R.6. Proofs: Modules

Proposition R.6.1. — *Let M be a left R-module and let N be a subgroup of M. Then the cosets of N in M partition M.*

Proof. —
To show: (a) If $m \in M$ then there exists $m' \in M$ such that $m \in m' + N$.
(b) If $(m_1 + N) \cap (m_2 + N) \neq \emptyset$ then $m_1 + N = m_2 + N$.

(a) Let $m \in M$.
Since $0 \in N$ then $m = m + 0 \in m + N$.
So $m \in m + N$.

(b) Assume $(m_1 + N) \cap (m_2 + N) \neq \emptyset$.
To show: (ba) $m_1 + N \subseteq m_2 + N$.
(bb) $m_2 + N \subseteq m_1 + N$.
Let $a \in (m_1 + N) \cap (m_2 + N)$.
So there exist $n_1, n_2 \in$N such that $a = m_1 + n_1$ and $a = m_2 + n_2$.
Then

$$m_1 = m_1 + n_1 - n_1 = a - n_1 = m_2 + n_2 - n_1 \quad \text{and}$$
$$m_2 = m_2 + n_2 - n_2 = a - n_2 = m_1 + n_1 - n_2.$$

(ba) Let $m \in m_1 + N$.
Then there exists $n \in N$ such that $m = m_1 + n$.
Then

$$m = m_1 + n = m_2 + n_2 - n_1 + n \in m_2 + N,$$

since $n_2 - n_1 + n \in N$.
So $m_1 + N \subseteq m_2 + N$.

(bb) Let $m \in m_2 + N$.
Then there exists $n \in N$ such that $m = m_2 + n$.
Since $n_1 - n_2 + n \in N$ then

$$m = m_2 + n = m_1 + n_1 - n_2 + n \in m_1 + N,$$

So $m_2 + N \subseteq m_1 + N$.

So $m_1 + N = m_2 + N$.

So the cosets of N in M partition M. □

Theorem R.6.2. — *Let N be a subgroup of a left R-module M. Then N is a submodule of M if and only if M/N with the operations given by*

$$(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N, \quad \textit{and}$$
$$r(m_1 + N) = rm_1 + N,$$

is a left R-module.

Proof. —
$\Longrightarrow$: Assume N is a submodule of M.
To show: (a) $(m_1 + N) + (m_2 + N) = (m_1 + m_2) + N$ is a well defined operation on M/N.
(b) The operation given by $r(m + N) = rm + N$ is well defined.

Notes of Arun Ram aram@unimelb.edu.au, Version: 7 April 2020

(c) If $m_1+N, m_2+N, m_3+N \in M/N$ then $\big((m_1+N)+(m_2+N)\big)+(m_3+N) = (m_1+N)+\big((m_2+N)+(m_3+N)\big)$.

(d) If $m_1+N, m_2+N \in M/N$ then $(m_1+N)+(m_2+N) = (m_2+N)+(m_1+N)$.

(e) $0+N = N$ is the zero in M/N.

(f) $-m+N$ is the additive inverse of $m+N$.

(g) If $r_1, r_2 \in R$ and $m+N \in M/N$, then $r_1\big(r_2(m+N)\big) = (r_1r_2)(m+N)$.

(h) If $m+N \in M/N$ then $1(m+N) = m+N$.

(i) If $r \in R$ and $m_1+N, m_2+N \in M/N$ then $r\big((m_1+N)+(m_2+N)\big) = r(m_1+N)+r(m_2+N)$.

(j) If $r_1, r_2 \in R$ and $m+N \in M/N$, then $(r_1+r_2)(m+N) = r_1(m+N)+r_2(m+N)$.

(a) We want the operation on M/N given by

$$\begin{array}{ccc} M/N \times M/N & \to & M/N \\ (m_1+N, m_2+N) & \mapsto & (m_1+m_2)+N \end{array}$$

to be well defined, i.e. a function.

Let $(m_1+N, m_2+N), (m_3+N, m_4+N) \in M/N \times M/N$ such that $(m_1+N, m_2+N) = (m_3+N, m_4+N)$.

