თანამედროვე ალგებრის ელემენტები

ვახტანგ ლომაძე

ზუსტ და საბუნებისმეტყველო მეცნიერებათა ფაკულტეტი, ივანე ჯავახიშვილის სახ. სახელმწიფო უნივერსიტეტი

ალგებრა სწავლობს ალგებრულ სტრუქტურებს, როგორიცაა მაგ. ჯგუფები, წრფივი სივრცეები, რგოლები, მოდულები, ველები.

1 ჯგუფები

კომპოზიციის კანონი S სიმრავლეზე, ეს არის წესი, რომელიც ყოველ წყვილს (a, b) ელემენტებისა S სიმრავლიდან უთანადებს ელემენტს, ვთქვათ p ელემენტს, იმავე S სიმრავლიდან.

ფორმალურად, კომპოზიციის კანონი არის ასახვა

$$f : S \times S \to S.$$

აღნიშვნა $f(a, b)$ არ არის მოსახერხებელი კომპოზიციის კანონისთვის. ნაცვლად, იყენებენ აღნიშვნას რომელიც გამოიყენება ჩვეულებრივი გამრავლებისა და მიმატებისთვის:

$$ab, a \times b, a + b.$$

ან კიდევ აღნიშვნას, რომელიც წააგავს მათ, მაგალითად $a \circ b$, $a \oplus b$.

Definition. ჯგუფი არის არაცარიელი სიმრავლე G კომპოზიციის კანონთან ერთად, რომელიც ასოციაციურია და გააჩნია ერთეულოვანი ელემენტი, და ისეთი, რომ ყოველ ელემენტს აქვს შებრუნებული.

აბელის ჯგუფი ეს არის ჯგუფი რომლის კომპოზიციის კანონი კომუტაციურია.როგორც წესი, აბელის ჯგუფში იყენებენ ადიციურ აღნიშვნას.

- **ჯგუფის მაგალითები**

აი რამდენიმე მარტივი მაგალითი ჯგუფისა:

$\mathbb{Z}^+$: მთელი რიცხვები შეკრებით;
$\mathbb{Q}^+$: რაციონალური რიცხვები შეკრებით;

$\mathbb{Q}^*$: ნულისგან განსხვავებული რაციონალური რიცხვები გამრავლებით;
$\mathbb{R}^+$: ნამდვილი რიცხვები შეკრებით;
$\mathbb{R}^*$: ნულისგან განსხვავებული ნამდვილი რიცხვები გამრავლებით;
$\mathbb{C}^+$: კომპლექსური რიცხვები შეკრებით;
$\mathbb{C}^*$: ნულისგან განსხვავებული კომპლექსური რიცხვები გამრავლებით.

ორი საინტერესო მაგალითია:
1) ნამდვილი ზოგადი წრფივი $n \times n$ ჯგუფი $GL_n(\mathbb{R})$:

$$GL_n(\mathbb{R}) = \{n \times n \text{ matrices } A \in \mathbb{R}^{n\times n} \text{ with} \det(A) \neq 0\}.$$

ასევე განისაზღვრება კომპლექსური ზოგადი წრფივი $n \times n$ ჯგუფი $GL_n(\mathbb{C})$.

2) X იყოს სიმრავლე. ბიექციურ ასახვას $f : X \to X$ ჰქვია X-ის გადანაცვლება. ცხადია, გადანაცვლებები ქმნიან ჯგუფს, რომელიც აღინიშნება $S(X)$ სიმბოლოთი. როდესაც $X = \{1, 2, ..., n\}$, მაშინ უფრო ხმარობენ S_n აღნიშვნას.

ზოგადი წრფივი ჯგუფი და გადანაცვლებათა ჯგუფი განსაკუთრებით მნიშვნელოვანია. ერთი მიზეზი ამისა არის ის, რომ იგინი მოიცავენ ბევრ სხვა ჯგუფს როგორც ქვეჯგუფს.

H ქვესიმრავლე G ჯგუფში იწოდება ქვეჯგუფად, თუ ის აკმაყოფილებს შემდეგ თვისებებს:
(a) (*ჩაკეტილობა*): თუ $a, b \in H$, მაშინ $ab \in H$;
(b) (*ერთეულოვანი*): $1 \in H$;
(c) (*შებრუნებულები*): თუ $a \in H$, მაშინ $a^{-1} \in H$.

ჯგუფის სხვა მაგალითებია:
1)

$$\mathbb{T} = \{z \in \mathbb{C} |\ |z| = 1\}.$$

$\mathbb{T}$ არის ჯგუფი გამრავლების მიმართ $\mathbb{C}$-ში და მას ეწოდება *წრიული ჯგუფი*.
2)

$$SO(2) = \{\begin{pmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{pmatrix} \mid \theta \in \mathbb{R}\}.$$

ამ ჯგუფს ჰქვია 2 ხარისხის სპეციალური ორთოგონული ჯგუფი. ჩვენ ვნახავთ, რომ ეს არის სიბრტყის ბრუნვათა ჯგუფი კოორდინატთა სათავის გარშემო.
3)

$$\{cos(2k\pi/n) + isin(2k\pi/n) |\ k = 0, 1, \ldots, n-1\}.$$

ეს არის n-ური რიგის ფესვების ჯგუფი ერთიანიდან. იგი იზომორფულია $\mathbb{Z}/n\mathbb{Z}$-ის.

Theorem 1 (კელის თეორემა) *ყოველი ჯგუფი არის ქვეჯგუფი გადანაცვლებათა ჯგუფის.*

Proof. ვთქვათ, გვაქვს ჯგუფი G. ჩვენ ვაჩვენებთ, რომ G არის ქვეჯგუფი $S(G)$ ჯგუფისა.

ყოველი $x \in G$, $\lambda_x : G \to G$ იყოს ასახვა განსაზღვრული ფორმულით $\lambda_x(g) = xg$ (ანუ მარცხნიდან გამრავლება x ელემენტზე). ყოველი $c \in G$, $\lambda_x(x^{-1}c) = x(x^{-1}c) = c$. ასე რომ λ_x არის "ზე-ასახვა". შემდეგ, ტოლობიდან $\lambda_x(a) = \lambda_x(b)$, ვღებულობთ, რომ $xa = xb$, ანუ $a = b$. ე.ი., λ_x არის ამავე დროს "ჩადგმა". ამრიგად, λ_x არის G სიმრავლის გადანაცვლება.

განვსაზღვროთ,

$$\phi : G \to S(G), \qquad \phi(x) = \lambda_x.$$

ეს არის ჰომომორფიზმი. მართლაც თუ $g \in G$, მაშინ

$$\lambda_{xy}(g) = (xy)g = x(yg) = \lambda_x(yg) = (\lambda_x \circ \lambda_y)(g).$$

იმის საჩვენებლად,რომ ეს ჰომომორფიზმი ინექციურია, დავუშვათ: $\phi(x) = \phi(y)$. მაშინ $\lambda_x(e) = \lambda_y(e)$, ანუ $xe = ye$, და მაშასადამე $x = y$. □

- **გადანაცვლებები**

გადანაცვლებას $\sigma \in S(X)$ ჰქვია ციკლი თუ მოიძებნება $a_1, a_2, \ldots, a_k \in X$ ისეთი, რომ

$$\sigma(a_1) = a_2, \sigma(a_2) = a_3, \ldots, \sigma(a_k) = a_1.$$

და $\sigma(x) = x$ ყველა სხვა $x \in X$. მას აღნიშნავენ $(a_1, a_2, \ldots, a_k)$ სიმბოლოთი. k-ს ჰქვია ციკლის სიგრძე. უნდა აღინიშნოს, რომ იგივურ ასახვასაც უწოდებენ ციკლს. მას განიხილავენ, როგორც 1 სიგრძის ციკლს.

