_i = \prod_{i=0}^{n-1} \frac{d_{i+1}}{d_i} = \frac{d_n}{d_0} = \frac{0}{1} = 0$$

Therefore, $p_i = 0$ for some i, which is a contradiction as p_i is prime.

4. Let $x \in Q_8$ be the element of order 4, and let $y \in D_8$ of order 4. We have the following composition series

$$Q_8 \supset \langle x \rangle \supset \langle x^2 \rangle \supset \{1\}$$

$$D_8 \supset \langle y \rangle \supset \langle y^2 \rangle \supset \{e\}$$

Furthermore, $Q_8/\langle x \rangle \cong \langle x \rangle/\langle x^2 \rangle \cong D_8/\langle y \rangle \cong \langle y \rangle/\langle y^2 \rangle \cong \mathbb{Z}/2\mathbb{Z}$. Hence, Q_8 and D_8 are nonisomorphic groups with the same composition factors.

5. Let H, K be normal subgroups of a group G. Let $g \in G$. We have that $gHKg^{-1} = gHg^{-1}gKg^{-1} = HK$. Therefore, HK is normal in G.

6. Let G_1, G_2 be groups. We have that $(G_1 \times G_2)/G_1 \cong G_2$ and $(G_1 \times G_2)/G_2 \cong G_2$. By Proposition 3.4, $G_1 \times G_2$ has composition series if and only if G_1, G_2 have composition series. Let

$$G_1 = H_0 \supset H_1 \supset ... \supset H_n = \{1_{G_1}\}$$

$$G_2 = K_0 \supset K_1 \supset ... \supset K_m = \{1_{G_2}\}$$

be composition series. Suppose that H is normal in H' and K is normal in K'. Let $(g, g') \in H' \times K'$. We have that

$$(g, g')(H \times K)(g, g')^{-1} = (g, g')(H \times K)(g^{-1}, g'^{-1}) = (gHg^{-1}) \times (g'Kg'^{-1}) = H \times K$$

Therefore, $H \times K$ is normal in $H' \times K'$. Define the homomorphism $\varphi : H' \times K' \to (H'/H) \times (K'/K)$ by $(g, g') \mapsto (g + H, g' + K)$. We have that this is a surjective homomorphism with kernel $H \times K$. Hence, $(H' \times K')/(H \times K) \cong (H'/H) \times (K'/K)$. Suppose that H, K are simple groups. Let $N \times M$ be a normal subgroup of $H \times K$. We have that for all $(g, 1_K) \in H \times K$, $N \times M \supset (g, 1_K)(N \times M)(g, 1_K)^{-1} = (gNg^{-1}) \times M$. Therefore, N is normal in H. Similarly, M is normal in K. We have the result that $N \times M$ is normal in $H \times K$ if and only if N is normal in H and M is normal in K, and the result $(H \times K)/(N \times M) \cong (H/N) \times (K/M)$. Therefore, $H \times K$ is simple if and only if H, K are simple and

$$G_1 \times G_2 = H_0 \times K_0 \supset H_1 \times K_1 \supset ... \supset H_n \times K_n = \{1_{G_1}\} \times \{1_{G_2}\}$$

is a composition series of $G_1 \times G_2$. By the Jordan-Holder theorem, any composition series of $G_1 \times G_2$ is equivalent to the above composition series.

7.

8. Let $\varphi : G_1 \to G_2$ be a group homomorphism. Let $g, h \in G_1$. Then,

$$\varphi([g, h]) = \varphi(ghg^{-1}h^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = [\varphi(g), \varphi(h)]$$

Let $x \in G_1'$. Then, $x = [g_1, h_1]^{n_1}...[g_k, h_k]^{n_k}$ for some $g_1, ..., g_k, h_1, ..., h_k \in G_1$ and $n_1, ..., n_k \in \mathbb{Z}$. Then,

$$\varphi(x) = \varphi([g_1, h_1]^{n_1}...[g_k, h_k]^{n_k}) = \varphi([g_1, h_1])^{n_1}...\varphi([g_k, h_k])^{n_k} = [\varphi(g_1), \varphi(h_1)]^{n_1}...[\varphi(g_k), \varphi(h_K)]^{n_k} \in G_2'$$

Therefore, $\varphi(G_1') \subseteq G_2'$.

9.

10. Let G be a group. Define inductively an increasing sequence $\{e\} = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots$ of subgroups of G as follows: for $i \geq 1$, Z_i is the subgroup of G corresponding to $Z(G/Z_{i-1})$.

(i) We first note that $Z_0 = \{e\}$ is normal in $Z_1 = Z(G)$ and Z_1 is normal in G. Suppose that Z_i is normal in G for all $i < n$. We have that Z_n corresponds to the subgroup $Z(G/Z_{n-1})$. We have that Z_n/Z_{n-1} is normal in G/Z_{n-1} as Z_n corresponds to the centre of G/Z_{n-1}. Hence, Z_n is normal in G by the Third Isomorphism Theorem.

(ii) Let G be a group. Suppose that G is nilpotent. We have that G has the normal series

$$\{e\} = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots \subseteq Z_n = G$$

for some $n \in \mathbb{N}$. Let $H = G/Z(G)$. Define inductively the increasing sequence $\{e\} = H_1 \subseteq H_2 \subseteq ...$ of subgroups of H as follows: for $i \geq 2$, H_i is the subgroup of H corresponding to $Z(H/H_{i-1})$. Suppose that for all $i < n$, $H_i = Z_i/Z(G)$. We have that H_n corresponds to the subgroup $Z(H/H_{n-1})$. Then,

$$\frac{H_n}{H_{n-1}} \cong Z\left(\frac{H}{H_{n-1}}\right) \cong Z\left(\frac{G/Z(G)}{Z_{n-1}/Z(G)}\right) \cong Z\left(\frac{G}{Z_{n-1}}\right) \cong \frac{Z_n}{Z_{n-1}} \cong \frac{Z_n/Z(G)}{H_{n-1}}$$

Then, $H_n = Z_n/Z(G)$. Therefore, we must have that H has the series

$$\{e\} = H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n = G/Z(G)$$

Therefore, $G/Z(G)$ is nilpotent. From the above chain of isomorphisms and using the same argument, we also have that if $G/Z(G)$ was nilpotent, then G is nilpotent

(iii) Let G be a p-group for some prime p. We have that $Z(G)$ is nontrivial and $G/Z(G)$ is also a p-group where $|G/Z(G)| < |G|$. Repeating, we have that $(G/Z(G))/(Z(G/Z(G)))$ is a p-group and is of order strictly less than $G/Z(G)$. Eventually, we reach the trivial group. $\{e\}$ is clearly nilpotent, hence, G is nilpotent by the previous part.

(iv) Let G be a nilpotent group. G has the central series

$$\{e\} = Z_0 \subseteq Z_1 \subseteq Z_2 \subseteq \cdots \subseteq Z_n = G$$

for some $n \in \mathbb{N}$. We have that Z_i/Z_{i-1} corresponds to the centre of a group, hence, it is abelian. Therefore, G is solvable.

(v) We have that S_3 has trivial centre. Hence, S_3 cannot be equal to Z_n for some n. Therefore, S_3 is not nilpotent.

11. Let H be a normal subgroup of a nilpotent group G. Let $r \geq 1$ be the smallest index such that there exists a nontrivial $h \in H \cap Z_r$. Let $g \in G$. We have that $[g,h] = ghg^{-1}h^{-1} \in H$ as $ghg^{-1}, h^{-1} \in H$. We note that $Z_r/Z_{r-1} = Z(G/Z_{r-1})$. Then, $ghZ_{r-1} = hgZ_{r-1}$ as $g \in G$ and $h \in Z_r$. Hence, $[g,h] = ghg^{-1}h^{-1} \in Z_{r-1}$. Therefore, $[g,h] \in H \cap Z_{r-1}$. By assumption, $[g,h] = 1$, so $h \in Z(G)$. Thus, H has a nontrivial intersection with $Z(G)$.

12. Let G be a finite nilpotent group and let H be a proper subgroup of G. As G is nilpotent, $Z(G)$ is trivial, otherwise, G is the trivial group. Suppose that H does not contain $Z(G)$. Then, there exists a $g \in Z(G)$ such that $g \notin H$. Let $ghg^{-1} \in gHg^{-1}$. As $g \in Z(G)$, we have that $ghg^{-1} \in H$. Furthermore, let $h \in H$. Then, $h = hgg^{-1} = ghg^{-1} \in gHg^{-1}$. By definition, $h \in N_G(H)$. Hence, H is properly contained in $N_G(H)$. Now, suppose that H does contain $Z(G)$. There exists an index r such that H contains Z_r but H does not contain Z_{r+1}. There then exists an $X \in Z_{r+1}$ such that $x \notin H$. From the previous exercise, not $[x,g] \in Z_r$ for any $g \in G$. Hence, $[x,g] \in H$. Thus, $xgx^{-1}g^{-1} \in H$. Suppose $h \in H$. Then, $xhx^{-1}h^{-1} \in H$. Thus, $xhx^{-1} \in H$, which means $x \in N_G(H)$. Therefore, H is properly contained in $N_G(H)$. Let P be a Sylow subgroup of G. We have that $N_G(N_G(P)) = N_G(P)$. However, $N_G(P)$ is properly contained in $N_G(N_G(P))$. Thus, $N_G(P)$ cannot be a proper subgroup of G. As $N_G(P)$ is not trivial, $N_G(P) = G$, that is, P is normal in G.

13. Let G be a group and let H, K be subgroups of G such that K is characteristic in H and H is characteristic in G. Let $\varphi \in \mathrm{Aut}_{\mathsf{Grp}}(G)$. We have that $\varphi(H) \subseteq H$, and so φ_H, the restriction of φ to H, is an automorphism of H, that is, $\varphi_H \in \mathrm{Aut}_{\mathsf{Grp}}(H)$. As K is characteristic in H, $\varphi_H(K) \subseteq K$. We have that $\varphi(K) = \varphi_H(K)$ as K is a subgroup of H. Therefore, K is characteristic in G. We have that

$$G^{(n)} \text{ char } G^{(n-1)} \text{ char ... char } G^{(1)} \text{ char } G$$

Via induction, $G^{(n)}$ char G for all $n \in \mathbb{N}$.

14. Let H be a nontrivial normal subgroup of a solvable group G. We have that G has the derived series

$$\{e\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

Let r be the largest index such that $K = H \cap G_r$ is nontrivial. Let $x, y \in K$. We have that $[x,y] \in H$ and $[x,y] \in G_{r+1}$. Therefore, $[x,y] \in H \cap G_{r+1}$. By assumption, $[x,y] \in \{e\}$. Thus, $[x,y] = e$. It follows that K is commutative. By a previous exercise, G_r is normal. Hence, K is normal.

15. Let G be a group of order p^2q. Suppose that $p > q$. By Sylow III, $n_p \equiv 1 \mod p$ and $n_p \mid q$. Then, $n_p = 1$. Denote the unique normal p-Sylow subgroup by N. We have that G/N is of order q, hence, abelian. Furthermore, N is of order p^2, hence, abelian. G/N and N are then both solvable, thus, G is solvable. Now, suppose that $p < q$. By Sylow III, $n_q \equiv 1 \mod q$ and $n_q \mid p^2$. We must have that $n_q \in \{1, p^2\}$. Suppose that $n_q = p^2$. Then, these Sylow subgroups contibute $p^2(q-1)$ elements of order q, hence, there can only be one Sylow subgroup of order p^2. Again, let N be the subgroup of order p^2, and we see that G is solvable. If $n_q = 1$, then let M be the unique normal subgroup of order q in G. We have that M is abelian, and G/M is also abelian as a group of order p^2. Hence, G is solvable. Finally, let $p = q$. If G is abelian, then G is solvable. Suppose G is noncommutative. As G is a p-group, $Z(G)$ is nontrivial. $Z(G)$ is either of order p or p^2. In both cases $Z(G)$ is abelian, and $G/Z(G)$ is abelian. Hence, $Z(G)$ and $G/Z(G)$ are solvable, which implies G is solvable. Therefore, all groups of order p^2q are solvable.

16. Note that p-groups and groups of order p^2q are solvable. We look at groups of order

$$6, 10, 14, 15, 21, 22, 24, 26, 30, 33, 34, 35, 36, 38, 39, 40, 42, 46, 48, 51, 54, 55, 56,$$

$$57, 58, 62, 65, 66, 69, 70, 72, 74, 77, 78, 80, 82, 84, 85, 86, 87, 88, 90, 91, 93, 94,$$

$$95, 96, 99, 100, 102, 104, 105, 106, 108, 110, 111, 112, 114, 115, 117, 118, 119$$

Note that groups of order pq where $q \not\equiv 1 \mod p$ with $p < q$ are cyclic, hence abelian and then solvable.

$$6, 10, 14, 15, 21, 22, 24, 26, 30, 34, 36, 38, 39, 40, 42, 46, 48, 54, 55, 56,$$

$$57, 58, 62, 66, 70, 72, 74, 78, 80, 82, 84, 86, 88, 90, 93, 94,$$

$$96, 99, 100, 102, 104, 105, 106, 108, 110, 111, 112, 114, 117, 118$$

By Feit-Thompson, every group of odd order is solvable.

$$6, 10, 14, 22, 24, 26, 30, 34, 36, 38, 40, 42, 46, 48, 54, 56, 58, 62, 66, 70, 72, 74, 78, 80, 82,$$

$$84, 86, 88, 90, 94, 96, 100, 102, 104, 106, 108, 110, 112, 114, 118$$

Let G be a group of order $2p$. Then, G contains a group of order p, N say. We have that $[G : N] = 2$, hence, normal. We have that G/N is abelian and N is abelian. Hence, G/N and N are both solvable. Thus, G is solvable.

$$24, 30, 36, 40, 42, 48, 54, 56, 66, 70, 72, 78, 80, 84, 88, 90, 96, 100, 102, 104, 108, 110, 112, 114$$

Let G be a group of order pq with $p < q$. By Sylow III, $n_q \equiv 1 \mod q$ and $n_q \mid p$. Then, $n_q = 1$. By N be the normal subgroup of G of order q. We have that N is abelian, and G/N is abelian. Therefore, G is solvable.

$$24, 30, 36, 40, 42, 48, 54, 56, 66, 70, 72, 78, 80, 84, 88, 90, 96, 100, 102, 104, 108, 110, 112, 114$$

Let G be a group of order pqr with $p < q < r$ prime. G is not simple or abelian, hence, it contains a normal subgroup N of possible orders pq, pr, qr, p, q, r. In all cases, N is solvable. We also have that G/N is solvable as it has an order of r, q, p, qr, pr, qp. Then, G is solvable.

$$24, 36, 40, 48, 54, 56, 72, 80, 84, 88, 90, 96, 100, 104, 108, 112$$

Let G be a group of order p^2q^2, $p < q$ prime. We have that G is not simple or abelian, hence, G contains a normal subgroup of possible orders $p, p^2, q, q^2, pq, pq^2, p^2q$, N say. G/N has possible orders $pq^2, q^2, p^2q, pq, p, q$ respectively. Hence, $N, G/N$ are both solvable. Therefore, G is solvable.

$$24, 40, 48, 54, 56, 72, 80, 84, 88, 90, 96, 104, 108, 112$$

Let G be a group of order $2^n \cdot 3$ with $n \geq 3$. We must have that G is simple or abelian and contains a normal subgroup of order 2^n, N say. N is a p-group, hence solvable. We also have that G/N is cyclic, hence solvable. Therefore, G is solvable.

$$40, 54, 56, 72, 80, 84, 88, 90, 104, 108, 112$$

Let G be a group of order $40 = 2^3 \cdot 5$. We have that G is not simple or abelian, hence, G contains a normal subgroup N with $|N| \in \{2, 2^2, 2^3, 2 \cdot 5, 2^2 \cdot 5\}$. Then, N is solvable. It also follows that G/N is solvable. With a similar argument, we can prove that $54 = 3^3 \cdot 2, 56 = 2^3 \cdot 7, 88 = 2^3 \cdot 11, 104 = 2^3 \cdot 13$ are solvable.

$$72, 80, 84, 90, 108, 112$$

Let G be a group of order $72 = 2^3 \cdot 3^2$. As G is not simple or abelian, G contains a normal subgroup N with $|N| \in \{2, 4, 8, 6, 12, 24, 18, 36\}$. N is then solvable, and G/N is solvable. Hence, G is solvable.

$$80, 84, 90, 108, 112$$

A group of order 80 is either abelian or not simple. Let G be a group of order 80. Then, G has a normal subgroup N with $|N| \in \{1, 2, 4, 8, 16, 5, 10, 20, 40\}$. Hence, N is solvable. We also have that G/N is solvable. Thus, G is solvable.

$$84, 90, 108, 112$$

Let G be a group of order 84. G is either abelian or not simple. We have that G has a normal subgroup N with $|N| \in \{2, 4, 6, 12, 14, 28, 42\}$. Hence, N is solvable. We also have that G/N is solvable. Thus, G is solvable.

$$90, 108, 112$$

We prove the final ones in a similar way by noting we have proven all of the lesser orders are solvable.

17. Suppose the statement "Every finite group of odd order is solvable" holds. Let G be a noncommutative finite simple group. Suppose that G has odd order. We have that the commutator of G, G', must be G itself as G is noncommutative and G is simple. Hence, G cannot be solvable, which is a contradiction. Therefore, G has even order. For the converse, suppose the statement "Every noncommutative finite simple group has even order" holds. Let G be a group of odd order. If G is abelian, then G is automatically solvable. Suppose G is noncommutative. As G has odd order, it is not simple, hence, G has a normal subgroup N. N is either abelian or noncommutative. If N is abelian, then N is solvable. If N is noncommutative, then as $|N|$ divides $|G|$, we have that N is of odd order, hence, not simple. N contains a normal subgroup of order M. Via induction, we get a chain of subgroups that either terminate with an abelian group, or eventually we end up with a group of prime order, which is also abelian. Thus, N is solvable. With the same argument, G/N is also solvable. Therefore, G is solvable.

4.4 - The Symmetric Group

1. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 2 & 7 & 5 & 3 & 4 & 6 \end{pmatrix} \in S_8$$

We have that $\sigma = \begin{pmatrix} 1 & 8 & 6 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 4 & 7 \end{pmatrix} \begin{pmatrix} 5 \end{pmatrix}$. Then, σ is of type $[6, 2, 1]$.

2.

3.

4.

5. We have that S_1 is the trivial group, and the class formula is then $1 = 1$. S_2 is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is abelian, hence, its class formula is $2 = 2$. S_3 is noncommutative and has trivial centre. The only possible class formula is $6 = 1 + 2 + 3$. S_4 has class formula $24 = 1 + 8 + 6 + 6 + 3$. S_5 has class formula $120 = 1 + 10 + 15 + 20 + 20 + 30 + 24$. S_6 has class formula $720 = 1 + 15 + 45 + 15 + 40 + 120 + 40 + 90 + 90 + 144 + 120$.

6. Let N be a normal subgroup of S_4. We note that S_4 has the class formula $24 = 1+8+6+6+3$. By Lagranges Theorem, $|N| \in \{1, 2, 3, 4, 6, 8, 12, 24\}$. As N is normal, it is the union of conjugacy classes. N must also contain the identity. We have that $4 = 1 + 3$ and $12 = 1 + 3 + 8$, and other divisors cannot be represented as a sum of numbers from the class formula. Hence, $|N| \in \{1, 4, 12, 24\}$.

7. We first prove that S_n is generated by 2-cycles of the form $(k, k+1)$. Let $(a\ b)$ be a 2-cycle in S_n. Without loss of generality, suppose $a > b$. We have that

$$(a\ b) = (b\ b+1)(b+1\ b+2)...(a-2\ a-1)(a-1\ a)(a-2\ a-1)...(b+1\ b+2)(b\ b+1)$$

By Lemma 4.11, the set of transpotitions generate S_n, hence, 2-cycles of the form $(k\ k+1)$ must generate S_n. Let $(1\ 2), (1\ 2\ ...\ n) \in S_n$. We have that

$$(k+1\ k+2) = (1\ 2\ ...\ n)^k (1\ 2)(1\ 2\ ...\ n)^{-k}$$

It follows that $S_n = \langle (1\ 2), (1\ 2\ ...\ n) \rangle$.

8. Let $n \geq 2$. Let H be the subgroup of S_n fixing 1. We have that for all $\sigma \in H$, σ is a permutation of $A = \{2, 3, ..., n\}$. We can see that $H = S_{|A|}$. Therefore, $H \cong S_{n-1}$. Let K be a subgroup of S_n properly containing H.

9.

10. Let $\sigma \in S_n$ be a permutation of type $[\lambda_1, ..., \lambda_r]$. Let $a_1, a_2, ..., a_n$ denote the multiplicities of $1, 2, 3, ..., n$ respectively that appear in $[\lambda_1, ..., \lambda_r]$. We have that the length of the conjugacy class that contains σ is

$$\frac{n!}{\prod_{i=1}^{n} (b_i!)(i^{b_i})}$$

where $b_i = 1$ if $a_i = 0$ and $b_i = a_i$ otherwise.

11. Let p be a prime integer. By the previous exercise, there are $(p-1)!$ p-cycles in S_p, which are all of order p. We have that each p-Sylow subgroup of S_p contains $p-1$ elements of order p. Each p-Sylow subgroup has nontrivial intersection with eachother, hence, the number of p-Sylow subgroups are $(p-1)!/(p-1) = (p-2)!$. By the Third Sylow Theorem, $(p-2)! \equiv 1 \mod p$, hence, $(p-1)! \equiv 1 \mod p$.

12.

13.

14. Let $n \geq 4$. We have that $Z(A_n)$ is trivial for all $n \geq 5$ as A_n is simple. Let $\sigma \in A_4$ be a nontrivial element. Suppose that $\sigma(a) = b$. Choose $c, d \neq a, b$. We have that $\sigma(b\ c\ d)(a) = b$ and $(b\ c\ d)\sigma(a) = c$. Hence, the center of A_4 is trivial.

15.

16.

17. Possible types for elements of A_4 are $[1,1,1,1], [2,2], [3,1]$. There is 1 element of type $[1,1,1,1]$ in A_4. There are $4!/(2 \cdot 2 \cdot 2) = 3$ elements of type $[2,2]$ in A_4. There are $4!/3 = 8$ elements of type $[3,1]$ in A_4. Hence, the class formula of A_4 is

$$|A_4| = 12 = 1 + 3 + 8$$

We can deduce that there is no normal subgroup of order 6 in A_4 as you cannot form 6 from $1, 3, 8$.

18. Let $n \geq 5$, and let H be a subgroup of A_n such that $[A_n : H] < n$. The action of A_n on A_n/H induces a homomorphism $\varphi : A_n \to S_{[A_n:H]}$. As $|A_n| = n!/2 > [A_n : H]! = |S_{[A_n:H]}|$, φ cannot be injective. As A_n is simple, $\ker \varphi$ must be A_n. This implies that $xH = H$ for all $x \in A_n$, which means that $H = A_n$. Therefore, if H is a subgroup of A_n, $[A_n : H] \geq 5$. For $n \geq 3$, A_n contains A_{n-1} and A_{n-1} is a nontrivial proper subgroup of A_n of index n.