Then $m_1+N = m_3+N$ and $m_2+N = m_4+N$.

To show: $(m_1+m_2)+N = (m_3+m_4)+N$.

To show: (aa) $(m_1+m_2)+N \subseteq (m_3+m_4)+N$.

(ab) $(m_3+m_4)+N \subseteq (m_1+m_2)+N$.

(aa) Since $m_1+N = m_3+N$ then $m_1 = m_1+0 \in m_3+N$

So there exists $k_1 \in N$ such that $m_1 = m_3+k_1$.

Similarly there exists $k_2 \in N$ such that $m_2 = m_4+k_2$.

Let $t \in (m_1+m_2)+N$.

Then there exists $k \in N$ such that $t = m_1+m_2+k$ for some $k \in N$.

Since addition is commutative then

$$\begin{aligned} t &= m_1+m_2+k \\ &= m_3+k_1+m_4+k_2+k \\ &= m_3+m_4+k_1+k_2+k. \end{aligned}$$

So $t = (m_3+m_4)+(k_1+k_2+k) \in m_3+m_4+N$.

So $(m_1+m_2)+N \subseteq (m_3+m_4)+N$.

(ab) Since $m_1+N = m_3+N$ then there exists $k_1 \in N$ such that $m_1+k_1 = m_3$.

Since $m_2+N = m_4+N$ then there exists $k_2 \in N$ such that $m_2+k_2 = m_4$.

Let $t \in (m_3+m_4)+N$.

Then there exists $k \in N$ such that $t = m_3+m_4+k$.

So

$$\begin{aligned} t &= m_3+m_4+k \\ &= m_1+k_1+m_2+k_2+k \\ &= m_1+m_2+k_1+k_2+k, \end{aligned}$$

since addition is commutative.

So $t = (m_1+m_2)+(k_1+k_2+k) \in (m_1+m_2)+N$.

So $(m_3+m_4)+N \subseteq (m_1+m_2)+N$.

So $(m_1+m_2)+N = (m_3+m_4)+N$.

So the operation given by $(m_1 + N) + (m_3 + N) = (m_1 + m_3) + N$ is a well defined operation on M/N.

(b) We want the operation given by

$$\begin{array}{rcl} R \times M/N & \to & M/N \\ (r, m + N) & \mapsto & rm + N \end{array}$$

to be well defined, i.e. a function.
Let $(r_1, m_1+N), (r_2, m_2+N) \in (R \times M/N)$ such that $(r_1, m_1+N) = (r_2, m_2+N)$.
Then $r_1 = r_2$ and $m_1 + N = m_2 + N$.
To show: $r_1m_1 + N = r_2m_2 + N$.
To show: (ba) $r_1m_1 + N \subseteq r_2m_2 + N$.
(bb) $r_2m_2 + N \subseteq r_1m_1 + N$.

(ba) Since $m_1+N = m_2+N$ then there exists $n_2 \in N$ such that $m_1 = m_2+n_2$.
Let $k \in r_1m_1 + N$.
Then there exists $n \in N$ such that $k = r_1m_1 + n$.
So

$$\begin{aligned} k &= r_1m_1 + n \\ &= r_2(m_2 + n_2) + n \\ &= r_2m_2 + r_2n_2 + n. \end{aligned}$$

Since N is a submodule then $r_2n_2 \in N$ and $r_2n_2 + n \in N$.
So $k = r_2m_2 + r_2n_2 + n \in r_2m_2 + N$.
So $r_1m_1 + N \subseteq r_2m_2 + N$.

(bb) Since $m_1+N = m_2+N$ then there exists $n_1 \in N$ such that $m_2 = m_1+n_1$.
Let $k \in r_2m_2 + N$.
Then there exists $n \in N$ such that $k = r_2m_2 + n$. So

$$\begin{aligned} k &= r_2m_2 + n \\ &= r_1(m_1 + n_1) + n \\ &= r_1m_1 + r_1n_1 + n. \end{aligned}$$

Since N is a submodule then $r_1n_1 \in N$ and $r_1n_1 + n \in N$.
So $k = r_1m_1 + r_1n_1 + n \in r_1m_1 + N$.
So $r_2m_2 + N \subseteq r_1m_1 + N$.
So $r_1m_1 + N = r_2m_2 + N$.

