Модули над пръстени от главни идеали и класификация на крайнопородените абелеви групи

Александър Гудев

1 Увод

Да разгледаме някои въпроси, които може да си зададе човек в линейната и висшата алгебра.

1. Често пъти при изучаване на групи и пръстени искаме да опишем крайни сборове на даден елемент със себе си, например $a + \cdots + a$. Това ни подтиква да използваме записа $n \cdot a$ по аналогия с умножението с цели числа, който дефинираме чисто формално по такъв начин:

$$n \cdot a = \begin{cases} \underbrace{a + \cdots + a}_{n \text{ пъти}}, & \text{ако } n > 0 \\ 0, & \text{ако } n = 0 \\ \underbrace{(-a) + \cdots + (-a)}_{n \text{ пъти}}, & \text{ако } n < 0 \end{cases}$$

   Това е чисто синтактична конструкция, която дефинираме изцяло извън разглежданата структура (група, пръстен, ...), и в такъв случай винаги, когато пишем $n \cdot a$, трябва да помним, че това е само съкратен запис, и формалното умножение, което използваме, не отговаря задължително на операциите в структурата.

   Например, когато доказваме простота на характеристиката на дадено поле F, пишем $p \cdot 1$, но изрично отбелязваме, че $p \in \mathbb{Z}$ не е задължително елемент на F, и формалното умножение тук няма връзка с операцията $*$ от полето.

   Естествено е да се запитаме, няма ли някакъв по-чист, по-алгебричен начин да опишем тази формална операция?

2. За нуждите на линейните изображения в линейно пространство над поле F въвеждаме понятието "матрица" с коефициенти от полето F. От ключово значение за намиране на обратни матрици, например, е обратимостта на всички ненулеви елементи в F.

   Търсейки собствени числа и собствени вектори, обаче, дефинираме характеристичния полином $\det(A - xI)$. Елементите на матрицата $A - xI$ в този случай се оказват *полиноми*, а добре знаем, множеството от полиномите над някое поле (пръстен) не е поле само по себе си.

   Това навежда на въпроса – какво ще стане, ако се откажем от обратимостта на скаларите в дефиницията на линейно пространство?

3. Точките с целочислени координати в равнината $\mathbb{Z} \times \mathbb{Z}$ не образуват линейно пространство над никое поле, въпреки че "се разпростират навсякъде".

   Защо? Ако полето е с ненулева характеристика $p \in \mathbb{N}$, тогава за кой да е вектор (a, b) имаме $0 = (p \cdot 1_F) \cdot (a, b) = (a, b) + \cdots + (a, b) = (p \cdot a, p \cdot b)$ и тогава $(a, b) = (0, 0)$. В другия случай, поле с нулева характеристика има просто подполе, изоморфно на $\mathbb{Q}$, а умножавайки дроби с $(1, 1)$ (например), излизаме от $\mathbb{Z} \times \mathbb{Z}$.

   Какво се чупи? Делението в полето е "несъвместимо" с целите числа. Ако се откажем от това свойство – и гледаме пръстени по принцип – какво ще стане?

4. В теорията на групите разглеждаме т.нар. *действие на група върху множество*, където свързваме дадена група G с някакво множество X посредством някаква операция $\cdot : G \times X \to X$. За множеството X нямаме практически никакви условия, освен естествените ограничения върху операцията – неутралност спрямо идентитета на групата и асоциативност.

   Като един много частен случай на това можем да разглеждаме и линейните пространства, където мултипликативната група на полето F *действа* върху множеството V.

   Какво ще стане, ако наложим някакви ограничения върху множеството X, и подсилим изискванията за G? В частност, ако поискаме X да бъде абелева група, а G - пръстен?

5. Известно е, че решенията на хомогенни линейни диференциални уравнения имат структура на линейно пространство: ако y_1, y_2 са решения на $a_0 y + a_2 y' + a_2 y'' + \ldots + a_n y^{(n)} = 0$, то очевидно и $\lambda y_1 + \mu y_2$ също решава това уравнение.

   Можем да забележим, обаче, че за дадено решение y_1, всяка производна $y_1^{(k)}$ също е решение за кое да е $k \in \mathbb{N}$, както и произволна комбинация на негови производни: $\lambda_0 y_1 + \lambda_1 y_1' + \ldots + \lambda_k y_1^{(k)}$.

   Така откриваме, че множеството решения $V \leq C^n(\mathbb{R})$ на диференциалното уравнение имат още по-богата структура от линейно пространство — върху тях можем да действаме не само с умножение със скалар, а можем да прилагаме *произволни полиноми от диференциални оператори* – тоест да действаме с елементи (оператори) $\theta : V \to V$ от вида $\theta = \lambda_n D^n + \ldots + \lambda_1 D + \lambda_0 I$, където D е диференциалният оператор, а $I = D^0$ е идентитетът.

   Тази полиномиална структура не е поле, а само пръстен, но е размуно да очакваме някакви резултати от нея.

Дефиниция 1. Ляв модул M над пръстена $(R, +, *)$ наричаме абелева група $(M, +)$, заедно с операция за скаларно умножение $\cdot : R \times M \to M$, изпълняваща следните свойства, където $a, b \in R$ и $m, n \in M$ са произволни:

1. $a \cdot (m + n) = a \cdot m + a \cdot n$
2. $(a + b) \cdot m = a \cdot m + b \cdot m$
3. $a \cdot (b \cdot m) = (a * b) \cdot m$
4. $1_R \cdot m = m$

Бележка. Аанлогично можем да дефинираме *десен* модул.

2 Примери

1. Всеки пръстен е модул над себе си с умножение (както всяко поле е пространство над себе си). И по-общо:
2. Всеки пръстен е модул над всеки свой подпръстен (подпръстените "действат" върху надпръстена). Обратното – подпръстен да е модул над пръстена – е изпълнено, само ако подпръстенът поглъща умножение с елементи извън себе си, тоест:
3. Ако $I \trianglelefteq R$ е идеал, то I е модул над R. Например $2\mathbb{Z} = \langle 2 \rangle \trianglelefteq \mathbb{Z}$ е модул над $\mathbb{Z}$, понеже умножение на кое да е цяло число с четно дава отново четен резултат.
4. Ако $n \in \mathbb{N}$, то R^n е модул над R с покомпонентно умножение: нека $a \in R$ и $(r_1, \ldots, r_n) \in R^n$. Тогава:
$$a \cdot (r_1, \ldots, r_n) = (a * r_1, \ldots, a * r_n)$$
   Ако X е крайно множество, то с $\oplus_X R$ бележим модула $R^{|X|}$.

   Както в линейната алгебра F^n е пространство над F за всяко поле F, тук обобщаваме F до пръстен - например, целочислените точки в пространството $\mathbb{Z}^3$ е модул над $\mathbb{Z}$.

5. Нека $R = \mathbb{Z}$. Какво можем да кажем за произволен модул M над R? Оказва се, че действието в случая е еднозначно определено:

   От дефиницията за модул, $1 \cdot m = m$. Тогава $2 \cdot m = (1+1) \cdot m = 1 \cdot m + 1 \cdot m = m + m$, аналогично $3 \cdot m = m + m + m$, и изобщо получаваме индуктивно $k \cdot m = \underbrace{m + \cdots + m}_{k \text{ пъти}}$, тоест операцията е определена за $k > 0$.

   При $k = 0$ очевидно[1] $k \cdot m = 0_M$. При $k = -1$ с още малко гимнастика[2] получаваме $(-1) \cdot m = -m$ и свеждаме до горния случай: $\forall k < 0 : k \cdot m = ((-k) * (-1)) \cdot m = (-k) \cdot ((-1) \cdot m) = \underbrace{(-m) + \cdots + (-m)}_{|k| \text{ пъти}}$.

   Тоест алгебрически можем да опишем формалното умножение на елементи в абелева група с число от по-рано като разгледаме групата като модул над целите числа.

   Именно този поглед върху абелевите групи ще използваме, за да сведем класификацията на крайнопородените абелеви групи до теоремата, която ще докажем.

   - Частен случай по тази точка: модулът $\mathbb{Z}/n\mathbb{Z}$ над пръстена $\mathbb{Z}$. Действието следва стандартните правила за умножение на остатъци: нека $k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$, $r \in \mathbb{Z}$, тогава $r \cdot (k + n\mathbb{Z}) \coloneqq (r * k) + \mathbb{Z}$.

6. Всеки хомоморфизъм на пръстени $\varphi : R \to M$ индуцира модул M над R, където операцията $\cdot : R \times M \to M$ е: $r \cdot m \coloneqq \varphi(r) *_M m$. Можем да си мислим, че пръстенът R *действа* чрез φ на M.

3 Понятия с аналози в линейната алгебра

Пренасяме директно някои дефиниции от линейната алгебра върху модули.

Дефиниция 2. Подмножество $N \subseteq M$ на модул $(M, +)$ над пръстена R наричаме **подмодул**, ако $(N, +)$ е подгрупа на $(M, +)$ и е затворено относно умножение с елементи на пръстена: $\forall r \in R, n \in N : r \cdot n \in N$.

Когато говорим за модул M и негов подмодул N, с цел подчертаване на връзката между тях или невъвеждане на нови променливи в контекста, ще наричаме M **надмодул** на N.

Бележка. Всеки пръстен R е модул над себе си. Тогава неговите подмодули са точно идеалите на R.