სხვა სიტყვებით, გადანაცვლება არის ციკლი თუ მას აქვს არა უმეტეს ერთი ორბიტისა, რომელიც შედგება ორი ან მეტი ელემენტისგან. ციკლის სიგრძე არის მისი ყველაზე დიდი ორბიტის ელემენტთა რიცხვი.

ამბობენ, რომ $\sigma = (a_1, a_2, \ldots, a_k)$ და $\tau = (b_1, b_2, \ldots, b_l)$ ციკლები განცალებულია, თუ $a_i \neq b_j$ ყველა i და j-თვის. ადვილი დასანახია, რომ თუ σ და τ განცალებული ციკლებია, მაშინ $\sigma\tau = \tau\sigma$.

Theorem 2 *ყოველი გადანაცვლება წარმოიდგინება (და ამასთანავე მხოლოდ ერთი გზით) როგორც განცალებული ციკლების ნამრავლი.*

Proof. შეგვიძლია ვიგულისხმოთ, რომ $X = \{1, 2, \ldots, n\}$. ვთქვათ, გვაქვს $\sigma \in S(X)$.

განვსაზღვროთ: $X_1 = \{\sigma(1), \sigma^2(1), \ldots\}$. შემდეგ, i იყოს ყველაზე პატარა მთელი რიცხვი, რომელიც არ ეკუთვნის X_1 სიმრავლეს, და განვსაზღვროთ $X_2 = \{\sigma(i), \sigma^2(i), \ldots\}$. თუ ასე გავაგრძელებთ, ეს პროცესი დასრულდება, რა თქმა უნდა. მივიღებთ არათანამკვეთ სიმრავლეებს $X_1, X_2, \ldots, X_r$, რომელთა გაერთიანება X-ის ტოლია. σ_i იყოს ციკლი, განსაზღვრული შემდეგნაირად

$$\sigma_i(x) = \begin{cases} \sigma(x) & \text{თუ } x \in X_i, \\ x & \text{სხვა შემთხვევაში} \end{cases}.$$

ცხადია, რომ

$$\sigma = \sigma_1\sigma_2 \ldots \sigma_r.$$

რადგან $X_1, X_2, \ldots, X_r$ არ იკვეთებიან, ეს ციკლები განცალებულია.

□

ყველაზე მარტივი გადანაცვლებებია 2-ციკლები. ასეთ ციკლებს ჰქვია ტრანსპოზიციები. ვინაიდან

$$(a_1, a_2, \ldots, a_k) = (a_1, a_k)(a_1, a_{k-1}) \ldots (a_1, a_3)(a_1, a_2),$$

სამართლიანია შემდეგი წინადადება.

Proposition 1 *ორი ან მეტი ელემენტისგან შემდგარი სიმრავლის ყოველი გადანაცვლება ჩაიწერება როგორც ტრანსპოზიციების ნამრავლი.*

ყველაზე ყველაზე მარტივი გადანაცვლება არის ტრანსპოზიცია, რომელსაც აქვს $(i, i+1)$ ფორმა. ასეთ ტრანსპოზიციას მარტივი ტრანსპოზიცია ჰქვია. მაგ. (7,8) არის მარტივი ტრანსპოზიცია, მაგრამ (7,10) - არა.

ყოველი ტრანსპოზიცია (და მაშასადამე ყოველი გადანაცვლება) არის მარტივი ტრანსპოზიციების ნამრავლი. ამის ჩვენება ადვილია ინდუქციის მეთოდით. მართლაც, ვთქვათ გვაქვს (k, l) ტრანსპოზიცია. თუ $l - k = 1$ მაშინ არაფერია დასამტკიცებელი. თუ კი $l - k \geq 2$, მაშინ

$$(k, l) = (l-1, l)(k, l-1)(l-1, l).$$

რა თქმა უნდა, გადანაცვლების დაშლა ტრანსპოზიციების ნამრავლად არ არის ერთადერთი.

Definition. გადანაცვლებას ჰქვია ლუწი (შეს. კენტი) თუ ის წარმოდგება ლუწი (შეს. კენტი) რაოდენობის ტრანსპოზიციების ნამრავლად.

Theorem 3 *გადანაცვლება არ შეიძლება ერთდროულად იყოს ლუწიც და კენტიც.*

Proof. განვიხილოთ n ცვლადის პოლინომი

$$P = \prod_{i<j} (s_i - s_j).$$

ყოველი σ გადანაცვლებისთვის, განვსაზღვროთ

$$P^\sigma = P(s_{\sigma(1)}, \ldots, s_{\sigma(n)}).$$

შევნიშნოთ, რომ

$$P^{\sigma\tau} = (P^\tau)^\sigma.$$

ასევე შევნიშნოთ, რომ თუ $\sigma = (k, k+1)$ არის მარტივი ტრანსპოზიცია, მაშინ ცხადია $P^\sigma = -P$.

დამტკიცება ამის შემდეგ ადვილი დასამთავრებელია. □

Exercise. k-ციკლი არის ლუწი მაშინ და მხოლოდ მაშინ, როცა k არის კენტი.

ლუწი გადანაცვლებები ქმნიან ქვეჯგუფს S_n-ში. ეს ყველაზე მნიშვნელოვანი ქვეჯგუფია, და იგი აღინიშნება A_n სიმბოლოთი.

Example. ჯგუფო A_4 არის ქვეჯგუფი S_4-ში და შედგება შემდეგი 12 გადანაცვლებისგან:

$$(1), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243).$$

- **იზომეტრიები**

Definition. ასახვას $M : \mathbb{R}^n \to \mathbb{R}^n$ ჰქვია იზომეტრია, ან მოძრაობა, თუ ის ინახავს მანძილს:

$$d(M(x), M(y)) = d(x, y).$$

იზომეტრიები ქმნიან ჯგუფს, რომელიც აღინიშნება $E(n)$ სიმბოლოთი. ხშირად მას ევკლიდეს ჯგუფს უწოდებენ. კომპოზიციის კანონი ამ ჯგუფში არის ასახვების კომპოზიცია. მეორე და მესამე რიგის ევკლიდეს ჯგუფები კარგადაა შესწავლილი. (ისინი შეისწავლეს ბევრად უფრო ადრე ვიდრე ჯგუფის ცნებას შემოიტანდნენ.)

თუ m მოძრაობას გადაჰყავს სიმრავლე (ფიგურა) F თავის თავში, ამბობენ, რომ იგი F-ის სიმეტრიაა. სიმრავლე F-ის სიმეტრიებისა არის $E(n)$-ის ქვეჯგუფი, და მას ჰქვია F-ის სიმეტრიების ჯგუფი.

Definition. ორთოგონული გარდაქმნა $A : \mathbb{R}^n \to \mathbb{R}^n$ არის წრფივი ასახვა, რომელიც ინახავს სკალარულ ნამრავლს.

ადვილი შესამოწმებელია, რომ ორთოგონული გარდაქმნა არის იზომეტრია. შემდეგი თეორემა ამბობს, რომ პარალელურ გადატანამდე სიზუსტით სამართლიანია შებრუნებული დებულებაც.

Theorem 4 *თუ $M : \mathbb{R}^n \to \mathbb{R}^n$ არის იზომეტრია, მაშინ*

$$M(p) = M(0) + A(p),$$

სადაც A არის ორთოგონული გარდაქმნა.