19. Let $n \geq 5$, and let C be a set with $|C| = k < n$. Let ρ be an action of A_n on C. ρ induces a homomorphism $\varphi : A_n \to S_k$. As $|A_n| = n!/2 > k! = |S_k|$, φ cannot be injective. Hence, $\ker \varphi$ is nontrivial. As A_n is simple, $\ker \varphi = A_n$. Therefore, ρ is the trivial action. Let N be the normal subgroup of A_4. We have that A_n/N is of order 3, and A_4 acts nontrivially on A_n/N. Let ρ be an action of A_4 on a set S where $|S| = 2$. We have that ρ induces a homomorphism $\varphi : A_4 \to S_2$. We have that $\ker \varphi = 1, N, A_n$. As $12 > 2$, φ cannot be injective, hence, $\ker \varphi = N$ or $\ker \varphi = A_n$. As $3 > 2$, we cannot have $\ker \varphi = N$ as A_n/N would be isomorphic to a subgroup of S_2. Hence, $\ker \varphi = A_n$. ρ is then the trivial action.

20.

21. We have that A_6 has the class formula

$$320 = 1 + 40 + 40 + 45 + 90 + 144$$

The only divisors of 320 that you can form from numbers in the class formula that contain 1 are 1 and 320. Hence, A_6 cannot contain a nontrivial normal subgroup. Hence, A_6 is simple.

22.

4.5 - Products of Groups

1.

2.

3.

4. Consider the sequence

$$0 \longrightarrow \mathbb{Z} \xrightarrow{2} \mathbb{Z} \longrightarrow \mathbb{Z}/\mathbb{Z} \longrightarrow 0$$

We have that $\varphi : \mathbb{Z} \to \mathbb{Z}$ given by $\varphi(x) = 2x$ is injective with image $2\mathbb{Z}$. Note this is the kernel of the canonical projection from $\mathbb{Z}$ to $\mathbb{Z}/2\mathbb{Z}$. We also have that the canonical projection is surjective. Therefore, the sequence is exact. We have that every subgroup H of $\mathbb{Z}$ such that $H \cap \mathbb{Z} = \{0\}$ must be the trivial subgroup, hence, the sequence does not split.

5.

6. Let N, H be groups and let $\theta : H \to \mathrm{Aut}_{\mathsf{Grp}}(N), h \mapsto \theta_h$ be a homomorphism. Define an operation $\bullet_\theta$ on the set $N \times H$ as follows: for $n_1, n_2 \in N$ and $h_1, h_2 \in H$, let

$$(n_1, h_1) \bullet_\theta (n_2, h_2) := (n_1\theta_{h_1}(n_2), h_1h_2)$$

Let $n_1, n_2, n_3 \in N$ and $h_1, h_2, h_3 \in H$, we have that

$$\begin{aligned}
[(n_1, h_1) \bullet_\theta (n_2, h_2)] \bullet_\theta (n_3, h_3) &= (n_1\theta_{h_1}(n_2), h_1h_2) \bullet_\theta (n_3, h_3) \\
&= (n_1\theta_{h_1}(n_2)\theta_{h_1h_2}(n_3), h_1h_2h_3) \\
&= (n_1\theta_{h_1}(n_2)\theta_{h_1}(\theta_{h_2}(n_3)), h_1h_2h_3) \\
&= (n_1\theta_{h_1}(n_2\theta_{h_2}(n_3)), h_1h_2h_3) \\
&= (n_1, h_1) \bullet_\theta (n_2\theta_{h_2}(n_3), h_2h_3) \\
&= (n_1, h_1) \bullet_\theta [(n_2, h_2) \bullet_\theta (n_3, h_3)]
\end{aligned}$$

Let $n \in N$ and $h \in H$. Note

$$(n, h) \bullet_\theta (1_N, 1_H) = (n\theta_h(1_N), h1_H) = (n1_N, h) = (n, h)$$

$$(1_N, 1_H) \bullet_\theta (n, h) = (1_N\theta_{1_H}(n), 1_Hh) = (\mathrm{Id}(n), h) = (n, h)$$

Then, $(1_H, 1_N)$ is the identity element in $N \rtimes_\theta H$. Finally,

$$(n, h) \bullet_\theta (\theta_{h^{-1}}(n^{-1}), h^{-1}) = (n\theta_h(\theta_{h^{-1}}(n^{-1})), hh^{-1}) = (nn^{-1}, 1_H) = (1_N, 1_H)$$

$$(\theta_{h^{-1}}(n^{-1}), h^{-1}) \bullet_\theta (n, h) = (\theta_{h^{-1}}(n^{-1})\theta_{h^{-1}}(n), h^{-1}h) = \theta_{h^{-1}}(n^{-1}n), h^{-1}h) = (\theta_{h^{-1}}(1_N), 1_H) = (1_N, 1_H)$$

Therefore, $N \rtimes_\theta H$ has inverses. It follows that $N \rtimes_\theta H$ is a group.

7.

8. Let N, H be solvable groups, and let $G = N \rtimes_\theta H$. We have that $N \times 1_H$ is normal in G by Proposition 5.10, and we also have that $G/(N \times 1_H) \cong 1_N \times H \cong H$. Note $N \cong N \times 1_H$, and so $N \times 1_H$ is solvable. We also have that $G/(N \times 1_H)$ is solvable as $1_N \times H \cong H$ is solvable. Therefore, G is solvable.

9. Let N, H be groups, and let $G = N \rtimes_\theta H$ be an abelian group. Let $n_1, n_2 \in N$ and $h_1, h_2 \in H$. As G is abelian,

$$\begin{aligned}
(1_N, 1_H) &= [(n_1, h_1), (n_2, h_2)] \\
&= ((n_1, h_1) \bullet_\theta (n_2, h_2)) \bullet_\theta ((n_2, h_2) \bullet_\theta (n_1, h_1))^{-1} \\
&= (n_1\theta_{h_1}(n_2), h_1h_2) \bullet_\theta (n_2\theta_{h_2}(n_1), h_2h_1)^{-1} \\
&= (n_1\theta_{h_1}(n_2), h_1h_2) \bullet_\theta (\theta_{(h_2h_1)^{-1}}((n_2\theta_{h_2}(n_1))^{-1}), (h_2h_1)^{-1}) \\
&= (n_1\theta_{h_1}(n_2)\theta_{h_1h_2}(\theta_{(h_2h_1)^{-1}}((n_2\theta_{h_2}(n_1))^{-1})), h_1h_2(h_2h_1)^{-1}) \\
&= (n_1\theta_{h_1}(n_2)\theta_{h_1h_2(h_2h_1)^{-1}}((n_2\theta_{h_2}(n_1))^{-1}), [h_1, h_2]) \\
&= (n_1\theta_{h_1}(n_2)\theta_{[h_1,h_2]}(\theta_{h_2^{-1}}(n_1)n_2^{-1}), [h_1, h_2]) \\
&= (n_1\theta_{h_1}(n_2)\theta_{[h_1,h_2]h_2^{-1}}(n_1)\theta_{[h_1,h_2]}(n_2^{-1}), [h_1, h_2])
\end{aligned}$$

Thus, $[h_1, h_2] = 1_H$. We have that then

$$1_N = n_1\theta_{h_1}(n_2)\theta_{[h_1,h_2]h_2^{-1}}(n_1)\theta_{[h_1,h_2]}(n_2^{-1}) = n_1\theta_{h_1}(n_2)\theta_{h_2^{-1}}(n_1)n_2^{-1}$$

Therefore, $n_1\theta_{h_1}(n_2) = n_2\theta_{h_2}(n_1)$. Then, for any $n \in N, h \in H$, $\theta_h(n) = 1_N\theta_h(n) = n\theta_h(1_N) = n1_N = n$. θ is then the trivial morphism. Hence, $G \cong N \times H$.

10. Let N be a normal subgroup of a finite group G, and assume $|N|$ and $|G/N|$ are relatively prime. Suppose in G there exists a subgroup H such that $|H| = |G/N|$. We have that $N \cap H$ is a subgroup of both N and H, hence, $|N \cap H|$ must divide both $|N|$ and $|H|$. As $|H|$ and $|N|$ are relatively prime, $|N \cap H| = 1$, thus $N \cap H$ is trivial. As N is normal in G, NH is a subgroup of G with order

$$|NH| = \frac{|N||H|}{|N \cap H|} = \frac{|N||H|}{1} = |N||H| = |N||G/N| = |G|$$

Thus, $G = NH$. By Proposition 5.11, $G \cong N \rtimes H$.

11. Let $n > 0$. We have that $D_{2n} = \langle x, y \mid x^n = y^2 = (xy)^2 = 1\rangle$. We have that $\langle x\rangle$ is normal in D_{2n} as $\langle x\rangle$ has index 2. If n is odd, then $\langle x\rangle \cap \langle y\rangle = 1$ by order considerations. If n is even, then the only possible way for $\langle x\rangle \cap \langle y\rangle$ is nontrivial is that if $x^{n/2} = y$. This implies $x^{n/2+1} = xy$ and so $x^{n+2} = 1$, which means $x^2 = 1$. For D_4, $\langle x\rangle \cap \langle y\rangle$ is still trivial. In all cases, $\langle x\rangle \cap \langle y\rangle = 1$. As $|\langle x\rangle| = n$ and $|\langle y\rangle| = 2$, $D_{2n} = \langle x\rangle\langle y\rangle$. By Proposition 5.11, $D_{2n} \cong \langle x\rangle \rtimes \langle y\rangle \cong C_n \rtimes C_2$.

12.

13.

14.

15.

16.

17.

4.6 - Finite Abelian Groups

1.

2.

3. Let G be a noncommutative group of order p^3 where p is prime. As G is a noncommutative p-group, $1 < |Z(G)| < p^3$. Hence, $|Z(G)| \in \{p, p^2\}$ by Lagranges Theorem. Suppose that $|Z(G)| = p^2$. We then have that $G/Z(G)$ is of order p and is then cyclic. Thus, G is abelian, which is a contradiction. We must have that $|Z(G)| = p$, and so $Z(G) \cong \mathbb{Z}/p\mathbb{Z}$. As $Z(G)$ is of order p, we must have that $G/Z(G)$ is of order p^2. As G is noncommutative, $G/Z(G)$ cannot be abelian, thus, $G/Z(G) \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

4. Abelian groups of order $400 = 2^4 \cdot 5^2$ are

$$\mathbb{Z}/400\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/200\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/100\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z},$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z},\ \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/80\mathbb{Z},\ \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/40\mathbb{Z},\ \mathbb{Z}/20\mathbb{Z} \times \mathbb{Z}/20\mathbb{Z}$$

5.

6.

7. Let $p > 0$ be a prime integer, G a finite abelian group, and denote $\rho : G \to G$ the homomorphism defined by $\rho(g) = pg$. Let A be a finite abelian group such that $pA = 0$. We have that $A \cong \oplus_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z}$ for some n and $d_1, ..., d_n \in \mathbb{Z}$. Then,

$$0 = pA = p\bigoplus_{i=1}^{n} \mathbb{Z}/d_i\mathbb{Z} = \bigoplus_{i=1}^{n} p\mathbb{Z}/d_i\mathbb{Z}$$

Hence, $0 = p\mathbb{Z}/d_i\mathbb{Z}$ for all d_i. We must have that every nontrivial $x \in \mathbb{Z}/d_i\mathbb{Z}$ has order which divides p. Thus, $|x| = p$. It follows that $d_i = p$ for all i. Therefore,

$$A \cong \bigoplus_{i=1}^{n} \mathbb{Z}/p\mathbb{Z}$$

for some n. Let $x \in \ker\rho$. We have that $px = 0$ by definition. Hence, $p\ker\rho = 0$. Let $x \in \text{coker } \rho$. We have that x corresponds to some $x' + \text{im } \rho$ as $\text{coker } \rho \cong G/\text{im } \rho$. We have that $p(x' + \text{im } \rho) = px' + \text{im } \rho = \rho(x') + \text{im } \rho = \text{im } \rho$. Hence, $p\text{coker } \rho = 0$. Note that

$$\ker\rho \cong \bigoplus_{i=1}^{n} \mathbb{Z}/p\mathbb{Z}, \text{ coker } \rho \cong \bigoplus_{i=1}^{m} \mathbb{Z}/p\mathbb{Z}$$

for some m, n. By the First Isomorphism Theorem, $G/\ker\rho \cong \text{im } \rho$, hence, $|G/\ker\rho| = |\text{im } \rho|$. Then,

$$|G/\ker\rho| = |\text{im } \rho| \implies |G|/|\ker\rho| = |\text{im } \rho| = |G|/|\text{im } \rho| = |\ker\rho| \implies |G/\text{im } \rho| = |\ker\rho| \implies |\text{coker } \rho| = |\ker\rho|$$

It follows that $m = n$. Therefore,

$$\ker\rho \cong \bigoplus_{i=1}^{n} \mathbb{Z}/p\mathbb{Z} \cong \text{coker } \rho$$

Let H be a subgroup of order p in G. Let $x \in H$. We have that $\rho(x) = px = 0$ as H is of order p. Therefore, $H \subseteq \ker\rho$. Now, suppose that H is a subgroup of index p in G. Let $x \in \text{im } \rho$. We have that $x = py$ for some y. We have that $x + \text{im } \rho = py + \text{im } \rho = p(y + \text{im } \rho) = \text{im } \rho$ as G/H has order p. Therefore, $x \in \text{im } \rho$ and $\text{im } \rho \subseteq H$. Now, let G_p be the set of subgroups of G of order p. For every $H \in G_p$, we have that H is contained in the kernel of ρ. Note that $\ker\rho \cong \text{coker } \rho$, hence, every element of G_p, H, corresponds to a unique subgroup of $\text{coker } \rho$, H'. We have that H' then corresponds to some $K/\text{im } \rho$ in $G/\text{im } \rho$. As H is of order p, we must have that K is of index p. There is then a correspondance between a subgroup of order p and a subgroup of index p. Therefore, the number of subgroups of order p in G is equal to the number of subgroups of index p in G.

8.

9.

10. Let G be a finite group of order n and let $G^\vee := \text{Hom}_{\mathsf{Grp}}(G, \mathbb{C}^*)$. Let $\sigma \in \text{Hom}_{\mathsf{Grp}}(G, \mathbb{C}^*)$ and let $g \in G$. We have that $\sigma(g)^n = \sigma(g^n) = \sigma(1_G) = 1$. Hence, $\sigma(g)$ is a root of 1 in $\mathbb{C}$. The image of every $\sigma \in G^\vee$ is then a root of 1 in $\mathbb{C}$. Let C_n be the cyclic group of order n. Let $\sigma \in C_n^\vee$ and let $x \in C_n$ be a generator. We have that $\sigma(x^k) = \sigma(x)^k$ for all $0 \leq k < n$, hence, σ is completely determined by $\sigma(x)$. We have that $\sigma(x)$ is a root of 1 in $\mathbb{C}$ and is the solution to $z^n = 1$. There are n possible z's that satisfy this equation, thus, there are n elements of $C_n^\vee$. Let $z_0 = \exp(2\pi i/n)$ and let $\sigma_0 : C_n \to \mathbb{C}^*$ be the homomorphism sending x to z_0. We have that $\sigma_0^k(x) = \exp(2\pi ik/n)$ for $0 \leq k < n$ and we note that $\sigma_0^i(x) \neq \sigma_0^j(x)$ for all $0 \leq i < j < n$. Therefore, $C_n^\vee$ is generated by σ_0. It follows that $C_n \cong C_n^\vee$. Let G_1, G_2 be groups and let K be an abelian group. We set to prove that

$$\text{Hom}_{\mathsf{Grp}}(G_1 \times G_2, K) \cong \text{Hom}_{\mathsf{Grp}}(G_1, K) \times \text{Hom}_{\mathsf{Grp}}(G_2, K)$$

Let Z be a group and $f_1 : Z \to \text{Hom}(G_1, K), f_2 : Z \to \text{Hom}(G_2, K)$ be group homomorphism. Suppose that there is a homomorphism ψ such that the following diagram commutes

$$\begin{tikzcd}
& & \text{Hom}_{\mathsf{Grp}}(G_2, K) \\
Z \arrow[r, "\psi"] \arrow[urr, bend left, "f_2"] \arrow[drr, bend right, "f_1"'] & \text{Hom}_{\mathsf{Grp}}(G_1 \times G_2, K) \arrow[ur, "\pi_2"] \arrow[dr, "\pi_1"'] & \\
& & \text{Hom}_{\mathsf{Grp}}(G_1, K)
\end{tikzcd}$$

where π_1 is defined by $\sigma(g_1, g_2) \mapsto \sigma(g_1, 0_{G_2})$ and π_2 is defined by $\sigma(g_1, g_2) \mapsto \sigma(0_{G_1}, g_2)$ for all $(g_1, g_2) \in G_1 \times G_2$. Let $z \in Z$ and $(g_1, g_2) \in G_1 \times G_2$. By commutativity,

$$[f_1(z)](g_1) = [(\pi_1 \circ \psi)(z)](g_1) = [\psi(z)](g_1, 0_{G_2})$$

$$[f_2(z)](g_2) = [(\pi_2 \circ \psi)(z)](g_2) = [\psi(z)](0_{G_1}, g_2)$$

Hence, for all $(g_1, g_2) \in G_1 \times G_2$ and $z \in Z$, we have that

$$[\psi(z)](g_1, g_2) = [\psi(z)](g_1, 0_{G_2}) + [\psi(z)](0_{G_1}, g_2) = [f_1(z)](g_1) + [f_2(z)](g_2)$$

This shows that ψ is unique. We also note that ψ is a homomorphism. Therefore, $\mathrm{Hom}_{\mathsf{Grp}}(G_1 \times G_2, K)$ satisfies the universal property for the product of $\mathrm{Hom}_{\mathsf{Grp}}(G_1, K)$ and $\mathrm{Hom}_{\mathsf{Grp}}(G_2, K)$. Hence,

$$\mathrm{Hom}_{\mathsf{Grp}}(G_1 \times G_2, K) \cong \mathrm{Hom}_{\mathsf{Grp}}(G_1, K) \times \mathrm{Hom}_{\mathsf{Grp}}(G_2, K)$$

We note that

$$(G \times K)^\vee = \mathrm{Hom}_{\mathsf{Grp}}(G \times K, \mathbb{C}^*) \cong \mathrm{Hom}_{\mathsf{Grp}}(G, \mathbb{C}^*) \times \mathrm{Hom}_{\mathsf{Grp}}(K, \mathbb{C}^*) = G^\vee \times K^\vee$$

Let G be a finite abelian group. We have that $G \cong \oplus_{i=1}^n C_{d_i}$ for some integers d_i. Via induction,

$$G^\vee \cong \left(\bigoplus_{i=1}^n C_{d_i} \right)^\vee \cong \bigoplus_{i=1}^n C_{d_i}^\vee \cong \bigoplus_{i=1}^n C_{d_i} \cong G$$

11.

12.

13.

14.

15. Let G be a finite abelian group and let $a \in G$ be an element of maximal order in G. We have that

$$G \cong \bigoplus_{i=1}^n \mathbb{Z}/d_i\mathbb{Z}$$

where $d_1 \mid ... \mid d_n$. a must be of order d_n as the representation is unique, and any $b \in G$ must be of order d_i, hence, $|b|$ divides $|a|$.

16.

V - Irreducibility and Factorisation in Integral Domains

5.1 - Chain Conditions and Existence of Factorisations

1. Let R be a Noetherian ring and let I be an ideal of R. Let J/I be an ideal of R/I. We have that J is an ideal of R, and since R is Noetherian, $J = (j_1, ..., j_n)$ for some $j_1, ..., j_n$. Let $x + I \in J/I$. We have that

$$x + I = (x_1 j_1 + ... + x_n j_n) + I = (x_1 j_1 + I) ... + (x_n j_n + I) = x_1(j_1 + I) + ... + x_n(j_n + I)$$

for some $x_1, ..., x_n \in R$. Hence, $J/I = (j_1 + I, ..., j_n + I)$. It follows that R/I is Noetherian.

2. Let R be a commutative ring such that $R[x]$ is Noetherian. We have that (x) is an ideal of $R[x]$, and, by the previous exercise, $R \cong R[x]/(x)$ is Noetherian. Therefore, R is a Noetherian ring.

3.

4. Let R be the ring of real-valued continuous functions on the interval $[0,1]$. Let $I_n = \{f \in R \mid \forall x \in [0,1/n], f(x) = 0\}$. Let $f, g \in I_n$, and let $x \in [0,1/n]$. Then, $(f-g)(x) = f(x) - g(x) = 0 - 0 = 0$. Hence, $f - g \in I_n$. Furthermore, let $r \in R$ and $f \in I_n$. Let $x \in [0,1/n]$. Then, $(rf)(x) = r(x)f(x) = r(x)0 = 0$. Hence, $rf \in I_n$. It follows that I_n is an ideal for all n. We note that each I_n is properly contained in I_{n+1} as for example f defined by $f(x) = 0$ for $x \in [0, 1/(n+1)]$ and $f(x) = x - (1/(n+1))$ otherwise is in I_{n+1}, but not in I_n. Hence, the sequence $I_1 \subseteq I_2 \subseteq I_3 \subseteq ...$ cannot stabilise. R cannot then be Noetherian.

5.

6. Let I be an ideal of $R[x]$, and let $A = \{0\} \cup \{a \in R \mid a \text{ is the leading coefficient of some element } f \in I\}$. Let $a, b \in A$ such that $a \neq b$. We have that there exists a polynomial f of degree n with leading coefficient a and a polynomial g of degree m with leading coefficient m. Without loss of generality, suppose that $m \leq n$. We have that $x^{n-m}g$ is a polynomial of degree n with leading coefficient a. Furthermore, as $a \neq b$, $f - g$ is a polynomial with leading coefficient $a - b$ that is in I as I is an ideal. Hence, $a - b \in A$. Note that $0 \in A$. We have that $(A, +)$ is a subgroup of $(R, +)$. Let $r \in R$ and $a \in A$ such that $ra \neq 0$. We have that there is a $f \in I$ such that f has leading coefficient a. As I is an ideal and $r \in R[x]$, $rf \in I$. rf has leading coefficient ra, and so $ra \in A$. We then have that A is an ideal of R.

7.

8.

9.