Дефиниция 3. Ако N е подмодул на модула M над пръстена R, то $N \trianglelefteq M$ е нормална подгрупа и съществува фактор-група M/N. **Фактор-модул** наричаме тази фактор-група с операцията $\cdot : R \times M/N \to M/N$, където $r \cdot (m + N) = (r \cdot m) + N$.

Коректност на дефиницията на операцията: нека $r \in R$ и $m + N = m' + N$. Тогава $m - m' \in N$ и от дефиницията на подмодул $r \cdot (m - m') \in N$, тоест $r \cdot m - r \cdot m' \in N$ и значи $r \cdot m + N = r \cdot m' + N$.

Дефиниция 4. Нека M е модул над R. Тогава:

- Множеството $\{m_1, \ldots, m_k\} \subseteq M$ наричаме **линейнонезависимо**, ако за кои да е коефициенти $\{r_i\}$, от $\sum_i r_i m_i = 0$ следва $r_i = 0 \, \forall i$. Произволно подмножество $S \subseteq M$ наричаме линейнонезависимо, ако всяко негово крайно подмножество с линейнонезависимо.

[1] Следва от аксиомите за дистрибутивност: $0 \cdot m = (0+0) \cdot m = 0 \cdot m + 0 \cdot m$ и с добавяме на $-(0 \cdot m)$ към двете страни излиза $0 = 0 \cdot m$

[2] Използваме, че $(-1) + 1 = 0$ и отново дистрибутивност: $(-1) \cdot m + m = (-1) \cdot m + 1 \cdot m = (-1+1) \cdot m = 0 \cdot m = 0_M$, тоест $(-1) \cdot m$ е обратният на m.

- **Обвивка** на множеството $S \subseteq M$ наричаме множеството от всички крайни линейни комбинации на елементи в B:

$$\operatorname{span}(B) = \left\{ \sum_{i=1}^{n} r_i m_i \,\middle|\, r_i \in R, \{m_i\}_{i=1}^{n} \subseteq B \right\}$$

  Казваме още, че B **поражда** модула M, ако $\operatorname{span}(B) = M$. Ако съществува крайно такова B, наричаме M **крайнопороден** модул.

- Едно подмножество $B \subseteq M$ се нарича **базис** на M, ако е линейнонезависимо и поражда модула M.

Сега по аналогия с линейни изображения дефинираме:

Дефиниция 5. Нека $f : M \to N$ е функция между модулите M и N над пръстена R.

- f се нарича **хомоморфизъм** на модули, ако е хомоморфизъм на групи, и освен това е съгласуван с умножението със скалар, тоест е изпълнено $f(r \cdot m) = r \cdot f(m)$ за всички $r \in R, m \in M$.
- Ако f е хомоморфизъм и биекция, то f наричаме **изоморфизъм**, а модулите M и N - изоморфни.
- Дефинираме още **ядрото** $\operatorname{Ker} f \coloneqq \{\, m \in M \mid f(m) = 0_N \,\}$ и **образа** $\operatorname{Im} f \coloneqq \{\, n \in N \mid \exists m : n = f(m) \,\}$ на хомоморфизма f.

Теорема 1 (Теорема за хомоморфизмите)**.** *Ако $f : M \to N$ е хомоморфизъм на модули, то $M/\operatorname{Ker} f \cong \operatorname{Im} f$.*

Бележка. Базис на модул M може да дефинираме и с т.нар. „универсално“ свойство: едно подмножество $B \subseteq M$ е базис, ако всяка функция $f : B \to N$ в някой модул N може да се продължи по единствен начин до хомоморфизъм.

Твърдение 2. *Нека M е модул над R с базис B. Всеки ХММ $\varphi : M \to N$ се определя еднозначно от стойностите си върху този базис. Тоест, ако $f : B \to N$ е произволна функция в някой модул N, то съществува единствен ХММ $\varphi : M \to N$ с $\varphi\big|_B = f$.*

Доказателство. Нека B е базис на модула M над R, N е модул над M и $f : B \to N$ е произволна функция. Определяме $\varphi : M \to N$ по следния начин:

Нека $m \in M$ е произволен елемент. Тогава $m = \sum_i r_i b_i$ за някои $r_i \in R, b_i \in B \,\forall i$, и това представяне е единствено. Значи можем да определим $\varphi(m) = \sum_i r_i f(b_i)$. Очевидно така дефинираното φ е ХММ и $\varphi\big|_B = f$.

Да допуснем сега, че има друг ХММ ψ с $\psi\big|_B = f$ и нека $m = \sum_i r_i b_i$ е произволен. Тогава:

$$\begin{aligned}(\varphi - \psi)(m) &= (\varphi - \psi)\left(\sum_i r_i b_i\right) = \sum_i r_i (\varphi - \psi)(b_i) \\ &= \sum_i r_i (\varphi(b_i) - \psi(b_i)) \\ &= \sum_i r_i (f(b_i) - f(b_i)) = \sum_i r_i 0_N = 0\end{aligned}$$

тоест $(\varphi - \psi) \equiv id$ и φ е единственият такъв ХММ. □

4 Значението на обратимостта в линейната алгебра

Ще обърнем внимание на някои основни твърдения от линйената алгебра и ще проследим ключовите разсъждения в доказателствата им, за да разберем какво се случва при модулите.

Мини-твърдение 4.1. Нека $\lambda \in F, v \in V$. Тогава в ЛП имаме следната естествена еквивалентност: $\lambda v = 0 \Leftrightarrow \lambda = 0 \vee v = 0$.

Доказателство. Щом F е поле, всеки ненулев елемент е обратим. Тогава имаме два случая за λ:

- $\lambda = 0$, тогава $\lambda v = 0v = 0$ (проверихме по-рано).
- $\lambda \neq 0$ и $\exists \lambda^{-1}$, тогава $\lambda v = 0 \Leftrightarrow \lambda^{-1}\lambda v = \lambda^{-1}0 \Leftrightarrow 1v = 0 \Leftrightarrow v = 0$

От втората точка пък директно излиза, че единственият линейнозависим (сам със себе си) вектор е нулевият.

Главна роля тук играе това, че в поле всички ненулеви скалари са обратими. □

Линейна независимост и базис

Сега ще разгледаме две твърдения, свързващи линейната независимост със свойството „принадлежност“ на линейна обвивка, и две техни следствия, свързващи линейната (не)зависимост на някакво множество с построяването на базис на пространството.

Мини-твърдение 4.2. Ако дадено множество вектори е линейнозависимо, то поне един от векторите може да се изрази като комбинация на (някои от) останалите.

Доказателство. Нека $\sum_i \lambda_i a_i = 0$ и $\exists k : \lambda_k \neq 0$. Тогава можем да напишем $\lambda_k a_k = -\sum_{i \neq k} \lambda_i a_i$ и използвайки обратимостта на ненулевите елементи, да умножим двете страни с λ_k^{-1} и да получим $a_k = \sum_{i \neq k} \left(-\frac{\lambda_i}{\lambda_k}\right) a_i$. □

Донякъде контрапозитивно[3] на 4.2 е следното:

Мини-твърдение 4.3. Ако един вектор не лежи в обвивката на някакви вектори, то той е независим от тях. И по-точно:

Нека $v \notin l(\{u_i\})$. Тогава $\mu v + \sum_i \lambda_i u_i = 0$ влече $\mu = 0$.

Доказателство. Отново лесно можем да се убедим в това, допускайки $\mu \neq 0$, и умножавай равенството с μ^{-1}. Така излиза $v = \sum_i \left(-\mu^{-1}\right) \lambda_i u_i \in l(\{u_i\})$, което е противоречие и значи $\mu = 0$. □

Да видим как 4.2 и 4.3 ни дават съществуване на базис, съдържащ се във/съдържащ дадено множество:

- От 4.2 получаваме, че ако V е крайнопородено от S линейно пространство, то S съдържа базис на V.

  Ако S е ЛНЗ, S е базис. В противен случа използваме, че линейната зависимост на S ни дава вектор, лежащ в обвивката на останалите, и него можем да отстраним, ненарушавайки обвивката – така след краен брой стъпки ще получим базис.

- Твърдение 4.3 пък можем ни дава следното: Ако V е крайнопородено, то всяко линейнонезависимо подмножество може да се допълни до базис.

За да си пречупим мисленето и да разберем какво се случва при модулите, даваме следното обобщение:

Ако $v \notin \text{span}(S)$, то v е независим спрямо S.	Ако S е линейнозависимо, то $\exists v \in S : v \in \text{span}(S \setminus \{v\})$
Ако S е ЛНЗ, то S е допълнимо до базис.	Ако $\text{span}(S) = V$, то S е редуцируемо до базис.

[3] Не е точно контрапозитивно, тъй като в 4.3 не изискваме даденото множество да е независимо

Ще видим как всяко от четирите (напълно естествени) твърдения се чупи в общия случай при модули. Ако трябва с едно изречение да го изразим: линейната обвивка на едно множество дава всички линейнозависими от него вектори, а всичко извън обвивката му е линейнонезависимо от него.