Proof. განვსაზღვროთ

$$A(p) = M(p) - M(0).$$

გვინდა ვაჩვენოთ, რომ A არის წრფივი და ინახავს სკალარულ ნამრავლს. უკანასკნელის სანახავად შევნიშნოთ, რომ

$$< x - y, x - y >= |x|^2 + |y|^2 - 2 < x, y > .$$

რადგანაც M იზომეტრიაა, გვექნება

$$2 < Ap, Aq >= |A(p)|^2 + |A(q)|^2 - |A(p) - A(q)|^2 =$$

$$|M(p) - M(0)|^2 + |M(q) - M(0)|^2 - |M(p) - M(q)|^2 =$$

$$|p|^2 + |q|^2 - |p - q|^2 = 2 < p, q > .$$

ვხედავთ, რომ A ინახავს სკალარულ ნამრავლს.

შემდეგ, რადგან A ინახავს სკალარულ ნამრავლს Ae_i $(i = 1, \ldots, n)$ ვექტორები ქმნიან ორთონორმულ ბაზისს $\mathbb{R}^n$-ში. გვექნება

$$< A(p + q), A(e_i) >=< p + q, e_i >=< p, e_i > + < q, e_i >=$$

$$< A(p), A(e_i) > + < A(q), A(e_i) >=< A(p) + A(q), A(e_i) > .$$

აქედან, ვხედავთ რომ

$$A(p + q) = A(p) + A(q).$$

მსგავსად, ყოველი c კონსტანტისთვის

$$< A(cp), A(e_i) >=< cp, e_i >= c < p, e_i >= c < A(p), A(e_i) >=< cA(p), A(e_i) >,$$

საიდანაც გამომდინარეობს რომ $A(cp) = cA(p)$.

დავინახეთ, რომ A არის წრფივი.

დამტკიცება დასრულებულია. □

ამრიგად, ყოველი იზომეტრია არის კომპოზიცია ორთოგონული წრფივი ასახვისა და პარალელური გადატანის. ამიტომაც, მას ხშირად უწოდებენ აფინურ ორთოგონულ გარდაქმნას.

ორთოგონული გარდაქმნების ჯგუფი აღინიშნება $O(n)$ სიმბოლოთი. თუ A არის ორთოგონული გარდაქმნა, მაშინ $\det(A) = \pm 1$. ამბობენ, რომ A არის სპეციალური ორთოგონული გარდაქმნა როცა $\det(A) = 1$. სპეციალური ორთოგონული გარდაქმნები ქმნიან ქვეჯგუფს; იგი აღინიშნება $SO(n)$ სიმბოლოთი.

ევკლიდეს ჯგუფი არის ქვეჯგუფი აფინურ გარდაქმნათა ჯგუფისა. თავის მხრივ, $E(n)$, როგორც ქვეჯგუფს, შეიცავს პარალელურ გადატანათა $T(n)$ ჯგუფს და ორთოგონულ $O(n)$ ჯგუფს. ყოველი ელემენტი $E(n)$-ში ჩაიწერება ერთი და მხოლოდ ერთი გზით როგორც კომპოზიცია პარალელური გადატანისა და ორთოგონული გარდაქმნისა (ან ორთოგონული გარდაქმნისა და პარალელური გადატანისა).

$T(n)$ არის ნორმალური ქვეჯგუფი $E(n)$-ში.

$E(n)$ არის ნახევრად-პირდაპირი ნამრავლი $O(n)$ და $T(n)$ ქვეჯგუფების. სხვა სიტყვებით, $O(n)$ არის $E(n)$-ის ფაქტორ-ჯგუფი $T(n)$-ის მიმართ:

$$O(n) = E(n)/T(n).$$

იზომეტრული წრფივი გარდაქმნა = ორთოგონული გარდაქმნა

- **სიბრტყის იზომეტრიები**

დაწვრილებით განვიხილოთ ორგანზომილებიანი შემთხვევა.
განვსაზღვროთ შემდეგი მოძრაობები:

(a) t_a, პარალელური გადატანა a ვექტორით: $t_a(x) = x + a$.
(b) ρ_θ, ბრუნვა θ კუთხით კოორდინატთა სათავის გარშემო:

$$\rho_\theta(x) = \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

(c) r, არეკვლა x_1-ღერძის მიმართ:

$$r(x) = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix}$$

ადგილი აქვს შემდეგ თანაფარდობებს

$$t_a t_b = t_{a+b}, \quad \rho_\phi \rho_\theta = \rho_{\phi+\theta}, \quad r^2 = 1;$$

$$\rho_\theta t_a = t_b \rho_\theta \quad \text{სადაც } b = \rho_\theta(a);$$

$$r t_a = t_b r \quad \text{სადაც } b = r(a);$$

$$r \rho_\theta = \rho_{-\theta} r.$$

ეს გარდაქმნები წარმოქმნიან მთელ ჯგუფს: ყოველი ელემენტი $E(2)$-ში არის მათი ნამრავლი. უფრო ზუსტად, სამართლიანია შემდეგი თეორემა.

Theorem 5 *თუ m არის მოძრაობა, მაშინ მოიძებნება ერთი და მხოლოდ ერთი ვექტორი a და ერთი და მხოლოდ ერთი კუთხე $\theta \in [0, 2\pi)$ ისეთი რომ*

$$m = t_a \rho_\theta \quad \text{ან} \quad m = t_a \rho_\theta r.$$

Proof. თეორემა 3-ის ძალით, $m = t_a A$, სადაც a არის ვექტორი და A არის ორთოგონული ოპერატორი.

ვთქვათ

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in O(2).$$

A-ს სვეტები ერთმანეთთან ორთოგონული ერთეულოვანი ვექტორებია. შეგვიძლია შევარჩიოთ კუთხე $\theta \in [0, 2\pi)$ ისე რომ

$$\begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} cos\theta \\ sin\theta \end{bmatrix}.$$

ვინაიდან $\begin{bmatrix} b \\ d \end{bmatrix}$ უნდა იყოს ერთეულოვანი და ორთოგონული $\begin{bmatrix} a \\ c \end{bmatrix}$-თან, არსებობს მხოლოდ ორი შესაძლებლობა

$$\begin{bmatrix} b \\ d \end{bmatrix} = \begin{bmatrix} -sin\theta \\ cos\theta \end{bmatrix} \quad \text{ან} \quad \begin{bmatrix} b \\ d \end{bmatrix} = \begin{bmatrix} sin\theta \\ -cos\theta \end{bmatrix}.$$

პირველი შემთხვევა იძლევა ბრუნვას კოორდინატთა სათავის გარშემო θ კუთხით (ან იგივურ ასახვას თუ კი $\theta = 0$).

მეორე შემთხვევა გვაძლევს არეკვლას $y = kx$ წრფის მიმართ, სადაც $k = tg(\theta/2)$. მართლაც, გავიხსენოთ რომ არეკვლა $px + qy = 0$ წრფის მიმართ მოიცემა ფორმულით

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} x \\ y \end{bmatrix} - 2(px + qy) \begin{bmatrix} p \\ q \end{bmatrix}.$$

(ვგულისხმობთ, რომ $p^2 + q^2 = 1$.) ჩვენი წრფე არის:

$$sin(\theta/2)x - cos(\theta/2)y = 0.$$

ასე რომ, ჩვენს შემთხვევაში არეკვლა მოიცემა ფორმულით

$$\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} x \\ y \end{bmatrix} - 2(sin(\theta/2)x - cos(\theta/2)y) \begin{bmatrix} sin(\theta/2) \\ -cos(\theta/2) \end{bmatrix}.$$

გვექნება

$$x - (2sin(\theta/2)x - 2cos(\theta/2)y)sin(\theta/2) =$$
$$x - 2sin^2(\theta/2)x + 2sin(\theta/2)cos(\theta/2)y = cos(\theta)x + sin(\theta)y.$$

