Лекция 1

Предварителни сведения за модули

1. Модули, бимодули

Навсякъде в настоящия курс разглежданите пръстени R са асоциативни и имат единица 1_R, освен ако не е специално указано. Да напомним, че асоциативен пръстен с единица R е абелева група $(R,+)$, в която е въведено умножение, изпълняващо асоциативния закон $(ab)c = a(bc)$ за произволни $a, b, c \in R$, съществува неутрален елемент относно умножението 1_R и са в сила дистрибутивни закони за събиране и умножение.
Накратко, R-модули са линейните пространства над R. Именно:

ОПРЕДЕЛЕНИЕ 1.1. *Непразното множество M е ляв (десен) модул над асоциативния пръстен с единица R, ако в M са определени две операции - събиране*

$$M \times M \longrightarrow M,$$

$$(x, y) \mapsto x + y$$

и ляво (дясно) умножение с $r \in R$,

$$R \times M \longrightarrow M, \quad \textit{съответно} \quad M \times R \longrightarrow M,$$

$$(r, x) \mapsto rx, \qquad\qquad (x, r) \mapsto xr,$$

изпълняващи следните аксиоми:
1. асоциативност на събирането

$$(x + y) + z = x + (y + z) \quad \textit{за } \forall x, y, z \in M;$$

2. съществуване на нулев елемент $0_M \in M$, така че

$$x + 0_M = 0_M + x = x \quad \textit{за } \forall x \in M;$$

3. за всеки елемент $x \in M$ съществува противоположен $-x \in M$, така че

$$x + (-x) = (-x) + x = 0_M;$$

4. комутативност на събирането

$$x + y = y + x \quad \textit{за } \forall x, y \in M;$$

5. дистрибутивност относно "векторен"множител

$$r(x + y) = rx + ry \quad (\textit{съответно}, \quad (x + y)r = xr + yr)$$

за $\forall r \in R$, $\forall x, y \in M$;
6. дистрибутивност относно "скаларен"множител

$$(r + s)x = rx + sx \quad (\textit{съответно}, \quad x(r + s) = xr + xs)$$

за $\forall r, s \in R$, $\forall x \in M$;
7. "асоциативност"

$$(rs)x = r(sx) \quad (\textit{съответно}, \quad x(rs) = (xr)s)$$

за $\forall r, s \in R$, $\forall x \in M$;
8. $1_R x = x$ (съответно, $x 1_R = x$) за $\forall x \in M$.

Очевидно, всеки ляв (десен) R-модул е абелева група относно събирането. Следващото Твърдение 1.2 доказва, че абелевата група $(M, +)$ задава еднозначно определена структура на $\mathbb{Z}$-модул.

Твърдение 1.2. *Понятията "абелева група"и "$\mathbb{Z}$-модул"са еквивалентни.*

Доказателство: Събирането на елементи $x \in M$ със себе си задава по естествен начин произведение на $n \in \mathbb{N}$ с $x \in M$. По-точно, nx е n-кратната сума на x със себе си. Полагаме $0x := 0_M$ и $(-n)x := -(nx)$ да е противоположният елемент на nx. Трябва да проверим верността на четирите аксиоми, които превръщат абелевата група $(M, +)$ в $\mathbb{Z}$-модул. Дистрибутивността над "векторен"множител се установява в 3 стъпки :

$$n(x+y) = (x+y)+\ldots+(x+y) = (x+\ldots+x)+(y+\ldots+y) = nx+ny \quad \text{за } n \in \mathbb{N},$$

$$0(x+y) = 0_M = 0_M + 0_M = 0x + 0y,$$

$$(-n)(x+y) = -[n(x+y)] = -(nx+ny) =$$

$$[-(nx)] + [-(ny)] = (-n)x + (-n)y$$

при $n \in \mathbb{N}$. За $m, n \in \mathbb{N}$, $m \geq n$, дистрибутивният закон над "скаларен"множител