So the operation is well defined.

(c) By the associativity of addition in M and the definition of the operation in M/N, if $m_1 + N, m_2 + N, m_3 + N \in M/N$ then

$$\begin{aligned} \big((m_1 + N) + (m_2 + N)\big) + (m_3 + N) &= \big((m_1 + m_2) + N\big) + (m_3 + N) \\ &= \big((m_1 + m_2) + m_3\big) + N \\ &= \big(m_1 + (m_2 + m_3)\big) + N \\ &= (m_1 + N) + \big((m_2 + m_3) + N\big) \\ &= (m_1 + N) + \big((m_2 + N) + (m_3 + N)\big). \end{aligned}$$

(d) By the commutativity of addition in M and the definition of the operation in M/N, if $m_1 + N, m_2 + N \in M/N$ then

$$\begin{aligned}(m_1 + N) + (m_2 + N) &= (m_1 + m_2) + N \\ &= (m_2 + m_1) + N \\ &= (m_2 + N) + (m_1 + N).\end{aligned}$$

(e) The coset $N = 0 + N$ is the zero in M/N since If $m + N \in M/N$ then

$$\begin{aligned}N + (m + N) &= (0 + m) + N \\ &= m + N \\ &= (m + 0) + N = (m + N) + N\end{aligned}$$

(f) If $m + N \in M/N$ then

$$\begin{aligned}(m + N) + (-m + N) &= m + (-m) + N \\ &= 0 + N \\ &= N \\ &= (-m + m) + N \\ &= (-m + N) + (m + N)\end{aligned}$$

So the additive inverse of $m + N$ is $(-m) + N$.

(g) Assume $r_1, r_2 \in R$ and $m + N \in M/N$.
Then, by definition of the operation,

$$\begin{aligned}r_1\big(r_2(m + N)\big) &= r_1(r_2 m + N) \\ &= r_1(r_2 m) + N \\ &= (r_1 r_2)m + N \\ &= (r_1 r_2)(m + N).\end{aligned}$$

(h) Assume $m + N \in M/N$.
Then, by definition of the operation,

$$\begin{aligned}1(m + N) &= (1m) + N \\ &= m + N.\end{aligned}$$

(i) Assume $r \in R$ and $m_1 + N, m_2 + N \in M/N$.
Then

$$\begin{aligned}r\big((m_1 + N) + (m_2 + N)\big) &= r\big((m_1 + m_2) + N\big) \\ &= r(m_1 + m_2) + N \\ &= (rm_1 + rm_2) + N \\ &= (rm_1 + N) + (rm_2 + N) \\ &= r(m_1 + N) + r(m_2 + N).\end{aligned}$$

(j) Assume $r_1, r_2 \in R$ and $m + N \in M/N$.

Then

$$\begin{aligned}(r_1+r_2)(m+N) &= \big((r_1+r_2)m\big)+N \\ &= (r_1m+r_2m)+N \\ &= (r_1m+N)+(r_2m+N) \\ &= r_1(m+N)+r_2(m+N).\end{aligned}$$

So M/N is a left R-module.

$\Longleftarrow$: Assume N is a subgroup of M and (M/N) is a left R-module with action given by $r(m+N)=rm+N$.

To show: N is a submodule of M.

To show: If $r\in R$ and $n\in N$ then $rn\in N$.

First we show: If $n\in N$ then $n+N=N$.

To show: (a) $n+N\subseteq N$.

(b) $N\subseteq n+N$.

(a) Let $k\in n+N$.
So there exists $n_1\in N$ such that $k=n+n_1$.
Since N is a subgroup, $k=n+n_1\in N$.
So $n+N\subseteq N$.

(b) Let $k\in N$.
Since $k-n\in N$ then $k=n+(k-n)\in n+N$.
So $N\subseteq n+N$.
Now assume $r\in R$ and $n\in N$.
Then, by definition of the R-action on M/N,

$$\begin{aligned}rn+N &= r(n+N) \\ &= r(0+N) \\ &= r\cdot 0+N \\ &= 0+N \\ &= N.\end{aligned}$$

So $rn=rn+0\in N$.