ასევე,

$$y + (2sin(\theta/2)x - 2cos(\theta/2)y)cos(\theta/2) =$$
$$y + 2sin(\theta/2)cos(\theta/2)x - 2cos^2(\theta/2)y = sin(\theta)x - cos(\theta)y.$$

□

Remark. ბრუნვა სიბრტყეში შეგვიძლია მივიღოთ ორი არეკვლის კომპოზიციით. მართლაც, ვთქვათ გვაქვს ორი L_1 და L_2 წრფე, და ვთქვათ მათ შორის კუთხე არის θ. ავიღოთ P წერტილი. ავრეკლოთ იგი პირველი წრფის მიმართ, და მიღებული წერტილი ავღნიშნოთ P'-ით. ეს უკანასკნელი ავრეკლოთ შემდეგ L_2-ის მიმართ და ანარეკლი წერტილი ავღნიშნოთ P''-ით. ადვილი

დასანახია, რომ P და P'' წერტილები ქმნიან 2θ-ის ტოლ კუთხეს O წერტილის გარშემო, ანუ კუთხე $< POP''$ უდრის 2θ-ს. (O არის წრფეების გადაკვეთის წერტილი.) ავღნიშნავთ, რომ ერთსა და იმავე წერტილის გარშემო ორი ბრუნვის კომპოზიცია არის ისევ ბრუნვა. კომპოზიცია არეკვლისა და ბრუნვისა, ან ბრუნვის და არეკვლის (კომპოზიცია არ არის გადანაცვლებადი!) არის არეკვლა.

2 (კომუტაციური) რგოლები

Definition. რგოლი ეს არის R სიმრავლე, რომელზეც მოცემულია ორი კომპოზიციის კანონი "$+$" და "$\cdot$". ეს კანონები უნდა აკმაყოფილებდნენ შემდეგ პირობებს:
(I) R არის აბელის ჯგუფი შეკრების მიმართ;
(II) გამრავლება არის ასოციაციური;
(III) გამრავლება არის დისტრიბუციული შეკრებასთან, ანუ

$$x(y+z) = xy + xz, \quad (x+y)z = xz + yz.$$

Example. რიცხვითი სიმრავლეები $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ და $\mathbb{C}$ წარმოადგენენ რგოლებს ჩვეულებრივი შეკრების და გამრავლების მიმართ.

Example. $\mathbb{Z}/n\mathbb{Z}$ არის რგოლი მოდულით n შეკრების და გამრავლების მიმართ.

Example. ნამდვილი პოლინომი არის გამოსახულება

$$p = a_0 s^n + a_1 s^{n-1} + \cdots + a_n,$$

სადაც $a_0, \ldots, a_n \in \mathbb{R}$ და s არის (ფორმალური) ცვლადი. პოლინომები შეგვიძლია შევკრიბოთ და ერთმანეთზე გადავამრავლოთ. ამ ოპერაციებით სიმრავლე პოლინომებისა $\mathbb{R}[s]$ არის რგოლი. თუ გვაქვს რგოლი R, ჩვენ შეგვიძლია ანალოგიურად ავაგოთ პოლინომები კოეფიციენტებით R-ში. მიღებული რგოლი აღინიშნება $R[s]$ სიმბოლოთი.

Example. სიმრავლე $M_n(\mathbb{R})$, რომელიც შედგება $n \times n$ ზომის მატრიცებისგან ნამდვილი კომპონენტებით ქმნიან რგოლს ჩვეულებრივი შეკრებისა და გამრავლების მიმართ. თუ გვაქვს რგოლი R, ჩვენ შეგვიძლია ანალოგიურად ავაგოთ $M_n(R)$, $n \times n$ ზომის მატრიცთა რგოლი კომპონენტებით R-ში.

Example. კვატერნიონების სიმრავლე

$$\mathbb{H} = \{a_1 + a_2 i + a_3 j + a_4 k : a_1, a_2, a_3, a_4 \in \mathbb{R}\},$$

სადაც i, j, k სიმბოლოებია ქმნის რგოლს. შეკრება ცხადია; გამრავლება განისაზღვრება შემდეგი წესიდან გამომდინარე:

$$i^2 = j^2 = k^2 = -1, \quad ijk = -1.$$

ეს რგოლი არის "არაკომუტაციური" ველი.

Definition. R რგოლს ჰქვია კომუტაციური, თუ $xy = yx$ ყოველი $x, y \in R$.

Definition. R რგოლს ჰქვია მთელობის არე, თუ ის არის კომუტაციური და აკმაყოფილებს პირობას: $xy = 0 \Rightarrow x = 0$ ან $y = 0$.

Definition. კომუტაციურ R რგოლს ჰქვია ველი, თუ $R\backslash 0$ არის ჯგუფი გამრავლების მიმართ.

Examples. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ და $\mathbb{C}$ მთელობის რგოლებია; $\mathbb{Z}/n\mathbb{Z}$ მთელობის რგოლია მაშინ და მხოლოდ მაშინ როცა n არის მარტივი რიცხვი; $M_n(\mathbb{R})$ არ არის მთელობის არე.

შეგახსენებთ, რომ ჰომომორფიზმი ერთი ჯგუფიდან მეორე ჯგუფში ეს არის ასახვა, რომელიც ინახავს ჯგუფის ოპერაციას. მსგავსად ამისა, რგოლების ჰომომორფიზმი არის ისეთი ასახვა, რომელიც ინახავს შეკრების და გამრავლების ოპერაციებს. უფრო ზუსტად, თუ R და S ორი რგოლია, მაშინ ასახვას $\phi : R \to S$ ჰქვია ჰომომორფიზმი თუ ის აკმაყოფილებს შემდეგ თვისებებს:

$$\phi(a + b) = \phi(a) + \phi(b), \quad \phi(-a) = -\phi(a), \quad \phi(0) = 0$$

და

$$\phi(ab) = \phi(a)\phi(b), \quad \phi(1) = 1.$$

თუ ჰომომორფიზმი $\phi : R \to S$ ბიექციურია როგოც ასახვა, მაშინ ამბობენ რომ ϕ არის იზომორფიზმი.

სიმრავლე ელემენტებისა რომლებიც ჰომომორფიზმს გადაყავს 0-ში მნიშვნელოვანია, და მას ეწოდება ბირთვი. უფრო ზუსტად, თუ $\phi : R \to S$ არის რგოლების ჰომომორფიზმი, მაშინ მისი ბირთვი განისაზღვრება, როგორც

$$ker(\phi) = \{r \in R : \phi(r) = 0\}.$$

Example. ყოველი მთელი n-თვის ასახვა $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, რომელიც მოიცემა ფორმულით

$$\phi(a) = a \mathrm{mod} n$$

არის ჰომომორფიზმი. მისი ბირთვი ტოლია $n\mathbb{Z}$-ის.

Example. R იყოს რგოლი ფუნქციებისა $f : X \to \mathbb{R}$. ავიღოთ ნებისმიერი $x \in X$, და განვსაღვროთ $ev_x : R \to \mathbb{R}$ ფორმულით $ev_x(f) = f(x)$ ყოველი $f \in R$.

ცენტრალურ ცნებას რგოლების თეორიაში წარმოადგენს იდეალის ცნება. იდეალი R რგოლში ეს არის ქვეჯგუფი $I \subseteq R$ ისეთი, რომ თუ $a \in I$, მაშინ $ar \in I$ ყოველი $r \in R$ ელემენტისთვის.

Example. ყოველ (არანულოვან) R რგოლში არის ორი იდეალი მაინც. სახელდობრ, $\{0\}$ და R. ამ იდეალებს ჰქვია ტრივიალური იდეალები.

იდეალს R რგოლში, რომელსაც აქვს ფორმა aR, ჰქვია *მთავარი იდეალი*.