$$(m+n)x = (x+\ldots+x) + (x+\ldots+x) = mx + nx,$$

$$(-m-n)x = -[(m+n)x] = -(mx+nx) = [-(mx)] + [-(nx)] = (-m)x + (-n)x,$$

$$(m-n)x = (x+\ldots+x) + [(-x)+\ldots+(-x)] = mx + n(-x) = mx + (-n)x,$$

$$(n-m)x = [-(m-n)]x = -[(m-n)x] =$$

$$-[mx + (-n)x] = [-(mx)] + [-(-n)x] = (-m)x + nx,$$

$$(m+0)x = mx = mx + 0_M = mx + 0x,$$

$$(0-n)x = (-n)x = 0_M + (-n)x = 0x + (-n)x,$$

$$(0+0)x = 0x = 0_M = 0_M + 0_M = 0x + 0x.$$

В третото равенство прилагаме към $n(-x)$ и $(-n)x$ единствеността на противоположния елемент на nx, както и равенствата $n0_M = 0_M$, $0x = 0_M$. В четвъртото равенство отъждествяваме $-(-n)x$ с nx в качеството им на противоположен елемент на $(-n)x$. Асоциативността е симетрична относно числовите множители съгласно комутативността на $\mathbb{Z}$. Затова е достатъчно да проверим, че

$$(m0)x = 0x = 0_M = m0_M = m(0x),$$

$$(mn)x = (x+\ldots+x) + \ldots + (x+\ldots+x) = m(nx),$$

$$[(-m)(-n)]x = (mn)x = m(nx) = -[(-m)(nx)] = (-m)[(-n)x],$$

$$[(-m)n]x = [m(-n)]x = (-mn)x = -[(mn)x] =$$

$$-[m(nx)] = (-m)(nx) = m[-(nx)] = m[(-n)x]$$

за $\forall m, n \in \mathbb{N}$. В третото тъждество от проверката на асоциативността приравняваме противоположните елементи $m(nx)$ и $(-m)[(-n)x]$ на $(-m)(nx)$, използвайки отново $0y = 0_M$ и $k0_M = 0_M$ за $\forall y \in M$, $\forall k \in \mathbb{Z}$. В четвъртото равенство вземаме предвид, че $m[-(nx)]$ е противоположният елемент на $m(nx)$. Ясно е, че $1x = x$ за $\forall x \in M$, Q.E.D.

Определение 1.3. *Нека R и S са асоциативни пръстени с единица. Ако M е ляв R-модул и десен S-модул с условието*

$$(rm)s = r(ms) \quad \text{за } \forall r \in R, \forall m \in M, \forall s \in S,$$

то казваме, че M е $R-S$-бимодул и записваме ${}_RM_S$.

Следващата лема предоставя стандартен пример за $R-R$-бимодул.

Лема 1.4. *Нека R е комутативен пръстен с единица. Тогава:*
(i) всеки ляв R-модул A има стандартна структура на $R-R$-бимодул, зададена по правилото

$$A \times R \longrightarrow A,$$
$$(a, r) \mapsto ra \qquad \text{за } \forall a \in A, \forall r \in R.$$

(ii) всеки десен R-модул B има стандартна структура на $R-R$-бимодул, зададена по правилото

$$R \times B \longrightarrow B,$$
$$(r, b) \mapsto br \qquad \text{за } \forall b \in B, \forall r \in R.$$

Доказателство: Ще разгледаме само (i), доколкото (ii) се доказва аналогично. Левият R-модул A е абелева група относно събирането, така че остава да проверим останалите 4 аксиоми за десен R-модул и условието за съгласуваност между лявата и дясната R-модулна структура. Дистрибутивността над "векторен"множител

$$(a_1 + a_2)r = r(a_1 + a_2) = ra_1 + ra_2 = a_1 r + a_2 r$$

и дистрибутивността над "скаларен"множител

$$a(r + s) = (r + s)a = ra + sa = ar + as$$

са рутинни. Комутативността на R се използва в "асоциативното свойство"

$$a(rs) = (rs)a = (sr)a = s(ra) = (ra)s = (ar)s.$$

Накрая, $a1_R = 1_R a = a$, с което установихме, че A е десен R-модул. Съгласуваността между лявата и дясната R-модулни структури отново използва комутативността на пръстена R, именно

$$(ra)s = (ar)s = a(rs) = a(sr) = (as)r = r(as), \qquad \text{Q.E.D.}$$

2. Подмодули и фактор-модули.