Завършваме този раздел с още няколко факта от линейната алгебра:

1. Може би почти тривиална забележка, но всяко подпространство $V' \leq V$ на едно крайнопородено пространство също е крайнопородено, като при това $\dim V' \leq \dim V$.
2. В горното, ако $V' \leq V$, то размерностите са равни, точно когато пространствата съвпадат: $\dim V' = \dim V \Leftrightarrow V = V'$. Тоест, ако едно подмножество е строго подпространство, то размерността му е строго по-ниска от тази на надпространството.
3. Линейната обвивка на един вектор е инвариантна относно умножението му със скалар: $\text{span}(\{v\}) = \text{span}(\{av\}) \forall a \in F$.
4. С елементарни преобразувания по редове и стълбове всяка матрица може да се приведе във вид на матрица с нули извън главния диагонал и само единици и нули по самия него.

5 От пространства към модули

Сега ще разгледаме къде се чупят аналогичните твърдения за модули:

1. Още по въпроса за $(\lambda v = 0 \Leftrightarrow \lambda = 0 \vee v = 0)$ намираме контрапример с кой да е краен модул над $\mathbb{Z}$ (на практика всички крайни абелеви групи).

   Например, в $\mathbb{Z}_6$ като модул над $\mathbb{Z}$ имаме, че $2 \cdot \overline{3} = \overline{3} + \overline{3} = \overline{6} = \overline{0}$, но нито 2 е нулев скалар, нито $\overline{3}$ е нулев вектор. В линейно пространство щяхме да умножим равенството с 2^{-1}, но 2 не е обратим елемент в пръстена $\mathbb{Z}$ и тази техника е неприложима тук.

2. Всеки пръстен е модул над себе си – да разгледаме $\mathbb{Z}$ над $\mathbb{Z}$ и множеството $S = \{2, 3\}$. Тогава S поражда целия пръстен, тъй като $\text{НОД}(2, 3) = 1$. Освен това, S е линейнозависимо: $2 \cdot 3 + (-3) \cdot 2 = 0$ е нетривиална комбинация на нулевия вектор. Очевидно, обаче, не можем да отстраним никой от елементите на S, запазвайки обвивката — нито $\{2\}$, нито $\{3\}$ пораждат целия модул.

   Тоест, при модули пораждащите множества не са задължително редуцируеми до базис.

   И обратно – множеството $\{2\}$ е линейнонезависимо, но не можем да го допълним до базис, тъй като всеки елемент извън обвивката е зависим от двойката (по същия начин като горе).

   Тук директно виждаме как пряката връзка от линейните пространства „линейна обвивка - линейна независимост“ се разкъсва.

   Причината да не можем да остраним никой от елементите на $\{2, 3\}$, запазвайки обвивката, е че никой от тях не може да се изрази чрез останалите: $2 \neq \lambda 3$ за всяко $\lambda \in \mathbb{Z}$. В линейно пространство щяхме да умножим нулевата комбинация с обратния елемент на някой от ненулевите коефициенти, но тук нито 2, нито (-3) имат обратни елементи.

3. Изобщо, възможно е един крайнопороден модул да няма *никакъв* базис. Трагизмът достига дори още по-големи висоти – един модул може изобщо да няма линейнонезависими вектори.

   По-горе отбелязахме, че в линейно пространство единственият линейнозависим вектор е нулевият.
   Връщайки се отново към модула $M = \mathbb{Z}_n$ над $\mathbb{Z}$ за кое да е фиксирано $n \in \mathbb{N}$, можем да забележим, че $n \cdot r = 0_M$ за кой да е остатък $r \in \mathbb{Z}_n$. Тоест, всеки елемент на модула е зависим... сам със себе си!

   Тези транс-структурни делители на нулата възникват дори когато самият пръстен няма делители на нулата, както $\mathbb{Z}$, поради самата връзка между двете алгебрични структури, индуцирана от операцията $\cdot$.

4. Заслужава си да обърнем внимание, че тези аномалии са изключително свързани с пръстена, над който разглеждаме модула.

   Като модул над $\mathbb{Z}$, наистина $M = \mathbb{Z}/n\mathbb{Z}$ от предната точка страда от нечовешка безбазисност. Ако вместо над $\mathbb{Z}$ обаче разгледаме M като модул над самия себе си (незабравяйки, че M е пръстен), веднага излиза, че $\{1_M\}$ е базис. И изобщо, кой да е пръстен R е модул над себе си с базис $\{1_R\}$.

5. Да обърнем внимание на проблема с размерностите - $2\mathbb{Z}$ е строго подмодул на $\mathbb{Z}$, но и двата модула се пораждат от единствен елемент - $\mathbb{Z} = \langle 1 \rangle, 2\mathbb{Z} = \langle 2 \rangle$.

   В случая на линейни пространства, подпространство от същата размерност трябва да съвпада с първоначалното пространство, но при модулите това не е задължително.

   Липсата на деление в пръстена е слабост, която се пренася върху линейната обвивка, и тя вече не може да покрие всички зависими вектори.

   Сега ще видим, че подмодулите могат не просто да не намалеят по размерност спрямо надмодула, но и да нараснат! По-късно ще видим определени условия, при които нарастване на размерността не може да настъпи.

6. Завършваме този списък с още един разтърсващ пример: разглеждаме пръстена $R = \mathbb{R}[x_1, x_2, \dots]$ на полиномите на изброимо безкрайно много променливи като модул над себе си. Значи R е крайнопороден и има базис $\{1_R\}$. Казахме, че в този случай идеалите на R образуват подмодули на R.

   Нека I е идеалът, породен от $\{x_i\}_{i=1}^{\infty} \subset R$, тоест $I = \{f \in R \mid f(0, \dots, 0) = 0\}$ - полиномите без свободен член. Ще проверим, че I не е крайнопороден.

   Доказателство. Допускаме обратното, нека I е крайнопороден: $I = \langle f_1, \dots, f_n \rangle, f_i \in R$, тогава сред пораждащите го полиноми f_i ще има краен брой променливи и можем да изберем променлива x_t извън всички тях. Тогава полиномът x_t ще лежи в идеала, тъй като няма свободен член, и значи се записва като комбинация $x_t = \sum_{i=1}^{n} r_i f_i$, където r_i са полиноми от R. В тази сума обаче всяко събираемо (след „разкриване на скобите“ в умноженията $r_i f_i$) е кратно на някоя променлива, различна от x_t, и няма как да получим сбор x_t. Противоречието означава, че допускането за крайнопородеността на I е грешно, значи I не е крайнопороден. □

   Излезе, че подмодулът $I \leq R$ не е крайнопороден, въпреки че модулът R има краен базис.

   С аналогични разсъждения можем да проверим, че в модула $M = R[x_1, \dots, x_n]$ над себе си, подмодулът $N = \langle x_1, \dots, x_n \rangle$ се поражда от най-малко n елемента, докато самият M се поражда директно от единицата:

   Отново допускаме, че $N = \langle f_1, \dots, f_k \rangle$ за някое $k < n$, тогава $f_i = x_{j_i} * f_i'$ и взимаме променлива $x_t \neq x_{j_i} \forall i$, която трябва да принадлежи на идеала, но всички f_i или не съдържат x_t, или са от степен поне 2. Тогава x_t не може да е комбинация на f_i и получаваме противоречие.

   Бележка. В последната ситуация, ако $n > 1$, то $N \leq M$ има строго по-голямо минимално пораждащо множество от M.

   При $n = 1$, обаче, подмодулът N има също толкова голямо пораждащо множество - $\langle x \rangle$. Можем да забележим, че в този случай $M = R[x]$ е област от главни идеали (ако R е поле), и тогава аномалията, която видяхме по-горе, не се случва. По-нататък ще видим, че изобщо над области от главни идеали имаме точна горна граница за броя пораждащи елементи на подмодули на крайнопороден модул.

Въпреки че един подмодул на крайнопороден модул не е задължително крайнопороден, то имаме следното твърдение:

Твърдение 3. *Ако M е крайнопороден модул над R и $N \leq M$ е произволен подмодул, то фактормодулът M/N също е крайнопороден.*

Доказателство. Тук просто взимаме съседните класове на пораждащите елементи: ако $M = \langle m_1, \ldots, m_n \rangle$, то очевидно $M/N = \langle m_1 + N, \ldots, m_n + N \rangle$. □

6 Анихилатор и периодичност

Ето две дефиниции, мотивирани от примерите в предната точка. Ще използваме първата във втората, която пък е първото стъпало към крайната цел - класификацията на крайнопородените модули.

6.1 Анихилатор

Видяхме, че при модулите е възможно $r \cdot m = 0$ за ненулев скалар r и ненулев вектор m. Да разучим въпроса за тези „транс-структурни“ делители на нулата по-подробно.

Дефиниция 6. Нека M е модул над R.

- *Анихилатор на елемента $m \in M$* наричаме множеството скалари, които го нулират: $\mathrm{Ann}(m) = \{ r \in R \mid r \cdot m = 0 \}$.
- *Анихилатор на множеството $S \subseteq M$* наричаме множеството скалари, които нулират всичко в S: $\mathrm{Ann}(S) = \{ r \in R \mid \forall m \in S : r \cdot m = 0 \}$.