Theorem 6 *ყოველი იდეალი მთელ რიცხვთა რგოლში არის მთავარი იდეალი.*

Proof. ვთქვათ I არის იდეალი მთელ რიცხვთა რგოლში. თუ ის ნულოვანია, მაშინ არაფერია დასამტკიცებელი. ამიტომ, ვიგულისხმოთ, რომ $I \neq \{0\}$. მაშინ ამ იდეალში აუცილებლად არის დადებითი რიცხვები. ვთქვათ m არის ყველაზე პატარა დადებითი მთელი, რომელიც ეკუთვნის I-ს. ავიღოთ ნებისმიერი $a \in I$. ჩვენ ვამტკიცებთ, რომ იგი m-ის ჯერადია. მართლაც, დავუშვათ რომ ასე არაა. მაშინ $a = mq + r$, სადაც $0 < r < m$. ცხადია $r = a - mq \in I$. და ვღებულობთ, რომ m არ ყოფილა ყველაზე პატარა დადებითი რიცხვი, რომელიც შედის I-ში.

□

ვთქვათ R არის კომუტაციური რგოლი (ერთიანით). ამბობენ რომ $u \in R$ არის შებრუნებადი, თუ მოიძებნება $v \in R$ ისეთი რომ $uv = 1$. ასეთი v მხოლოდ ერთი შეიძლება იყოს, და მას u-ს შებრუნებული ჰქვია. შებრუნებადი ელემენტები ქმნიან ჯგუფს. მას უწოდებენ R-ის მულტიპლიკაციურ ჯგუფს და აღნიშნავენ R^* სიმბოლოთი.

რა თქმა უნდა, არ უნდა ველოდოთ იმას 0-ს ჰქონდეს შებრუნებული (თუ კი რგოლი განსხვავებულია $\{0\}$-გან).

Example. ელემენტი $\mathbb{Z}/n\mathbb{Z}$ შებრუნებადია მაშინ და მხოლოდ მაშინ, როცა იგი არ არის ნულის გამყოფი. ანუ $a \mathrm{mod} n$ შებრუნებადია მაშინ და მხოლოდ მაშინ როცა a თანამარტივია n-თან. შეგახსენებთ, რომ თუ n დადებითი მთელი რიცხვია, მაშინ მისი ეილერის რიცხვი განისაზღვრება როგორც რიცხვი იმ მთელი დადებითი რიცხვებისა რომლებიც ნაკლებია n-ზე და თანამარტივია მასთან. იგი აღინიშნება $\varphi(n)$ სიმბოლოთი.

Proposition 2 (ეილერის თეორემა) *ვთქვათ n არის მთელი დადებითი რიცხვი. მაშინ ყოველი მთელი a-თვის, რომელიც თანამარტივია n-თან,*

$$a^{\varphi(n)} \equiv 1 (mod n).$$

Proof. გვექნება

$$(a \mathrm{mod} n)^{\varphi(n)} = 1 \mathrm{mod} n.$$

□

Corollary 1 (ფერმას მცირე თეორემა) *ვთქვათ p არის მარტივი რიცხვი. მაშინ ყოველი მთელი a-თვის, რომელიც არ იყოფა p-ზე,*

$$p | a^{p-1} - 1.$$

Proposition 3 *ველში მხოლოდ ორი იდეალია. პირუკუ, თუ რგოლს გააჩნია მხოლოდ ორი იდეალი, მაშინ ის აუცილებლად ველია.*

მთელ რიცხვთა რგოლში გვაქვს თეორემა ნაშთით გაყოფის შესახებ. მსგავსი თეორემა სამართლიანია აგრეთვე პოლინომთა რგოლში.

Theorem 7 *ვთქვათ F არის ველი, და ვთქვათ f და $g \neq 0$ პოლინომებია კოეფიციენტებით F-ში. მაშინ არსებობს ერთი და მხოლოდ ერთი წყვილი პოლინომებისა $q, r \in F[s]$ ისეთი, რომ*

$$g = fq + r \quad \text{და} \quad \deg(r) < \deg(g).$$

Proof. მტკიცდება ინდუქციით g-ს ხარისხის მიმართ.

□

Corollary 2 *ვთქვათ f არის პოლინომი $F[s]$-ში, და ვთქვათ a არის ელემენტი F-ში ისეთი რომ $f(a) = 0$. მაშინ $s - a$ ყოფს f პოლინომს.*

Corollary 3 *(ერთი ცვლადის) პოლინომთა რგოლი კოეფიციენტებით ველში არის მთავარ იდეალთა რგოლი.*

მთავარ იდეალთა რგოლები წარმოადგენენ ყველაზე მარტივ კლასს ველების შემდეგ. ეს ძალიან ვიწრო კლასია. მნიშვნელოვანია ე.წ. ნოეტერის რგოლები. ეს რგოლები აკმაყოფილებენ სასრულობის გარკვეულ პირობას. რგოლს ჰქვია ნოეტერის თუ მისი ყოველი იდეალი წარმოქმნილია სასრული რაოდენობა ელემენტებით.

ვიცით, რომ ერთი ცვლადის პოლინომთა რგოლი კოეფიციენტებით ველში არის მთავარ იდეალთა რგოლი. მრავალი ცვლადის პოლინომთა რგოლისთვის სამართლიანია შემდეგი სახელგანთქმული თეორემა.

Theorem 8 (ჰილბერტის თეორემა ბაზისის შესახებ) *პოლინომთა რგოლი კოეფიციენტებით ველში არის ნოეტერის რგოლი.*

ვთქვათ I არის იდეალი R რგოლისა. I-ს მოსაზღვრე კლასები ეს არის სიმრავლეები

$$a + I, \quad a \in R.$$

Proposition 4 *(a) არსებობს ერთაედერთი რგოლის სტრუქტურა მოსაზღვრე კლასების R/I სიმ- რავლეზე ისეთი რომ კანონიკური ასახვა $\pi : R \to R/I$, რომელიც აგზავნის a-ს $a + I$-ში, არის ჰომომორფიზმი.*

(b) π-ს ბირთვი არის I-ს ტოლი.

Example. რგოლი $\mathbb{Z}[i]/(1 + 3i)$ იზომორფულია $\mathbb{Z}/10$ რგოლის. მართლაც, გავამრავლოთ $-1 = 3i$ ტოლობის ორივე მხარე $-i$-ზე. მივიღებთ: $i = 3$. შეგვიძლია დავასკვნათ, რომ კანონიკური ჰომომორფიზმი

$$\mathbb{Z} \to \mathbb{Z}[i]/(1 + 3i)$$

სიურექციულია. ვნახოთ ბირთვი. ვთქვათ x გადადის 0-ში. მაშინ

$$x = (a + bi)(1 + 3i) = (a - 3b) + (3a + b)i,$$

საიდანაც ვღებულობთ, რომ $x = 10a$. 10 მართლაც გადადის 0-ში: $i^2 = -1$, და მაშასადამე $3^2 = -1$, ანუ $10 = 0$.

გავიხსენოთ, რომ მთელობის არე R არის არანულოვანი რგოლი ნულის გამყოფების გარეშე. სხვა სიტყვებით, მას აქვს ის თვისება, რომ თუ $ab = 0$, მაშინ ან $a = 0$ ან $b = 0$.

Theorem 9 *ვთქვათ R არის მთელობის არე. მაშინ არსებობს ჩადგმა R-სა ველში.*

Proof. კონსტრუქცია იგივეა რაც რაციონალური რიცხვების აგების კონსტრუქცია.