Определение 1.5. *Непразното подмножество N на ляв (десен) R-модул M се нарича ляв (десен) подмодул, ако:*
(i) за $\forall x, y \in N$ е в сила $x - y \in N$ (т.е. $(N, +)$ е подгрупа на $(M, +)$) и
(ii) за $\forall r \in R$ и $\forall x \in N$ е изпълнено $rx \in N$ (съответно, $xr \in N$).

Лема 1.6. *Нека $X = \{x_j \,|\, j \in J\}$ е подмножество на ляв (десен) R-модул M. Тогава подмножеството $N = N_X$ на крайните суми от вида $r_{j_1}x_{j_1} + \ldots + r_{j_k}x_{j_k}$ (съответно, $x_{j_1}r_{j_1} + \ldots + x_{j_k}r_{j_k}$) с $r_{j_s} \in R$, $x_{j_s} \in X$, е подмодул на M. Казваме, че N_X е подмодулът на M, породен от X.*

Доказателство: Съгласно Определение 1.5, достатъчно е да отбележим, че

$$\left(\sum_{p=1}^{k} r_{j_p} x_{j_p}\right) - \left(\sum_{q=1}^{l} s_{j_q} x_{j_q}\right) = \sum_{p=1}^{k} r_{j_p} x_{j_p} + \sum_{q=1}^{l} (-s_{j_q}) x_{j_q} \in N_X$$

и

$$s\left(\sum_{p=1}^{k} r_{j_p} x_{j_p}\right) = \sum_{p=1}^{k} (s r_{j_p}) x_{j_p} \in N_X, \qquad \text{Q.E.D.}$$

Ако N е ляв (десен) подмодул на левия (десния) R-модул M, то подгрупата $(N, +)$ е нормална в абелевата група $(M, +)$, така че фактор-групата $(M/N, +)$ е коректно определена. Задаваме ляво (дясно) умножение с $r \in R$ по правилото

$$R \times (M/N) \longrightarrow (M/N) \qquad (\text{ съответно } (M/N) \times R \longrightarrow (M/N)$$
$$(r, x + N) \mapsto rx + N \qquad\qquad (x + N, r) \mapsto xr + N.$$

Тази операция е коректна, т.е. не зависи от избора на представител на съседния клас от M относно N. По-точно, ако $x+N=x'+N$, то $x'-x\in N$, така че $rx'-rx=r(x'-x)\in N$ и $rx'+N=rx+N$. (Аналогично, за десен R-подмодул N на десен R-модул M.) Твърдим, че така зададеното ляво (дясно) умножение с $r\in R$ върху M/N задава структура на ляв (десен) R-модул върху $(M/N,+)$. За да установим верността на това твърдение, трябва да проверим последните четири аксиоми от Определение 1.1 за R-модул. Ще изложим разглежданията само за леви R-модули, доколкото десният случай е напълно аналогичен. Използвайки определенията за събиране и умножение с $r\in R$ в M/N, както и съответните аксиоми в левия R-модул M, забелязваме, че

$$r((x+N)+(y+N))=r(x+y+N)=r(x+y)+N=$$

$$rx+ry+N=(rx+N)+(ry+N)=r(x+N)+r(y+N),$$

$$(r+s)(x+N)=(r+s)x+N=rx+sx+N=(rx+N)+(sx+N)=r(x+N)+s(x+N),$$

$$(rs)(x+N)=(rs)x+N=r(sx)+N=r(sx+N)=r[s(x+N)],$$

$$1_R(x+N)=1_Rx+N=x+N$$

за произволни $r,s\in R$ и $x+N,y+N\in M/N$.