Например, в пръстена $\mathbb{Z}_{21}$ над $\mathbb{Z}$, анихилаторът на $\overline{7} \in \mathbb{Z}_{21}$ е

$$\mathrm{Ann}(\overline{7}) = \{r \in \mathbb{Z} \,|\, r \cdot \overline{7} = 0\} = \{r \in \mathbb{Z} \,|\, 7r \equiv 0 \bmod 21\} = 3\mathbb{Z}$$

Тук може да ни направи впечатление връзката между 7, 21 и 3, и да забележим, че $\langle \overline{7} \rangle \cong \mathbb{Z}/3\mathbb{Z}$. В сила е следното твърдение:

Твърдение 4. *Нека R е пръстен, M е модул над R и $m \in M$. Разглеждаме модула, породен от този елемент: $\langle m \rangle = l(\{m\})$. Тогава $\langle m \rangle \cong R/\mathrm{Ann}(m)$.*

Доказателство. Разглеждаме хомоморфизма (на модули[4]) $\varphi : R \to M$, дефиниран с $\varphi(r) = r \cdot m$. Тогава по теоремата за хомоморфизмите имаме, че $R/\operatorname{Ker}(\varphi) \cong \operatorname{Im}(\varphi)$, и в случая $\operatorname{Ker}(\varphi) = \mathrm{Ann}(m)$, а $\operatorname{Im}(\varphi) = \langle m \rangle$. □

Бележка. Тук можем да направим аналогия с теоремата за орбитите и стабилизаторите при действие на група върху множество X. Тя казва, че дължината на орбитата на един елемент от X е индексът на стабилизатора му.

В случая, пръстенът R „действа“ върху модула M, и орбитата на m под това действие е подмодулът $\langle m \rangle = Rm$, а ролята на стабилизатор на даден елемент играе анихилаторът му. И така, индексът на анулатора в пръстена е дължината на орбитата на елемента m. Тоест на всеки елемент на орбитата $\langle m \rangle$ съответства по един съседен клас на анихилатора.

Тези особени случаи на ненулеви вектори, които отиват в нулата под действието на ненулеви скалари от пръстена, заслужават специално внимание.
Ако в пръстена R има делители на нулата, съществуването на такива е тривиално, затова в следващата подсекция разглеждаме само пръстени без делители на нулата. В допълнение ще поискаме и комутативност на R, за да работи и следващото твърдение (5).

[4]Не забравяме (както аз), че R също е модул над R, както M. Тоест φ наистина е ХММ на модули.

6.2 Периодични и точни модули

Дефиниция 7. Нека R е област на цялост и M е модул над него. Един елемент $m \in M$ се нарича **периодичен**, ако има нетривиален анихилатор: $\mathrm{Ann}(m) \neq \{0\}$.

Обозначаваме множеството на периодичните вектори в M с M_t. Модулът M се нарича **периодичен модул**, ако всички вектори са периодични, и **точен**, ако $M_t = \{0\}$.

Бележка. Веднага разсейваме всякакви съмнения, че горната характеризация покрива всички модули. $\mathbb{Z} \times \mathbb{Z}_n$ над $\mathbb{Z}$ за $n \leq 2$ не е нито точен:

$$n \cdot (0, \overline{k}) = (0, \overline{n}) = (0, \overline{0}) \Rightarrow \mathrm{Ann}\left((0, \overline{1})\right) \neq \{0\} \Rightarrow \left((0, \overline{1})\right) \in M_t,$$

нито периодичен: $\forall k : k \cdot (1, \overline{0}) = (k, \overline{0}) \neq (0, \overline{0})$

Твърдение 5. *Ако R е област на цялост, то M_t е подмодул на на M, а M/M_t е точен.*

Доказателство. $M_t \subseteq M$, значи за да е подмодул остава да проверим затвореностите:

- Нека m и n са периодични. Тогава има скалари $r, s \in R$ със свойството $r \cdot m = s \cdot n = 0$ и за да получим $m + n \in M_t$, взимаме скалара $r * s$ и проверяваме:

$$\begin{aligned}(r * s) \cdot (m + n) &= (r * s) \cdot m + (r * s) \cdot n \\ &= (s * r) \cdot m + (r * s) \cdot n \\ &= s \cdot (r \cdot m) + r \cdot (s \cdot n) \\ &= s \cdot 0 + r \cdot 0 = 0 + 0 = 0\end{aligned}$$

  тоест наистина $m + n$ е също периодичен вектор.

  Обръщаме внимание, че тук е съществено пръстенът да е комутативен, за да направим размяната $r * s = s * r$.

- Нека m е периодичен с $t \cdot m = 0$ и $r \in R$ е произволно. Искаме $r \cdot m \in M_t$. Взимаме t и проверяваме: $t \cdot (r \cdot m) = (t * r) \cdot m = (r * t) \cdot m = r \cdot (t \cdot m) = r \cdot 0 = 0$, значи $r \cdot m \in M_t$. Тук отново съществено използвахме комутативността на R.

Тогава M_t е затворен относно събиране на вектори и умножение със скалар, следователно е подмодул.

Проверката, че M/M_t е точен, е също толкова директна, сега искаме $(M/M_t)_t = \{0\}$.

Нека $m + M_t \in (M/M_t)_t$ е произволен периодичен елемент. Тогава има $r \in R \setminus \{0\}$, за което $r \cdot (m + M_t) = 0_{M/M_t} = M_t$. Тоест $(r \cdot m) + M_t = M_t$, или $r \cdot m \in M_t$. Това ни дава друг скалар $s \in R \setminus \{0\}$, за който $s \cdot (r \cdot m) = 0_M$, тоест $(s * r) \cdot m = 0_M \Leftrightarrow m \in M_t \Leftrightarrow m + M_t = M_t = 0_{M/M_t}$ и значи M/M_t е точен. □

Пример 6.1. В частния случай на модул над $\mathbb{Z}$, периодични са елементите от краен ред на абелева група. Последното твърдение пък се явява обобщение на факта, че фактор-групата на една абелева група по подгрупата от крайните ѝ елементи няма елементи от краен ред освен неутралния.

Пример 6.2. Да онагледим последното твърдение с още един пример. Да вземем $M = 2\mathbb{Z} \times 3\mathbb{Z} \times \mathbb{Z}_p$ за някое $p \in \mathbb{N}$ като модул над $\mathbb{Z}$.

Произволен вектор $(n, m, \overline{r}) \in M$ тогава е периодичен, точно когато $n = m = 0$ — в противен случай първите две компоненти няма да се нулират при умножение с цяло число, а умножавайки $(0, 0, \overline{r})$ с p ще получим $(0, 0, p \cdot \overline{r} = \overline{0}) = 0_M$.

Значи $M_t = \{0_{2\mathbb{Z}}\} \times \{0_{3\mathbb{Z}}\} \times \mathbb{Z}_p$. Ако факторизираме по него, получаваме

$$M/M_t = \frac{2\mathbb{Z} \times 3\mathbb{Z} \times \mathbb{Z}_p}{\{\,(0_{2\mathbb{Z}}, 0_{3\mathbb{Z}})\,\} \times \mathbb{Z}_p} \cong \frac{2\mathbb{Z} \times 3\mathbb{Z}}{\{\,(0_{2\mathbb{Z}}, 0_{3\mathbb{Z}})\,\}} \cong 2\mathbb{Z} \times 3\mathbb{Z}$$

В този простичък пример можем да направим едно интересно наблюдение: $M \cong M_t \times (M/M_t)$, тоест нашият модул се представя като директна сума от периодичния си подмодул и точен модул. Още повече, тук точният модул $M/M_t \cong 2\mathbb{Z} \times 3\mathbb{Z}$ има базис - $\{(2,3)\}$. Целта на този документ е да проучим именно това явление.

Пример 6.3. Заслужава си да се спомене, че един периодичен модул не е задължително да е краен, както в примерите с остатъци. Във фактор-модула $\mathbb{Q}/\mathbb{Z}$ над $\mathbb{Z}$ например елементите са съседните класове от вида $\frac{p}{q} + \mathbb{Z}$, където $\frac{p}{q}$ е правилна дроб[5], т.е. в интервала $[0, 1)$. Очевидно тогава, умножавайки (в смисъл на операцията „умножение със скалар“) по знаменателя q, получаваме $q \cdot (\frac{p}{q} + \mathbb{Z}) = p + \mathbb{Z} = \mathbb{Z} = 0_{\mathbb{Q}/\mathbb{Z}}$, тоест всеки елемент е периодичен и значи самият модул е периодичен.

7 Свободни модули

Дефиниция 8. Един модул M се нарича **свободен**, ако притежава базис.

Оказва се, че теоремата за съществуване на базис на лиенйно пространство над F продължава да е в сила и при далеч по-слаби изисквания от това F да е поле - достатъчно е F да е пръстен с деление.

Твърдение 6. *Ако R е тяло и M е модул над R, то M е свободен модул. В частност, ако R е поле, то всяко линейно пространство над R има базис.*

Доказателство. Върви дословно както за линейни пространства, тъй като доказателството не използва други свойства на F, освен обратимостта, нужна за твърдението, че всеки вектор извън дадена обвивка е независим с всички вектори в нея – което е индукционната стъпка в доказателството. □

Твърдение 7. *Ако един модул M над R има базис B, то $M \cong R^{(B)} = \oplus_B R$. В частност, ако базисът е краен с $|B| = n < \infty$, то $M \cong R^n$, тоест можем да разглеждаме свободните модули като множества наредени n-орки, т.е. като декартово произведение на n копия на пръстена.*

Проверяваме само крайнопородения случай.

Доказателство. Нека $B = \{e_i\}$. Естествено е да дефинираме изображението $\varphi : M \to R^n$ с

$$\varphi(v) = \varphi\left(\sum_i \lambda_i e_i\right) = (\lambda_1, \ldots, \lambda_n) \in R^n.$$

Очевидно φ е хомоморфизъм.