განვიხილოთ წილადები a/b, სადაც $a, b \in R$ და $b \neq 0$. ორ a_1/b_1 და a_2/b_2 წილადს დავუძახოთ ექვივალენტური თუ $a_1b_2 = a_2b_1$. ადვილი შესამოწმებელია, რომ ეს მიმართება მართლაც ექვივალენტობის მიმართებაა. ანუ აქვს რეფლექსურობის, ტრანზიტულობის და სიმეტრიულობის თვისებები.

R რგოლის წილადების ველი F არის წილადთა ექვივალენტობის კლასთა სიმრავლე. შეკრება და გამრავლება განისაზღვრება როგორც არითმეტიკაში:

$$(a/b)(c/d) = ac/bd, \quad a/b + c/d = \frac{ad + bc}{bd}.$$

შევნიშნოთ, რომ R შეგვიძლია განვიხილოთ როგორც F-ის ქვერგოლი. ამისთვის საჭიროა $a \in R$ გავაიგივეოთ $a/1$ წილადთან. ამის გაკეთება მართლაც შეიძლება რადგან $a/1 = b/1$ მხოლოდ იმ შემთხვევაში, როცა $a = b$.

□

როგორც მაგალითი, განვიხილოთ პოლინომთა რგოლი $F[s]$, სადაც F არის ველი. ეს მთელობის არეა. მის წილადთა ველს ჰქვია რაციონალურ ფუნქციათა ველი კოეფიცინეტებით F-დან. ეს ველი ჩვეულებრივ აღინიშნება $F(s)$ სიმბოლოთი. ამრიგად

$$F(s) = \{\text{ექვივალენტობის კლასები წილადებისა } f/g, \text{ სადაც } f, g$$

არიან პოლინომები და g არ არის ნულოვანი პოლინომი$\}$.

3 მთელი (და პოლინომური) მატრიცების დიაგონალიზაცია

ვილაპარაკებთ იმაზე თუ როგორ გავამარტივოთ მთელი (და პოლინომური) მატრიცი ელემენტარული გარდაქმნების მეშვეობით.

ვთქვათ R არის რგოლი, და ვთქვათ მოცემული გვაქვს მატრიცი A კომპონენტებით ამ რგოლიდან. შემდეგ გარდაქმნებს ჰქვია ელემენტარული.

(a) ორ სტრიქონის ადგილების გაცვლა;

(b) სტრიქონის გამრავლება შებრუნებად ელემენტზე;

(c) ერთ სტრიქონს მიმატება სხვა სტრიქონისა გამრავლებულს რაიმე ელემენტზე;

ჩვენ ჩამოვთვალეთ ელემენტარული გარდაქმნები სტრიქონების მიმართ. ანალოგიურად, განისაზღვრება ელემენტარული გარდაქმნები სვეტების მიმართ.

ყველა ეს ელემენტარული გარდაქმნა შეიძლება განხორციელებულ იქნას სპეციალურ მატრიცებზე გამრავლებით.

ყოველი $i \neq j$ განვსაზღვროთ

$$E_{i,j} = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$$

$E_{ij}A$ არის მატრიცი, რომელიც მიიღება A-გან მასში i-ური და j-ური სტრიქონების გაცვლით.

ყოველი i-თვის და ყოველი შებრუნებადი m-თვის განვსაზღვროთ

$$E_i(m) = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & m & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$$

ეს არის დიაგონალური მატრიცი, რომლის ყველა დიაგონალური ელემენტი 1-ის ტოლია გარდა i-ური პოზიციისა, სადაც იგი m-ს ტოლია. $E_i(m)A$ არის მატრიცი რომელიც მიიღება A-გან i-ური სტრიქონის გამრავლებით m-ზე.

ყოველი $i \neq j$ და ყოველი m ელემენტისთვის განვსაზღვროთ

$$E_{i,j}(m) = \begin{bmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \ddots & & & \\ & & m & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{bmatrix}$$

ეს არის ერთეულოვანი მატრიცი, მხოლოდ m ელემენტით (i,j) ადგილას. $E_{i,j}(m)A$ არის მატრიცი, რომელიც მიიღება A-გან i-ურ სტრიქონს j-ური სტრიქონის m-ზე ნამრავლის მიმატებით.

Lemma 1 *ვთქვათ P არის მატრიცი კომპონენტებით R რგოლში. იგი შებრუნებადია მაშინ და მხოლოდ მაშინ როცა $\det(P)$ არის შებრუნებადი ელემენტი R რგოლში.*

Proof. "მაშინ" თუ P შებრუნებადია, მაშინ მოიძებნება Q ისეთი, რომ $PQ = I$. აქედან $\det(P)\det(Q) = 1$.

"მხოლოდ მაშინ" განვსაზღვროთ მიერთებული მატრიცი $\tilde{P}$ ზუსტად ისე როგორც წრფივ ალგებრაში. გვექნება

$$P\tilde{P} = dI.$$

თუ d შებუნებადია, მაშინ ჩვენ შეგვიძლია განვსაზღვროთ

$$P^{-1} = d^{-1}\tilde{P}.$$

გვექნება:

$$PP^{-1} = I.$$

□

კერძოდ, ელემენტარული მატრიცები შებრუნებადია. შებრუნებადი მატრიცების სიმრავლე აღინიშნება $GL(R)$ სიმბოლოთი.

Corollary 4 *მთელი P მატრიცი შებრუნებადია მაშინ და მხოლოდ მაშინ როცა* $\det(P) = \pm 1$.

Corollary 5 *პოლინომური P მატრიცი შებრუნებადია მაშინ და მხოლოდ მაშინ როცა* $\det(P)$ *არანულოვანი კონსტანტაა.*

Theorem 10 *ვთქვათ A არის მთელი მატრიცი. ელემენტარული გარდაქმნების მეშვეობით იგი შეიძლება დაყვანილ იქნას შემდეგ სახეზე*

$$A' = \begin{bmatrix} d_1 & & & 0 & \cdots & 0 \\ & \ddots & & & & \\ & & d_r & 0 & \cdots & 0 \\ 0 & & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & & 0 & 0 & \cdots & 0 \end{bmatrix},$$

სადაც დიაგონალური კომპონენტები არაუარყოფითია და $d_1|d_2 \ldots |d_r$.

Proof. თუ $A = 0$, მაშინ არაფერია დასამტკიცებელი. ამიტომ, ვიგულისხმოთ რომ $A \neq 0$.

ნაბიჯი 1. სტრიქონების და სვეტების გადანაცვლებით, შეგვიძლია მივაღწიოთ იმას რომ მარცხენა ზედა კუთხეში გვქონდეს აბსოლუტური მნიშვნელობით ყველაზე პატარა ელემენტი. პირველი სტრიქონის -1-ზე გამრავლების შედეგად, თუ ეს აუცილებელია, ეს ზედა მარცხენა ელემენტი a_{11} გახდება დადებითი.

ნაბიჯი 2. ავიღოთ $a_{i1} \neq 0$ ($i > 1$), და გავყოთ a_{11}-ზე. გვექნება: $a_{i1} = a_{11}q + r$. i-ურ სტრიქონს გამოვაკლოთ პირველი სტრიქონი q-ზე გამრავლებული. ამით a_{i1} შეიცვლება r-ით. თუ $r \neq 0$, მაშინ ჩვენ ვუბრუნდებით პირველ ნაბიჯს. და ა.შ. იგივეს ვაკეთებთ სტრიქონების მიმართ. და საბოლოოდ მივიღებთ მატრიცს, სადაც პირველ სტრიქონსა და პირველ სვეტში ყველა ელემენტი ნულის ტოლია გარდა ერთისა. ეს ერთი ელემენტი მარცხენა ზედა ელემენტი. სხვა სიტყვებით, ჩვენ ვღებულობთ შემდეგი სახი მატრიცს

$$A' = \begin{bmatrix} a_{11} & 0 \\ 0 & B \end{bmatrix}.$$

ნაბიჯი 3. დავუშვათ, რომ რომელიღაც b ელემენტი B მატრიცში არ იყოფა a_{11}-ზე. ამ შემთხვევაში, პირველ სტრიქონს ვუმატებთ იმ სტრიქონს, რომელიც ამ ელემენტს შეიცავს. მივიღებთ მატრიცს რომლის პირველი სვეტში არის ეს b ელემენტი. ვუბრუნდებით მეორე ნაბიჯს.