10. Let R be an Artinian ring, and let I be an ideal of R. Let $J_1 \supseteq J_2 \supseteq J_3 \supseteq ...$ be a decending chain of ideal in R/I. By the correspondance theorem, there exists ideals $A_1, A_2, ...$ such that $A_1/I, A_2/I, ...$ are isomorphic to $J_1, J_2, ...$, respectively. We have that the chain $A_1 \supseteq A_2 \supseteq ...$ must stabilise as R is Artinian. The chain must stabilise to some A_n. Hence, $A_n/I = A_{n+1}/I = ...$, therefore, the chain $J_1 \supseteq J_2 \supseteq ...$ must stabilise too. It follows that R/I is Artinian. Now, further suppose that R is an Artinian integral domain. Let $r \in R$ be a non trivial element in R. The sequence $(r) \supseteq (r^2) \supseteq (r^3) \supseteq ...$ must stabilise, therefore, $(r^n) = (r^{n+1})$ for some $n \in \mathbb{Z}$. We have that $r^n = xr^{n+1}$ for some $x \in R$, which means that $r^n(1 - rx) = 0$. As R is an integral domain, if $r^n = 0$, then $r = 0$, which contradicts our assumption, and if $1 - rx$, then r is a unit. As r was arbitrary, R must be a field. Finally, let R be an Artinian ring, and let P be a prime ideal of R. We have that R/P is Artinian, and R/P must be an integral domain. As R/P is an Artinian integral domain, it must be a field. Hence, P is a maximal ideal. We conclude that Artinian rings have Krull dimension 0.

11.

12. Let R be an integral domain. Suppose that $a \in R$ is irreducible. Suppose that there is a proper principle ideal (r) such that (r) properly contains (a). We have that $a \in (r)$ and so $a = rx$ for some $x \in R$. As a is irreducible, r is a unit or x is a unit. If r is a unit, $(r) = R$. If x is a unit, then $r = ax^{-1} \in (a)$ and so $(a) = (r)$. It follows that (a) is maximal among proper princple ideals of R. For the converse, suppose that (a) is maximal among proper principle ideals of R. Suppose that $a = xy$ for some $x, y \in R$. We have that $a \in (y)$ as $a = xy$, and so (a) is contained in (y). By maximality, $(y) = R$ or $(y) = (a)$. If $(y) = R$, then y is a unit. If $(y) = (a)$, then $y = ka$ for some $k \in R$. Then, $a = xy = xka$, and so $(1 - xk)a = 0$. As R is an integral domain, $1 - xk = 0$ as $a \neq 0$. As $1 - xk = 0$, x is then a unit. Therefore, a is irreducible in R.

13. We have that $\mathbb{Z}$ is an integral domain, that is also a PID. By the previous exercise, if $p \in \mathbb{Z}$ is irreducible, then (p) is maximal among proper principle ideals, and as $\mathbb{Z}$ is a PID, (p) is maximal, hence, prime. p is then prime. For the converse, if $p \in \mathbb{Z}$ is prime. Suppose that $p = ab$ for some $a, b \in \mathbb{Z}$. As $p = ab$, we must have that $p \mid ab$. BY primality, $p \mid a$ or $p \mid b$. Without loss of generality, assume $p \mid a$. Then, $a = px$ for some $x \in \mathbb{Z}$. We have that $p = ab = pxb$, and so $p - pxb = 0$. Then, $p(1 - xb) = 0$. As $\mathbb{Z}$ is an integral domain and $p \neq 0$, we have that $1 - xb = 0$, hence, b is a unit. Therefore, p is irreducible in $\mathbb{Z}$.

14. Let R be a commutative ring and let $a, b \in R$. Suppose that there exists $a + (b) \in R/(b)$ is prime. Let $x + (a), y + (a) \in R/(a)$ such that $b + (a) \mid (x + (a))(y + (a))$. Then, $b + (a) \mid xy + (a)$. There then exists a $k + (a) \in R/(a)$ such that $xy + (a) = (k + (a))(b + (a)) = kb + (a)$. So, $xy - kb \in (a)$. Thus, there is a $q \in R$ such that $xy - kb = qa$, and we have that $xy - qa = kb$. We must have that $xy - qa \in (b)$ and $xy + (b) = qa + (b)$. Then, $a + (b) \mid (x + (b))(y + (b))$. As $a + (b)$ is prime, without loss of generality, assume $a + (b) \mid x + (b)$. There is then an $s + (b) \in R/(b)$ such that $x + (b) = (a + (b))(s + (b)) = as + (b)$. We then have that $x - as \in (b)$. There is then a $z \in R$ such that $x - as = zb$, and so $x - zb = as$, in which then $x - zb \in (a)$. We have that $x + (a) = zb + (a)$. Finally, $b + (a) \mid x + (a)$. Therefore, $b + (a)$ is prime.

15. Identify $S = \mathbb{Z}[x_1, ..., x_n]$ in a natural way with a subring of $R = \mathbb{Z}[x_1, x_2, x_3, ...]$. Suppose that $f \in S$ and nontrivial, and let $g \in R$ such that $(f) \subseteq (g)$ in R. Suppose that g can be written as $g = p + r$ where p contains no terms with the variables $x_1, ..., x_n$ and $r \in S$. As $f \in (f) \subseteq (g)$, we must have that $f = k \cdot g$ for some $k \in R$. Then, $f = kp + kr$. As $f \in S$ and $p \notin S$, we must have that $kp = 0$. We must have that $k = 0$ or $p = 0$. Then, $f = kr$. As $r \in S$, we must also have that $k \in S$. If $k = 0$, then $f = 0$, which is a contradiction. Hence, $p = 0$. It follows that $g = r \in S$. Let

$$(f_1) \subseteq (f_2) \subseteq (f_3) \subseteq ...$$

be a chain of ascending principle ideals in R. We have that f_1 is contained in some subring of R corresponding to $S = \mathbb{Z}[x_1, ..., x_m]$ for some m. We then have that $f_2, f_3, ... \in S$. By Hilberts Basis Theorem, S is Noetherian as $\mathbb{Z}$ is Noetherian. Then, the chain must stabilise. Therefore, R is Noetherian, and so R is a domain with factorisations.

16.

17. Let $\mathbb{Z}[\sqrt{-5}]$ be the subring of $\mathbb{C}$ defined by $\mathbb{Z}[\sqrt{-5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$.

(i) Define $\varphi : \mathbb{Z}[t] \to \mathbb{Z}[\sqrt{-5}]$ by the rule $f \mapsto f(\sqrt{-5})$. Let $f \in \ker \varphi$. If $\deg f \geq 2$, then $f = g(t^2 + 5) + r$ for some $g, r \in \mathbb{Z}[t]$ where $\deg r < 2$. As $f \in \ker \varphi$, we have that $0 = f(\sqrt{-5}) = g(\sqrt{-5})0 + r(\sqrt{-5}) = r(\sqrt{-5})$. Hence, $r(\sqrt{-5}) = 0$. As $\deg r < 2$, we have that $r(x) = at + b$ for some $a, b \in \mathbb{Z}$. Then, $a\sqrt{-5} + b = 0$. It follows that $a = b = 0$ as $a, b \in \mathbb{Z}$. Therefore, $f = g(t^2 + 5)$, and so $f \in (t^2 + 5)$. If $\deg f < 2$, then $f(t) = at + b$ for some a, b. We have that $f(\sqrt{-5}) = a\sqrt{-5} + b$ and so $f(t) = 0$ as $a, b \in \mathbb{Z}$. For the reverse inclusion, let $f \in (t^2 + 5)$. Then, $f = g(t^2 + 5)$ for some $g \in \mathbb{Z}[t]$. We have that $\varphi(f) = f(\sqrt{-5}) = g(\sqrt{-5})0 = 0$. Hence, $f \in \ker \varphi$. Thus, $\ker \varphi = (t^2 + 5)$. By the first isomorphism theorem,

$$\frac{\mathbb{Z}[t]}{(t^2 + 5)} \cong \mathbb{Z}[\sqrt{-5}]$$

(ii) Note that $\mathbb{Z}$ is Noetherian as every ideal is principle, hence, finitely generated. By Hilbers basis theorem, $\mathbb{Z}[t]$ is Noetherian. By a previous exercise, we finally have that $\mathbb{Z}[t]/(t^2 + t)$ is Noetherian.

(iii) Define $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{Z}$ by $N(a + ib\sqrt{5}) = a^2 + 5b^2$. Let $z_1 = a_1 + b_1 i\sqrt{5}, z_2 = a_2 + b_2 i\sqrt{5} \in \mathbb{Z}[\sqrt{-5}]$. We have that

$$\begin{aligned}
N(z_1 z_2) &= N((a_1 + b_1 i\sqrt{5})(a_2 + b_2 i\sqrt{5})) \\
&= N((a_1 a_2 - 5b_1 b_2) + (a_1 b_2 + a_2 b_1) i\sqrt{5}) \\
&= a_1^2 a_2^2 - 10 a_1 a_2 b_1 b_2 + 25 b_1^2 b_2^2 + 5 a_1^2 b_2^2 + 10 a_1 a_2 b_1 b_2 + 5 a_2^2 b_1^2 \\
&= a_1^2 a_2^2 + 25 b_1^2 b_2^2 + 5 a_1^2 b_2^2 + 5 a_2^2 b_1^2 \\
&= (a_1^2 + 5b_1^2)(a_2^2 + 5b_2^2) \\
&= N(a_1 + b_1 i\sqrt{5}) N(a_2 + b_2 i\sqrt{5}) \\
&= N(z_1) N(z_2)
\end{aligned}$$

(iv) Suppose there are $u, v \in \mathbb{Z}[\sqrt{-5}]$ such that $uv = 1$. Note that $N(1) = 1$. Then, $1 = N(1) = N(uv) = N(u)N(v) = (a_1^2 + 5b_1^2)(a_2^2 + 5b_2^2)$ where $u = a_1 + ib_1\sqrt{5}, v = a_2 + ib_2\sqrt{5}$. As $N(z) \geq 0$ for all z, we have that $a_1^2 + 5b_1^2 = 1$ and $a_2^2 + 5b_2^2 = 1$. As $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, we must have that $b_1, b_2 = 0$, hence, $a_1, a_2 = \pm 1$. We have that 1 and -1 are units in $\mathbb{Z}[\sqrt{-5}]$.

(v) Suppose that there exists $u, v \in \mathbb{Z}[\sqrt{-5}]$ such that $uv = 2$. We have that $2 = N(2) = N(uv) = N(u)N(v) = (a_1^2 + 5b_1^2)(a_2^2 + 5b_2^2)$ where $u = a_1 + ib_1\sqrt{5}, v = a_2 + ib_2\sqrt{5}$. As $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ and $N(z) \geq 0$ for all z, we have that $a_1^2 + 5b_1^2 = 2$ and $a_2^2 + 5b_2^2 = 1$ without loss of generality. Note there are no solutions in $\mathbb{Z}$ to $a_1^2 + 5b_1^2 = 2$. Hence, no such u, v exist. For a similar reason, we find that no such u, v exist in $\mathbb{Z}[\sqrt{-5}]$ such that $3 = uv$. Suppose there are u, v such that $1 + i\sqrt{5} = uv$. Then, $6 = N(1 + i\sqrt{5}) = N(u)N(v) = (a_1^2 + 5b_1^2)(a_2^2 + 5b_2^2)$. We have that $a_1^2 + 5b_1^2 = 6$ and $a_2^2 + 5b_2^2 = 1$ has the solution $a_1 = b_1 = 1$ and $a_2 = 1, b_2 = 0$, which correspond to $1 + i\sqrt{5} = (1 + i\sqrt{5}) \cdot 1$. We also have that $a_1^2 + 5b_1^2 = 3$ and $a_2^2 + 5b_2^2 = 2$ has no solutions. Therefore, $1 + i\sqrt{5}$ is irreducible. For a similar reason, $1 - i\sqrt{5}$ is irreducible. We conclude that $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ are irreducible.

(vi) Note that $6 \in (2), (3)$ but $6 = (1 - i\sqrt{5})(1 + i\sqrt{5})$, and $1 - i\sqrt{5}, 1 + i\sqrt{5} \notin (2), (3)$. Hence, $(2), (3)$ are not prime. We also note that $6 \in (1 + i\sqrt{5}), (1 - i\sqrt{5})$ but $6 = 2 \cdot 3$ and $2, 3 \notin (1 + i\sqrt{5}), (1 - i\sqrt{5})$. Hence, $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ are not prime in $\mathbb{Z}[\sqrt{-5}]$. This also shows that $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

5.2 - UFDs, PIDs and Euclidean Domains

1. Let R be a UFD, and let $a, b, c \in R$.

(i) Suppose that $(a) \subseteq (b)$. We then have that $a \in (a) \subseteq (b)$, and so $a = xb$ for some $x \in R$. As R is a UFD, $x = p_1p_2...p_n$ and $b = q_1q_2...q_m$ for irreducibles $p_1, ..., p_n$ and $q_1, ..., q_m$. We then have that $a = xb = p_1...p_nq_1...q_m$. By uniqueness, the multiset of irreducible factors of b is contained in the multiset of irreducible factors of a. For the converse, suppose that the the multiset of irreducible factors of b is contained in the multiset of irreducible factors of a. Then, $a = a_1...a_nb_1b_2...b_n$ where $b = b_1...b_n$ by assumption. It follows that $a \in (b)$. Therefore, $(a) \subseteq (b)$.

(ii) Suppose that a and b are associates. Then, $(a) = (b)$. By the previous parts, we must have that the multiset of irreducible factors of b is contained in the multiset of irreducible factors of a and the multiset of irreducible factors of a is contained in the multiset of irreducible factors of b. Therefore, the multiset of irreducible factors of b is the same as the multiset of irreducible factors of a. Similarly, if the multiset of irreducible factors of b is the same as the multiset of irreducible factors of a, then $(a) \subseteq (b)$ and $(b) \subseteq (a)$, hence, $(a) = (b)$.

(iii) As R is a UFD, $bc = p_1...p_n, b = q_1...q_m$ and $c = r_1...r_k$ for some irreducible $p_1, ..., p_n, q_1, ..., q_m$ and $r_1, ..., r_k$. We have that $p_1...p_n$ and $q_1...q_mr_1...r_k$ are factorisations into irreducibles for bc, and so $n = m + k$ and p_i and q_j are associates or p_i and r_j are associates. Therefore, the irreducible factors of bc is the collection of all irreducible factors of b and c.

2. Let R be a UFD and let $a, b, c \in R$ such that $a \mid bc$ and $\gcd(a, b) = 1$. As $a \mid bc$, we have that $(bc) \subseteq (a)$. By Lemma 2.1, the multiset of irreducibles of a is contained in the multiset of irreducibles of bc, which is the collection of all irreducibles of b and c. As $\gcd(a, b) = 1$, the entirety of the irreducible factors of a is contained in the irreducible factors of c. Therefore, $(c) \subseteq (a)$, and so $a \mid c$.

3.

4. Let $x, y \in \mathbb{Z}[x, y]$. Suppose that there exists an f such that $(x, y) \subseteq (f)$. We have that $x \in (f)$ and $y \in (f)$, so $x = fg$ and $y = fh$ for some $g, h \in \mathbb{Z}[x, y]$. As $\mathbb{Z}$ is an integral domain, $\mathbb{Z}[x, y]$ is an integral domain and so $\deg(f) + \deg(g) = 1$ and $\deg(f) + \deg(h) = 1$. Suppose that $\deg(f) = 1$, then $f = ax + by + c$ for some $a, b, c \in \mathbb{Z}$ and we have that $g = d, h = e$ for some $e, d \in \mathbb{Z}$. We have that $x = fg = (ax + by + c)d = adx + bdy + cd$. Then, $ad = 1, bd = 0$ and $cd = 0$. Note that $g \neq 0$, so $c = b = 0$. Furthermore, $y = fh = (ax + by + c)e = aex$. Hence, $ae = 0$. This implies that $a = 0$ as $h \neq 0$. It follows that $f = 0$, which cannot happen. Now suppose that $\deg(f) = 0$. Then, $f = a$ for some a. We have that $x = ag$ and $y = ah$, where $\deg(g) = \deg(h) = 1$. Let $g = bx + cy + d$. Then, $x = abx + acy + ad$, and so $ab = 1, ac = 0$ and $ad = 0$. As $f \neq 0$, we must have that $c = 0, d = 0$. Let $h = ex + iy + j$. Then, $y = ah = aex + aiy + aj$. It follows that $j = e = 0$ and $ai = 1$. So far we have that $g = bx, h = iy$ with $ab = ai = 1$. We must have that $f = \pm 1$, so f is a unit. Therefore, $(f) = R = (1)$. It follows that $\gcd(x, y) = 1$. Now, suppose that there exist $f, g \in \mathbb{Z}[x, y]$ such that $fx + gy = 1$. We have that f, g cannot exist as $fx + gy$ is always of degree greater than 1 if they are not both nonzero.

5. Let R be the subset of $\mathbb{Z}[t]$ consisting of polynomials of the form $f = a_0 + a_2t^2 + ... + a_nt^n$. Let $f = a_0 + a_2t^2 + ... + a_mt^m, g = b_0 + b_2t^2 + ... + b_nt^n$ be elements of R. Without loss of generality, suppose that $\deg f \geq \deg g$. We can write g as $b_0 + b_2t^2 + ... + b_n + b_{n+1}t^{n+1} + ... + b_mt^m$ where $b_i = 0$ for $i > n$. Then, $f-g = (a_0-b_0)+(a_2-b_2)t^2+...+(a_m-b_m)t^m \in R$. Furthermore, $fg = (a_0+a_2t^2+...+a_mt^m)(b_0+b_2t^2+...+b_nt^n) = a_0b_0 + (a_0b_2 + a_2b_0)t^2 + ... + a_mb_nt^{n+m} \in R$. Hence, R is a subring. It follows that R is an integral domain as $\mathbb{Z}[t]$ is an integral domain. Note that the divisors of t^5 in R are $\{\pm1, \pm t^2, \pm t^3, \pm t^5\}$, and the divisors of t^6 in R are $\{\pm1, \pm t^2, \pm t^3, \pm t^4, \pm t^6\}$. The common divisors of t^5 and t^6 in R are then $\{\pm1, \pm t^2, \pm t^3\}$. We have that $t^5 \mid t^5$ and $t^5 \mid t^6$, however, $t^5 \nmid x$ for any common divisor x of t^5 and t^6 in R.

6.

(i) Let R be an integral domain with the property that the intersection of any family of principal ideals in R is necessarily a principal ideal. Let $x, y \in R$. Let F be the set of common divisors of x and y, and let

$$I = \bigcap_{a \in F} (a)$$

By assumption, $I = (d)$ for some $d \in R$. We have that for any $a \in F$, $a \mid x$ and $a \mid y$, hence, $(x), (y) \subseteq (a)$. Thus, $(x), (y) \subseteq \bigcap_{a \in F}(a) = (d)$, and so $d \mid x$ and $d \mid y$. Let $c \in R$ such that $c \mid x$ and $c \mid y$. By definition, $c \in F$. Hence, $(d) = \bigcap_{a \in F}(a) \subseteq (c)$. Hence, $c \mid d$. It follows that greatest common divisors in R and $d = \gcd(x, y)$.

(ii)

7. Let R be a Noetherian domain, and assume for all $a, b \in R$, the greatest common divisor of a and b are a linear combination of a and b. Let I be an ideal of R. As R is Noetherian, $I = (a_1, ..., a_n)$ for $a_1, ..., a_n \in R$. Let $d = \gcd(a_1, a_2)$. By assumption, we have that $d = xa_1 + ya_2$ for some x, y. Let $r \in I$. Then, $r = a_1x_1 + ... + a_nx_n$. We have that $d \mid a_1$ and $d \mid a_2$. Hence, $a_1 = b_1d$ and $a_2 = b_2d$. We have that

$$r = a_1x_1 + a_2x_2 + ... + a_nx_n = b_1dx_1 + b_2dx_2 + ... + a_nx_n = d(b_1x_1 + b_2x_2) + ... + a_nx_n \in (d, a_3, ..., a_n)$$

For the converse, let $r \in (d, a_3, ..., a_n)$. Then,

$$r = x_0d + x_3a_3 + ... + x_na_n = x_0(xa_1 + ya_2) + x_3a_3 + ... + x_na_n = x_0xa_1 + x_0ya_2 + x_3a_3 + ... + x_na_n \in I$$

Therefore, $(a_1, a_2, ..., a_n) = (d, a_3, ..., a_n)$. Doing this process recursively, we have that $I = (d')$ for some d'. We conclude that R is a PID.

8.

9. Let R be a UFD and let P be a prime ideal of height 1. Note that P is not the 0 ideal and we have that $(0) \subset P$. Let $a \in P$ be a nonzero element of P. If $(a) = P$, then we are done. Hence, assume the opposite i.e $(a) \neq P$. As R is a UFD, $a = q_1...q_n$ for irreducibles $q_1, ..., q_n \in R$. As $a \in P$, we have that $q_1...q_n \in P$, hence, $q = q_i \in P$ for some q. Note that q is prime as R is a UFD. We have that (q) is a prime ideal such that $(0) \subset (q) \subseteq P$. Thus, as P is of height 1, we must have that $(q) = P$ as (q) is nonzero.

10. Let R be a Noetherian domain and suppose that every prime ideal of height 1 is principle. Let $a \in R$ be an irreducible element. By Krull's Hauptidealsatz, a is contained in some prime ideal of height 1, P say. By assumption, $P = (x)$ for some $x \in R$. Hence, $a \in (x)$ and so $a = xy$ for some y. As a is irreducible, x is a unit or y is a unit. As $P = (x)$ is prime, x cannot be a unit, thus, y is a unit. Therefore, a and x are associates, and so $(a) = (x)$. We have that a is prime. As R is Noetherian, we have that the a.c.c for principal ideals hold in R. By Theorem 2.5, its necessary that R is a UFD.

11.

12. Let R be a commutative ring and suppose that $R[x]$ is a PID. Suppose that there is an $f \in R[x]$ such that $(x) \subset (f) \subset R$, where the inclusions are proper. We must have that $x \in (f)$ and so that $x = fg$ for some $g \in R[x]$. As $R[x]$ is a PID, $1 = \deg(x) = \deg(fg) = \deg(f) + \deg(g)$. Suppose that $\deg f = 1$. Then, $f = ax + b$ for some $a, b \in R$ and $g = c \in R$. Thus, $x = fg = (ax + b)c = acx + bc$. Hence, $ac = 1$ and $bc = 0$. We have that c is a unit, and so $bc = 0 \implies b = 0$ as $R[x]$ is a PID. We have that $f = ax$ where $ab = 0$ for some $b \in R$. Then, $bf = bax = abx = x \in (x)$. Therefore, $(f) = (x)$, which is a contradiction. Now, suppose that $\deg f = 0$. We have that $f = a \in R$ and $g = bx + c$ where $b, c \in R$. Then, $x = fg = a(bx + c) = abx + ac$, hence, $ab = 1$ and $ac = 0$. Note a is a unit, and $c = 0$. As a is a unit, $(f) = (a) = R$, which is another contradiction. We can conclude f does not exist, and (x) is a maximal ideal. $R \cong R[x]/(x)$ is then a field.

13.

14.