Проверяваме за биекция:

- Нека $\varphi(\sum_i \lambda_i e_i) = \varphi(\sum_i \mu_i e_i)$. Тогава $(\lambda_1, \ldots, \lambda_n) = (\mu_1, \ldots, \mu_n)$, тоест $\lambda_i = \mu_i \forall i$ и значи $\sum_i \lambda_i e_i = \sum_i \mu_i e_i$. Следователно φ е инекция.
- За всеки вектор $(\lambda_1, \ldots, \lambda_n) \in R^n$ очевидно $\sum_i \lambda_i e_i$ е праобраз. Тогава φ е сюрекция.

Следователно φ е изоморфизъм и $M \cong R^n$. □

Със следващото твърдение подсигуряваме, че при краен базис броят на копията на пръстена, на чието произведение е изоморфен модулът, е еднозначно определен:

Твърдение 8. *Ако R е ненулев комутативен пръстен, то $R^m \cong R^n$ като модули над R влече $m = n$.*

[5] Ако не е, можем да отделим най-голямата по абсолютна стойност цяла част и да я „прехвърлим“ на $\mathbb{Z}$. Формално, елементите в един съседен клас се различават с елемент от подмодула, т.е. с цяло число, и тогава можем да вземем най-малкия положителен представител.

Доказателство. Ще сведем задачата до познатата теорема от линейната алгебра, че $V \cong W \Leftrightarrow \dim V = \dim W$ за произволни крайнопородени ЛП.

Най-напред ще извадим от ръкава[6] един максимален идеал на R: всеки собствен идеал на R **не** съдържа единицата и тогава произволно обединение на собствени идеали (в частност, нарастващи редици от такива) също няма да съдържа единицата, тоест отново е собствен идеал.

Тогава по лемата на Цорн съществува максимален такъв (собствен) идеал[7] I. От висшата алгебра знаем, че в такъв случай R/I е поле – и тук използваме комутативността на R. Ще докажем, че $(R/I)^n \cong (R/I)^m$ като на модули над R/I и от линейната алгебра ще получим $n = m$.

Нека $R^n \cong R^n$ и $\varphi : R^n \to R^m$ е изоморфизъм. Ще докажем, че $R^n/IR^n \cong R^m/IR^m$ като модули над R/I и $R^k/IR^k \cong (R/I)^k$, пак като модули над R/I, откъдето вече $(R/I)^n \cong (R/I)^m$.

1. Между R^n/IR^n и R^m/IR^m директно построяваме хомоморфизма $(\vec{r} + IR^n) \mapsto (\varphi(\vec{r}) + IR^m)$. Тъй като φ е изоморфизъм, то и последното изображение е биекция.
2. Доказваме $R^k/IR^k \cong (R/I)^k$ с теорема за хомоморфизмите за изображението $\big((r_1, \ldots, r_k) + IR^k\big) \mapsto (r_1 + I, \ldots, r_k + I)$, което очевидно е сюрекция, а ядрото му е IR^k.

□

Това на пръв поглед очевидно твърдение може да се стори някому безинтересно и незаслужаващо внимание, но в действителност истината при пръстени е много по-сурова и горното твърдение изобщо не е вярно, ако се откажем от допускането за комутативност на R:

Пример 7.1. Да разгледаме множеството $E = \mathbb{CFM}_{\mathbb{N}}(R)$ от безкрайните (и по редове, и по колони) матрици с краен брой ненулеви колони. Очевидно сборът на две матрици в E е коректно определен (има краен брой ненулеви колони).

Всяка матрица в E от някой номер нататък има изцяло нулеви колони, и това позволява коректно да дефинираме произведението, както за крайни матрици (ред по стълб):

$$\begin{pmatrix} \boldsymbol{a_{1,1}} & \cdots & \boldsymbol{a_{1,n}} & 0 \cdots \\ \vdots & \ddots & \vdots & \vdots \\ \boldsymbol{a_{m,1}} & \cdots & \boldsymbol{a_{m,n}} & 0 \cdots \\ a_{m+1,1} & \cdots & a_{m+1,n} & 0 \cdots \\ \vdots & & \vdots & \vdots \end{pmatrix} \times \begin{pmatrix} \boldsymbol{b_{1,1}} & \cdots & \boldsymbol{b_{1,m}} & 0 \cdots \\ \vdots & \ddots & \vdots & \vdots \\ \boldsymbol{b_{n,1}} & \cdots & \boldsymbol{b_{n,m}} & 0 \cdots \\ b_{n+1,1} & \cdots & b_{n+1,m} & 0 \cdots \\ \vdots & & \vdots & \vdots \end{pmatrix}$$

Тъй като само краен брой m от стълбовете на дясната матрица са ненулеви, то в произведението редовете на лявата след m-тия не оказват влияние. Аналогично, редовете на дясната след n-тия също не участват в произведението, и в резултата ненулеви елементи може да има единствено в горната лява $m \times n$-подматрица.

Тогава E образува пръстен с естественото събиране и умножение на матрици.

За този пръстен се оказва, че $E \cong E^2$ като модули над E. Как? Да разгледаме следното изображение:

$$\varphi : E \to E^2$$
$$\left(\vec{a_1}, \vec{b_1}, \ldots, \vec{a_n}, \vec{b_n}, \vec{0}, \ldots\right) \mapsto \left(\left(\vec{a_1}, ..., \vec{a_n}, \vec{0}, ...\right), \left(\vec{b_1}, ..., \vec{b_n}\vec{0}, ...\right)\right)$$

На всяка финитно-стълбова матрица A съпоставяме две матрици - една от четните и една от нечетните стълбове на A. Очевидно φ е биекция, като обратното изображение „слива“ две матрици в една по обратния начин. Също толкова очевидно е, че φ е ХММ на групи.

За да не се отклоняваме твърде от темата, ще пропуснем проверката, че $\varphi(A * B) = A \cdot \varphi(B)$. В крайна сметка φ е изоморфизъм на модули, и това осмисля твърдението 8.

[6] на Цорн

[7] максимален по смисъл на включване на множества

Последният пример мотивира следната дефиниция, която няма да използваме по-нататък, но си струва да отбележим:

Дефиниция 9. Казваме, че един пръстен R е инвариантен относно дължините на базисите, ако от $R^n \cong R^m$ като модули над R следва $n = m$.

И така, твърдение 8 всъщност казва, че комутативните пръстени са инвариантни относно дължините на базисите.

Сега ще видим, че при свободните модули аномалии като транс-структурни делители на нулата не могат да се появят.

Твърдение 9. *Нека R е област на цялост[8], а M е свободен модул над него. Тогава M е точен.*

Основното разсъждение тук е, че базисите дават единствено представяне на нулата, докато периодичността, или делителите на нулата, дават *различни* представяния на нулата. В известен смисъл базисите ни „предпазват“ от аномалии с нулата.

Доказателство. Нека M има базис $B = \{b_i\}$, $m \in M$ и $r \cdot m = 0$. Ще докажем, че $r = 0_R \vee m = 0_M$. Имаме:

$$0 = r \cdot m = r \cdot \sum_i r_i \cdot b_i = \sum_i r \cdot (r_i \cdot b_i) = \sum_i (r * r_i) \cdot b_i$$

Тъй като B е базис, то единственото представяне на нулата в него е с нулеви коефициенти, значи $r * r_i = 0 \ \forall i$. R няма делители на нулата, и значи или $r = 0_R$, или $r_i = 0_R \forall i$. Последното пък е еквивалентно на $m = 0_M$ □

Наличието на базис изключва възможността за периодични елементи. Отсъствието на такива обаче далеч не е достатъчно, за да бъде един модул свободен:

Пример 7.2. Като модул над $R = \mathbb{Z}[x]$, идеалът-подмодул $I = \langle 2, x \rangle \leq R$ очевидно няма периодични елементи, тъй като самият $\mathbb{Z}[x]$, както и неговите идеали, образуват област на цялост – умножение с ненулев полином не може да намали степента.

I е точен, но в него не можем и да съзнуваме за базис. Защо? Надмодулът му R над R се поражда от $\{1_R\}$, тоест в R максималният брой линейнонезависими вектори е 1. Тогава всеки базис на I съдържа най-много един елемент, но от висшата алгебра знаем, че $I \leq R$ не е главен идеал и не може да се породи от само един елемент.

Следователно I не допуска базис, въпреки че е точен модул над R. На всичкото отгоре е и подмодул на свободен модул!

В основата на последния контрапример стои фактът, че пръстенът R съдържа неглавни идеали. В други отношения модулите I и R имат доста апетитни свойства - и двата са точни и крайнопородени. Логично е да се запитаме, не можем ли да издействаме свобода на крайнопороден точен модул, когато неговият пръстен е на главни идеали?

Сега преместваме фокус именно върху модули над области от главни идеали.

8 Модули над пръстени от главни идеали

Твърдение 10. *Нека M е точен крайнопороден модул над област от главни идеали R. Тогава M допуска краен базис.*

Бележка. И трите условия са ключови. Ако се откажем от условието за

[8] Припомняме, че в самата дефиниция на периодичен и точен модул поискахме пръстенът да е област на цялост, тоест с това условие не стесняваме общността на твърдението.

- крайнопороденост, имаме контрапример – $\mathbb{Q}$ над $\mathbb{Z}$;
- R да бъде ОГИ – вж. примера с $\langle 2, x\rangle \leq R[x]$;
- M да бъде точен – $\mathbb{Z}_n$ над $\mathbb{Z}$ не е свободен. (Заб.: все пак е крайнопороден)

За удобство в някои от следващите твърдения прилагаме следната лема. Ще я използваме, за да извършваме индуктивно разсъждения върху размерностите на модулите.