So N is a submodule of M.

□

Proposition R.6.3. — *Let $f\colon M\to N$ be an R-module homomorphism. Then*
(a) $\ker f$ *is a submodule of* M.
(b) $\mathrm{im} f$ *is a submodule of* N.

Proof. —

(a) By condition (a) in the definition of R-module homomorphism, f is a group homomorphism.
By Proposition 1.1.13 (a)REFERENCE FIX THIS, $\ker f$ is a subgroup of M.
To show: If $r\in R$ and $k\in\ker f$ then $rk\in\ker f$.
Assume $r\in R$ and $k\in\ker f$.
Then, by the definition of R-module homomorphism,

$$f(rk)=rf(k)=r\cdot 0=0.$$

So $rk\in\ker f$.
So $\ker f$ is a submodule of M.

(b) By condition (a) in the definition of R-module homomorphism, f is a group homomorphism.
By Proposition 1.1.13 (b)REFERENCE FIX THIS, $\mathrm{im} f$ is a subgroup of N.
To show: If $r \in R$ and $a \in \mathrm{im} f$ then $ra \in \mathrm{im} f$.
Assume $r \in R$ and $a \in \mathrm{im} f$.
Then there exists $m \in M$ such that $a = f(m)$.
By the definition of R-module homomorphism,

$$ra = rf(m) = f(rm).$$

So $ra \in \mathrm{im} f$.
So $\mathrm{im} f$ is a submodule of N. □

Proposition R.6.4. — *Let $f: M \to N$ be an R-module homomorphism. Let 0_M be the zero in M. Then*
(a) $\ker f = (0_M)$ *if and only if f is injective.*
(b) $\mathrm{im} f = N$ *if and only if f is surjective.*

Proof. — Let 0_M and 0_N be the zeros in M and N respectively.
(a) $\Longrightarrow$: Assume $\ker f = \{0_M\}$.
To show: If $f(m_1) = f(m_2)$ then $m_1 = m_2$.
Assume $f(m_1) = f(m_2)$.
Then, by the fact that f is a homomorphism,

$$0_N = f(m_1) - f(m_2) = f(m_1 - m_2).$$

So $m_1 - m_2 \in \ker f$.
Since $\ker f = \{0_M\}$ then $m_1 - m_2 = 0_M$.
So $m_1 = m_2$.
So f is injective.

$\Longleftarrow$: Assume f is injective.
To show: (aa) $\{0_M\} \subseteq \ker f$.
(ab) $\ker f \subseteq \{0_M\}$.
(aa) Since $f(0_M) = 0_N$ then $0_M \in \ker f$.
So $\{0_M\} \subseteq \ker f$.
(ab) Let $k \in \ker f$.
Then $f(k) = 0_N$.
So $f(k) = f(0_M)$.
Thus, since f is injective then $k = 0_M$.
So $\ker f \subseteq (0_M)$.
So $\ker f = (0_M)$.
(b) $\Longrightarrow$: Assume $\mathrm{im} f = N$.
To show: If $n \in N$ then there exists $m \in M$ such that $f(m) = n$.
Assume $n \in N$.
Then $n \in \mathrm{im} f$.
So there exists $m \in M$ such that $f(m) = n$.
So f is surjective.

$\Longleftarrow$: Assume f is surjective.
To show: (ba) $\mathrm{im} f \subseteq N$.
(bb) $N \subseteq \mathrm{im} f$.

(ba) Let $x \in \mathrm{im} f$.
Then there exists $m \in M$ such that $x = f(m)$.
By the definition of f, $f(m) \in N$.
So $x \in N$.
So $\mathrm{im} f \subseteq N$.

(bb) Assume $x \in N$.
Since f is surjective there exists $m \in M$ such that $f(m) = x$.
So $x \in \mathrm{im} f$.
So $N \subseteq \mathrm{im} f$.

So $\mathrm{im} f = N$.

