

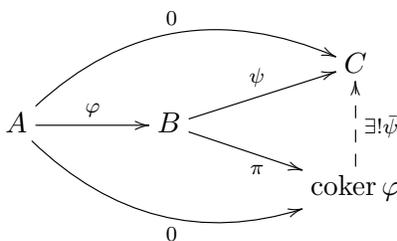
Problem 1. Cokernels in Ab. Let $\varphi : A \rightarrow B$ be a homomorphism of **abelian** groups.

- (a) State the universal property of the cokernel $\pi : B \rightarrow \text{coker } \varphi$.

We say that $\pi : B \rightarrow \text{coker } \varphi$ is the cokernel of $\varphi : A \rightarrow B$ if

- $\pi \circ \varphi = 0$, and
- for all homomorphisms $\psi : B \rightarrow C$ such that $\psi \circ \varphi = 0$, there exists a unique homomorphism $\bar{\psi} : \text{coker } \varphi \rightarrow C$ such that $\bar{\psi} \circ \pi = \psi$.

We can summarize these two conditions with the following diagram:

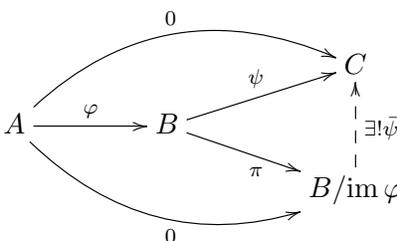


- (b) State the universal property of the quotient homomorphism $\pi : B \rightarrow B/\text{im } \varphi$.

We say that $\pi : B \rightarrow B/\text{im } \varphi$ is a quotient homomorphism if

- $\text{im } \varphi \subseteq \ker \pi$, and
- for all homomorphisms $\psi : B \rightarrow C$ such that $\text{im } \varphi \subseteq \ker \psi$, there exists a unique homomorphism $\bar{\psi} : B/\text{im } \varphi \rightarrow C$ such that $\bar{\psi} \circ \pi = \psi$.

We can summarize these two conditions with the following diagram:



- (c) Use your answers from (a) and (b) to show that $\pi : B \rightarrow B/\text{im } \varphi$ is the cokernel of φ .

Observe that the two diagrams are the same.

[Remark: This argument also works in the category Grp as long as $\text{im } \varphi \subseteq B$ is a normal subgroup. More generally, the cokernel of $\varphi : A \rightarrow B$ is the quotient homomorphism $\pi : B \rightarrow B/\langle \text{im } \varphi \rangle^B$, where $\langle \text{im } \varphi \rangle^B$ is the conjugate closure of $\text{im } \varphi$ in B .]

Problem 2. Independent and Spanning Sets. Let R be a ring. By an “ R -module” we will mean a **left** R -module.

- (a) State the universal property of the free R -module generated by the set A .

We say that F is the free R -module generated by A if

- we have a set function $i : A \rightarrow F$, and

- for all R -modules M and set functions $j : A \rightarrow M$ there exists a unique R -module homomorphism $\varphi : F \rightarrow M$ such that $\varphi \circ i = j$.

We can summarize these two conditions with the following diagram:

$$\begin{array}{ccc}
 F & \overset{\exists! \varphi}{\dashrightarrow} & M \\
 & \swarrow i & \nearrow j \\
 & A &
 \end{array}$$

- (b) Let M be an R -module and let $A \rightarrow M$ be an indexed subset of M . State what it means for this subset to be: (1) R -linearly independent, (2) R -spanning, and (3) an R -basis. Use the universal property from part (a) in your answer.

Consider an indexed subset $j : A \rightarrow M$ and let $i : A \rightarrow F$ be the free module generated by A . Then by part (a) there exists a canonical R -module homomorphism $\varphi : F \rightarrow M$ such that $\varphi \circ i = j$. We say that

- (1) $A \rightarrow M$ is R -linearly independent if φ is injective,
- (2) $A \rightarrow M$ is R -spanning if φ is surjective,
- (3) $A \rightarrow M$ is an R -basis if φ is bijective.

- (c) Prove that an R -module has a basis if and only if it free.

Proof. If $i : A \rightarrow F$ is the free module generated by A then the canonical homomorphism $\varphi : F \rightarrow F$ is the identity map. Since the identity map is bijective we conclude that $A \rightarrow F$ is a basis. Conversely, let M be an R -module and let $j : A \rightarrow M$ be a basis. If $i : A \rightarrow F$ is the free module generated by A this means that the canonical morphism $\varphi : F \rightarrow M$ satisfying $\varphi \circ i = j$ is a bijection, hence it is an isomorphism of R -modules. \square

[Remark: In the next problem I will use the fact that the free R -module F generated by $i : A \rightarrow F$ can be identified with the collection of formal sums $\sum_{a \in A} r_a i_a$ in which $r_a = 0$ for all but finitely many $a \in A$.]

Problem 3. Vector Spaces are Free. Let K be a field and let V be a K -module.

- (a) Prove that every minimal K -spanning subset of V is a basis.