Лема 11. *Ако $\varphi : M \to M$ е идемпотентен ендоморфизъм върху свободен модул* $\operatorname{Im}\varphi$*, то* $M \cong \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi$.

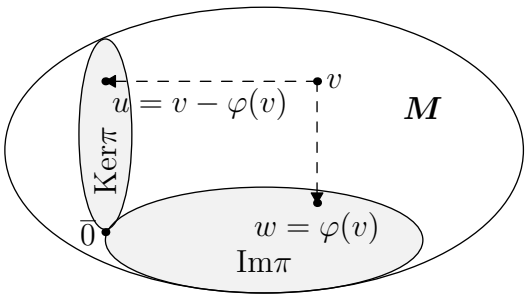
Може да се окаже изненадващо, но в общия случай не можем от теоремата за изоморфизмите просто да „прехвърлим“ ядрото от другата страна със знак $\times$.

Например, $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$, но за $n \geq 2$ не е вярно, че $\mathbb{Z} \cong n\mathbb{Z} \times \mathbb{Z}_n$ със стандартните операции при декартово произведение на групи. Ако допуснем съществуването на такъв изоморфизъм ψ, получаваме противоречие:

$$\begin{aligned}
(k, \overline{0}) &= (k, \overline{0+0}))\\
(k, \overline{0}) &= (k, \overline{0}) + (k, \overline{0})\\
\mathbf{0}_{n\mathbb{Z}\times\mathbb{Z}_n} &= (k, \overline{0})\\
\psi(\mathbf{0}) &= \psi((k, \overline{0}))\forall k\\
(k, \overline{0}) &\in \operatorname{Ker}\psi\\
\operatorname{Ker}\psi &\neq \{0\}
\end{aligned}$$

Доказателство Ще приемем, че $\varphi(M) \leq N \leq M$ и ще построим директен изоморфизъм $\psi : M \to \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi$.

Нека $v \in M$ е произволен. Търсим представяне във вида $v = u + w$, където $u \in \operatorname{Ker}\varphi$, а $w \in \operatorname{Im}\varphi$. Естествен избор за w е просто $\varphi(v)$.



Тогава единствената възможност за u остава $u = v - w = v - \varphi(v)$:

$$v = \underbrace{(v - \varphi(v))}_{\text{Искаме да е от } \operatorname{Ker}\varphi} + \underbrace{\varphi(v)}_{\text{от } \operatorname{Im}\varphi}$$

Трябва да проверим, обаче, дали наистина $v - \varphi(v) \in \operatorname{Ker}\varphi$:

$$\begin{aligned}
&v - \varphi(v) \in \operatorname{Ker}\varphi\\
\Leftrightarrow\ &\varphi(v - \varphi(v)) = 0\\
\Leftrightarrow\ &\varphi(v) - \varphi(\varphi(v)) = 0\\
\Leftrightarrow\ &\varphi(v) - \varphi(v) = 0\ \checkmark
\end{aligned}$$

Значи е коректно да дефинираме функцията $\psi : M \to \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi$ по този начин:

$$\psi(v) = (v - \varphi(v),\, \varphi(v))$$

Очевидно ψ е ХММ. Остава да проверим дали е биекция:

- Нека $(u, w) \in \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi$. За сюрекция трябва да намерим $m \in M : \psi(m) = (u, w)$.

  От $w \in \operatorname{Im}\varphi$ имаме $\exists v \in M : \varphi(v) = w$. Тогава $m = \varphi(v) + u$ ще свърши работа:

$$\begin{aligned}
\psi(m) &= (m - \varphi(m), \varphi(m))\\
&= (\varphi(v) + u - \varphi(\varphi(v) + u), \varphi(\varphi(v) + u))\\
&= (\varphi(v) + u - \varphi(\varphi(v)) - \varphi(u), \varphi(\varphi(v)) + \varphi(u))\\
&= (\varphi(v) + u - \varphi(v) - 0, w + 0)\\
&= (u, w)
\end{aligned}$$

Значи ψ е сюрекция.

- Нека $\psi(v) = \psi(v')$ за някои $v, v' \in M$. След прехвърляне от едната страна и разкриване на скоби излиза директно $v = v'$. В тези сметки няма интересни разсъждения.

Значи ψ е изоморфизъм и $M \cong \operatorname{Ker}\varphi \oplus \operatorname{Im}\varphi$. □

По-рано обещахме, че над области от главни идеали подмодулите на свободен модул също са свободни модули, като допускат не по-големи базиси от тези на надмодула.[9] Това можем да получим като следствие от последното твърдение:

Твърдение 12. *Ако R е област от главни идеали, всеки подмодул N на свободен модул M е свободен с ранг, не по-голям от този на M.*

Доказателство. Нека $M = R^n$ (по твърдение 7). С индукция по n:

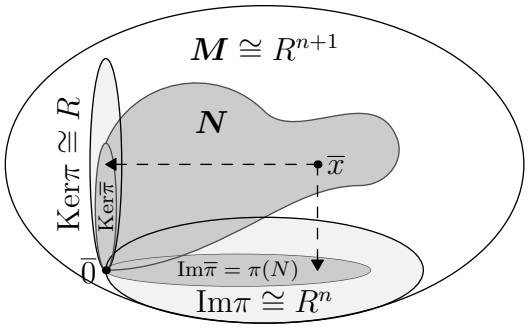
1. При $n = 1$, $M = R$ и $N \leq M$ е идеал на R. R е област от главни идеали, значи $N = \langle x \rangle$ за някое $x \in N$ и $\{x\}$ е базис на N с дължина $1 \leq \dim M$.
2. Нека всички подмодули на R^n са свободни от ранг най-много n. Ще докажем твърдението за $M = R^{n+1}$.

   За да използваме индукционната хипотеза, разглеждаме M като директната сума $R \oplus R^n$ и проекцията му $\pi : (R \oplus R^n) \twoheadrightarrow \pi(M) \cong R^n$ върху втората компонента:

   $$\pi(r_1, \ldots, r_n) = (0, r_2, \ldots, r_n)\,.$$

   Така разлагаме M на две части - $\operatorname{Im}\pi$ и $\operatorname{Ker}\pi$.

   В качеството си на проекция π изпълнява $\pi \circ \pi = \pi$. Да разгледаме рестрикцията на π върху N: $\overline{\pi} \coloneqq \pi|_N : N \to R^n$.



   Прилагайки с малка уговорка[10] предишната лема, получаваме $N \cong \operatorname{Im}\overline{\pi} \oplus \operatorname{Ker}\overline{\pi}$.

   Значи $N = \operatorname{Ker}\overline{\pi} \oplus \operatorname{Im}\overline{\pi}$. И двата компонента на сумата са свободни:

   - По индукция имаме, че $\operatorname{Im}\overline{\pi}$ е свободен модул от ранг най-много n като подмодул на $\operatorname{Im}\pi \cong R^n$;
   - $\operatorname{Ker}\overline{\pi} \leq \operatorname{Ker}\pi \cong R$ и щом е (изоморфен на) подмодул на пръстен, значи е (изоморфен на) идеал на R, който пък от своя страна е област от главни идеали. Значи $\operatorname{Ker}\overline{\pi}$ е главен идеал и свободен модул над пръстена си,

   и тогава N също е свободен.

Така по индукция получаваме твърдението за всяко $n \in \mathbb{N}$. □

За следващата теорема ще бъде удобно да дадем еквивалентно условие за това един модул да бъде крайнопороден:

Лема 13. *M е крайнопороден от S модул над R точно когато съществува епиморфизъм върху M от свободния модул R^S.*

Доказателство. На практика асоциираме всеки пораждащ елемент на M с една „координатна ос“ в R^S.

[9] Припомняме твърдение 8, откъдето свободните модули над област от главни идеали (използваме тяхната комутативност) имат строго определена размерност (ранг).

[10] Не е проблем да считаме, че $\pi(M) \leq N$, тъй като винаги можем да намерим изоморфно копие N' на $\pi(N)$ в самия модул N със съответен изоморфизъм $h : \pi(N) \cong N'$, за който $h \circ \overline{\pi} = id$, и да доказваме твърдението за $\pi' = h \circ \pi$.

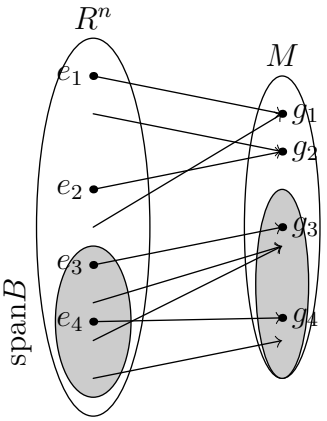
- В лявата посока, ако $f : M \twoheadrightarrow R^n$ е епиморфизъм, то образите на базисните вектори e_i в R^n са (крайно) пораждащо множество: $M = \text{span}\{f(e_i)\}_{i=1}^n$.
- Обратно, ако $M = \text{span}\{a_i\}_{i=1}^n$, то можем да построим търсения хомоморфизъм (по твърдение 2 за универсалното свойство), задавайки го в стандартния базис на R^n: $f(e_i) = a_i$.