Определение 1.7. *За произволен ляв (десен) R-модул M и негов ляв (десен) подмодул N, определеният по-горе ляв (десен) R-модул M/N се нарича фактор-модул на M относно N.*

Съществуването на фактор-модул относно всеки подмодул е много важно свойство на модулите. От задължителния курс по алгебра е известно, че то няма аналог за пръстени. С други думи, съществуват подпръстени S на асоциативен пръстен R, за които абелевата група $(R/S,+)$ не наследява умножението от R. Ако S е идеал на R, т.е. ляв и десен R-модул, то R/S има естествена структура на пръстен, наречен фактор-пръстен на R по S.

Лема-Определение 1.8. *Ако N и P са леви (десни) подмодули на ляв (десен) R-модул M, то множеството*

$$N+P:=\{x+y\,|\,x\in N,y\in P\}$$

е ляв (десен) подмодул на M, наречен сума на N и P.
Модулите N и P са подмодули на $N+P$.

Доказателство: Ако $x_1,x_2\in N$ и $y_1,y_2\in P$, то $(x_1+y_1)-(x_2+y_2)=(x_1+y_1)+[(-x_2)+(-y_2)]=[x_1+(-x_2)]+[y_1+(-y_2)]=(x_1-x_2)+(y_1-y_2)\in N+P$. Тук използвахме единствеността на противоположния елемент, за да заместим $-(x_2+y_2)$ с $(-x_2)+(-y_2)$ съгласно $(x_2+y_2)+[(-x_2)+(-y_2)]=0_M$. Да отбележим, че $x_1-x_2\in N$ и $y_1-y_2\in P$, доколкото $(N,+)$ и $(P,+)$ са подгрупи на $(M,+)$. За произволни $r\in R$, $x\in N$ и $y\in P$ имаме $r(x+y)=rx+ry$ с $rx\in N$ и $ry\in P$ в случая на леви подмодули. Разглежданията за десни R-модули са аналогични.
Подгрупите $(N,+)$ и $(P,+)$ на $(M,+)$ съдържат нейния неутрален елемент 0_M. Следователно $N=\{x+0_M\,|\,x\in N\}$ и $P=\{0_M+y\,|\,y\in P\}$ са подмножества на $N+P=\{x+y\,|\,x\in N,y\in P\}$. Съгласно затвореността на N и P относно изваждане и леви (десни) умножения с $r\in R$, стигаме до заключението, че N и P са подмодули на $N+P$, Q.E.D.

3. Хомоморфизми на модули.

Определение 1.9. *Изображението $f : M \to N$ на леви (десни) R-модули е хомоморфизъм на леви (десни) R-модули, ако*

$$f(x+y) = f(x) + f(y) \quad \text{за } \forall x, y \in M \text{ и}$$

$$f(rx) = rf(x) \quad (\text{ съответно, } f(xr) = f(x)r) \text{ за } \forall r \in R, \forall x \in M.$$

Хомоморфизмът $f : M \to N$ на леви (десни) R-модули се нарича мономорфизъм, ако произволни различни $x, y \in M$ имат различни образи $f(x) \neq f(y)$. Хомоморфизмът $f : M \to N$ на леви (десни) R-модули се нарича епиморфизъм, ако за всяко $y \in N$ съществува $x \in M$, така че $f(x) = y$. Хомоморфизмът $f : M \to N$ на леви (десни) R-модули е изоморфизъм, ако той е едновременно мономорфизъм и епиморфизъм.