Proof. Let $j : A \rightarrow V$ be a minimal spanning set and assume for contradiction that there exists a linear relation

$$\sum_{a \in A} r_a j_a = 0$$

in which $r_{a'} \neq 0$ for some $a' \in A$. Then since K is a field we can divide by $r_{a'}$ to get

$$j_{a'} = \sum_{a \neq a'} \left(-\frac{r_a}{r_{a'}} \right) j_a.$$

Finally, given any element $u = \sum_{a \in A} s_a j_a \in V$ we can write

$$u = \sum_{a \neq a'} \left(s_a - \frac{s_{a'} r_a}{r_{a'}} \right) j_a,$$

which contradicts the minimality of $j : A \rightarrow V$. We conclude that $j : A \rightarrow V$ is K -linearly independent, hence it is a basis. \square

- (b) Prove that every maximal K -independent subset of V is a basis. [It then follows from Zorn's Lemma that every vector space has a basis, but don't prove this.]

Proof. Let $j : A \rightarrow V$ be a maximal K -independent set. To show that the set is K -spanning, consider any $u \in V \setminus \text{im } j$. By maximality of $j : A \rightarrow V$ there exists a K -linear relation

$$ru + \sum_{a \in A} r_a j_a = 0$$

in which not all coefficients are zero. If $r = 0$ then we obtain a nontrivial relation $\sum_{a \in A} r_a j_a = 0$, which contradicts the independence of A . Hence $r \neq 0$. Then since K is a field we can divide by r to obtain

$$u = \sum_{a \in A} \left(-\frac{r_a}{r} \right) j_a.$$

We conclude that $j : A \rightarrow V$ is a K -spanning set, hence it is a basis. \square

- (c) If the vector space V is **finitely generated**, prove (without using Zorn's Lemma) that V has a basis. [Hint: Let $u_1, u_2, \dots, u_n \in V$ be a K -spanning set. If this set is **not** K -linearly independent then ...]

Proof. Let $u_1, u_2, \dots, u_n \in V$ be a K -spanning set. If this set is not K -linearly independent then we know from part (a) that the K -spanning set is **not minimal**. That is, there exists an element u_i such that $\{u_1, \dots, u_n\} \setminus \{u_i\}$ is still a K -spanning set. If this smaller set is still not K -linearly independent we can repeat the argument until a K -linearly independent K -spanning set is reached. \square

Problem 4. Cyclic Modules. Let R be a ring. We say that a (left) R -module M is cyclic if it has an R -spanning set of size one.

- (a) If $I \subseteq R$ is a (left) ideal, prove that the abelian quotient group R/I is a (left) R -module (i.e., construct a well-defined (left) linear R -action).

Proof. For all $r \in R$ and $s + I \in R/I$ we will define $r(s + I) := rs + I$. To show that this operation is well-defined, suppose that $s_1 + I = s_2 + I$, i.e., $s_1 - s_2 \in I$. Then since I is a left ideal we have

$$rs_1 - rs_2 = r(s_1 - s_2) \in I,$$

and it follows that $r(s_1 + I) = rs_1 + I = rs_2 + I = r(s_2 + I)$ as desired. Then to show that the (well-defined) operation $\lambda_r(s + I) = rs + I$ defines a ring homomorphism $\lambda : R \rightarrow \text{End}_{\text{Ab}}(R/I)$, note that for all $r_1, r_2 \in R$ and $s + I \in R/I$ we have

$$\begin{aligned} (r_1 + r_2)(s + I) &= (r_1 + r_2)s + I \\ &= (r_1s + r_2s) + I \\ &= (rs_1 + I) + (rs_2 + I) \\ &= r_1(s + I) + r_2(s + I) \end{aligned}$$

and

$$\begin{aligned} (r_1r_2)(s + I) &= (r_1r_2)s + I \\ &= r_1(r_2s) + I \\ &= r_1(r_2s + I) \end{aligned}$$

$$= r_1(r_2(s + I));$$

note that for all $r \in R$ and $s_1 + I, s_2 + I \in R/I$ we have

$$\begin{aligned} r((s_1 + I) + (s_2 + I)) &= r((s_1 + s_2) + I) \\ &= r(s_1 + s_2) + I \\ &= (rs_1 + rs_2) + I \\ &= (rs_1 + I) + (rs_2 + I) \\ &= r(s_1 + I) + r(s_2 + I); \end{aligned}$$

and, finally, note that for all $s + I \in R/I$ we have $1(s + I) = 1s + I = s + I$. \square

(b) Let $I \subseteq R$ be a (left) ideal of R . Prove that the (left) R -module R/I is cyclic.

Proof. I claim that $\{1 + I\} \subseteq R/I$ is an R -spanning set of size one. Indeed, for all $r + I \in R/I$ we have $r + I = r(1 + I)$. \square

(c) If M is a cyclic (left) R -module, prove we have $M \approx R/I$ for some (left) ideal $I \subseteq R$. [Hint: Use the definition of spanning from Problem 2(b).]

Proof. If $\{m\} \subseteq M$ is an R -spanning set then we obtain a canonical surjective R -module homomorphism $\varphi : R \rightarrow M$ defined by $m \mapsto rm$. [We can think of R as the free R -module generated by one element.] Then by the 1st Isomorphism Theorem for modules we obtain an isomorphism $M = \text{im } \varphi \approx R/\ker \varphi$, where $\ker \varphi$ is a left R -submodule of R (i.e., a left ideal). \square