15. Let R be a Euclidean domain. There exists a Euclidean valuation on R, v say. For $a \neq 0$, let $\overline{v}(a) = \min\{v(ab) \mid b \in R\}$. Let $a, b \in R$ such that $b \nmid a$. Then, $a = qb + r$ for some q, r with $r \neq 0$ and $v(b) > v(r)$. Let $r^*, q^* \in R$ such that $a = q^*b + r^*$ with $v(r^*)$ minimal and $v(b) > v(r^*)$. Suppose, for contradiction, $\overline{v}(r^*) \geq \overline{v}(b)$. Then, $\min\{v(r^*x) \mid x \in R\} \geq \min\{v(bx) \mid x \in R\}$. Let $x \in R$ such that $\overline{v}(b) = v(bx)$. Again, as v is a Euclidean valuation and since $a \nmid b$, $a = bxp + k$ for some p, k with $v(bx) > v(k)$. Thus, $v(k) < v(b) \leq \min\{v(by) \mid y \in R\} = \overline{v}(b) = \overline{v}(b) = v(bx)$. We note that $a = b(xp) + k$ with $v(b) > v(k)$. As $v(r^*)$ is minimal, we have that $v(r^*) \leq v(k) < v(bx) = \overline{v}(b)$. Then, $\overline{v}(r^*) \leq v(r^*) < \overline{v}(b)$, which is a contradiction. We must have that $\overline{v}(r^*) < \overline{v}(b)$. It follows that $\overline{v}$ is a Euclidean valuation on R. Furthermore, we note that for nonzero $a, b \in R$,

$$\overline{v}(ab) = \min\{v(abx) \mid x \in R\} \geq \min\{v(ay) \mid y \in R\} = \overline{v}(a)$$

16. Let R be a Euclidean domain with Euclidean valuation v, and assume that $v(ab) \geq v(b)$ for all nonzero $a, b \in R$. Let $x, y \in R$ be nonzero elements of R that are associates. There exists some unit u such that $x = uy$. Then, $v(x) = v(uy) \geq v(y)$ and $v(y) = v(u^{-1}x) \geq v(x)$. Hence, $v(x) = v(y)$. Let w be a unit in R. We have that w is an associate to 1. Hence, $v(w) = v(1)$. Let $x \in R$ be a nonzero element. Then, $v(x) = v(x1) \geq v(1) = v(w)$. Therefore, $v(w)$ is minimal.

17. Let R be a Euclidean domain that is not a field. Let v be its associated Euclidean valuation. As R is not a field, the set $A = \{v(x) \mid x \text{ is not a unit}\}$ is nonempty. Let $c \in R$ such that $v(c) \in A$ is minimal. Let $a \in R$. As R is a Euclidean domain, there exists $r, q \in R$ such that $a = qc + r$ with either $r = 0$ or $v(r) < v(c)$. If $r = 0$, then we are done. Suppose that $r \neq 0$. Then, $v(r) < v(c)$ and so $v(r) \notin A$ by minimality of $v(c)$. Hence, r is a unit. Therefore, for all $a \in R$, there exists $q, r \in R$ such that $a = qc + r$ where either $r = 0$ or r is a unit.

18.

19. Let v be a discrete valuation on a field k.

(i) Let $R = \{a \in k^* \mid v(a) \geq 0\} \cup \{0\}$. Let $x, y \in R$ such that $x \neq y$. We then have that $x - y \in R$. Note that $v(1_k) = 0$ as v is a homomorphism so that $1_k \in R$. Further note that $0 = v(1_k) = v(-1_k \cdot -1_k) = 2v(-1_k)$. Hence, $v(-1_k) = 0$. We have that

$$v(x - y) \geq \min\{v(x), v(-y)\} = \min\{v(x), v(-1_k) + v(y)\} = \min\{v(x), v(y)\} \geq 0$$

as $v(x), v(y) \geq 0$. Thus, $x - y \in R$. Furthermore, $v(xy) = v(x) + v(y) \geq 0$ as $v(x), y(y) \geq 0$. Hence, R is a subring of k.

(ii) Let $a, b \in R$ with $b \neq 0$. Suppose that $v(a) \geq v(b)$. Then, $v(a) - v(b) \geq 0$, and so $v(ab^{-1}) = v(a) - v(b) \geq 0$. Hence, $ab^{-1} \in R$. Then, $a = ab^{-1}b + 0$. Suppose now $v(a) < v(b)$. Note $a = b \cdot 0 + a$. It follows that R is a Euclidean domain.

(iii) Let p be a fixed prime integer. Let $v_p : \mathbb{Q}^* \to \mathbb{Z}$ be a map of abelian groups defined by sending a/b, where $\gcd(a,b) = 1$, to $\max\{k \in \mathbb{Z} : p^k \mid a\}$. Let $k \in \mathbb{Z}$. Then, $v_p(p^k) = k$, hence, v_p is surjective. Let $a_1/b_1, a_2/b_2 \in \mathbb{Q}^*$. We have that $a_1 = p^m z_1$ and $a_2 = p^n z_2$ where $\gcd(z_1, p) = \gcd(z_2, p) = 1$. Then,

$$v_p\left(\frac{a_1}{b_1} \cdot \frac{a_2}{b_2}\right) = v_p\left(\frac{p^n z_1 p^m z_2}{b_1 b_2}\right) = p^n p^m = v_p(p^n) v_p(p^m) = v_p\left(\frac{p^n z_1}{b_1}\right) v_p\left(\frac{p^m z_2}{b_2}\right) = v_p\left(\frac{a_1}{b_1}\right) v_p\left(\frac{a_2}{b_2}\right)$$

Furthermore,

$$v_p\left(\frac{a_1}{b_1} + \frac{a_2}{b_2}\right) = v_p\left(\frac{a_1 b_2 + a_2 b_1}{b_1 b_2}\right) = v_p\left(\frac{p^n z_1 b_2 + p^m z_2 b_1}{b_1 b_2}\right) = \min\{p^n, p^m\} = \min\left\{v_p\left(\frac{p^n z_1}{b_1}\right), v_p\left(\frac{p^m z_2}{b_2}\right)\right\}$$

$$= \min\left\{v_p\left(\frac{a_1}{b_1}\right), v_p\left(\frac{a_2}{b_2}\right)\right\}$$

Therefore, v_p is a discrete valuation. Let $R = \{a/b \in \mathbb{Q}^* \mid v_p(a/b) \geq 0\} \cup \{0\}$ and let R' be the set of rational numbers a/b with b not divisible by p. Let $a/b \in R$. Then, $v(a/b) \geq 0$ and so $p^k \mid a$ for some $k \geq 0$. As $\gcd(a,b) = 1$, b cannot be divisible by p. Thus, $a/b \in R'$. Now let $a/b \in R'$. We have that $a = p^k z$ for some k and where $\gcd(p, z) = 1$ and $k \geq 0$. We then have that $v_p(a/b) = v_p(p^k z/b) = k$ as k is not reduced by b. Hence, $a/b \in R$. It follows that $R = R'$. Therefore, the set of rational numbers a/b with b not divisible by p is a DVR.

20. Let R be a DVR with discrete valuation v. Let $t \in R$ such that $v(t) = 1$, and let I be an ideal of R. Let $n = \min\{v(x) \mid x \in I\}$. Note that $v(t^n) = nv(t) = n$. Let $x \in I$. We have that $v(x) \geq n = v(t^n)$. Then, $v(xt^{-n}) \geq 0$. Hence, $xt^{-n} \in R$. Let $y = xt^{-n}$, then $yt^n = x$. Thus, $x \in (t^n)$, and so $I \subseteq (t^n)$. Now, let $y \in (t^n)$. We have that $y = at^n$ for some $a \in R$. Let $x \in I$ such that $v(x)$ is minimal, that is, $v(x) = n$. Then, $v(y) = v(a) + v(t^n) = v(a) + n \geq n = v(x)$. Hence, $v(yx^{-1}) \geq 0$ and so $yx^{-1} \in R$. Let $yx^{-1} = z \in R$. Then, $y = zx \in I$. Therefore, $I = (t^n)$.

21. Let R be an integral domain. Suppose that R admits a Dedekind-Hasse valuation, and let v be such a valuation. Let I be an ideal of R, and let b be an element of I such that $v(b)$ is minimal. Note that $b \in I$, so $(b) \subseteq I$. Let $a \in I$ such that $(a, b) \neq (b)$. Then, $as = bq + r$ with $v(r) < v(b)$ for some $s, q, r \in R$ such that $as + bq = r$. We have that $r = as + bq \in (a, b) \subseteq I$ as $a, b \in I$. This is a contradiction as $v(r) < v(b)$, but $v(b)$ is assumed to be minimal. Thus, $(a, b) = (b)$, and so $a \in I$. It follows that $I = (b)$, and R is a PID. For the converse, suppose that R is a PID. For nonzero $a \in R$, let $v(a)$ be the size of the multiset of irreducible factor of a. Note this is well-defined as R is a UFD since it is a PID. Let $x, y \in R$. If $y \mid x$, then $(x, y) = (y)$. Suppose that $y \nmid x$. As R is a PID, $(x, y) = (d)$ for some $d \in R$. As R is a UFD, $\gcd(x, y)$ exists, and we have that $\gcd(x, y) = d$. We also have that $d = ax + by$ for some $a, b \in R$. We have that $d \mid y$, which means that $v(d) \leq v(y)$. Suppose that $v(d) = v(y)$, then $d = y$, and so $y = d = \gcd(x, y)$. Hence, $y \mid x$, which cannot happen. Thus, $v(d) < v(y)$. It follows that v is a Dedekind-Hasse valuation.

22. Let $R \subseteq S$ be an inclusion of integral domains, and assume that R is a PID. Let $a, b \in R$ and let $d \in R$ be a gcd for a and b. Consider (a, b) and (d) as ideals of R. As R is a PID, $(a, b) = (c)$ for some $c \in R$. As d is a gcd of a and b, we have that $(a, b) \subseteq (d)$ and (d) is minimal with this property. Note that $(c) = (a, b) \subseteq (d)$, and $(d) \subseteq (c)$ by minimality as $(a, b) \subseteq (c)$. Hence, $(c) = (d)$, and so $(a, b) = (d)$. We have that $d \in (a, b)$, and so $ax + by = d$ for some $x, y \in R$. Now consider (a, b) and (d) as ideals of S. Let $t \in (a, b)$. Then, $t = ap + bq$ for some $p, q \in S$. As $d \mid a$ and $d \mid b$ in R, $a = r_1 d$ and $b = r_2 d$ for some $r_1, r_2 \in R$. Then, $t = ap + bq = r_1 dp + r_2 dq = d(r_1 p + r_2 q) \in (d)$. For the reverse inclusion, let $t \in (d)$. Then, $t = sd$ for some $s \in S$. And so $t = sd = s(ax + by) = sax + sby \in (a, b)$. Hence, $(a, b) = (d)$ as ideals of S. It follows that d is the gcd of a and b in S.

23.

24. Suppose, for contradiction, that the list of prime elements in $\mathbb{Z}$ were finite. Let $P = \{p_1, ..., p_n\}$ be such a list. Consider $x = p_1 p_2 ... p_n + 1$. If x was prime, then $x > p_i$ for all $1 \leq i \leq n$, and so $x \notin P$. However, this is a contradiction as x must be in P as it is prime. Now, suppose x was not prime. We note that $p_i \nmid x$ for all i as it leaves a remainder of 1. We must have that x must contain a prime not in the list. Therefore, P is not complete. We conclude that such a list P cannot exist.

25.

5.3 - Intermezzo: Zorn's Lemma

1. Let $\preceq$ be a well-ordering on a non-empty set Z. Let $a, b \in Z$. Then, $\{a, b\}$ is a subset of Z, and, by assumption, must have a least element. If a is the least element of $\{a, b\}$, then $a \preceq b$, and if b is the least element of $\{a, b\}$, then $b \preceq a$. Hence, $(Z, \preceq)$ is a total order.

2. Let $\preceq$ be a total ordering on a non-empty set Z. Suppose that $\preceq$ is a well-ordering on Z. Let $z_1 \succeq z_2 \succeq ...$ be a decending chain in Z. Consider the set $A = \{z_i | i \in \mathbb{N}\} \subseteq Z$. By assumption, A must have a least element, and such an element must be of the form z_k for some $k \in \mathbb{N}$. We must have that $z_m \succeq z_k$ for all $m \in \mathbb{N}$. Thus, $z_n \succeq z_k$ for all $n > k$. Therefore, $z_k = z_{k+1} = ...$ and so the decending chain must stabilise. For the converse, suppose that $\preceq$ is not a well-ordering on Z. We have that there must exist a subset A of Z such that A does not have a least element. Choose $z_1 \in A$. As A does not have a least element, there exists a $z_2 \in A$ such that $z_1 \succeq z_2$ and $z_1 \neq z_2$. We keep finding z_i in such a way to construct a decreasing chain of elements of A that does not stabilise. Therefore, the converse holds. We have that $\preceq$ is a well-ordering on Z if and only if every decending chain in Z stabilises.

3. Suppose that the Axiom of Choice holds. Let $f : A \to B$ be a surjective function. Consider the set of preimages $A = \{f^{-1}(\{b\}) | b \in B\}$. As f is surjective, we have that $f^{-1}(\{b\})$ is non-empty for all $b \in B$. We note that A is a collection of non-empty disjoint sets. By the Axiom of Choice, for each $f^{-1}(\{b\})$, we can choose some $a' \in f^{-1}(\{b\})$ and we have that $f(a') = b$. Define $f^{-1} : B \to A$ by sending b to such an a'. We have that for each $b \in B$, $(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a') = b$. Thus, f^{-1} is a right inverse of f. Now, let $f : A \to B$ be a set-function with a right inverse, $f^{-1} : B \to A$. For every $b \in B$, we have that $f^{-1}(b) = a \in A$ and $f(a) = b$. Thus, f is surjective. For the converse, suppose that every surjective function has a right inverse, and if a set-function has a right inverse, then it is surjective. Let $\mathfrak{A}$ be a collection of disjoint non-empty sets. Define $f : \bigcup_{A \in \mathfrak{A}} A \to \mathfrak{A}$ by sending $a \in \bigcup_{A \in \mathfrak{A}} A$ to the set A in which $a \in A \in \mathfrak{A}$. f is trivially surjective, thus, f has a right inverse, f^{-1} say. For each $A \in \mathfrak{A}$, we can choose $f^{-1}(A) = a$. Therefore, the Axiom of Choice holds.

4. Let A be a set such that there exists a bijection $a_n : \mathbb{Z}^{>0} \to A$ where $a \mapsto a_i$ with $i \in \mathbb{Z}^{>0}$. Note that if $a \in A$, then $a = a_i$ for some $i \in \mathbb{Z}^{>0}$ as a_n is bijective. Define a relation $\preceq$ on A by $a_i \preceq a_j$ if and only if $i \leq j$. We have that $a_i \preceq a_i$ as $i \leq i$, hence, $\preceq$ is transitive. Suppose that $a_i \preceq a_j$ and $a_j \preceq a_k$. Then, $i \leq j$ and $j \leq k$. As $\leq$ on $\mathbb{Z}^{>0}$ is transtive, $i \leq k$. Hence, $a_i \preceq a_k$ and so $\preceq$ is transitive. Suppose now that $a_i \preceq a_j$ and $a_j \preceq a_i$. Then, $i \leq j$ and $j \leq i$. Hence, $i = j$ and so $a_i = a_j$, which means that $\preceq$ is antisymmetric. Therefore, $\preceq$ is an order relation. Let A' be a subset of A. Consider the set $N = \{i \mid a_i \in A'\} \subseteq \mathbb{Z}^{>0}$. By the well-ordering principle, N has a least element, i' say. For all $a_i \in A'$, we have that $a_{i'} \preceq a_i$ as $i' \leq i$ for all i. Hence, $a_{i'}$ is the least element of A'. Therefore, $\preceq$ is a well-order on A. It follows that $\mathbb{Z}$ and $\mathbb{Q}$ by taking your favourite bijection between $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{Z}^{>0}$.

5.

6.

7.

8. Let G be a nontrivial finitely generated group, and let $\mathfrak{F}$ be the family of proper subgroups of G. Note $\mathfrak{F}$ is not empty as it contains the trivial subgroup. Order $\mathfrak{F}$ via inclusion, and let A be a chain of $\mathfrak{F}$. Let $H = \bigcup_{S \in A} S$. Let $x, y \in H$, then there exists proper subgroups S, S' of G such that $x \in S$ and $y \in S'$. As A is a chain, $S \subseteq S'$ or $S' \subseteq S$. Without loss of generality, assume that $S \subseteq S'$. Then, $x, y \in S'$. Hence, $x - y \in S' \subseteq H$, and so H is a subgroup of G. Assume that $H = G$. As G is finitely generated, $G = \langle a_1, ..., a_n \rangle$ for some $a_1, ..., a_n \in G$. For each $a_i \in \{a_1, ..., a_n\}$, there is a proper subgroup $S_i \in A$ such that $a_i \in S_i$. As A is a chain, for each i, j, $S_i \subseteq S_j$ or $S_j \subseteq S_i$. Let S' be the maximal element among these S_i's. Then, $a_i \in S'$ for all i, and so $S' = G$, which contradicts the assumption that S' is a proper subgroup of G. Therefore, H is a proper subgroup of G. Note H is an upper bound for A and by Zorn's Lemma, there exists a maximal element in $\mathfrak{F}$. Let H be a proper subgroup of $(\mathbb{Q}, +)$. Suppose that H is maximal. Let $x \in \mathbb{Q} - H$. We must have that $\langle H, x \rangle = \mathbb{Q}$ by maximality of H. Let $y \in H$. There exists integers a, b with $a, b \neq 0$ such that $y/x = a/b$. As $\langle H, x \rangle = \mathbb{Q}$, we have that $x/a = h + nx$ for some

$h \in H$ and $n \in \mathbb{Z}$. Then, $x = ah + anx = ah + nby \in H$ as $h \in H, y \in H$ and $a, n, b \in \mathbb{Z}$, which is a contradiction. Therefore, such a H cannot exist. It follows that $(\mathbb{Q}, +)$ does not have maximal subgroups.

9. Let R be the rng consisting of the abelian group $(\mathbb{Q}, +)$ and multiplication defined by $qr = 0$ for all $q, r \in \mathbb{Q}$. Trivially, if I is an ideal of R, then $(I, +)$ is a subgroup of $(\mathbb{Q}, +)$. Let A be a subgroup of $\mathbb{Q}$. Let $x \in A$ and let $r \in R$. Then, $rx = 0 \in A$. Therefore, A is an ideal of R. Hence, the ideals of R are precicely the subgroups of $(\mathbb{Q}, +)$. As $(\mathbb{Q}, +)$ does not have any maximal subgroups, R does not have any maximal ideals.

10.

11.

12. We first prove the following: "Let $(Z, \preceq)$ be a nonempty poset. Assume every chain in Z has a lower bound; then there exists minimal elements, that is, there exists elements $u \in Z$ such that $a \preceq u \implies u = a$". Let Z be a nonempty poset ordered by the relation $\preceq$, and assume that every chain in Z has a lower bound. Define a relation on Z, $\preceq'$, by setting $a \preceq' b$ if and only if $b \preceq a$. For all $a \in Z$, we have that $a \preceq a$ as $\preceq$ is an order relation. Thus, $a \preceq' a$ for all $a \in Z$. Suppose that $a \preceq' b$ and $b \preceq' c$. Then, $b \preceq a$ and $c \preceq a$. As $\preceq$ is transitive, $c \preceq a$, and so $a \preceq' c$. Finally, suppose that $a \preceq' b$ and $b \preceq' a$. Then, $b \preceq a$ and $a \preceq b$. Hence, $a = b$. Let A be a chain in $(Z, \preceq')$. For each $a, b \in A$, we have that $a \preceq' b$ or $b \preceq' a$, which means $b \preceq a$ or $a \preceq b$. Thus, A is a chain in $(Z, \preceq)$. By assumption, A has a lower bound with respect to $\preceq$, u say. For all $a \in A$, $u \preceq a$, and so $a \preceq' u$ for all $a \in A$. Hence, u is an upper bound of A with respect to $\preceq'$. By Zorn's Lemma, there exists maximal elements in $(Z, \preceq')$. Let m be such a maximal element in $(Z, \preceq')$. We have that if $a \in Z$ and $m \preceq' a$, then $m = a$. Hence, if $a \in Z$ and $a \preceq m$, we have that $m \preceq a$, and so $m = a$. Therefore, m is a minimal element of $(Z, \preceq)$. Let R be a commutative ring and let $K \subseteq R$ be a proper ideal. Let $\mathfrak{F}$ be the family of prime ideals containing K. Order $\mathfrak{F}$ via inclusion and let A be a chain in $\mathfrak{F}$. Let $J = \bigcap_{I \in A} I$. We note that J is an ideal as an intersection of a family of ideals. Let $x, y \in R$ such that $x, y \notin J$. Then, there exists prime ideals I, I' such that $x \notin I$ and $y \notin I'$. As A is a chain, assume that $I \subseteq I'$ without loss of generality. Then, $x, y \notin I$, and so $xy \notin I$ by the primality of I. Therefore, $xy \notin J$. It follows that J is prime and is a lower bound of A. Therefore, $\mathfrak{F}$ must have minimal elements.

13. Let R be a commutative ring, and let N be its nilradical. Let $r \notin N$. Let $\mathfrak{F}$ be the family of ideals of R do not contain any power of r^k of r for $k > 0$. We order $\mathfrak{F}$ via inclusion. Let A be a chain of ideals of $\mathfrak{F}$ and let $J = \bigcup_{I \in A} I$. Let $x, y \in J$, then there exists $I, I' \in A$ such that $x \in I$ and $y \in I'$. As A is a chain, $I \subseteq I'$ or $I' \subseteq I$. Without loss of generality, assume $I \subseteq I'$. Then, $x, y \in I$. As I' is an ideal, $x - y \in I \subseteq J$. Now, let $x \in J$ and $r \in R$. As $x \in J$, $x \in I$ for some ideal $I \in A$. Thus, $rx \in I \subseteq J$. It follows that J is an ideal. Furthermore, J does not contain any power r^k of r for $k > 0$ as no ideal $I \in A$ does. Note further that J is an upper bound of A. By Zorn's Lemma, there exists maximal elements in $\mathfrak{F}$. Let M be a maximal element of $\mathfrak{F}$. Suppose that there exists $x, y \notin M$ however $xy \in M$. Let $\langle M, x \rangle$ be the ideal generated by M and x. We have that $\langle M, x \rangle$ properly contains M, and by maximality of M, $\langle M, x \rangle$ must not be in $\mathfrak{F}$ and so contains a power of r. Hence, $r^n \in (x)$ for some n. Similarly, $r^m \in (y)$ for some m. Thus, $r^n = kx$ and $r^m = k'y$ for some $k, k' \in R$. We have that $xy \in M$ implies $kk'xy \in M$, thus, $r^{n+m} \in M$, which is a clear contradiction. Thus, M must be prime. We conclude that if $r \notin N$, then there exists a prime ideal of R, $\mathfrak{p}$, such that $\mathfrak{p}$ does not contain r. Therefore, r is not contained in the intersection of all prime ideals.