ასე თუ გავაგრძელებთ, ცხადია მივიღებთ საჭირო მატრიცს.

□

Theorem 11 *ვთქვათ A არის მატრიცი ელემენტებით პოლინომთა $F[s]$ რგოლში, სადაც F არის ველი. ელემენტარული გარდაქმნების მეშვეობით იგი შეიძლება დაყვანილ იქნას შემდეგ*

სახეზე

$$A' = \begin{bmatrix} d_1 & & & 0 & \cdots & 0 \\ & \ddots & & & & \\ & & d_r & 0 & \cdots & 0 \\ 0 & & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & & 0 & 0 & \cdots & 0 \end{bmatrix},$$

სადაც d_i უნიტარული პოლინომებია და $d_1|d_2 \dots |d_r$.

Proof. დამტკიცება იგივეა.

Theorem 12 *ვთქვათ W არის თავისუფალი აბელის ჯგუფი რანგით m, და ვთქვათ S არის ქვეჯგუფი W-ში. მაშინ არსებობს W-ს ბაზისი $w_1, \dots, w_m$ და S-ს ბაზისი $u_1, \dots, u_n$ შემდეგი თვისებებით:*

(a) $n \leq m$;

(b) $\forall k$, $u_k = d_k w_k$;

(c) $d_1| \dots |d_r$.

Proof. შეგვიძლია ვიგულისხმოთ, რომ $W = \mathbb{Z}^m$. ავიღოთ სვეტები $A_1, \dots, A_n$ რომლებიც ქმნიან S ქვეჯგუფს, და განვიხილოთ $A = [A_1 \dots A_n]$ მატრიცი.

შევარჩიოთ P, Q როგორც წინა თეორემაში. გვექნება კომუტაციური დიაგრამა

$$\begin{array}{ccc} \mathbb{Z}^n & \xrightarrow{A} & \mathbb{Z}^m \\ P\downarrow & & \downarrow Q \\ \mathbb{Z}^n & \xrightarrow{D} & \mathbb{Z}^m \end{array}$$

საიდანაც ვღებულობთ რაც გვინდა.

□

4 მოდულები

R იყოს კომუტაციური რგოლი. R-მოდული M ეს არის აბელის ჯგუფი (კომპოზიციის კანონით რომელიც აღინიშნება პლიუსით "+") სკალარულ $R \times M \to M$ გამრავლებასთან ერთად (იწერება ასე: $r, v \mapsto rv$), რომელიც აკმაყოფილებს შემდეგ აქსიომებს:

(i) $1x = x$,

(ii) $(rs)x = r(sx)$,

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

(iv) $r(x + y) = rx + ry$.

შევნიშნოთ, რომ ეს ზუსტად წრფივი სივრცის აქსიომებია. თუ F არის ველი, მაშინ F-მოდული იგივეა რაც F-წრფივი სივრცე. ასე რომ მოდულები წრფივი სივრცეების ბუნებრივ განზოგადებას წარმოადგენენ.

მაგრამ ის ფაქტი, რომ რგოლში ელემენტები არ არიან საზოგადოდ შებრუნებადი მოდულებს ხდის ძალიან რთულ ობიექტებად.

მოდულის ცხადი მაგალითია R^n, სვეტების სიმრავლე კომპონენტებით რგოლიდან. კომპოზიციის კანონები განისაზღვრება შემდეგნაირად:

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} + \begin{bmatrix} y_1 \\ \vdots \\ y_n \end{bmatrix} = \begin{bmatrix} x_1 + y_1 \\ \vdots \\ x_n + y_n \end{bmatrix}, \qquad a \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} ax_1 \\ \vdots \\ ax_n \end{bmatrix}.$$

აი სხვა მაგალითები.

Examples. 1) იდეალი R რგოლში არსი R-მოდული. კერძოდ, თვითონ R არის R-მოდული.
2)$R = \mathbb{Z}$; მაშინ $\mathbb{Z}$-მოდული იგივეა რაც აბელის ჯგუფი (განვსაზღვრავთ: $nx = x + \cdots + x$).
3) $R = F[s]$, სადაც F არის ველი; მაშინ R-მოდული იგივეა რაც F-წრფივი სივრცე წრფივ გარდაქმნასთან ერთად.

ვთქვათ M, N არიან ოდულები. ასახვას $f : M \to N$ ჰქვია ჰომომორფიზმი (ან წრფივი) თუ

$$f(x + y) = f(x) + f(y) \ \text{ და } \ f(ax) = af(x).$$

ჰომომორფიზმების კომპოზიცია ისევ ჰომომორფიზმია.
ქვემოდული M-ში არის ისეთი ქვეჯგუფი, რომელიც ჩაკეტილია რგოლის ელემენტებზე გამრავლების მიმართ. M/N ფაქტორსიმრავლეს აქვს მოდულის ბუნებრივი სტრუქტურა განსაზღვრული შემდეგნაირად: $(x + N) + (y + N) = (x + y) + N$ და $a(x + N) = ax + N$. ბუნებრივი ასახვა $M \to M/N$ არის R-ჰომომორფიზმი.
თუ $f : M \to N$ არის ჰომომორფიზმი, მისი ბირთვი არის სიმრავლე

$$Ker(f) = \{x \in M |\ f(x) = 0\};$$

ცხადია იგი არის M-ის ქვემოდული. სახე f ჰომომორფიზმისა არის სიმრავლე $Imf = f(M)$; იგი N-ის ქვემოდულია. f-ის კობირთვი განისაძღვრება, როგორც

$$Coker(f) = N/lm(f);$$

ეს არის N-ის ფაქტორმოდული.
ვთქვათ M და N ორი R-მოდულია. M-დან N-ში ჰომომორფიზმების სიმრავლე აღინიშნება $Hom(M, N)$ სიმბოლოთი. მას განიხილავენ როგორც მოდულს: $f + g$ და af განისაზღვრება შემდეგი წესებით

$$(f + g)(x) = f(x) + g(x), \quad (af)(x) = af(x).$$

შევნიშნოთ, რომ ყოველი M მოდულისთვის გვაქვს ბუნებრივი იზომორფიზმი

$$Hom(A, M) \simeq M.$$

იგი მოიცემა შემდეგი წესით: $f \mapsto f(1)$.
თუ M, N არიან R-მოდულებია, მაშინ მათი პირდაპირი ჯამი $M \oplus N$ არის სიმრავლე (x, y) წყვილებისა, სადაც $x \in M$ $y \in N$. ცხადია, ეს არის R-მოდული თუ შეკრებას და სკალარებზე გამრავლებას განვსაზღვრავთ შემდეგი გზით:

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2) \qquad a(x, y) = (ax, ay).$$

უფრო ზოგადად, თუ $(M)_{i\in I}$ არის R-მოდულების ნებისმიერი ოჯახი, ჩვენ შეგვიძლია განვსაზღვროთ მათი პირდაპირი ჯამი

$$\bigoplus_{i\in I} M_i;$$

მისი ელემენტებია (x_i), სადაც $x_i \in M_i$ $(i \in I)$ და თითქმის ყველა $x_i = 0$. თუკი მოვხსნით შეზღუდვას x_i ელემენტებზე, მივიღებთ პირდაპირ ნამრავლს

$$\prod_{i\in I} M_i.$$

შევნიშნავთ, რომ პირდაპირი ჯამი და პირდაპირი ნამრავლი ერთი და იგივეა, როცა ინდექსების I სიმრავლე არის სასრული.