  Всяко $m \in M$ е комбинация на елементите $\{a_i\}$ и значи има праобраз в R^n, тоест така построеният хомоморфизъм е сюрекция.

□

Твърдение 14 (Paul Gareth, 2.0.7)**.** *Ако R е област от главни идеали и M е крайнопороден модул над него, то всеки подмодул $N \leq M$ е също крайнопороден.*

С други думи твърдението гласи, че ако се откажем от условието M да бъде точен, то вместо краен базис, ще получим крайно пораждащо множество. Тоест, наличието на периодични елементи чупи линейната независимост, но все пак имаме крайно пораждане.



Доказателство За всеки крайнопороден модул M над R имаме епиморфизъм $\varphi : R^d \twoheadrightarrow M$ за някое $d \in \mathbb{N}$. Липсата на точност тук означава, че някои от копията на R от R^d се изпращат в периодичната част на M и при това изпращане се „смачкват“.

Праобразът на $N \leq M$ в R^d обаче е подмодул $\varphi^{-1}(N) \leq R^d$ на свободен модул, и като такъв, също е свободен с някой базис $B = \{x_1, \ldots, x_m\}$ с $|B| \leq \dim M$ от твърдение 12. Въпросният базис, ако M беше точен, щеше да се изобрази в базис[11] на N. В общия случай обаче можем само да използваме, че $\text{span}(B) = \varphi^{-1}(N)$ и значи $\text{span}(\varphi(B)) = N$, с което намерихме (крайно) пораждащо множество $\varphi(B)$ на N.

□

Бележка. По-рано отбелязахме, че линейнонезависимите множества не са задължително допълними до базис, и в частност, базис на подмодул не е задължително допълним до базис на надмодула.

Например $2\mathbb{Z} \times 2\mathbb{Z} \leq \mathbb{Z} \times \mathbb{Z}$, но не можем да допълним базиса $\{(0,2),(2,0)\}$ на $(2\mathbb{Z})^2$ до базис на $\mathbb{Z}^2$.

Можем, обаче, да направим нещо близко: да намерим базис на подмодула, в който всеки вектор е кратен на съответен базисен вектор на надмодула.

В примера тук, при стандартния базис $\mathbb{Z}^2 = \langle e_1, e_2\rangle = \langle (1,0),(0,1)\rangle$ имаме „кратен“ базис $(2\mathbb{Z})^2 = \langle 2e_1, 2e_2\rangle = \langle (2,0),(0,2)\rangle$

Дефиниция 10. Ако M и M' са свободни модули, $M' \leq M$, и имат базиси съответно $\{v_1, \ldots, v_n\}$ и $\{a_1 v_1, \ldots, a_m v_m\}$, за които $a_i \mid a_{i-1} \forall i > 1$, то тези базиси се наричат **подравнени**.

С тази дефиниция вече можем да формулираме голямата теорема:

Теорема 15. *Над ОГИ, ако M е свободен модул от ранг $n \geq 1$ и $M' \leq M$, то M и M' допускат подравнени базиси.*

Бележка. Важно е да отбележим, че теоремата не казва, че по даден базис на M можем да намерим негов кратен, за N.

Нито пък, че при даден базис на N, можем да намерим базис на M, кратен на него.

Тази теорема ни дава „нови“ базиси на M и N.

Всъщност, такива неща не можем и да искаме. Да вземем $M = \mathbb{Z}^2$ с базиса $B = \{(1,0),(0,1)\}$ и неговия подмодул $N = \langle (1,1)\rangle \times \langle (-1,1)\rangle$ с базиса $B' = \{(1,1),(-1,1)\}$.

[11] тъй като φ е сюрекция, значи изоморфизъм и пренася базисите

Тогава нито за B' съществува базис на M, на който B' да е кратен, нито за B съществува базис на N, кратен на B.

Съществуват, обаче, съвсем други базиси на двата модула, които са подравнени: $M = \langle (0,1),(1,1) \rangle$ и $N = \langle (0,2),(1,1) \rangle$.

Доказателство Нека M е свободен модул от ранг n над област от главни идеали R и $M' \leq M$ е негов подмодул.

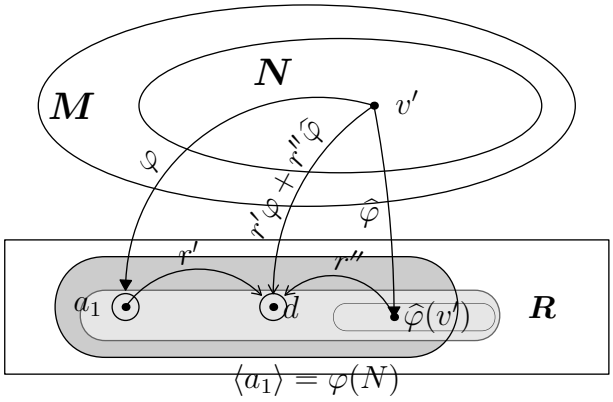
Да намерим подравнени базиси на тези модули в известен смисъл означава да намерим такива наредени координатни оси, които по двойки са „успоредни“, а във всяка следваща двойка оси единичният вектор от подмодула е кратно по-дълъг от единичния на подмодула в предната двой оси.

Ще започнем с (една) „най-къса“ координатна ос. Разглеждаме всевъзможните линейни функционали $\mathrm{Hom}(M,R)$, ще изберем такъв, който „запазва“ възможно най-много информация за подмодула N.

За целта разглеждаме проекциите $\{\ \varphi(N) \mid \varphi \in \mathrm{Hom}(M,R)\ \}$ на N върху R - те са подмодули, значи идеали и можем да изберем максимален по включване сред тях. Нека φ е проекция, за която $\varphi(N) \leq R$ е максимален. Имаме, че R е ОГИ, значи $\varphi(N)$ се поражда от някой скалар $a_1 \neq 0$. Да обозначим някой негов праобраз с v'.

Ще проверим следното:

Мини-твърдение 8.1. Всеки образ на v' през линеен функционал $\widehat{\varphi}$ е кратен на a_1.



Доказателство. На езика на идеалите всъщност твърдението гласи, че $\langle a_1 \rangle \supseteq \langle \widehat{\varphi}(v') \rangle$.

Да разгледаме най-големия общ делител d на a_1 и $\langle \widehat{\varphi}(v') \rangle$. От Безу имаме $d = r'a_1 + r''\widehat{\varphi}(v') = r'\varphi(v') + r''\widehat{\varphi}(v')$, т.е. d е линейна комбинация на два образа на v' под действието на два линейни функционала. Тогава самото d е образ на v' под линейната комбинация $\psi = r'\varphi + r''\widehat{\varphi} : N \to R$.

Тогава имаме следните две включвания:

1. $\langle d \rangle \leq \psi(N)$, защото $\mathrm{Im}\,\psi$ е идеал на R и също е ОГИ.
2. $\langle d \rangle \supseteq \langle \widehat{\varphi}(v') \rangle \cup \langle a_1 \rangle$, тъй като d е НОД на $\widehat{\varphi}(v')$ и a_1.

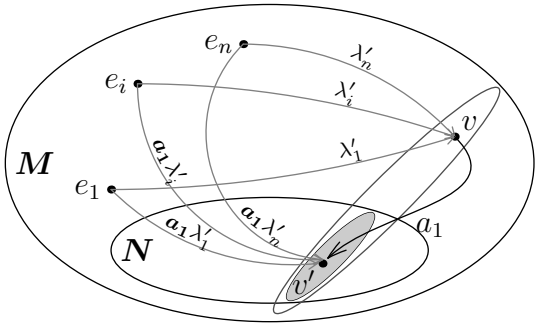
Получихме, че за произволен линеен функционал $\widehat{\varphi}$, $\varphi(N) = \langle a_1 \rangle \leq \langle d \rangle \leq \psi(N)$. Тъй като така избрахме φ, обаче, че $\varphi(N)$ да бъде максимален, то от $\varphi(N) \leq \psi(N)$ следва, че $\varphi(N) = \psi(N)$, а от предните включвания и $\langle a_1 \rangle = \langle d \rangle$.

Тоест излезе, че $\langle a_1 \rangle + \langle \widehat{\varphi}(v') \rangle = \langle d \rangle = \langle a_1 \rangle$, т.е. $\langle a_1 \rangle \supseteq \langle \widehat{\varphi}(v') \rangle$ и a_1 дели $\widehat{\varphi}(v')$ за произволно $\widehat{\varphi} : \mathrm{Hom}(M,R)$. □

Имаме, че всяка проекция на v' върху пръстена е кратна на a_1. Какво ще стане, ако разложим v' в някой базис на M?

Нека $\{e_i\}$ е базис на M. Тогава $v' = \sum_i \lambda_i e_i$.

Всяка координата $\lambda_i \in R$ на v' е образ на линеен функционал, проектиращ i-тата координата на кой да е вектор от M върху пръстена. По горните разсъждения, всяко λ_i е кратно на a_i и можем да го напишем



като $\lambda_i = a_1\lambda_i'$. Тогава:

$$v' = \sum_i \lambda_i e_i = \sum_i a_1\lambda_i e_i = a_1 \sum_i \lambda_i' e_i = a_1 v,$$

полагайки $v = \sum_i \lambda_i' e_i$. Представихме v' като умножение на друг вектор с a_1! Прилагаме φ от двете страни:

$$\begin{aligned} \varphi(v') &= \varphi(a_1 v) \\ a_1 &= a_1\varphi(v) \\ a_1(1-\varphi(v)) &= 0 \\ a_1 \neq 0 &\Rightarrow \varphi(v) = 1 \end{aligned}$$

И така, сега имаме вектори $v \in M, av \in N$, и проекция φ, за която $v \overset{\varphi}{\mapsto} 1_R$.