14. Let R be a commutative ring and let $J(R)$ be its Jacobson radical i.e the intersection of all maximal ideals of R. Suppose that $r \in J(R)$ and suppose that there is an $s \in R$ such that $1 + rs$ is not a unit. By Proposition 3.5, there is a maximal ideal $\mathfrak{m}$ of R such that $\mathfrak{m} \supseteq (1 + rs) \ni 1 + rs$. However, as $r \in J(R)$, r must be contained in every maximal ideal of R, thus, $r \in \mathfrak{m}$. And so we must have that $rs \in \mathfrak{m}$. As $1 + rs, rs \in \mathfrak{m}$, $1 \in \mathfrak{m}$, which contradicts the maximality of $\mathfrak{m}$. Therefore, $1 + rs$ must be a unit for all s. For the converse, let $r \in R$ and suppose that $1 + rs$ is a unit for all $s \in R$. Assume that $r \notin \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$. As $\mathfrak{m}$ is maximal, $\langle \mathfrak{m}, r \rangle = R$, and so there exists an element $m \in \mathfrak{m}$ and $x \in R$ such that $m + xr = 1$. Hence, $1 - xr \in \mathfrak{m}$. As $1 + rs$ is a unit for all s, $\mathfrak{m} = R$, which is contradiction. We must have that $r \in \mathfrak{m}$ for all maximal ideals $\mathfrak{m}$ of R.

15.

5.4 - Unique Factorisation In Polynomial Rings

1. Let R be a ring, and let I be an ideal of R. Define a map $f : R[x] \to (R/I)[x]$ by sending $a_0 + a_1x + ... + a_nx^n$ to $(a_0 + I) + (a_1 + I)x + ... + (a_n + I)x^n$. This map is clearly surjective. Furthermore, $\ker f = RI[x]$. Hence, $R[x]/IR[x] \cong (R/I)[x]$.

2. Let R be the ring of integers, and let $I = (2)$. We have that $R/I \cong \mathbb{F}_2$ is a field, hence, I is maximal. However, $R[x]/IR[x] \cong \mathbb{F}_2[x]$ is not a field as x is not invertible, hence, $IR[x]$ is not maximal.

3. Let R be a PID and let $f \in R[x]$. If f is very primitive, then it is clearly primite. Suppose that f is primitive. Let $\mathfrak{p}$ be a prime ideal of R. As R is a PID, then $\mathfrak{p}$ is a principle prime idel of R. As f is primitive, $f \notin \mathfrak{p}R[x]$. Therefore, f is very primitive. Consider the UFD $R = \mathbb{Z}[x]$. Let $f \in \mathbb{Z}[x, y]$ be the polynomial $f = 2 + xy$. Note f is not very primitive as $(2, x) \neq (1)$, however, f is primitive as $\gcd(2, x) = 1$.

4. Let R be a commutative ring and let $f, g \in R[x]$. Suppose that fg is very primitive. Then, for all prime ideals $\mathfrak{p}$ of R, $fg \notin \mathfrak{p}R[x]$. As $\mathfrak{p}R[x]$ is an ideal, $f, g \notin \mathfrak{p}R[x]$. Hence, f, g are very primitive. For the converse, suppose that both f and g are very primitive. For all prime ideals $\mathfrak{p}$ of R, we have that $f \notin \mathfrak{p}R[x]$ and $g \notin \mathfrak{p}R[x]$. By Corollary 4.2, $\mathfrak{p}R[x]$ is prime, hence, $fg \notin \mathfrak{p}R[x]$. Thus, fg is very primitive.

5.

6.

(i)

(ii)

7. Let S be a multiplicatively closed subset of a commutative ring R. Define a relation $\sim$ on the set of pairs $(a, s) \in R \times S$ by setting $(a, s) \sim (a', s')$ if and only if there exists a $t \in S$ such that $t(s'a - sa') = 0$.

(i) We verify $\sim$ is an equivalence relation. We have that $(a, s) \sim (a, s)$ for all $(a, s) \in R \times S$ as $1(as - as) = 0$ and $1 \in S$. Suppose that $(a, s) \sim (a', s')$ for some $(a, s), (a', s') \in R \times S$. Then, there exists a $t \in S$ such that $t(as' - a's) = 0$. By multiplication of $-1 \in R$ on both sides, we obtain $t(sa' - s'a) = 0$. Hence, $(a', s') \sim (a, s)$. Finally, suppose that $(a, s) \sim (a', s')$ and $(a', s') \sim (a'', s'')$. There exists $t, t' \in S$ such that $t(s'a - sa') = 0$ and $t'(s''a' - s'a'') = 0$. Thus, $ts'a = tsa'$ and $t's''a' = t's'a''$. So $tt's's''a = tt's''a' = tst's'a''$, and $tt's'(s''a - sa'') = 0$. Note $tt's' \in S$ as $t, t', s' \in S$. Hence, $(a, s) \sim (a'', s'')$. Therefore, $\sim$ is an equivalence relation.

(ii) Denote the equivalence class of (a, s) by a/s, and let $S^{-1}R$ denote the set of equivalence classes. Define the operation $+, \cdot$ on the set of equivalence classes under $\sim$ as below

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'}, \quad \frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'}$$

Let $a/s, a'/s', b/t, b'/t' \in S^{-1}R$ such that $a/s = b/t$ and $a'/s' = b'/t'$. We note that there exists $u, u' \in S$ such that $u(at - bs) = 0$ and $u'(a't' - b's') = 0$. Then,

$$\begin{aligned} uu'(tt'(as' + a's) - ss'(bt' + b't)) &= uu'(tt'as' + tt'a's - ss'bt' - ss'b't) \\ &= uu'(s't'(at - bs) + st(a't' - b's')) \\ &= u's't'u(at - bs) + ustu'(a't' - b's') \\ &= 0 \end{aligned}$$

Therefore,

$$\frac{a}{s} + \frac{a'}{s'} = \frac{as' + a's}{ss'} = \frac{bt' + b't}{tt'} = \frac{b}{t} + \frac{b'}{t'}$$

Furthermore,

$$\begin{aligned}
uu'(aa'tt' - bb'ss') &= uu'(aa'tt' - a't'bs + a't'bs - bb'ss') \\
&= uu'(a't'(at - bs) + bs(a't' - b's')) \\
&= u'a't'u(at - bs) + ubsu'(a't' - b's') \\
&= 0
\end{aligned}$$

Therefore,

$$\frac{a}{s} \cdot \frac{a'}{s'} = \frac{aa'}{ss'} = \frac{bb'}{tt'} = \frac{b}{t} \cdot \frac{b'}{t'}$$

We have that $+, \cdot$ are well-defined operations.

(iii) We now prove $S^{-1}R$ forms a ring under the above operations. We have that $0/1 \in S^{-1}R$ and that for all $a/s \in S^{-1}R$, $a/s + 0/1 = (a1 + 0s)/s1 = a/s$. Hence, $0/1$ is an identity element under $+$. Furthermore, for each $a/s \in S^{-1}R$, $(-a)/s \in S^{-1}R$ and $a/s + (-a)/s = (as + (-a)s)/s^2 = 0/s^2$. We have that $0/s^2 = 0/1$ as for any $t \in S$, $t(0 \cdot 1 - 0 \cdot s^2) = t0 = t$. Hence, $(-a)/s$ is the inverse element for any $a/s \in S^{-1}R$. We also have that for any triplet $a/s, a'/s', a''/s'' \in S^{-1}R$,

$$\begin{aligned}
\left(\frac{a}{s} + \frac{a'}{s'}\right) + \frac{a''}{s''} &= \frac{as' + a's}{ss'} + \frac{a''}{s''} \\
&= \frac{s''(as' + a's) + a''ss'}{ss's''} \\
&= \frac{as's'' + a'ss'' + a''ss'}{ss's''} \\
&= \frac{as's'' + s(a's'' + a''s')}{ss's''} \\
&= \frac{a}{s} + \frac{a's'' + a''s'}{s's''} \\
&= \frac{a}{s} + \left(\frac{a'}{s'} + \frac{a''}{s''}\right)
\end{aligned}$$

Therefore, $+$ is associative. Finally, we note that $a/s + a'/s' = (as' + a's)/ss' = (a's + as')/s's = a'/s' + a/s$. Therefore, $S^{-1}R$ forms an abelian group under $+$. Now, we note that $1/1 \in S^{-1}R$, and we have that for any $a/s \in S^{-1}R$, $a/s \cdot 1/1 = (a1)/(s1) = a/s$. Therefore, $S^{-1}R$ has an identity element. Next, we note that for any triplet $a/s, a'/s', a''/s'' \in S^{-1}R$

$$\begin{aligned}
\left(\frac{a}{s} \cdot \frac{a'}{s'}\right) \cdot \frac{a''}{s''} &= \frac{aa'}{ss'} \cdot \frac{a''}{s''} \\
&= \frac{aa'a''}{ss's''} \\
&= \frac{a}{s} \cdot \frac{a'a''}{s's''} \\
&= \frac{a}{s} \cdot \left(\frac{a'}{s'} \cdot \frac{a''}{s''}\right)
\end{aligned}$$

Therefore, $\cdot$ is associative. Note also $a/s \cdot a'/s' = aa'/ss' = a'a/s's = a'/s' \cdot a/s$. Finally,

$$\begin{aligned}
\frac{a}{s} \cdot \frac{a'}{s'} + \frac{a}{s} \cdot \frac{a''}{s''} &= \frac{aa'}{ss'} + \frac{aa''}{ss''} \\
&= \frac{aa'ss'' + aa''ss'}{s^2 s' s''} \\
&= \frac{s}{s} \cdot \frac{aa's'' + aa''s'}{ss's''} \\
&= \frac{1}{1} \cdot \frac{aa's'' + aa''s'}{ss's''} \\
&= \frac{aa's'' + aa''s'}{ss's''} \\
&= \frac{a}{s} \cdot \frac{a's'' + a''s'}{s's''} \\
&= \frac{a}{s} \cdot \left(\frac{a'}{s'} + \frac{a''}{s''}\right)
\end{aligned}$$

And so $S^{-1}R$ is a commutative ring. Define the map $\ell : R \to S^{-1}R$ by sending a to $a/1 \in S^{-1}R$. We have that $\ell(1) = 1/1$ which is the multiplicative identity in $S^{-1}R$. Furthermore,

$$\ell(a+b) = \frac{a+b}{1} = \frac{a1 + b1}{1 \cdot 1} = \frac{a}{1} + \frac{b}{1} = \ell(a) + \ell(b)$$

$$\ell(ab) = \frac{ab}{1} = \frac{a \cdot b}{1 \cdot 1} = \frac{a}{1} \cdot \frac{b}{1} = \ell(a)\ell(b)$$

for any $a, b \in R$. Hence, ℓ is a ring homomorphism.

(iv) Let $s \in S$. We have that

$$\ell(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s1}{1s} = \frac{s}{s} = \frac{1}{1}$$

Hence, $\ell(s)$ is invertible.

(v) Let R' be a commutative ring and $f : R \to R'$ a ring homomorphism such that $f(s)$ is invertible for every $s \in S$. Suppose there exists a ring homomorphism α such that the following diagram commutes

$$\begin{tikzcd}
S^{-1}R \arrow[rr, "\alpha"] & & R' \\
& R \arrow[ul, "\ell"] \arrow[ur, "f"'] &
\end{tikzcd}$$

We have that $f = \alpha \circ \ell$. For each $r \in R$, we have that $f(r) = (\alpha \circ \ell)(r) = \alpha(r/1)$. Hence, for any $a/s \in S^{-1}R$,

$$\alpha\left(\frac{r}{s}\right) = \alpha\left(\frac{r}{1}\frac{1}{s}\right) = \alpha\left(\frac{r}{1}\right)\alpha\left(\frac{1}{s}\right) = f(r)\alpha\left(\frac{s}{1}\right)^{-1} = f(r)f(s)^{-1}$$

which gives uniqueness of α. We verify α is a ring homomorphism. Let $r/s, r'/s' \in S^{-1}R$.

$$\begin{aligned}
\alpha\left(\frac{r}{s} + \frac{r'}{s'}\right) &= \alpha\left(\frac{rs' + r's}{ss'}\right) = f(rs' + r's)f(ss')^{-1} \\
&= (f(r)f(s') + f(r')f(s))f(s)^{-1}f(s')^{-1} \\
&= f(r)f(s)^{-1} + f(r')f(s')^{-1} \\
&= \alpha\left(\frac{r}{s}\right) + \alpha\left(\frac{r'}{s'}\right)
\end{aligned}$$

$$\begin{aligned}
\alpha\left(\frac{r}{s}\cdot\frac{r'}{s'}\right) &= \alpha\left(\frac{rr'}{ss'}\right) = f(rr')f(ss')^{-1}\\
&= f(r)f(r')f(s)^{-1}f(s')^{-1}\\
&= f(r)f(s)^{-1}f(r')f(s')^{-1}\\
&= \alpha\left(\frac{r}{s}\right)\cdot\alpha\left(\frac{r'}{s'}\right)
\end{aligned}$$

Finally, $\alpha(1/1) = f(1)f(1)^{-1} = 1$. Therefore, α is a ring homomorphism. It follows that ℓ is initial among ring homomorphisms $f : R \to R'$ such that $f(s)$ is invertible for every $s \in S$.

(vi) Suppose that R is an integral domain and suppose S is a multiplicative subset of R such that $0 \notin S$. Suppose there exists $a/s, a'/s' \in S^{-1}R$ such that $(a/s)\cdot(a'/s') = 0/1$. Then, $aa'/ss' = 0/1$ and so there exists a $t \in S$ such that $t(aa'1 - 0ss') = 0$. Hence, $taa' = 0$. As R is an integral domain either $t = 0$ or $aa' = 0$. As $t \in S$ and $0 \notin S$, $t \neq 0$, so that $aa' = 0$. As R is an integral domain either $a = 0$ or $a' = 0$. Then, either $a/s = 0/1$ or $a'/s' = 0/1$. Therefore, $S^{-1}R$ is an integral domain.

(vii) Let R be a commutative ring and let S be a multiplicative subset of R. Suppose that $0 \in S$. Then, $a/s = a'/s'$ for all $a, a' \in R$ and $s, s' \in S$ as $0(as' - a's) = 0$. Hence, $S^{-1}R$ is the zero ring. For the converse, suppose that $S^{-1}R$ is the zero ring. Then, $1/1 = 0/1$ and so there exists a $t \in S$ such that $t(1\cdot 1 - 0\cdot 1) = 0$. Then, $t = 0$. And so $0 \in S$.

8.

9. Let R be a commutative ring, and S a multiplicative subset of R

(i) Suppose that I is an ideal of R such that $I \cap S = \emptyset$. Let $I^e = S^{-1}I$. Let $x/s, y/s' \in I^e$. We have tht $xs', ys \in I$ as $x, y \in I$ and I is an ideal. Thus, $xs' - ys \in I$. Hence, $(x/s) - (y/s') = (xs' - ys)/ss' \in I^e$. Furthermore, let $r/s \in S^{-1}R$ and $i/s' \in I^e$. Then, $(r/s)(i/s') = ri/ss' \in I^e$ as $ri \in I$. Suppose that $I^e = S^{-1}R$. Then, $1/1 \in I^e$, and so $1 \in I$. However, $1 \in S$, but we had assumed $I \cap S =$. Therefore, I^e must be a proper ideal of $S^{-1}R$.

(ii) Let $\ell : R \to S^{-1}R$ be the natural homomorphism, and let J be a proper ideal of $S^{-1}R$. Further, let $J^c = \ell^{-1}(J)$. As the preimage of an ideal is an ideal, J^c is an ideal. Suppose that there exists an element $x \in J^c \cap S$. Then, $x \in J^c$ and $x \in S$. As $x \in J^c$, we have that $\ell(x) \in J$. As $x \in S$, $\ell(x)$ is a unit in $S^{-1}R$. Therefore, $J = R$. However, this is a contradiction as J is a proper ideal. Hence, $J^c \cap S = \emptyset$.

(iii) Let J be a proper ideal of $S^{-1}R$. Let $x/s \in (J^c)^e$. Then, $x \in \ell^{-1}(J)$ and so $\ell(x) = x/1 \in J$. As J is an ideal, $x/s = (1/s)(x/1) \in J$. For the reverse inclusion, let $x/s \in J$. Then, as J is an ideal, $x/1 = (s/1)(x/s) \in J$, and so $x \in \ell^{-1}(J) = J^c$. Hence, $x/s \in (J^c)^e$. Now, let $x \in (I^e)^c$. Then, $x/1 = \ell(x) = S^{-1}I$. Hence, $x \in I$ and so $x \in \{a \in R \mid (\exists s \in S)\ sa \in I\}$ as $1x = x$. For the reverse inclusion, let $x \in \{a \in R \mid (\exists s \in S)\ sa \in I\}$. There is a $s \in S$ such that $sx \in I$. Hence, $\ell(x) = x/1 = sx/s \in S^{-1}I$. Thus, $x \in (I^e)^c$.

(iv) Let $S = \{1, x, x^2, ...\}$ in $R = \mathbb{C}[x, y]$ and let $I = (xy)$. We have that $y \in (I^e)^c$ as $xy \in (xy)$, however, $y \notin (xy)$. Therefore, it does not necessarily hold that $(I^e)^c = I$.

10. Let R be a commutative ring and S a multiplicative subset of R. We set to prove that the assignment $\mathfrak{p} \mapsto S^{-1}$ is an inclusion-preserving bijection between the set of prime ideals of R disjoint from S and the set of prime ideals of $S^{-1}R$. Let $\mathfrak{p}, \mathfrak{p}'$ be prime ideals of R such that $\mathfrak{p} \subseteq \mathfrak{p}'$. Let $x/s \in S^{-1}\mathfrak{p}$. Then, $x \in \mathfrak{p} \subseteq \mathfrak{p}'$. Hence, $x/s \in S^{-1}\mathfrak{p}'$. Let $\mathfrak{p}$ be a prime ideal of R disjoint from S. We have that $(\mathfrak{p}^e)^c = \{a \in R \mid (\exists s \in S)\ sa \in \mathfrak{p}\} \supseteq \mathfrak{p}$. Let $x \in (\mathfrak{p}^e)^c$. Then, there exists some $s \in S$ such that $sx \in \mathfrak{p}$. Either $s \in \mathfrak{p}$ or $x \in \mathfrak{p}$. If $s \in \mathfrak{p}$, then $x \in \mathfrak{p} \cap S$, which cannot occur. Hence, $x \in \mathfrak{p}$. It follows that $\mathfrak{p} = (\mathfrak{p}^e)^c$. Therefore, the assignment has a left inverse, so that the assignment is injective. Let J be a prime ideal of $S^{-1}R$. Let $x, y \in R$ such that $xy \in J^c$. Then, $\ell(xy) = xy/1 = (x/1)(y/1)$ is contained in J. Hence, either $x/1 \in J$ or $y/1 \in J$. Therefore, either $x \in J^c$ or $y \in J^c$. It follows that J^c is a prime ideal in R. Also note that $(J^c)^e = J$. Hence, the assignment has a right inverse. It follows that the assignment is surjective. We conclude that the assignment is a inclusion-preserving bijection.

11. Let R be a commutative ring and let $\mathfrak{p}$ be a prime ideal of R. Let $S = R - \mathfrak{p}$. As $\mathfrak{p}$ is a prime ideal, $1 \notin \mathfrak{p}$, so that $1 \in S$. Let $x, y \in S$. Then, $x, y \notin \mathfrak{p}$, and so $xy \notin \mathfrak{p}$, otherwise $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ by the primality of $\mathfrak{p}$. Therefore, $xy \in S$. It follows that S is a multiplicative subset of R. By the previous exercise, there is a inclusion-preserving bijection between the set of prime ideals disjoint from S and the set of prime ideals of $R_\mathfrak{p}$. A prime ideal disjoint from S is the same as a prime ideal contained in $\mathfrak{p}$ as $S = R - \mathfrak{p}$. Therefore, there exists an inclusion-preserving bijection from the set of prime ideals contained in $\mathfrak{p}$ and the set of prime ideals of $R_\mathfrak{p}$. We claim the prime ideal of $R_\mathfrak{p}$ associated with $\mathfrak{p}$ in R, $\mathfrak{m}$, is maximal. Suppose there exists an ideal I such that $\mathfrak{m} \subseteq I$. Then, there exists an ideal J in R that is associated with I and $\mathfrak{p} \subseteq J$, as the association is inclusion preserving. However, J is contained in $\mathfrak{p}$, hence, $J = \mathfrak{p}$ and so $\mathfrak{m} = I$. It follows that $\mathfrak{m}$ is a maximal ideal. Let $\mathfrak{m}'$ in $R_\mathfrak{p}$ be a maximal ideal. $\mathfrak{m}'$ is associated with some prime ideal $\mathfrak{p}'$ of R that is contained in $\mathfrak{p}$. We have that $\mathfrak{p}' \subseteq \mathfrak{p}$, hence, $\mathfrak{m}' \subseteq \mathfrak{m}$. Thus, $\mathfrak{m} = \mathfrak{m}'$, which makes $\mathfrak{m}$ unique. We conclude that $R_\mathfrak{p}$ is a local ring.

12. Let R be a commutative ring, and let M be an R-module. Suppose that $M = 0$. Then, M has no prime ideals, and it holds that $M_\mathfrak{p} = 0$ vacuously for all prime ideals $\mathfrak{p}$ of R. Now, suppose that for all prime ideals $\mathfrak{p}$ of R, $M_\mathfrak{p} = 0$. Let $\mathfrak{m}$ be a maximal ideal of R. Then, $\mathfrak{m}$ is a prime ideal, and so by assumption, $M_\mathfrak{m} = 0$. Now, suppose that for all maximal ideals $\mathfrak{m}$ of R, $M_\mathfrak{m} = 0$. Suppose, for contradiction, $M \neq 0$. There exists $x \in M$ such that $x \neq 0$. We have that the set $\{r \in R \mid rx = 0\}$ is a proper ideal of R, and by Proposition 3.5, it is contained in some maximal ideal $\mathfrak{m}$. By assumption, $M_\mathfrak{m} = 0$. Hence, $x/1 = 0/1$ in $M_\mathfrak{m}$. There then exists a $t \in R - \mathfrak{m}$ such that $tx = 0$. However, as $\mathfrak{m}$ contains I, t cannot be an element of $R - \mathfrak{m}$ as $t \in I$. Therefore, $M = 0$.

13.