□

Theorem R.6.5. —
(a) *Let $f\colon M \to N$ be an R-module homomorphism and let $K = \ker f$. Define*

$$\begin{array}{rccc} \hat{f}\colon & M/\ker f & \to & N \\ & m + K & \mapsto & f(m). \end{array}$$

Then $\hat{f}$ is a well defined injective R-module homomorphism.
(b) *Let $f\colon M \to N$ be an R-module homomorphism and define*

$$\begin{array}{rccc} f'\colon & M & \to & \mathrm{im} f \\ & m & \mapsto & f(m). \end{array}$$

Then f' is a well defined surjective R-module homomorphism.
(c) *If $f\colon M \to N$ is an R-module homomorphism, then*

$$M/\ker f \simeq \mathrm{im} f$$

where the isomorphism is an R-module isomorphism.

Proof. —

(a) To show: (aa) $\hat{f}$ is well defined.
(ab) $\hat{f}$ is injective.
(ac) $\hat{f}$ is an R-module homomorphism.

(aa) To show: (aa) If $m \in M$ then $\hat{f}(m + K) \in N$.
(aab) If $m_1 + K = m_2 + K \in M/K$ then $\hat{f}(m_1 + K) = \hat{f}(m_2 + K)$.

(aaa) Assume $m \in M$.
$\hat{f}(m + K) = f(m)$ and $f(m) \in N$, by the definition of $\hat{f}$ and f.

(aab) Assume $m_1 + K = m_2 + K$.
Then there exists $k \in K$ such that $m_1 = m_2 + k$.
To show: $\hat{f}(m_1 + K) = \hat{f}(m_2 + K)$, i.e.,
To show: $f(m_1) = f(m_2)$.
Since $k \in \ker f$ then $f(k) = 0$ and

$$f(m_1) = f(m_2 + k) = f(m_2) + f(k) = f(m_2) + 0 = f(m_2).$$

So $\hat{f}(m_1 + K) = \hat{f}(m_2 + K)$.

So $\hat{f}$ is well defined.

(ab) To show: If $\hat{f}(m_1 + K) = \hat{f}(m_2 + K)$ then $m_1 + K = m_2 + K$.
Assume $\hat{f}(m_1 + K) = \hat{f}(m_2 + K)$.
Then $f(m_1) = f(m_2)$.
So $f(m_1) - f(m_2) = 0$.

So $f(m_1 - m_2) = 0$.
So $m_1 - m_2 \in \ker f$.
So there exists $k \in \ker f$ such that $m_1 - m_2 = k$.
So there exists $k \in \ker f$ such that $m_1 = m_2 + k$.
To show: (aba) $m_1 + K \subseteq m_2 + K$.
(abb) $m_2 + K \subseteq m_1 + K$.

(aba) Let $m \in m_1 + K$.
Then there exists $k_1 \in K$ such that $m = m_1 + k_1$.
So $m = m_2 + k + k_1 \in m_2 + K$, since $k + k_1 \in K$.
So $m_1 + K \subseteq m_2 + K$.

(abb) Let $m \in m_2 + K$.
Then there exists $k_2 \in K$ such that $m = m_2 + k_2$,
So $m = m_1 - k + k_2 \in m_1 + K$ since $-k + k_2 \in K$.
So $m_2 + K \subseteq m_1 + K$.
So $m_1 + K = m_2 + K$.

So $\hat{f}$ is injective.

(ac) To show: (aca)If $m_1 + K, m_2 + K \in M/K$ then $\hat{f}(m_1 + K) + \hat{f}(m_2 + K) = \hat{f}\big((m_1 + K) + (m_2 + K)\big)$.
(acb) If $r \in R$ and $m + K \in M/K$ then $\hat{f}\big(r(m+K)\big) = r\hat{f}(m+K)$.