Следствие 1.10. *Понятията "хомоморфизъм $f : M \to N$ на абелеви групи"и "хомоморфизъм $f : M \to N$ на $\mathbb{Z}$-модули"са еквивалентни.*

Доказателство: За естествената структура на $\mathbb{Z}$-модул, въведена в Твърдение 1.2 трябва да докажем, че $f(zx) = zf(x)$ за $\forall z \in \mathbb{Z}$, $\forall x \in M$. Ако $n \in \mathbb{N}$, то

$$f(nx) = f(x + \ldots + x) = f(x) + \ldots + f(x) = nf(x),$$

$$f((-n)x) = f(-(nx)) = -f(nx) = -[nf(x)] = (-n)f(x),$$

$$f(0x) = f(0_M) = 0_N, \quad \text{Q.E.D.}$$

Лема 1.11. *Ако $f : M \to N$ и $g : N \to P$ са хомоморфизми на леви (десни) R-модули, то композицията $gf : M \to P$ е хомоморфизъм на леви (десни) R-модули.*
Още повече, ако f и g са мономорфизми, то gf е мономорфизъм. Ако f и g са епиморфизми, то gf е епиморфизъм.

Доказателство: За произволни $x, y \in M$ пресмятаме непосредствено, че

$$(gf)(x+y) = g[f(x+y)] = g[f(x)+f(y)] = g[f(x)] + g[f(y)] = (gf)(x) + (gf)(y),$$

доколкото f и g са хомоморфизми на леви (десни) R-модули. В случая на леви R-модули имаме

$$(gf)(rx) = g[f(rx)] = g[rf(x)] = r\{g[f(x)]\} = r(gf)(x)$$

за $\forall r \in R$, $\forall x \in M$. Следователно gf е хомоморфизъм на леви R-модули.
Ако f е мономорфизъм, то за произволни $x \neq y$ от M следва, че $f(x) \neq f(y)$. Сега мономорфизмът g ги трансформира в $(gf)(x) = g[f(x)] \neq g[f(y)] = (gf)(y)$, с което се установява, че gf е също мономорфизъм.
Щом g е епиморфизъм, всеки елемент на P има вида $g(y)$ за някое $y \in N$. Аналогично, епиморфността на f гарантира съществуването на $x \in M$ с $f(x) = y$. В резултат, $(gf)(x) = g(y)$ и всеки елемент на P е образ на някое $x \in M$ под действие на gf. Следователно gf е епиморфизъм, Q.E.D.

Определение 1.12. *Ако $f : M \to N$ е хомоморфизъм на леви (десни) R-модули, то множеството*

$$Ker(f) := \{x \in M \mid f(x) = 0_N\}$$

се нарича ядро на f, а множеството

$$Im(f) := \{f(x) \mid x \in M\}$$

се нарича образ на f.

Лема 1.13. *Нека $f : M \to N$ е хомоморфизъм на леви (десни) R-модули. Тогава*
(i) $Ker(f)$ е ляв (десен) подмодул на M;
(ii) $Im(f)$ е ляв (десен) подмодул на N;
(iii) f е мономорфизъм тогава и само тогава, когато $Ker(f) = \{0_M\}$;
(iv) f е епиморфизъм тогава и само тогава, когато $Im(f) = N$.

Доказателство: (i) За произволно $x \in M$ имаме $f(-x) = -f(x)$, съгласно единствеността на противоположния елемент $-f(x)$ на $f(x)$ и тъждеството $f(x) + f(-x) = f(x + (-x)) = f(0_M) = 0_N$. От своя страна, $f(0_M) = 0_N$ се получава от $f(z) = f(z+0_M) = f(z)+f(0_M)$ чрез прибавяне на $-f(z)$ към двете страни. И така, ако $x, y \in Ker(f)$, то $f(x - y) = f(x + (-y)) = f(x) + f(-y) = f(x) + [-f(y)] = f(x) - f(y) = 0_N - 0_N = 0_N$ показва, че $x - y \in Ker(f)$. За произволни $r \in R$ и $x \in Ker(f)$ пресмятаме $f(rx) = rf(x) = r0_N = 0_N$. Да напомним, че $u = 1_R u = (1_R + 0_R)u = 1_R u + 0_R u = u + 0_R u$ за $u \in N$ и $r \in R$ води до $0_N = 0_R u$ след прибавяне на $-u$ към двете страни. Сега $r0_N = r(0_R u) = (r0_R)u = 0_R u = 0_N$. С това проверихме, че $Ker(f)$ е ляв (десен) подмодул на M.
(ii) Непосредствено се убеждаваме, че $f(x) - f(y) = f(x) + f(-y) = f(x - y) \in Im(f)$ и $rf(x) = f(rx) \in Im(f)$ за произволни $x, y \in M$, $r \in R$.
(iii) Ако f е мономорфизъм, то за всяко $0_M \neq x \in M$ следва, че $0_N = f(0_M) \neq f(x)$. С други думи, $Ker(f)$ се състои само от 0_M. Обратно, ако $Ker(f) = \{0_M\}$ и $f(x) = f(y)$ за $x, y \in M$, то $0_N = f(x)-f(y) = f(x-y)$ определя, че $x-y = 0_M$ или $x = y$. Това доказва, че f е мономорфизъм.
Твърдението (iv) е очевидно, Q.E.D.