14. Let M be an R-module, S a multiplicative subset of M, and $\hat{N}$ a submodule of $S^{-1}M$. Let $x/s \in (\hat{N}^c)^e$. Then, $x \in \ell^{-1}(\hat{N})$ and so $x/1 \in \hat{N}$. Therefore, $x/s = (x/1)(1/s) \in \hat{N}$. For the converse, let $x/s \in \hat{N}$. We have that $x/1 = xs/s = s(x/s) \in \hat{N}$. Hence, $\ell(x) \in \hat{N}$. Thus, $x \in \hat{N}^c$. Therefore, $x/s \in (\hat{N}^c)^e$. Suppose that M is a Noetherian R-module, and let $\hat{N}$ be a submodule of $S^{-1}M$. We have that $\hat{N}^c$ is a submodule of M, hence, it is finitely generated, that is, $\hat{N}^c = \langle x_1, ..., x_n \rangle$ for some $x_1, ..., x_n \in M$. We have that $x/s \in (\hat{N}^c)^e$. Then, $x \in \hat{N}^c$ and so $x = r_1x_1 + ... + r_nx_n$ for some $r_1, ..., r_n \in R$. Thus,

$$\frac{x}{s} = \frac{r_1x_1 + ... + r_nx_n}{s} = \frac{r_1x_1}{s} + ... + \frac{r_nx_n}{s} = r_1\frac{x_1}{s} + ... + r_n\frac{x_n}{s} \in \langle x_1/s, ..., x_n/s \rangle$$

Therefore, $\hat{N} = (\hat{N}^c)^e = \langle x_1/s, ..., x_n/s \rangle$ and so $S^{-1}M$ is Noetherian.

15.

16. HALF DONE Let R be a Noetherian domain, and let $s \in R$ be a prime element. Let $S = \{s^n | n \geq 0\}$. Suppose that R is a UFD. We have that $S^{-1}R$ is a Noetherian domain by a previous exercise. Let $\hat{\mathfrak{p}}$ be a prime ideal of $S^{-1}R$ that is of height 1. $\hat{\mathfrak{p}}^c$ is a prime ideal of R of height 1 as contraction is a inclusion preserving bijection between the set of prime ideals of R disjoint from S, and the set of prime ideals of $S^{-1}R$. As R is a Noetherian domain that is a UFD, $\hat{\mathfrak{p}}^c$ is principal, that is, $\hat{\mathfrak{p}}^c = (p)$ for some $p \in R$. Let $x \in S^{-1}(p)$. Then, $x = (rp)/s^n$ for some $r \in R, n \geq 0$. We have that $x = (rp)/s^n = (r/s^n)(p/s) \in (p/s)$. Let $x \in (p/s)$. Then, $x = (r/s^n)(p/s) = rp/s^{n+1} \in S^{-1}(p)$ where $r/s^n \in S^{-1}R$. Therefore, $\hat{\mathfrak{p}} = (\hat{\mathfrak{p}}^c)^e$ is principal. Therefore, $S^{-1}R$ is a UFD.

17. Let F be a field and suppose that F has characteristic 0. The the map $\varphi : \mathbb{Z} \to F$ is injective and has kernel $\ker \varphi = \{0\}$. By the First Isomorphism Theorem F contains an isomorphic copy of $\mathbb{Z}$, Z say. We must have that $\mathbb{Q} = K(\mathbb{Z}) \cong K(Z)$, and by definition $K(\mathbb{Z}) = \mathbb{Q}$ is the smallest field containing $\mathbb{Z}$. As F is a field, it must contain an isomorphic copy to $\mathbb{Q}$. For the converse, suppose that F contains an isomorphic copy of $\mathbb{Q}$, Q say. We have that the inclusion map $i :\hookrightarrow F$ is a ring homomorphism. Let $f : \mathbb{Z} \to Q$ be the unique ring homomorphism from $\mathbb{Z}$ to Q. As $\mathbb{Q}$ has characteristic 0, f has the trivial kernel. Furthermore, i has the trivial kernel as a homomorphism of fields. Therefore, $f \circ i : \mathbb{Z} \to F$ has trivial kernel. It follows that F has characteristic 0 as $\mathbb{Z}$ is initial in Ring. Now, suppose that F has characteristic p prime. The unique map $\varphi : \mathbb{Z} \to F$ has kernel $p\mathbb{Z}$, and so $\mathbb{Z}/p\mathbb{Z}$ embeds into F. For the converse, suppose that F contains an isomorphic copy of $\mathbb{Z}/p\mathbb{Z}$. We have that the inclusion map $i : \mathbb{Z}/p\mathbb{Z} \to F$ is a ring homomorphism. Let $f : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ be the canonical homomorphism. We have that f has kernel $p\mathbb{Z}$ and i has the trivial kernel as a homomorphism of fields. It follows that $i \circ f : \mathbb{Z} \to F$ has kernel $p\mathbb{Z}$, and so F has characteristic p.

18. Let R be an integral domain. Let $u \in R$ be a unit. There is a $v \in R$ such that $uv = 1 \in R$. View u, v as constant polynomials in $R[x]$, then $uv = 1 \in R[x]$. Hence, the units of R are units of $R[x]$ when viewed as constant polynomials. Let $f \in R[x]$ be a unit and let $g \in R[x]$ such that $fg = 1$. As R is an integral domain, $R[x]$ is an integral domain. Therefore, $0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g)$. It follows that $\deg(f) = \deg(g) = 0$, and so f, g are constant polynomials and can be viewed as elements of R. As $fg = 1$, $f, g \in R$ are units in R.

19. Let R be a commutative ring, and let $a \in R$ be a nilpotent element such that $x^n = 0$ for some $n > 0$. Let $u = 1 - x + x^2 + ... + (-1)^{n-1}x^{n-1}$. We have that

$$\begin{aligned}
(1+x)u &= (1+x)(1 - x + x^2 + ... + (-1)^{n-1}x^{n-1}) \\
&= 1 - x + x^2 + ... + (-1)^{n-1}x^{n-1} + x(1 - x + x^2 + ... + (-1)^{n-1}x^{n-1}) \\
&= 1 - x + x^2 + ... + (-1)^{n-1}x^{n-1} + x - x^2 + x^3 + ... + (-1)^{n-1}x^n \\
&= 1 + (-1)^{n-1}x^n \\
&= 1
\end{aligned}$$

Therefore, $1 + x$ is a unit.

20. Let R be a commutative ring, and let $f = a_0 + a_1x + ... + a_dx^d \in R[x]$. Suppose that a_0 is a unit, and $a_1, ..., a_d$ are nilpotent in R. Define $g = 1 + a_1a_0^{-1}x + ... + a_da_0^{-1}x^d$. For any $0 < i \leq d$, we have that a_i is nilpotent, and so there exists a n such that $a_i^n = 0$. Furthermore, $(a_ia_0^{-1}x^i)^n = a_i^na_0^{-n}x^{ni} = 0a_0^{-n}x^{ni} = 0$, which means $a_ia_0^{-1}x^i$ is nilpotent. By the previous exercise, it follows g is a unit. As g is a unit, and a_0 is a unit, we have that $f = a_0g$ is a unit. For the converse, suppose that $f = a_0 + a_1x + ... + a_dx^d \in R[x]$ is a unit. There exists a $g = b_0 + b_1x + ... + b_ex^e \in R[x]$ such that $fg = 1$. Hence,

$$fg = a_0b_0 + (a_1b_0 + a_0b_1)x + ... + (a_{d-1}b_e + a_db_{e-1})x^{d+e-1} + a_db_ex^{d+e} = 1$$

It follows that $a_0b_0 = 1$, so b_0 is a unit, and the coefficients of x^k of fg is 0 for all $k > 0$. Note that $a_db_e = 0$. Suppose for all $k < i$, $a_d^{k+1}b_{e-k} = 0$. We have that the coefficient of x^i is $\sum_{m+n=i} a_mb_n$, and is equal to 0. Thus, $a_d^i \sum_{m+n=i} a_mb_n = 0$, and so $a_d^{i+1}b_{e-i} = 0$ using the induction hypothesis. It follows by the principle of mathematical induction that $a_d^{i+1}b_{e-i} = 0$ for all i. Therefore, $a_d^{e+1}b_0 = 0$. As b_0 is a unit, a_d is nilpotent. Then, $-a_dx^d$ is nilpotent, and so $f - a_dx^d$ is a unit by a previous exercise. Applying this reasoning to $f - a_dx^d$, we find that a_{d-1} is nilpotent. We find that $a_1, ..., a_d$ are nilpotent. Therefore, $f = a_0 + a_1x + ... + a_dx^d$ is a unit in $R[x]$ if and only if a_0 is a unit, and $a_1, ..., a_d$ are nilpotent.

21.

22.

23.

24.

25. Let $f, g, h \in \mathbb{C}[t]$ be non-constant polynomials such that $f^n + g^n = h^n$ for some $n > 2$. Suppose that f, g, h are not relatively prime. Let $d = \gcd(f, g, h)$. Then, $f = df', g = dg'$ and $h = dh'$ for some polynomials $f', g', h' \in \mathbb{C}[t]$. As $f^n + g^n = h^n$, we have that $(df')^n + (dg')^n = (dh')^n$. Hence, $d^n(f'^n + g'^n - h'^n) = 0$. As $\mathbb{C}$ is a field, $\mathbb{C}[t]$ is an integral domain, hence, $d^n = 0$ or $f'^n + g'^n = h'^n$. As $d \neq 0$, $d^n \neq 0$, thus, $f'^n + g'^n = h'^n$. In particular, we have found relatively prime polynomials such that they solve Fermats Last Theorem for complex polynomials. Without loss of generality, let f, g, h be relatively prime non-constant polynomials such that $f^n + g^n = h^n$ with $n > 2$. Suppose futher f, g, h have minimal degree. We have that

$$f^n = h^n - g^n = h^n(1 - (g/h)^n) = h^n \prod_{i=1}^{n}(1 - \zeta^i(g/h)) = \prod_{i=1}^{n}(h - \zeta^i g)$$

As $\mathbb{C}$ is a field, $\mathbb{C}[t]$ is a UFD, hence, there exists irreducible polynomials $p_1, ..., p_k$ such that $f = p_1...p_k$. Furthermore, $f^n = p_1^n...p_k^n$, and using unique factorisation, $h - \zeta^i g = \alpha_i^n$ for all i for some polynomial $\alpha_i \in \mathbb{C}[t]$. Let $h - g = a^n, h - \zeta g = b^n$ and $h - \zeta^2 g = c^n$ for some polynomials $a, b, c \in \mathbb{C}[t]$. We have that

$$(1+\zeta)b^n = (1+\zeta)(h-\zeta g) = h - \zeta g + \zeta h - \zeta^2 g = (h - \zeta^2 g) + \zeta(h-g) = c^n + \zeta a^n$$

And so $(1+\zeta)b^n = c^n + \zeta a^n$. We can then find complex numbers $\lambda, \mu, \nu \in \mathbb{C}$ such that $(\lambda a)^n + (\mu b)^n = (\nu c)^n$. As $a^n = h - g$, the degree of a is strictly less than the degree of h, g. Similarly, the degree of b, c is strictly less that the degree of h, g. This contradicts the initial assumption. Therefore, there cannot exist non-constant polynomials $f, g, h \in \mathbb{C}[t]$ such that $f^n + g^n = h^n$.

5.5 - Irreducibility of Polynomials

1. Let $f(x) \in \mathbb{C}[x]$. Suppose that $a \in \mathbb{C}$ is a complex number such that $f(a) = f'(a) = ... = f^{(n-1)}(a) = 0$ and $f^{(n)}(a) \neq 0$. By Taylor's Theorem,

$$f(x) = f(a) + f'(a)(x-a) + ... + \frac{f^{(n-1)}(a)}{(n-1)!}(x-a)^{n+1} + \frac{f^{(n)}(a)}{n!}(x-a)^n + h(x)(x-a)^{n+1}$$

for some function $h(x)$. By assumption,

$$f(x) = \frac{f^{(n)}(a)}{n!}(x-a)^n + h(x)(x-a)^{n+1} = (x-a)^n\left(\frac{f^{(n)}(a)}{n!} + h(x)(x-a)\right)$$

We have that $g(x) = \frac{f^{(n)}(a)}{n!} + h(x)(x-a)$ is non-zero at $x = a$ as $f^{(n)}(a) \neq 0$. Hence, $a \in \mathbb{C}$ is a root of f with multiplicity n. For the converse, suppose that a is a root of f with multiplicity of n. Then, $f = (x-a)^n g$ for some $g \in \mathbb{C}[x]$ where $g(a) \neq 0$. For $0 \leq i \leq n-1$, we have that

$$f^{(i)}(x) = \sum_{k=0}^{i} \binom{i}{k} \frac{d^k}{dx^k}[(x-a)^n] \frac{d^{i-k}}{dx^{i-k}} g = \sum_{k=0}^{i} \binom{i}{k} \frac{n!}{k!}(x-a)^{n-k} g^{(i-k)}$$

And it follows that $f^{(i)}(a) = 0$. For $i = n$, we have that

$$f^{(n)}(x) = \sum_{k=0}^{n} \binom{n}{k} \frac{n!}{k!}(x-a)^{n-k} g^{n-k} = g(x) + \sum_{k=0}^{n-1} \binom{n}{k} \frac{n!}{k!}(x-a)^{n-k} g^{n-k}$$

Thus, $f^{(n)}(a) = g(a) \neq 0$. Therefore, $a \in \mathbb{C}$ is a root of f if and only if $f(a) = f'(a) = ... = f^{(n-1)}(a) = 0$ and $f^{(n)}(a) \neq 0$. Suppose that $f(x) \in \mathbb{C}[t]$ has multiple roots i.e there exists an $a \in \mathbb{C}$ that is a root of f with multiplicity $r > 1$. Then, $f(a) = f'(a) = 0$ from above. Thus, $(x-a) \mid f$ and $(x-a) \mid f'(a)$, and so $\gcd(f, f') \neq 1$. For the converse, suppose that $\gcd(f, f') \neq 1$. Then, there exists a $g \in \mathbb{C}[t]$ such that $g \mid f$ and $g \mid f'$, hence, $f = gh_1$ and $f' = gh_2$ for some $h_1, h_2 \in \mathbb{C}[t]$. Taking the derivative of $f = gh_1$, we have that $g'h_1 + gh_1' = f' = gh_2$. As $g \in \mathbb{C}[t]$ and $\mathbb{C}$ is algebraically closed, g must have a root $a \in \mathbb{C}$. Then, $g'(a)h_1(a) + g(a)h_1'(a) = g(a)h_2(a)$ and so $g'(a)h_1(a) = 0$. If $g'(a) = 0$, then $g(a) = g'(a) = 0$, and so g has a factor $(x-a)^r$ with $r > 1$. If $h_1(a) = 0$, then $x - a \mid h_1$ and $h_1 = (x-a)h_3$. Since $g(a) = 0$, we have that $g = (x-a)g_1$. Hence, $f = (x-a)^2 g_1 h_1$, and so f has multiple roots. Therefore, f has multiple roots if and only if $\gcd(f, f') \neq 1$.

2. Let F be a subfield of $\mathbb{C}$, and let $f(x) \in F[x]$ be an irreducible polynomial. As f is irreducible, $\gcd(f, f') = 1$ in $F[x]$, otherwise, there would exist a polynomial $g \in F[x]$ that divides f, which contradicts the assumption of irreducibility. We have that $F[x] \subseteq \mathbb{C}[x]$ is an inculsion of integral domain and $F[x]$ is a PID. By exercise 2.22, $\gcd(f, f') = 1$ in $\mathbb{C}[x]$. Hence, using the previous exercise, $f \in \mathbb{C}[x]$ has no multiple roots.

3.

4. Notice that $f(x) = x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$. Hence, f is reducible in $\mathbb{Z}[x]$. Suppose that f has rational roots. Let $c = p/q \in \mathbb{Q}$ with $\gcd(p, q) = 1$ be such a root. By Proposition 5.5, $p \mid 1$ and $q \mid 1$ in $\mathbb{Z}$. Hence, $c \in \{-1, 1\}$. We see that $f(1) = 3$ and $f(-1) = 3$ so c cannot be rational. Therefore, f does not have rational roots.

5.

6.

7. Let R be an integral domain, and let $f \in R[x]$ be a polynomial of degree d. Let $r_1, ..., r_{d+1}$ be distinct elements of R. Suppose that $g \in R[x]$ is a polynomial of degree d that agrees with f at r_i for each i. Then, $f - g$ is a polynomial of degree atmost d with atleast $d + 1$ roots. By Lemma 5.1, this cannot occur unless $f - g$ is the zero polynomial. Therefore, $f = g$. Hence, f is uniquely determined by its value at $d + 1$ distinct elements of R.

8.

9.

10.

11.

12.

13.

14.

15.

16.

17.

18. Let $f \in \mathbb{Z}[x]$ be a cubic polynomial with odd leading coefficient, and both $f(0), f(1)$ are odd. Suppose that $f(x) = a_3x^3 + a_2x^2 + a_1x + a_0$. Consider the polynomial $g(x) = a_3^{-1}f(x) = x^3 + b_2x^2 + b_1x + b_0$. Note that for any $r \in \mathbb{Z}$,

$$\begin{aligned} g(r) - g(1) &= r^3 + b_2r^2 + b_1r + b_0 - 1 - b_2 - b_1 - b_0 \\ &= (r^3 - 1) + b_2(r^2 - 1) + b_1(r - 1) \\ &= (r - 1)[(r^2 + r + 1) + b_2(r + 1) + b_1] \end{aligned}$$

$$\begin{aligned} g(r) - g(0) &= r^3 + b_2r^2 + b_1r + b_0 - b_0 \\ &= r(r^2 + b_2r + b_1) \end{aligned}$$

Hence, $r \mid g(r) - g(0)$ and $(r - 1) \mid g(r) - g(1)$. Suppose that g is reducible. By Proposition 5.3, g has a root in $\mathbb{Q}$. Let $c = p/q$ where $\gcd(p, q) = 1$ and $p, q \in \mathbb{Z}$ be such a root. By Proposition 5.5, $p \mid b_0$ and $q \mid 1$. Thus, $c = p \in \mathbb{Z}$. We have that $c \mid -g(0)$ and $c - 1 \mid -g(1)$. By assumption, $g(0)$ is odd, so c has to be odd. Furthermore, $g(1)$ is odd, so $c - 1$ is odd. This is a contradiction, and so c cannot exist. Therefore, g is irreducible in $\mathbb{Q}$. As $f = a_3^{-1}g$, and $a_3 \in \mathbb{Q}$ is a unit, since g is irreducible in $\mathbb{Q}$, f is irreducible in $\mathbb{Q}$.

19. Note that $\sqrt{2}$ is the root of the polynomial $f(x) = x^2 - 2 \in \mathbb{Z}[x]$. By Eisensteins criterion, $f(x)$ is irreducible in $\mathbb{Z}[x]$. By Corollary 4.17, f is irreducible in $\mathbb{Q}[x]$, and so $f = x^2 - 2$ does not reduce to $(x - \sqrt{2})(x + \sqrt{2})$ in $\mathbb{Q}[x]$. Therefore, $\sqrt{2} \notin \mathbb{Q}$.

20. Let $f(x) = x^6 + 4x^3 + 1 \in \mathbb{Z}[x]$. Consider

$$\begin{aligned} f(x+1) &= (x+1)^6 + 4(x+1)^3 + 1 \\ &= x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 + 4(x^3 + 3x^2 + 3x + 1) + 1 \\ &= x^6 + 6x^5 + 15x^4 + 24x^3 + 27x^2 + 18x + 6 \end{aligned}$$

Note that $3 \mid 6, 15, 24, 27, 18$, $3 \nmid 1$ and $3^2 \nmid 6$. Hence, $f(x+1)$ is irreducible by Eisensteins Criterion. Therefore, $f(x)$ is irreducible in $\mathbb{Z}[x]$.

21. Suppose that n is not prime. There exists $p, q \in \mathbb{Z}$ such that $n = pq$. Then,

$$\begin{aligned} 1 + x + x^2 + ... + x^{n-1} &= \frac{x^n - 1}{x - 1} \\ &= \frac{x^{pq} - 1}{x - 1} \\ &= \frac{(x^p)^q - 1}{x - 1} \\ &= \frac{(x^p - 1)(1 + x^p + x^{2p} + ... + x^{p(q-1)})}{x - 1} \\ &= (1 + x + x^2 + ... + x^{p-1})(1 + x^p + x^{2p} + ... + x^{p(q-1)}) \end{aligned}$$

Therefore, $1 + x + x^2 + ... + x^{n-1}$ is reducible in $\mathbb{Z}$.

22. Let R be a UFD, and let $a \in R$ be a non-unit element that is not divisible by the square of some irreducible element in its factorisation. Let p be such an element. As R is a UFD, since p is irreducible, p is prime. Let $f(x) = x^n - a$ for some $n \geq 1$. We have that $1 \notin (p)$ and $-a \in (p)$. Furthermore, $-a \notin (p)^2$ by assumption. Therefore, f is irreducible by Eisensteins Criterion.

23. Let $f(x, y) = y^5 + x^2y^3 + x^3y^2 + x \in \mathbb{C}[x, y]$. We can view $\mathbb{C}[x, y]$ as $(\mathbb{C}[x])[y]$. We have that $(x) \subseteq \mathbb{C}[x]$ is a prime ideal as $\mathbb{C}[x]/(x) \cong \mathbb{C}$ is a field. Note that $x, x^2, x^3 \in \mathbb{C}[x]$, $1 \notin (x)$, and $x \notin (x)^2$. Therefore, by Eisensteins Criterion, $f(x, y)$ is irreducible in $\mathbb{C}[x, y]$.

24.

5.6 - Further Remarks and Examples

1. Let I, J be ideals of a commutative ring R. Define the map $f_1 : \mathbf{0} \to I \cap J$ by $f_1(0) = 0$ where $\mathbf{0}$ is the zero ring. We have that $\text{im } f_1 = \{0\}$. Let $f_2 : I \cap J \to R$ be the inclusion map. We have that $\text{im } f_1 = \ker f_2 = \{0\}$ and note that $\text{im } f_2 = I \cap J$. Define the map $\varphi : R \to R/I \times R/J$ by $r \mapsto (r + I, r + J)$. We have that

$$\begin{aligned} \ker \varphi &= \{x \in R \mid \varphi(x) = (I, J)\} \\ &= \{x \in R \mid (x + I, x + J) = (I, J)\} \\ &= \{x \in R \mid x \in I, x \in J\} \\ &= \{x \in R \mid x \in I \cap J\} \\ &= I \cap J \\ &= \text{im } f_2 \end{aligned}$$

Now, define the map $f_3 : R/I \times R/J \to R/I + J$ by $(x + I, y + J) \mapsto (x - y) + (I + J)$. We have that

$$\begin{aligned} \ker f_3 &= \{(x + I, y + J) \in R/I \times R/J \mid f_3(x + I, y + J) = I + J\} \\ &= \{(x + I, y + J) \in R/I \times R/J \mid (x - y) + I + J = I + J\} \\ &= \{(x + I, y + J) \in R/I \times R/J \mid x + I + J = y + I + J\} \\ &= \{(x + I, y + J) \in R/I \times R/J \mid \exists (i, i' \in I, j, j' \in J), x + i + j = y + i' + j'\} \\ &= \{(x + I, y + J) \in R/I \times R/J \mid \exists (i, i' \in I, j, j' \in J), x = y + (i' - i) + (j' - j)\} \end{aligned}$$

Hence, if $(x+I, y+J) \in \ker f_3$, there exists $i, i' \in I$ and j, j' so that $x = y + (i' - i) + (j' - j)$, hence, $(x+I, y+J) = (y + j'' + I, y + J)$ for some $j'' \in J$. We have that $\varphi(y + j'') = (y + j'' + I, y + J)$, hence, $(x + I, y + J) \in \text{im } \varphi$. Furthermore, if $(x + I, y + J) \in \text{im } \varphi$, then, there exists some $z \in R$ such that $(z + I, z + J) = (x + I, y + J)$ and so $x - z \in I$ and $y - z \in J$. Hence, $x - y \in I + J$, and so $(x + I, y + I) \in \ker f_3$. Therefore, $\text{im } \varphi = \ker f_3$. Finally, we have that f_3 is surjective as if $x + I + J \in R/I + J$, then $f_3(x + I, J) = x + I + J$. It follows that the following is an exact sequence of R-modules

$$\mathbf{0} \longrightarrow I \cap J \longrightarrow R \xrightarrow{\varphi} \frac{R}{I} \times \frac{R}{J} \longrightarrow \frac{R}{I+J} \longrightarrow \mathbf{0}$$

We now prove the Chinese Remainder Theorem for $k = 2$. Let I, J be ideals of a commutative ring R such that $I + J = (1)$. We obtain the exact sequence,

$$\mathbf{0} \longrightarrow I \cap J \longrightarrow R \xrightarrow{\varphi} \frac{R}{I} \times \frac{R}{J} \longrightarrow \mathbf{0} \longrightarrow \mathbf{0}$$

By exactness, φ must be surjective, and we obtain the isomorphism $R/I \cap J \cong R/I \times R/J$.