А ако погледнем цялата ос $\langle v\rangle$, то последното ни дава $\langle v\rangle \overset{\varphi}{\mapsto} \langle 1_R\rangle = R$, което подсказва, че ще искаме да вземем v в базиса на M, а $v = a_1 v$ - в базиса на N.

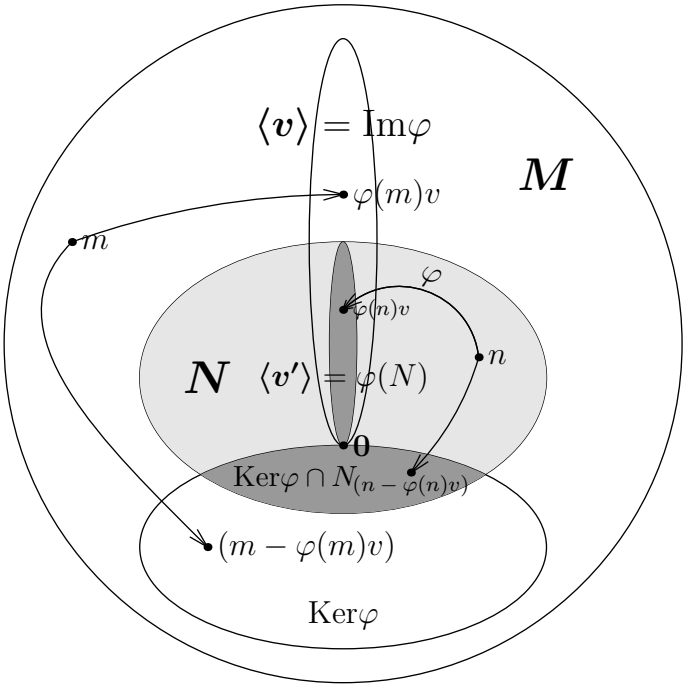
Тогава първите подравнени оси ще бъдат $\langle v\rangle$ и $\langle v'\rangle$. Да намерим останалите!

Представяме M и N като директни суми на първите оси с подмодули от по-ниски размерности:

1. $M \cong \operatorname{Ker}\varphi \oplus \langle v\rangle$, като използваме лема 11 за изображението $(r \mapsto rv)\circ\varphi$ (тук $r \mapsto rv$ е изоморфизъм от R в $\langle v\rangle$).
2. $N \cong (N \cap \operatorname{Ker}\varphi) \oplus \langle av\rangle$, отново с лема 11, но за рестрикцията $\varphi|_N : N \to \varphi(N) = \langle av\rangle = (v')$.

Готови сме да задвижим индуктивната стъпка.

От $M \cong \operatorname{Ker}\varphi \oplus \langle v\rangle$ имаме $\dim(\operatorname{Ker}\varphi) = \dim M - \dim\langle v\rangle = n-1$. Тогава можем да приложим индукционната хипотеза за ядрото (което е свободен модул) и неговия подмоул $\operatorname{Ker}\varphi \cap N$, което ни дава техни подравнени базиси — $\{v_i\}_{i=2}^n$ за $\operatorname{Ker}\varphi$ и $\{a_i v_i\}_{i=2}^k$ за $\operatorname{Ker}\varphi \cap N$.



Прибавяйки v и $v' = a_1 v$ към тях, получаваме подравнени базиси за M и N.

Дъното на индукцията е при $n = 1$, тогава $M \cong R = \langle 1\rangle$ и N е главен идеал с $N = \langle a\rangle = \langle a * 1\rangle$ за някой пораждащ елемент a. □

9 Теоремата

Нужно ни е още едно твърдение:

Твърдение 16. *Нека за $i = 1, \ldots, n$ A_i са модули над пръстена R и $B_i \leq A_i$ са техни съответни подмодули.*

Тогава $(A_1 \oplus \cdots \oplus A_n)/(B_1 \oplus \cdots \oplus B_n) \cong A_1/B_1 \oplus \cdots \oplus A_n/B_n$

Доказателството е чисто техническо и просто следва дефинициите, излишно е да пълним повече място тук.

Вече можем да докажем резултата от този документ с досега формулираните твърдения:

Теорема 17. *Нека R е област от главни идеали и M е крайнопороден модул над R. Тогава съществуват скалари $\{a_i\}_{i=1}^m$, изпълняващи $a_i \mid a_{i+1} \forall i = 1, \ldots, m-1$, и степен n, т.ч. $M \cong R^n \oplus (R/a_1) \oplus \cdots \oplus (R/a_n)$.*

Доказателство. Последователно:

- По твърдение 14 имаме епиморфизъм $f : M \twoheadrightarrow R^r$.
- По теоремата за хомоморфизмите имаме $R^r / \operatorname{Ker} f \cong M$.
- Теорема 15 ни дава подравнени базиси на свободния модул R^r и подмодула му $\operatorname{Ker} f \leq R^r$:
  - $R^r = \operatorname{span}\{v_1, \ldots, v_r\}$
  - $\operatorname{Ker} f = \operatorname{span}\{a_1 v_1, \ldots, a_m v_m\}$.

  където $a_i \mid a_{i+1}$ за $i = 1, \ldots, m-1$.
- Тогава можем да разпишем

$$M \cong R^r / \operatorname{Ker} f = (\oplus_{i=1}^r R)/(\langle a_1 v_1 \rangle \oplus \cdots \oplus \langle a_m v_m \rangle)$$

- Отчитайки, че $\langle a_i v_i \rangle \cong a_i R$:

$$M \cong (\oplus_{i=1}^r R)/(a_1 R \oplus \cdots \oplus a_m R)$$

- По последното твърдение можем да разпаднем:

$$M \cong (R/(a_1 R)) \oplus \ldots \oplus (R/(a_m R)) \oplus R^{r-m}$$

- Като идеали, $a_i R = \langle a_i \rangle$, и така получаваме търсеното представяне на модула:

$$M \cong R/\langle a_1 \rangle \oplus \ldots \oplus R/\langle a_m \rangle \oplus R^{r-m}$$

□

10 Някои бележки

- Всеки крайнопороден модул над ОГИ се разлага на периодичен и точен модул: $M \cong F \oplus T$, където $F = R^n$, а $T = \oplus_i (R/\langle a_i \rangle)$.
- В частния случай, когато R е поле, идеалите $(R/\langle a_i \rangle)$ могат да са само R и $\{0\}$. Тогава в разлагането $T \cong \{0\}$ и получваме, че крайнопородените линейни пространства имат вида R^n.
- Като следствие на теоремата в случая $R = \mathbb{Z}$ получаваме класификацията на крайнопородените абелеви групи:

  Твърдение 18. *Ако G е крайнопородена абелева група, то съществуват числа $a_1, \ldots, a_m$, всяко от които дели следващото, и $n \in \mathbb{N}$, т.ч. $G \cong \mathbb{Z}^n \times \mathbb{Z}_{a_1} \times \cdots \times \mathbb{Z}_{a_m}$.*
- Представянето на M от теоремата е единствено, тоест степента n и множеството $\{a_i\}$ са еднозначно определени.
- Използвайки китайската теорема за остатъците, можем да приведем всеки крайнопороден модул във вида $M \cong R^n \oplus (R/\langle p_1^{\alpha_1} \rangle) \oplus \cdots \oplus (R/\langle p_m^{\alpha_m} \rangle)$, където p_i са прости елементи от пръстена R.

11 Приложения

Жорданова нормална форма Нека T е линеен оператор в пространството $V = F^n$ над алгебрически затворено поле F. Тогава можем да погледнем на V като *модул* над $F[T]$ - пръстенът от полиноми с променлива „операторът“ T.

Така на всеки вектор $v \in V$ действаме със скалара $c = a_m T^m + \cdots + a_1 T + a_0 Id$ по следния начин:

$$c \cdot v = a_m T^m(v) + \cdots + a_1 T(v) + a_0 v$$

Гледайки на V като на модул над $F[T]$, крайномерността му като пространство влече крайнопороденост като модул, и по теоремата за крайнопородените модули получаваме $V \cong \oplus_i F[T]/(T - \lambda_i)^{k_i}$ (във формата на неразложими множители, вместо на инвариантни фактори - тук използваме алгебрическата затвореност на F, за да разложим докрай на линейни множители). Тогава се оказва, че матрицата на T в базиса на V, съгласуван с това представяне, е точно в жорданова нормална форма.

Решенията на линейни хомогенни диференциални уравнения Подобно на горната конструкция, пространството от решенията на едно линейно хомогенно диференциално уравнение могат да се разглеждат като модул над $F[D]$, където D е операторът за диференциране. Оттук могат да се изведе всъщност „рецептата“ за тяхното решаване.

12 Източници

- Keith Conrad, Modules over PID
- Benjamin Levine, Finitely generated modules over a PID
- William Adkins, Steven Weintraub – Algebra. An approach via module theory
- Paul Garrett, Abstract algebra, #11 Finitely-generated modules
- Dexter Chua, notes on lectures by O. Randal-Williams, Groups, Rings and Modules
- Много страници в Wikipedia и въпроси и отговори в math.stackexchange.com