Определение 1.14. *За произволен хомоморфизъм $f : M \to N$ на леви (десни) R-модули, фактор-модулът*

$$Coker(f) := N/Im(f)$$

се нарича коядро на f.

4. Пропускване на модулни структури и хомоморфизми. Ньотерови изоморфизми.

Лема-Определение 1.15. *Ако M е ляв (десен) модул над асоциативен пръстен с единица R, то множеството*

$$\mathrm{Ann}_R(M) := \{r \in R \,|\, rx = 0_M \text{ за } \forall x \in M\},$$

(съответно, $\mathrm{Ann}_R(M) := \{r \in R \,|\, xr = 0_M \text{ за } \forall x \in M\}$) е ляв (десен) идеал на R, наречен анулатор на M.
В частност, ако пръстенът R е комутативен, то анулаторът $\mathrm{Ann}_R(M)$ на всеки R-модул M е двустранен идеал в R.

Доказателство: Ще разгледаме само случая на ляв модул M. За произволни $r, s \in \mathrm{Ann}_R(M)$ и $x \in M$ е в сила $(r - s)x = rx - sx = 0_M - 0_M = 0_M$, така че $(\mathrm{Ann}_R(M), +)$ е подгрупа на $(R, +)$. Освен това, за всяко $t \in R$ имаме $(tr)x = t(rx) = t0_M = 0_M$, така че $\mathrm{Ann}_R(M)$ е ляв идеал на R, Q.E.D.

Лема 1.16. *Нека R е асоциативен пръстен с единица, M е ляв (десен) R-модул, а I е двустранен идеал на R, съдържащ се в анулатора $\mathrm{Ann}_R(M)$. Тогава M има естествена структура на ляв (десен) R/I-модул, в която*

$$(R/I) \times M \longrightarrow M, \quad (\text{ съответно } M \times (R/I) \longrightarrow M),$$

$$(r + I, x) \mapsto rx, \qquad (\text{ съответно } (x, r + I) \mapsto xr).$$

Доказателство: По предположение, $(M, +)$ е абелева група. За проверка на коректността на умножението с $r + I \in R/I$, да изберем $r + I = r' + I$. Тогава $r' - r = r_o \in I \subseteq \mathrm{Ann}_R(M)$, така че $r'x = (r + r_o)x = rx + r_o x = rx + 0_M = rx$. Дистрибутивността над "векторен"множител

$$(r + I)(x + y) = r(x + y) = rx + ry = (r + I)x + (r + I)y,$$

дистрибутивността над "скаларен"множител

$$[(r + I) + (s + I)]x = [(r + s) + I]x = (r + s)x = rx + sx = (r + I)x + (s + I)x,$$

"асоциативността"

$$[(r + I)(s + I)]x = (rs + I)x = (rs)x = r(sx) = (r + I)(sx) = (r + I)[(s + I)x]$$

и $(1_R + I)x = 1_R x = x$ се проверяват непосредствено. С това се установява, че M е R/I-модул, Q.E.D.
За формулиране на следващото твърдение трябва да определим понятието комутативна диаграма от R-модули.