2. Let R be a commutative ring, and let $a \in R$ be an element in R such that $a^2 = a$. We have that $1 \in (a) + (1-a)$ as $a + 1 - a = 1$, thus, by the Chinese Remainder Theorem, $R/(a)(1-a) \cong R/(a) \times R/(1-a)$. Let $r \in (a)(1-a)$. Then $r = xay(1-a)$ for some $x, y \in R$. Note that $r = xay(1-a) = xya(1-a) = xy(a-a^2) = xy(a-a) = xy0 = 0$. Therefore, $r = 0$. It follows that $(a)(1-a)$ is trivial, hence, $R \cong R/(a)(1-a) \cong R/(a) \times R/(1-a)$. We have that (a) is a ring with identity a as for every $ax \in (a)$, we have that $aax = a^2x = ax$ and (a) is an ideal of R. Define the map $\varphi : R \to (a)$ by $\varphi(x) = ax$. Note that $\varphi(r(1-a)) = ar(1-a) = r(a-a^2) = r(a-a) = 0$, hence, $(1-a) \subseteq \ker \varphi$. Suppose that $x \in \ker \varphi$. Then, $ax = 0$. Note that $x = ax + (1-a)x = (1-a)x \in (1-a)$. Therefore, we have that $\ker \varphi = (1-a)$. By the first isomorphism theorem, $R/(1-a) \cong (a)$. By a similar argument, $(1-a)$ can be viewed as a ring with identity $1-a$, and $R/(a) \cong (1-a)$. As $R \cong R/(a) \times R/(1-a)$, we have that

$$R \cong (a) \times (1-a)$$

3.

4. Let R be a finite commutative ring, and let p be the smallest prime dividing $|R|$. Let $I_1, ..., I_k$ be proper ideals of R such that $I_i + I_j = (1)$ for $i \neq j$. By the CRT,

$$\frac{R}{I_1 ... I_k} \cong \frac{R}{I_1} \times ... \times \frac{R}{I_k}$$

Then,

$$\frac{|R|}{|I_1 ... I_k|} = \left| \frac{R}{I_1 ... I_k} \right| = \left| \frac{R}{I_1} \times ... \times \frac{R}{I_k} \right| = \left| \frac{R}{I_1} \right| ... \left| \frac{R}{I_k} \right| = \frac{|R|^k}{|I_1| ... |I_k|}$$

Thus, $|R|^{k-1} = |I_1|...|I_k|/|I_1...I_k| \leq |I_1|...|I_k|$. As p is the smallest prime divisor of $|R|$, by Lagranges Theorem, $|I_i| \leq |R|/p$ for each i. Hence, $|I_1|...|I_k| \leq (|R|/p)^k$. Therefore, $|R|^{k-1} \leq (|R|/p)^k$. By taking the logarithm base p of both sides, we have that $(k-1)\log_p |R| \leq k(\log_p |R| - 1)$, and so $k \leq \log_p |R|$.

5. Let $\varphi : \mathbb{Z}[x] \to \mathbb{Z}[x]/(x) \times \mathbb{Z}[x]/(2)$ be the canonical map. Suppose there exists an $f \in \mathbb{Z}[x]$ such that $\varphi(f) = (1 + (x), (2))$. Then, $f - 1 \in (x)$ and $f \in (2)$. There exists $g, h \in \mathbb{Z}[x]$ such that $f - 1 = xg$ and $f = 2h$. Hence, $xg + 1 = 2h$. Write $g = g_0 + g_1x + ... + g_nx^n$ and $h = h_0 + h_1x + ... + h_mx^m$. Thus, $1 + g_0x + g_1x^2 + ... + g_nx^{n+1} = 2h_0 + 2h_1x + ... + 2h_mx^m$. It follows that $2h_0 = 1$, which means that $h_0 = 1/2$. This is a contradiction as $h \in \mathbb{Z}$. Therefore, such an $f \in \mathbb{Z}$ cannot exist, and so φ is not surjective.

6. Let R be a UFD

(i) Let $a, b \in R$ such that $\gcd(a, b) = 1$. Let $x \in (ab)$. Then, $x = kab$ for some $k \in R$ and so $x = kab \in (a)$ and $x = kab \in (b)$. Thus, $x \in (a) \cap (b)$. For the converse, suppose that $x \in (a) \cap (b)$. Then, $x = ra = r'b$ for some $r, r' \in R$. As $\gcd(a, b) = 1$, we have that there exists $p, q \in R$ such that $ap + bq = 1$. Then,

$$x = ra = ra1 = ra(ap + bq) = (ra)ap + rq(ab) = (r'b)ap + rq(ab) + r'p(ab) = ab(rq + r'p) \in (ab)$$

Therefore, $(a) \cap (b) = (ab)$.

(ii)

7. Note that

$$x^{100} + (x^2+1)\sum_{n=0}^{49}(-1)^n x^{2n} = 1$$

Consider $f = x^{100} + x(x^2+1)\sum_{n=0}^{49}(-1)^n x^{2n}$. We have that

$$f \equiv x(x^2+1)\sum_{n=0}^{49}(-1)^n x^{2n} \mod x^{100} \equiv x(1-x^{100}) \mod x^{100} \equiv x \mod x^{100}$$

$$f \equiv x^{100} \mod (x^2+1) \equiv 1-(x^2+1)\sum_{n=0}^{49}(-1)^n x^{2n} \mod (x^2+1) \equiv 1 \mod (x^2+1)$$

We simplify f as $f = -x^{101} + x^{100} + x$, and we have that f satisfies our required properties.

8. Let $n \in \mathbb{Z}$ be a positive integer and $n = p_1^{a_1}...p_r^{a_r}$ its prime factorisation.

(i) For $i \neq j$, we have that $\gcd(p_i^{a_i}, p_j^{a_j}) = 1$ as p_i, p_j are prime. By Bezouts lemma, there exists x, y such that $p_i^{a_i}x + p_j^{a_j}y = 1$. Hence, $(p_i^{a_i}) + (p_j^{a_j}) = (1)$. By the CRT, $\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1^{a_1})...(p_r^{a_r}) \cong \mathbb{Z}/(p_1^{a_1}) \times ... \times \mathbb{Z}/(p_r^{a_r})$.

(ii) Let A, B be rings. Let $(x,y) \in A^* \times B^*$. Then, $x \in A^*$ and $y \in B^*$. We have that there exists $x^{-1} \in A$ and $y^{-1} \in B$ such that $xx^{-1} = 1 \in A$ and $yy^{-1} = 1 \in B$. We have that $(x,y)(x^{-1}, y^{-1}) = (xx^{-1}, yy^{-1}) = (1,1) \in A \times B$. Hence, $(x,y) \in (A \times B)^*$. For the reverse, suppos that $(x,y) \in (A\times B)^*$. There exists a $(x', y') \in A \times B$ such that $(x,y)(x',y') = (1,1)$. Hence, $xx' = 1$ and $yy' = 1$. Therefore, $x \in A^*$ and $y \in B^*$, so that $(x,y) \in A^* \times B^*$. It follows that $(A\times B)^* \cong A^* \times B^*$. Via induction, we have that $(A_1 \times ... \times A_n)^* \cong A_1^* \times ... \times A_n^*$ for rings $A_1, ..., A_n$. Therefore,

$$(\mathbb{Z}/(n))^* \cong (\mathbb{Z}/(p_1^{a_1}))^* \times ... \times (\mathbb{Z}/(p_r^{a_r}))^*$$

(iii) Note that for any prime p and integer a, there are p^{a-1} integers that are not relatively prime to p^a that are less than or equal to p^a, namely, $p, 2p, ..., p^{a-1}p$. Hence, there are $p^a - p^{a-1} = p^{a-1}(p-1)$ integers that are relatively prime to p^a that are less than or equal to p^a. It follows that $|(\mathbb{Z}/(p^a))^*| = \phi(p^a) = p^{a-1}(p-1)$. Therefore,

$$\phi(n) = |(\mathbb{Z}/(n))^*| = |(\mathbb{Z}/(p_1^{a_1}))^*|...|(\mathbb{Z}/(p_r^{a_r}))^*| = \phi(p_1^{a_1})...\phi(p_r^{a_r}) = p_1^{a_1-1}(p_1-1)...p_r^{a_r-1}(p_r-1)$$

9. Let I be a nonzero ideal of $\mathbb{Z}[i]$. Let $z + I \in \mathbb{Z}[i]/I$. As $\mathbb{Z}[i]$ is a Euclidean domain, it is a PID, and so $I = (a)$ for some $a \in \mathbb{Z}[i]$. We have that $z = qa + r$ for some $q, r \in \mathbb{Z}[i]$ where either $r = 0$ or $N(r) < N(a)$. Hence, $z + I = (qa+r) + I = r + I$. There are a finite number of $r \in \mathbb{Z}[i]$ with $N(r) < N(a)$. Hence, $\mathbb{Z}[i]/I$ is finite.

10. Let $z, w \in \mathbb{Z}[i]$ be associate elements in $\mathbb{Z}[i]$. There exists a unit $u \in \mathbb{Z}[i]$ such that $z = uw$. Hence, $N(z) = N(uw) = N(u)N(w) = N(w)$. For a partial converse, suppose that $(z) = (w)$ and $N(z) = N(w)$. We have that there exists an $a \in \mathbb{Z}[i]$ such that $z = aw$. Hence, $N(w) = N(z) = N(aw) = N(a)N(w)$, so that $N(a) = 1$. It follows that $a\bar{a} = 1$, thus, a is a unit in $\mathbb{Z}[i]$. Therefore, z and w are associates.

11.

12. Let $z, w \in \mathbb{Z}[i]$ with $w \neq 0$. Write $z = a + bi$ and $w = c + di$. Suppose that $w \mid z$ in $\mathbb{Z}[i]$. Then, $z = aw$ for some $a \in \mathbb{Z}[i]$. Suppose that $w \nmid z$. We have that $zw^{-1} = x + yi$ where $x = \frac{ac+bd}{c^2+d^2}$ and $y = \frac{bc-ad}{c^2+d^2}$. Let

$$e = \begin{cases} \lfloor x \rfloor & \text{if } x \leq \lfloor x \rfloor + 1/2 \\ \lceil x \rceil & \text{if } x > \lfloor x \rfloor + 1/2 \end{cases} \quad f = \begin{cases} \lfloor y \rfloor & \text{if } y \leq \lfloor y \rfloor + 1/2 \\ \lceil y \rceil & \text{if } y > \lfloor y \rfloor + 1/2 \end{cases}$$

Then, $|e - x| \leq 1/2$ and $|e - y| \leq 1/2$. Set $q = e + fi$. We have that

$$N(zw^{-1} - q) = N(x + yi - e - fi) = (x-e)^2 + (y-f)^2 \leq 1/2 < 1$$

Hence, $N(z - qw) < N(w)$. Set $r = z - qw$, then $z = qw + r$ with $N(r) < N(w)$. It follows that $\mathbb{Z}[i]$ is a Euclidean domain.

13. Denote the set $\{a+b\sqrt{2} \mid a,b\in\mathbb{Z}\} \subseteq \mathbb{C}$ by $\mathbb{Z}[\sqrt{2}]$.

(i) Let $a+b\sqrt{2}, c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. We have that $a+b\sqrt{2}-(c+d\sqrt{2}) = (a-c)+(b-d)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ and $(a+b\sqrt{2})(c+d\sqrt{2}) = (ac+2bd)+(bc+ad)\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Also note $0,1 \in \mathbb{Z}[\sqrt{2}]$. Hence, $\sqrt{2}$ is a subring of $\mathbb{C}$. Define the map $\varphi : \mathbb{Z}[t] \to \mathbb{Z}[\sqrt{2}]$ by sending $t \mapsto \sqrt{2}$. Suppose that $f \in (t^2-2)$. Then, $f = g(t)(t^2-2)$ for some $g \in \mathbb{Z}[t]$, and so $\varphi(f) = g(t)0 = 0$. Hence, $f \in \ker\varphi$. For the reverse inclusion, suppose that $f \in \ker\varphi$. Write $f = \sum_{i=0}^n a_i t^i$. As $f \in \ker\varphi$, we have that

$$\begin{aligned}
0 &= \sum_{i=0}^n a_i(\sqrt{2})^i \\
&= \sum_{i=0, i \text{ even}}^n a_i 2^{\frac{i}{2}} + \sqrt{2}\sum_{i=0, i \text{ odd}}^n a_i 2^{\frac{i-1}{2}}
\end{aligned}$$

Hence,

$$\sum_{i=0, i \text{ odd}}^n a_i 2^{\frac{i-1}{2}} = \sum_{i=0, i \text{ even}}^n a_i 2^{\frac{i}{2}} = 0$$

Now,

$$\begin{aligned}
f(-\sqrt{2}) &= \sum_{i=0}^n a_i(-\sqrt{2})^i \\
&= \sum_{i=0, i \text{ even}}^n a_i 2^{\frac{i}{2}} - \sqrt{2}\sum_{i=0, i \text{ odd}}^n a_i 2^{\frac{i-1}{2}} \\
&= 0
\end{aligned}$$

Therefore, $(t-\sqrt{2})(t+\sqrt{2}) = t^2-2$ is a factor of f and so $f = g(t)(t^2-2)$ for some $g \in \mathbb{Z}[t]$. Thus, $f \in (t^2-2)$. It follows that $\ker\varphi = (t^2-2)$, and by the first isomorphism theorem,

$$\mathbb{Z}[\sqrt{2}] \cong \frac{\mathbb{Z}[t]}{(t^2-2)}$$

(ii) Define the function $N : \mathbb{Z}[\sqrt{2}] \to \mathbb{Z}$ by $N(a+b\sqrt{2}) = a^2-2b^2$. Let $z = a+b\sqrt{2}, w = c+d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$. Then,

$$\begin{aligned}
N(zw) &= N((a+b\sqrt{2})(c+d\sqrt{2})) \\
&= N((ac+2bd)+(bc+ad)\sqrt{2}) \\
&= (ac+2bd)^2 - 2(bc+ad)^2 \\
&= (ac)^2 + 4abcd + 4(bd)^2 - 2(bc)^2 - 4abcd - 2(ad)^2 \\
&= (ac)^2 + 4(bd)^2 - 2(bc)^2 - 2(ad)^2 \\
&= a^2(c^2-2d^2) - 2b^2(c^2-2d^2) \\
&= (a^2-2b^2)(c^2-2d^2) \\
&= N(a+b\sqrt{2})N(c+d\sqrt{2}) \\
&= N(z)N(w)
\end{aligned}$$

(iii) We first prove that a $z \in \mathbb{Z}[\sqrt{2}]$ is a unit if and only if $N(z) = \pm 1$. Suppose that $z \in \mathbb{Z}[\sqrt{2}]$ is a unit. Then, there exists a $w \in \mathbb{Z}$ such that $zw = 1$. Hence, $1 = N(1) = N(zw) = N(z)N(w)$. Thus, as $N(z)$ is an integer, $N(z) \in \{-1,1\}$. For the converse, suppose that $N(z) = \pm 1$. Write $z = a+b\sqrt{2}$. Then, $N(z) = a^2-2b^2 = \pm 1$ so $(a+b\sqrt{2})(a-b\sqrt{2}) = \pm 1$. It follows that $z = a+b\sqrt{2}$ is a unit. Now, note that $N(1+\sqrt{2}) = -1$, hence, $1+\sqrt{2}$ is a unit. Consider $u_n = (1+\sqrt{2})^n$ where $n \in \mathbb{N}$. Then, $N(u_n) = N((1+\sqrt{2})^n) = N(1+\sqrt{2})^n = (-1)^n$. Thus, u_n is a unit. It follows that $\mathbb{Z}[\sqrt{2}]$ has infinite many units.

(iv) Let $z = a + b\sqrt{2} \in \mathbb{R}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{R}\}$. There exists a $x, y \in \mathbb{Z}$ such that $|a - x| \le 1/2$ and $|b - y| \le 1/2$. Let $w = x + y\sqrt{2}$. Then,

$$|N(z - w)| = |N((a - x) + (b - y\sqrt{2}))| = |(a - x)^2 - 2(b - y)^2| \le |a - x|^2 + 2|b - y|^2 \le \frac{3}{4} < 1$$

Therefore, for any $z \in \mathbb{R}[\sqrt{2}]$, there exists a $w \in \mathbb{Z}[\sqrt{2}]$ such that $|N(z - w)| < 1$. Now, let $z, w \in \mathbb{Z}[\sqrt{2}]$ with $w \neq 0$. We have that there exists a $q \in \mathbb{Z}[\sqrt{2}]$ such that $|N(zw^{-1} - q)| < 1$. Therefore, $|N(z - qw)| < |N(w)|$. Let $r = z - qw$. We have that $z = qw + r$ with $|N(r)| < |N(w)|$. Therefore, $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

14.

(i) Define the norm $N : \mathbb{Z}[\sqrt{-2}] \to \mathbb{Z}$ by $N(a + b\sqrt{-2}) = a^2 + 2b^2$. Let $z = a + b\sqrt{2} \in \mathbb{R}[\sqrt{-2}] = \{a + b\sqrt{-2} \mid a, b \in \mathbb{R}\}$. There exists a $x, y \in \mathbb{Z}$ such that $|a - x| \le 1/2$ and $|b - y| \le 1/2$. Let $w = x + y\sqrt{-2}$. Then,

$$N(z - w) = N((a - x) + (b - y\sqrt{-2})) = (a - x)^2 + 2(b - y)^2 \le |a - x|^2 + 2|b - y|^2 \le \frac{3}{4} < 1$$

Therefore, for any $z \in \mathbb{R}[\sqrt{-2}]$, there exists a $w \in \mathbb{Z}[\sqrt{-2}]$ such that $N(z - w) < 1$. Now, let $z, w \in \mathbb{Z}[\sqrt{-2}]$ with $w \neq 0$. We have that there exists a $q \in \mathbb{Z}[\sqrt{-2}]$ such that $N(zw^{-1} - q) < 1$. Therefore, $N(z - qw) < N(w)$. Let $r = z - qw$. We have that $z = qw + r$ with $N(r) < N(w)$. Therefore, $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

(ii) **FOR WHEN YOU'RE FEELING PARTICULARLY ADVENTUROUS**

(iii)

(iv)

15. Let $k \in \mathbb{Z}$ and suppose that $n = a^2 + b^2$ for some $a, b \in \mathbb{Z}$. We have that $\{[n^2]_4 \mid n \in \mathbb{Z}\} = \{[0]_4, [1]_4\}$, and so $\{[n^2]_4 + [m^2]_4 \mid n, m \in \mathbb{Z}\} = \{[0]_4, [1]_4, [2]_4\}$. Therefore, $k \not\equiv 3 \mod 4$. By taking the contrapositive, if $k \equiv 3 \mod 4$, then k is not the sum of two squares.

16. Let $m, n \in \mathbb{Z}$ and suppose that there exists $a, b, c, d \in \mathbb{Z}$ such that $m = a^2 + b^2$ and $n = c^2 + d^2$. We have that

$$\begin{aligned}
mn &= (a^2 + b^2)(c^2 + d^2) \\
&= (a - bi)(a + bi)(c + di)(c - di) \\
&= [(a - bi)(c + di)][(a + bi)(c - di)] \\
&= [(ac + bd) + (ad - bc)i][(ac + bd) + (bc - ad)i] \\
&= (ac + bd)^2 + (ad - bc)^2 + [(ad - bc)(ac + bd) + (ac + bd)(bc - ad)]i \\
&= (ac + bd)^2 + (ad - bc)^2
\end{aligned}$$

Therefore, if m, n can be represented as a sum of two squares, then their product, mn, can also be represented as a sum of two squares.

17. Let n be a positive integer.

(i) Suppose that n is the sum of two squares. Then, $n = a^2 + b^2 = N(a + bi)$. Hence, n is the norm of some complex number. Now, suppose that n is the norm of some Gaussian integer. Then, $n = N(a+bi)$ for some $a, b \in \mathbb{Z}$. We have that $N(a + bi) = a^2 + b^2$, thus, n is the sum of two squares.

(ii) Suppose that each integer prime factor p of n such that $p \equiv 3 \mod 4$ appears with an even power in n. Let $n = p_1^{a_1}...p_m^{a_m}$ be a prime factorisation of n. Suppose that $p_i \equiv 3 \mod 4$, then $p_i^2 \equiv 1 \mod 4$. It follows that $p_i^{a_i} \equiv 1 \mod 4$ as a_i is even by assumption. By Theorem 6.11, $p_i^{a_i}$ is then the sum of two squares. For any prime p_i in the factorisation of n, if $p_i = 2$, then $2 = 1^2 + 1^2$, and if $p_i \equiv 1 \mod 4$, then $p^{a_i} \equiv 1 \mod 4$, and it is the sum of two squares by Theorem 6.11. We have that every $p_i^{a_i}$ in the factorisation is the sum of two squares. By a previous exercise, the product of integers that can be written as a sum of two squares can also be written as a sum of two squares, hence, n is the sum of two squares. For the converse, suppose that n is the sum of two squares, in particular, suppose that there exists $a, b \in \mathbb{Z}$ such that $n = a^2 + b^2$. By the previous part, n is then the norm of a Gaussian integer, $n = N(z)$ say. We can factor $a^2 + b^2$ as a product of primes $p_1^{a_1}...p_m^{a_m}$ where $a_1, ..., a_m \in \mathbb{N}$. Furthermore, as $\mathbb{Z}[i]$ is a UFD, z has a prime factorisation, $w_1^{b_1}...w_k^{b_k}$ say. We then have that

$$p_1^{a_1}...p_m^{a_m} = a^2 + b^2 = n = N(z) = N(w_1^{b_1}...w_k^{b_k}) = N(w_1)^{b_1}...N(w_k)^{b_k}$$

Suppose that $p_i \equiv 3 \mod 4$. By Lemma 6.7, for each i, $N(w_i)$ is prime or the square of a prime. It follows that $p_i^{a_i} = N(w_{j_1})^{b_{j_1}}...N(w_{j_v})^{b_{j_v}}$ for some $j_1, ..., j_v$. We have that $p_i^{a_i} = N(w_{j_1}^{b_{j_1}}...w_{j_v}^{b_{j_v}})$ so $p_i^{a_i} \equiv 1 \mod 4$ as $p_i^{a_i}$ is the norm of a Gaussian integer and so the sum of two squares. It follows that a_i must be even.