(aca) Let $m_1 + K, m_2 + K \in M/K$.
Since f is a homomorphism,

$$\begin{aligned}
\hat{f}(m_1 + K) + \hat{f}(m_2 + K) &= f(m_1) + f(m_2) \\
&= f(m_1 + m_2) \\
&= \hat{f}\big((m_1 + m_2) + K\big) \\
&= \hat{f}\big((m_1 + K) + (m_2 + K)\big).
\end{aligned}$$

(acb) Let $r \in R$ and $m + K \in M/K$.
Since f is a homomorphism,

$$\begin{aligned}
\hat{f}\big(r(m + K)\big) &= \hat{f}(rm + K) \\
&= f(rm) \\
&= rf(m) \\
&= r\hat{f}(m + K).
\end{aligned}$$

So $\hat{f}$ is an R-module homomorphism.

So $\hat{f}$ is a well defined injective R-module homomorphism.

(b) To show: (ba) f' is well defined.
(bb) f' is surjective.
(bc) f' is an R-module homomorphism.

(ba) and (bb) are proved in Ex. 2.2.3 a), Part I. YIKES FIX THIS

(bc) To show: (bca) If $m_1, m_2 \in M$ then $f'(m_1 + m_2) = f'(m_1) + f'(m_2)$.
(bcb) If $r \in R$ and $m \in M$ then $f'(rm) = rf'(m)$.

(bca) Let $m_1, m_2 \in M$.
Then, since f is a homomorphism,

$$f'(m_1 + m_2) = f(m_1 + m_2) = f(m_1) + f(m_2) = f'(m_1) + f'(m_2).$$

(bcb) Let $m_1, m_2 \in M$.

Then, since f is an R-module homomorphism,

$$f'(rm) = f(rm) = rf(m) = rf'(m).$$

So f' is an R-module homomorphism.

So f' is a well defined surjective R-module homomorphism.

(c) Let $K = \ker f$.

By (a), the function

$$\begin{array}{cccc} \hat{f}\colon & M/K & \to & N \\ & m+K & \mapsto & f(m) \end{array}$$

is a well defined injective R-module homomorphism.

By (b), the function

$$\begin{array}{ccccc} \hat{f}'\colon & M/K & \to & \operatorname{im} \hat{f} & \\ & m+K & \mapsto & \hat{f}(m+K) & = f(m) \end{array}$$

is a well defined surjective R-module homomorphism.

To show: (ca) $\operatorname{im} \hat{f} = \operatorname{im} f$.

(cb) $\hat{f}'$ is injective.

(ca) To show: (caa) $\operatorname{im} \hat{f} \subseteq \operatorname{im} f$.

(cab) $\operatorname{im} f \subseteq \operatorname{im} \hat{f}$.

(caa) Let $n \in \operatorname{im} \hat{f}$.

Then there is some $m + K \in M/K$ such that $\hat{f}(m+K) = n$.

Let $m' \in m + K$.

Then there exists $k \in K$ such that $m' = m + k$.

Then, since f is a homomorphism and $f(k) = 0$,

$$\begin{aligned} f(m') &= f(m+k) \\ &= f(m) + f(k) \\ &= f(m) \\ &= \hat{f}(m+k) \\ &= n. \end{aligned}$$

So $n \in \operatorname{im} f$.

So $\operatorname{im}\hat{f} \subseteq \operatorname{im} f$.

(cab) Let $n \in \operatorname{im} f$.

Then there exists $m \in M$ such that $f(m) = n$.

So $\hat{f}(m+K) = f(m) = n$.

So $n \in \operatorname{im} \hat{f}$.

So $\operatorname{im} f \subseteq \operatorname{im} \hat{f}$.

So $\operatorname{im} f = \operatorname{im} \hat{f}$.

(cb) To show: If $\hat{f}'(m_1 + K) = \hat{f}'(m_2 + K)$ then $m_1 + K = m_2 + K$.

Assume $\hat{f}'(m_1 + K) = \hat{f}'(m_2 + K)$.

Then $\hat{f}(m_1 + K) = \hat{f}(m_2 + K)$.

Since $\hat{f}$ is injective then $m_1 + K = m_2 + K$.

So $\hat{f}'$ is injective.

Thus

$$\begin{array}{cccc} \hat{f}'\colon & M/K & \to & \operatorname{im} f \\ & m+K & \mapsto & f(m) \end{array}$$

is a well defined bijective R-module homomorphism.

$\square$