Определение 1.17. *Комутативна диаграма от леви (десни) R-модули е граф с върхове леви (десни) R-модули и ребра - хомоморфизми на тези модули, така че композицията на хомоморфизмите, отговарящи на ребрата на някакъв път от модул A до модул B съвпада със съответните композиции по всички пътища от A до B, за произволни модули A и B.*

Примери: 1. Диаграмата

$$\begin{tikzcd} A \arrow[d, "f"'] \arrow[dr, "h"] & \\ B \arrow[r, "g"] & C \end{tikzcd}$$

е комутативна, ако $gf = h$.
2. Диаграмата

$$\begin{tikzcd} A \arrow[r, "\alpha"] \arrow[d, "\delta"'] & B \arrow[d, "\beta"] \\ C \arrow[r, "\gamma"] & D \end{tikzcd}$$

е комутативна, ако $\beta\alpha = \gamma\delta$.

Твърдение 1.18. *Нека $f : M \to N$ е хомоморфизъм на леви (десни) R-модули, а K е ляв (десен) подмодул на ядрото $Ker(f)$. Тогава съществува единствен хомоморфизъм на леви (десни) R-модули $\overline{f} : M/K \to N$, затварящ комутативната диаграма*

$$\begin{tikzcd} M \arrow[d, "\pi"'] \arrow[dr, "f"] & \\ M/K \arrow[r, "\overline{f}"] & N \end{tikzcd} ,$$

$f = \overline{f}\pi$, където $\pi : M \to M/K$ е естественият епиморфизъм $\pi(m) := m + K$, $m \in M$ с ядро K.
При това, f е епиморфизъм тогава и само тогава, когато $\overline{f}$ е епиморфизъм. Ядрото $Ker(\overline{f}) = Ker(f)/K$.

Доказателство: Определяме изображението

$$\overline{f} : M/K \longrightarrow N,$$

$$\overline{f}(m+K) := f(m).$$

То е коректно зададено, доколкото за $m+K = m'+K$ е изпълнено $m'-m \in K \subseteq Ker(f)$, откъдето $f(m') - f(m) = 0_N$ и $\overline{f}(m+K) = f(m) = f(m') = \overline{f}(m'+K)$. Твърдим, че $\overline{f}$ е хомоморфизъм на леви (десни) R-модули. Наистина, за произволни $x, y \in M$ и $r \in R$ е изпълнено

$$\overline{f}((x+K)+(y+K)) = \overline{f}((x+y)+K) = f(x+y) = f(x)+f(y) = \overline{f}(x+K)+\overline{f}(y+K) \text{ и}$$

$$\overline{f}(r(x+K)) = \overline{f}(rx+K) = f(rx) = rf(x) = r\overline{f}(x+K).$$

Хомоморфизмът $\overline{f}$ удовлетворява гореспоменатата комутативна диаграма, доколкото $\overline{f}\pi(m) = \overline{f}(m+K) = f(m)$ за $\forall m \in M$. Ако $g : M/K \to N$ е хомоморфизъм на леви (десни) R-модули, изпълняващ условието $g\pi = f$, то за всяко $m \in M$ имаме

$$g(m+K) = g\pi(m) = f(m) = \overline{f}(m+K).$$

Следователно g съвпада с $\overline{f}$ или $\overline{f}$ е единствен с посочените свойства.
От определението на $\overline{f}$ е ясно, че всеки елемент на N има вида $f(m)$ за някое $m \in M$ точно когато може да се представи като $\overline{f}(m+K)$. Това означава, че f е епиморфизъм тогава и само тогава, когато $\overline{f}$ е епиморфизъм.
По определение, ядрото