18. Suppose that $a^2 = b^2 \mod p$ where $a \neq b$ and $0 \leq a, b \leq (p-1)/2$. We have that $a^2 - b^2 = 0 \mod p$. Since p is prime, we have that $a = b \mod p$ or $a = -b \mod p$. As $a \neq b$ and $0 \leq a, b \leq (p-1)/2$, we cannot have that $a = b \mod p$. Assume $a = -b \mod p$. Then, $a = tp - b$ for some $t \in \mathbb{Z}$. As $0 \leq b \leq (p-1)/2$, we have that $(p(2t-1)+1)/2 \leq tp - b \leq tp$. For any $t \in \mathbb{Z}$, we have that $(p+1)/2 \leq b$ or $b \leq 0$, which cannot occur. Therefore, it cannot occur that $a^2 = b^2 \mod p$ where $a \neq b$ and $0 \leq a, b \leq (p-1)/2$. Furthermore, suppose that $a \neq b$ and $0 \leq a, b \leq (p-1)/2$, and $-1 - a^2 = -1 - b^2 \mod p$. Then, $a^2 = b^2 \mod p$, which we have shown to be impossible. It follows that the numbers a^2 with $0 \leq a \leq (p-1)/2$ represent $(p+1)/2$ distinct classes modulo p, aswell as the numbers of the form $-1 - b^2$ with $0 \leq b \leq (p-1)/2$. By the pigeonhole principle, there exists a, b such that $a^2 = -1 - b^2 \mod p$ as there are in total $p+1$ congruence classes represented by a^2 or $-1-b^2$ and there are p congruence classes in $\mathbb{Z}/p\mathbb{Z}$. Therefore, there exists an $n \in \mathbb{Z}$ such that $a^2 = -1 - b^2 + np$. Hence, there is an n such that $np = 1 + a^2 + b^2$.

19. Let $\mathbb{I} \subseteq \mathbb{H}$ be the set of quarternions of the form $\frac{a}{2}(1+i+j+k) + bi + cj + dk$ with $a, b, c, d \in \mathbb{Z}$

(i) Let $\frac{a}{2}(1+i+j+k) + bi + cj + dk$, $\frac{a'}{2}(1+i+j+k) + b'i + c'j + d'k$ be elements of $\mathbb{I}$. Then,

$$\begin{aligned}
&\frac{a}{2}(1+i+j+k) + bi + cj + dk - \frac{a'}{2}(1+i+j+k) + b'i + c'j + d'k \\
&\quad = \frac{a-a'}{2}(1+i+j+k) + (b-b') + (c-c')j + (d-d')k \in \mathbb{I}
\end{aligned}$$

as $a - a', b - b', c - c', d - d' \in \mathbb{Z}$. Now, let $a + bi + cj + dk, a' + b'i + c'j + d'k \in \mathbb{I}$. Furthermore, we have that

$$\begin{aligned}
(a + bi + cj + dk)(a' + b'i + c'j + d'k) &= aa' - bb' - cc' - dd' \\
&+ (ab' + ba' + cd' - dc')i \\
&+ (ac' - bd' + ca' + db')j \\
&+ (ad' + bc' - cb' + da')k \in \mathbb{I}
\end{aligned}$$

by looking at cases of $a, a', b, b', c, c', d, d'$. It follows that $\mathbb{I}$ is a subring of $\mathbb{H}$.

(ii) Note that $N : \mathbb{H} \to \mathbb{R}^+$ is a homomorphism of the quarternions to the positive reals. Hence, it is multiplicative. It follows that for all $w_1, w_2 \in \mathbb{I}$, we have that $N(w_1 w_2) = N(w_1)N(w_2)$ as $\mathbb{I}$ is a subring of $\mathbb{H}$. Let $w = \frac{a}{2}(1+i+j+k) + bi + cj + dk \in \mathbb{I}$. We have that

$$\begin{aligned}
N(w) &= N\Big(\frac{a}{2} + \Big(\frac{a}{2} + b\Big)i + \Big(\frac{a}{2} + c\Big)j + \Big(\frac{a}{2} + d\Big)k\Big) \\
&= \Big(\frac{a}{2}\Big)^2 + \Big(\frac{a}{2} + b\Big)^2 + \Big(\frac{a}{2} + c\Big)^2 + \Big(\frac{a}{2} + d\Big)^2 \\
&= \frac{a^2}{4} + \frac{a^2}{4} + ab + b^2 + \frac{a^2}{4} + ac + c^2 + \frac{a^2}{4} + ad + d^2 \\
&= a^2 + b^2 + c^2 + d^2 + a(b + c + d) \in \mathbb{Z}
\end{aligned}$$

(iii) Let $u \in \mathbb{I}$ be a unit. There exists a $v \in \mathbb{I}$ such that $uv = 1 \in \mathbb{I}$. We have that $1 = N(1) = N(uv) = N(u)N(v)$. As $N(u), N(v)$ are positive integers, we have that $N(u) = 1$. We may write u as $\frac{a}{2}(1+i+j+k)+bi+cj+dk$. Then, $N(u) = a^2+b^2+c^2+d^2+a(b+c+d) = 1$. As $a,b,c,d \in \mathbb{Z}$, we must have that $a,b,c,d \in \{-2,-1,0,1,2\}$. We note that if $a = 0$, then $N(u) = b^2+c^2+d^2$ and only one of b,c,d can be non zero otherwise $N(u) > 1$. When $a = 0$, the only solutions are $(b,c,d) = (\pm 1, 0, 0), (0, \pm 1, 0), (0, 0, \pm 1)$. Take note of the solution $(a,b,c,d) = (\pm 1, 0, 0, 0)$ aswell. Suppose that $a = \pm 1$, then $N(u) = 1 + b^2 + c^2 + d^2 \pm (b+c+d)$. The only solutions are then $(a,b,c,d) = (\pm 1, \mp 1, 0, 0), (\pm 1, 0, \mp 1, 0), (\pm 1, 0, 0, \mp 1), (\pm 1, \mp 1, \mp 1, 0), (\pm 1, \mp 1, 0, \mp 1), (\pm 1, 0, \mp 1, \mp 1), (\pm 1, \mp 1, \mp 1, \mp 1)$. Finally, suppose that $a = \pm 2$. Then, $N(u) = 4 + b^2 + c^2 + d^2 + \pm 2(b+c+d)$. The only solutions are $(a,b,c,d) = (\pm 2, \mp 1, \mp 1, \mp 1)$. Therefore, there are 24 units of $\mathbb{I}$, namely, $\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$.

(iv) Let $w \in \mathbb{I}$. Choose z being of the form $\frac{a}{2}(\pm 1 \pm i \pm j \pm k)$ such that $\overline{w} + z$ is of the form $a + bi + cj + dk$ where a,b,c,d are integers divisible by 2. We have that $N(w) + wz = w\overline{w} + wz = w(\overline{w} + z)$ is of the form $p + qi + rj + sk$ where p,q,r,s are integers as $\overline{w} + z$ is divisible by 2 and it cancels with the half on the w if w does not have integer coefficients. And so $w(\overline{w} + z)$ can be written as a product of integer quarternions. Thus, $wz = w(\overline{w} + z) - N(w)$ is of the form $a + bi + cj + dk$ where $a,b,c,d \in \mathbb{Z}$.

20.

(i) We prove a preliminary result. Let $q = q_1 + q_2 i + q_3 j + q_4 k \in \mathbb{H}$. Choose some $n_1 \in \mathbb{Z} \cup (\frac{1}{2} + \mathbb{Z})$ such that $|q_1 - n_1| \leq 1/4$. If n_1 is an integer, we can find integers n_2, n_3, n_4 such that $|q_i - n_i| \leq 1/2$ for $i = 1,2,3$. Similarly, if n_1 is a half integer, we can find half integers n_2, n_3, n_4 such that $|q_i - n_i| \leq 1/2$ for $i = 1,2,3$. Let $z = n_1 + n_2 i + n_3 j + n_4 k$. We have that $z \in \mathbb{I}$ and

$$\begin{aligned} N(q - z) &= N((q_1 - n_1) + (q_2 - n_2)i + (q_3 - n_3)j + (q_4 - n_4)k) \\ &= (q_1 - n_1)^2 + (q_2 - n_2)^2 + (q_3 - n_3)^2 + (q_4 - n_4)^2 \\ &\leq (1/4)^2 + (1/2)^2 + (1/2)^2 + (1/2)^2 \\ &= 13/16 \\ &< 1 \end{aligned}$$

Therefore, for any $q \in \mathbb{H}$, we can find a $z \in \mathbb{I}$ such that $N(q - z) < 1$. Let $z, w \in \mathbb{I}$ with $w \neq 0$. We have that there exists a $q \in \mathbb{I}$ such that $N(zw^{-1} - q) < 1$. We have that $N(z - qw) = N(w)N(zw^{-1} - q) < N(w)$, and $z = qw + z - qw$. Hence, we can find $q, r \in \mathbb{I}$ such that $z = qw + r$ with $N(r) < N(w)$.

(ii) Let I be a non-trivial left-ideal of $\mathbb{I}$. Let $A = \{N(x) \mid x \in I\} \subseteq \mathbb{Z}^{\geq 0}$. A has a minimal nonzero element, and so there exists a $w \in I$ such that $N(w)$ is minimal. We conjecture $I = \mathbb{I}w$. Let $rw \in \mathbb{I}w$. As $w \in I$, we must have that $rw \in I$. Hence, $\mathbb{I}w \subseteq I$. Now, let $z \in I$. We have that $z = qw + r$ for some $q, r \in \mathbb{I}$ where $N(r) < N(w)$. As $z, qw \in \mathbb{I}$, we must have that $r = z - qw \in \mathbb{I}$. As $N(w)$ is minimal among nonzero norms of elements of I, we must have that $N(r) = 0$. Thus, $r = 0$ and $z = qw \in \mathbb{I}w$. Therefore, $I = \mathbb{I}w$.

(iii) Let $z, w \in \mathbb{I}$ with $w \neq 0$. We have that there exists q, r such that $z = qw + r$ where $N(r) < N(w)$. Suppose that d is a right divisor of z, w. Then, $z = z'd$ and $w = w'd$ for some z', w'. Hence, $r = z - qw = z'd - qw'd = (z' - qw')d$, and so d is a right divisor of r. Now, suppose that d is a right divisor of w, r. Then, $w = w'd$ and $r = r'd$ for some w', r', and so $z = qw + r = qw'd + r'd = (qw' + r')d$. Thus, d is a right divisor of z. It follows that the set of right divisors of z and w is the same as the set of right divisors of w and r. Given $z, w \in \mathbb{I}$, we can apply division with remainder repeatedly:

$$z = q_1 w + r_1$$

$$w = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$...$$

This process clearly terminates as $N(r_i)$ is a positive integer and $N(r_{i+1}) < N(r_i)$ for all i. Thus, the table of divisions with remainders must be as follows:

$$z = q_1 w + r_1$$

$$w = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

$$\dots$$

$$r_{N-3} = r_{N-2} q_{N-2} + r_{N-1}$$

$$r_{N-2} = r_{N-1} q_{N-1}$$

with $r_{N-1} \neq 0$. From above, we must have that the set of right divisors of z, w is the set as the set of right divisors of r_{N-1}. Therefore, the greatest common right divisor of z, w must be r_{N-1}. Furthermore, from substition and working backwards, there exists $\alpha, \beta \in \mathbb{I}$ such that $\alpha z + \beta w = r_{N-1}$.

21.

(i) Let $z \in \mathbb{I}$ and $n \in \mathbb{Z}$. Suppose that $(N(z), n) = 1$. Let d be a common right divisor of z and n. Then, $z = pd$ and $n = p'd$ for some $p, p' \in \mathbb{I}$. As $(N(z), n) = 1$, there exists $a, b \in \mathbb{Z}$ such that $aN(z) + bn = 1$. Thus, $a\bar{z}z + bn = 1$, and so $a\bar{z}pd + bp'd = 1$. Therefore, d is a right divisor of 1. We must have that the greatest common right divisor of z and n is 1 (up to associates). For the converse, suppose that the greatest common right divisor of z and n is 1. From the previous exercise, there exists α, β such that $\alpha z + \beta n = 1$. Then, $N(\alpha)N(z) = N(\alpha z) = N(1 - \beta n) = (1 - \beta n)(1 - \overline{\beta} n) = 1 - n(\beta + \overline{\beta}) + N(\beta)n = qn + 1$ for some $q \in \mathbb{Z}$. Let d be a divisor of $N(z)$ and n. Then, $N(z) = pd$ and $n = p'd$ so that $N(\alpha)pd = qp'd + 1$. Thus, $d \mid 1$. It follows all divisors divide 1, and so $(N(z), n) = 1$.

(ii) Let p be an odd prime. By a previous exercise, there exists a n with $0 < n < p$ such that $np = 1 + a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Let $z = 1 + ai + bj$. We have that $N(z) = 1 + a^2 + b^2 = np$. Note that $p \mid N(z)$ and $p \mid p$, thus by the previous exercise, the greatest common right divisor of z and p is not a unit. Suppose that up is a right divisor of z where u is a unit. Then, $z = (z_0 + z_1 i + z_2 j + z_3 k)up$ for some $w = z_0 + z_1 i + z_2 j + z_3 k \in \mathbb{I}$. We have that $N(z) = p^2 N(w) = np$, and so $n = pN(w)$. As $0 < n < p$, this cannot occur as the norm of a integral quarternion is an integer. Therefore, an associate of p cannot be a right divisor of z. It follows that the greatest common right divisor of p and z is not a unit and not an associate of p.

(iii) Let p be an odd prime. By the previous exercise, there exists a right divisor of p that is not a unit or an associate of p, $q \in \mathbb{I}$ say. Then, $p = xq$ for some $x \in \mathbb{I}$. As q is not a unit or an associate of p, x is not a unit. Therefore, p is not irreducible in $\mathbb{I}$. Suppose $p = 2$. Then, $p = (1 + i)(1 - i)$. We know that $1 + i, 1 - i$ are not units in $\mathbb{I}$, and so p is not irreducible. Let q be a prime integer. q is not irreducible so there exists $z, w \in \mathbb{I}$ that are not units and $q = zw$. We have that $q^2 = N(zw) = N(z)N(w)$. As q is prime and $N(z) \neq 1, N(w) \neq 1$, it must be that $N(z) = N(w) = q$. Therefore, every positive prime integer is the norm of some integral quarternions.

(iv) Let $n \in \mathbb{N}$. Then, there exists primes $p_1, \dots, p_m$ and $a_1, \dots, a_m \in \mathbb{N}$ such that $n = p_1^{a_1} \dots p_m^{a_m}$. We have that for each p_i there exists a $z_i \in \mathbb{I}$ such that $p_i = N(z_i)$. Thus,

$$n = N(z_1)^{a_1} \dots N(z_m)^{a_m} = N(z_1^{a_1} \dots z_m^{a_m})$$

Hence, n is the norm of some integral quarternion.

(v) Let $n \in \mathbb{N}$. From above, $n = N(w)$ for some $w \in \mathbb{I}$. From a previous exercise, there exists a unit $u \in \mathbb{I}$ such that $uw = a + bi + cj + dk$ where $a, b, c, d \in \mathbb{Z}$. Thus,

$$n = N(w) = N(u)N(w) = N(uw) = N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$$

And we are done.

VI - Linear Algebra

6.1 - Free Modules Revisited

4.

(i)

(ii) Let V be a Lie algebra with Lie bracket $[\cdot,\cdot] : V \times V \to V$. Let $u, v \in V$. As V is a vector space, $u+v \in V$, and so $[u+v, u+v] = 0$. Also note $[u,u] = [v,v] = 0$. We have that

$$\begin{aligned}
[u,v] + [v,u] &= [u,u] + [u,v] + [v,u] + [v,v] \\
&= [u, u+v] + [v, u+v] \\
&= [u+v, u+v] \\
&= 0
\end{aligned}$$

Hence, $[u,v] = -[v,u]$.

(iii) Suppose V is a k-algebra where k is a field. Define $[\cdot,\cdot] : V \times V \to V$ by $[u,v] = uv - vu$. Let $a, b \in k$ and $u, v, w \in V$. We have that

$$\begin{aligned}
[au + bv, w] &= (au + bv)w - w(au + bv) \\
&= auw + bvw - awu - bwv \\
&= a(uw - wu) + b(vw - wv) \\
&= a[u,w] + b[v,w]
\end{aligned}$$

$$\begin{aligned}
[w, au + bv] &= w(au + bv) - (au + bv)w \\
&= awu + bwv - auw - bvw \\
&= a[w,u] + b[w,v]
\end{aligned}$$

Furthermore, for all $v \in V$, we have that $[v,v] = vv - vv = 0$. Finally, for all $u, v, w \in V$,

$$\begin{aligned}
[[u,v],w] + [[v,w],u] + [[w,u],v] &= [uv - vu, w] + [vw - wv, u] + [wu - uw, v] \\
&= (uv - vu)w - w(uv - vu) + (vw - wv)u - u(vw - wv) + (wu - uw)v - v(wu - uw) \\
&= uvw - vuw - wuv + wvu + vwu - wvu - uvw + uwv + wuv - uwv - vwu + vuw \\
&= 0
\end{aligned}$$

Therefore, V is a Lie algebra with Lie bracket $[\cdot,\cdot]$.

(iv)

(v)

12. Let V be a vector space over a field k, and let $R = \mathrm{End}_{k-\mathsf{Vect}}(V)$ be its ring of endomorphisms.

(i) Let Z be an R-module and $f_i : Z \to R$ be R-module homomorphisms for $i = 1,2,3,4$. If $\varphi(u,v) = (\psi_1(u,v), \psi_2(u,v)) \in \mathrm{End}_{k-\mathsf{Vect}}(V \oplus V)$, define the maps $\pi_i : \mathrm{End}_{k-\mathsf{Vect}}(V \oplus V) \to R$ for $i = 1,2,3,4$ by $\pi_1(\varphi) = \psi_1(u,0), \pi_2(\varphi) = \psi_1(0,v), \pi_3(\varphi) = \psi_2(u,0)$ and $\pi_4(\varphi) = \psi_2(0,v)$. Let $\varphi = (\psi_1, \psi_2)$ and $\varphi' = (\psi_1', \psi_2')$ be elements of $\mathrm{End}_{k-\mathsf{Vect}}(V \oplus V)$ and $r(u) \in R$. We have that

$$\begin{aligned}
\pi_1(\varphi + \varphi') &= \pi_1((\psi_1, \psi_2) + (\psi_1', \psi_2')) \\
&= \pi_1((\psi_1 + \psi_1', \psi_2 + \psi_2')) \\
&= (\psi_1 + \psi_1')(u,0) \\
&= \psi_1(u,0) + \psi_1'(u,0) \\
&= \pi_1((\psi_1, \psi_2)) + \pi_1((\psi_1', \psi_2')) \\
&= \pi_1(\varphi) + \pi_1(\varphi')
\end{aligned}$$

$$\begin{aligned}
\pi_1(r\cdot\varphi) &= \pi_1(r(u)\cdot(\psi_1,\psi_2))\\
&= \pi_1((r\circ\psi_1, r\circ\psi_2))\\
&= (r\circ\psi_1)(u,0)\\
&= r(\psi_1(u,0))\\
&= r\cdot\pi((\psi_1,\psi_2))\\
&= r\pi_1(\varphi)
\end{aligned}$$

In a similar way, π_2,π_3,π_4 are also R-module homomorphisms. Suppose that the following diagram is commutative for $i=1,2,3,4$:

$$\begin{tikzcd}
 & \mathrm{End}_{k-\mathsf{Vect}}(V\oplus V) \arrow[d, "\pi_i"] \\
Z \arrow[ur, "f"] \arrow[r, "f_i"'] & R = \mathrm{End}_{k-\mathsf{Vect}}(V)
\end{tikzcd}$$

for some $f: Z\to \mathrm{End}_{k-\mathsf{Vect}}(V\oplus V)$. For $z\in Z$, we have that $f(z)\in \mathrm{End}_{k-\mathsf{Vect}}(V\oplus V)$. For $u,v\in V$, we may write $f(z)[u,v]=(\psi_1(u,v),\psi_2(u,v))$. As the above diagram is commutative, we have that for each z and u,v, $\pi_1(f(z)[u,v])=f_1$ so $\psi_1(u,0)=f_1(z)[u]$. Similarly, $\psi_1(0,v)=f_2(z)[v], \psi_2(u,0)=f_3(z)[u]$ and $\psi_2(0,v)=f_4(z)[v]$. Hence, $f(z)[u,v]=(\psi_1(u,v),\psi_2(u,v))=(\psi_1(u,0)+\psi_1(0,v),\psi_2(u,0)+\psi_2(0,v))=(f_1(z)[u]+f_2(z)[v], f_3(z)[u]+f_4(z)[v])$. Hence, f is unique. We prove that f is a homomorphism. Let $z,w\in Z$ and $r\in R$. Then,

$$\begin{aligned}
f(z+w)[u,v] &= (f_1(z+w)[u]+f_2(z+w)[v], f_3(z+w)[u]+f_4(z+w)[v])\\
&= (f_1(z)[u]+f_1(w)[u]+f_2(z)[v]+f_2(w)[v], f_3(z)[u]+f_3(w)[u]+f_4(z)[v]+f_4(w)[v])\\
&= (f_1(z)[u]+f_2(z)[v], f_3(z)[u]+f_4(z)[v])+(f_1(w)[u]+f_2(w)[v], f_3(w)[u]+f_4(w)[v])\\
&= f(z)[u,v]+f(w)[u,v]
\end{aligned}$$

$$\begin{aligned}
f(rz) &= (f_1(rz)[u]+f_2(rz)[v], f_3(rz)[u]+f_4(rz)[v])\\
&= (rf_1(z)[u]+rf_2(z)[v], rf_3(z)[u]+rf_4(z)[v])\\
&= r(f_1(z)[u]+f_2(z)[v], f_3(z)[u]+f_4(z)[v])\\
&= rf(z)
\end{aligned}$$

using the properties of R-module homomorphisms as f_i are R-module homomorphisms via assumption. It follows that $\mathrm{End}_{k-\mathsf{Vect}}(V\oplus V)$ satisfies the universal property for R^4. Therefore, $\mathrm{End}_{k-\mathsf{Vect}}(V\oplus V)\cong R^4$.

(ii)