$$Ker(\overline{f}) := \{m+K \in M/K \,|\, \overline{f}(m+K) = f(m) = 0_N\} =$$

$$\{m+K \in M/K \,|\, m \in Ker(f)\} = Ker(f)/K, \text{ Q.E.D.}$$

Твърдение 1.19. *(i) (Теорема за хомоморфизмите) За произволен хомоморфизъм $f : M \to N$ на леви (десни) R-модули, фактор-модулът $M/Ker(f)$ е изоморфен на модула $Im(f)$.*
(ii) Ако N и P са леви (десни) подмодули на ляв (десен) R-модул M, то

$$N/(N \cap P) \simeq (N+P)/P.$$

(iii) Ако $P \subseteq N$ са леви (десни) подмодули на ляв (десен) R-модул M, то

$$(M/P)/(N/P) \simeq (M/N).$$

Доказателство: (i) Съгласно Твърдение 1.18 съществува единствен хомоморфизъм на леви (десни) R-модули

$$\overline{f} : M/Ker(f) \longrightarrow Im(f)$$

с условието

$$\overline{f}\pi(m) = \overline{f}(m + Ker(f)) = f(m)$$

за $\forall m \in M$ и естествения епиморфизъм $\pi : M \to M/Ker(f)$. Ще докажем, че $\overline{f}$ е изоморфизъм. Наистина, ако $\overline{f}(m+Ker(f)) = f(m) = f(m') = \overline{f}(m'+Ker(f))$, то $f(m'-m) = 0_N$. Следователно $m'-m \in Ker(f)$ и $m'+Ker(f) = m+Ker(f)$. Това доказва, че $\overline{f}$ е мономорфизъм. От друга страна, за $\forall f(m) \in Im(f)$ съществува $m+Ker(f) \in M/Ker(f)$ с $\overline{f}(m+Ker(f)) = f(m)$, така че $\overline{f}$ е епиморфизъм.
(ii) В Лема-Определение 1.8 доказахме, че $N+P$ е подмодул на M, а P е подмодул на $N+P$. Следователно можем да образуваме фактор-модула $(N+P)/P$ и да разгледаме изображението

$$g : N \longrightarrow (N+P)/P,$$

$$g(n) := n + P \quad \text{за } \forall n \in N.$$

Непосредствено проверяваме, че g е хомоморфизъм на леви (десни) R-модули,

$$g(n_1+n_2) = (n_1+n_2)+P = (n_1+P)+(n_2+P) = g(n_1)+g(n_2),$$
$$g(rn) = rn+P = r(n+P) = rg(n).$$

Следователно можем да приложим Теоремата за хомоморфизмите (i) и да получим изоморфизма на R-модули

$$N/Ker(g) \simeq Im(g).$$

По определение, $Ker(g) := \{n \in N \,|\, n+P = P\} = \{n \in N \,|\, n \in P\} = N \cap P$. Образът $Im(g) = (N+P)/P$, защото всеки елемент на $(N+P)/P$ има вида $n+P = g(n)$.

(iii) Да разгледаме изображението

$$h : (M/P) \longrightarrow (M/N),$$
$$h(m+P) := m+N \quad \text{за } \forall m \in M.$$

То е коректно зададено, понеже от $m+P = m'+P$ следва, че $m'-m \in P \subseteq N$, откъдето $h(m+P) = m+N = m'+N = h(m'+P)$. Освен това, h е хомоморфизъм на леви (десни) R-модули, съгласно

$$h((m_1+P)+(m_2+P)) = h((m_1+m_2)+P) = (m_1+m_2)+N =$$
$$(m_1+N)+(m_2+N) = h(m_1+P)+h(m_2+P) \text{ и}$$
$$h(r(m+P)) = h(rm+P) = rm+N = r(m+N) = rh(m+P).$$

Теоремата за хомоморфизмите (i) дава изоморфизъм на R-модули

$$(M/P)/Ker(h) \simeq Im(h).$$

Тук $Ker(h) := \{m+P \,|\, h(m+P) = m+N = N\} = \{m+P \,|\, m \in N\} = N/P$ и $Im(h) = (M/N)$, защото всяко $m+N \in M/N$ може да се представи като $m+N = h(m+P)$, Q.E.D.