თავისუფალი R-მოდული ეს არის მოდული, რომელიც იზომორფულია მოდულისა $\oplus_{i\in I} M_i$, სადაც ყოველი $M_i = R$. ეს უკანასკნელი აღინიშნება კიდევ, როგორც $R^{(I)}$. სასრულად წარმოქმნილი თავისუფალი მოდული ამრიგად არის მოდული, რომელიც იზომორფულია შემდეგი პირდაპირი ჯამისა

$$R \oplus \cdots \oplus R.$$

თუ გვაქვს n შესაკრები, მაშინ ეს უკანასკნელი აღინიშნება R^n სიმბოლოთი.

- **წარმოქმნელები და თანაფარდობები მოდულებში**

ჩვენ ვიგულისხმებთ, რომ R არის ნოეტერის რგოლი.

ვთქვათ A არის $q \times p$ ზომის მატრიცი კომპონენტებით R რგოლში. მაშინ იგი იძლევა სასრულად წარმოქმნილ R-მოდულს

$$M = R^q/AR^p.$$

პირუკუ, ვთქვათ, მოცემული გვაქვს სასრულად წარმოქმნილი M მოდული. ამოვირჩიოთ წარმომქმნელთა სისტემა $(v_1, \ldots, v_q)$. ეს წარმომქმნელები განსაზღვრავენ სიურექციულ ჰომომორფიზმს

$$f : R^q \to M : \quad f\begin{bmatrix} x_1 \\ \vdots \\ x_q \end{bmatrix} = x_1v_1 + \cdots + x_qv_q.$$

ამ ჰომომორფიზმის ბირთვი ავღნიშნოთ N ასოთი. გვექნება: $M \simeq R^q/N$. ავიღოთ ახლა N მოდულის წარმომქმნელთა სისტემა $(w_1, \ldots, w_p)$, და მისი მეშვეობით ავაგოთ სიურექციული ჰომომორფიზმი

$$g : R^p \to N,$$

როგორც ეს გავაკეთეთ მაღლა. ამის შემდეგ განვიხილოთ კომპოზიცია g ჰომომორფიზმისა $N \subseteq R^q$ ჩადგმის ჰომომორფიzმთან. ეს იქნება ჰომომორფიზმი

$$R^p \to R^q,$$

რომელიც წარმოადგენს რაღაც A მატრიცზე გამრავლებას (მარცხნიდან). ყოველ ასეთ A მატრიცს ჰქვია M მოდულის მატრიცული წარმოდგენა.

ცხადია, ბევრ სხვადასხვა მატრიცს შეუძლია წარმოადგინოს ერთიდაიგივე (იზომორფიზმამდე სიზუსტით) მოდული.

Lemma 2 *A იყოს მატრიცი. შემდეგი A' მატრიცები წარმოადგენენ იგივე მოდულს რაც A:*

(a) $A' = QAP^{-1}$, სადაც $P, Q \in GL(R)$;

(b) A' მიიღება ნულოვანი სვეტის წაშლით (თუ კი ამისთანა არის A-ში);

(c) A' მიიღება A-ში i-ური სტრიქონის და j-ური სვეტის წაშლით თუ ჩვენი მატრიცის j-ური სვეტი უდრის e_i-ს.

(e_i აღნიშნავს სვეტს, რომლის i-ურ ადგილას არის 1 და რომლის ყველა სხვა კომპონენტი 0-ის ტოლია.)

Proof. (a) გამომდინარეობს შემდეგი კომუტაციური დიაგრამიდან

$$\begin{array}{ccc} \mathbb{Z}^n & \stackrel{A}{\to} & \mathbb{Z}^m \\ P\downarrow & & \downarrow Q \\ \mathbb{Z}^n & \stackrel{A'}{\to} & \mathbb{Z}^m \end{array}.$$

(b) ვთქვათ $A = [A'\ 0]$. მაშინ $AR^m = A'R^{m-1} + 0R = A'R^{m-1}$. ასე რომ $R^q/AR^m = R^q/A'R^{m-1}$.

Example. ვთქვათ $R = \mathbb{Z}$, და ვთქვათ მოცემული გვაქვს

$$A = \begin{bmatrix} 3 & 8 & 7 & 9 \\ 2 & 4 & 6 & 6 \\ 1 & 2 & 2 & 1 \end{bmatrix}.$$

ეს მატრიცი შეიძლება გამარტივდეს შემდეგნაირად:

$$A \to \begin{bmatrix} 0 & 2 & 1 & 6 \\ 0 & 0 & 2 & 4 \\ 1 & 2 & 2 & 1 \end{bmatrix} \to$$

$$\begin{bmatrix} 2 & 1 & 6 \\ 0 & 2 & 4 \end{bmatrix} \to \begin{bmatrix} 2 & 1 & 6 \\ -4 & 0 & -8 \end{bmatrix} \to \begin{bmatrix} -4 & -8 \end{bmatrix} \to \begin{bmatrix} 4 \end{bmatrix}$$

ამრიგად ჩვენი A მატრიცი წარმოადგენს იგივე მოდულს რასაც 4, ანუ $M = \mathbb{Z}/4\mathbb{Z}$ მოდულს.

Example. მატრიცი $\begin{bmatrix} 4 \\ 0 \end{bmatrix}$ ვერ მარტივდება. იგი წარმოადგენს $M = \mathbb{Z}/4 \oplus \mathbb{Z}$ მოდულს.

- **სასრულად წარმოქმნილი აბელის ჯგუფების სტრუქტურული თეორემა**

Theorem 13 *ვთქვათ V არის სასრულად წარმოქმნილი აბელის ჯგუფი. მაშინ არსებობს $r \geq 0$ და $d_1, \ldots, d_k \geq 2$ ისეთი, რომ $d_1 | \ldots | d_k$ და*

$$V \simeq \mathbb{Z}^r \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \mathbb{Z}/d_k\mathbb{Z}.$$

ყველა ეს მთელი რიცხვი ცალსახად განისაზღვრება.

Proof. ავიღოთ ჩვენი ჯგუფისთვის რომელიმე A წარმოდგენა. თეორემა ? და ლემა ძალით, შეგვიძლია ვიგულისხმოთ, რომ A არის დიაგონალური დადებითი ელემენტებით დიაგონალზე და ყოველი ეს დიაგონალური ელემენტი ყოფს შემდგომს. შემდეგ, ჩვენ იმავე ლემის ძალით შეგვიძლია ამოვაგდოთ ნულოვანი სვეტები.

A მატრიცი მიიღებს ასეთ ფორმას

$$\begin{bmatrix} d_1 & & & \\ & \cdot & & \\ & & \cdot & \\ & & & d_r \\ 0 & \cdot & \cdot & 0 \end{bmatrix}.$$

Remark. მსგავსი თეორემა სამართლიანია მოდულებისთვის განსაზღვრულთ მთავარ იდეალთა რგოლზე.

5 ველები

შეგახსენებთ, რომ ველი არის (კომუტაციური) რგოლი რომლის არანულოვანი ელემენტები ქმნიან ჯგუფს გამრავლების მიმართ.

ვთქვათ, F არის ველი და L/F მისი გაფართოება. და ვთქვათ $f \in F[s]$ არის პოლინომი კოეფიციენტებით F ველში. ამბობენ, რომ $c \in L$ არის ფესვი ამ პოლინომის თუ $f(c) = 0$.

Example. $s^2 - 2$ პოლინომს არ გააჩნია ფესვი რაციონალურ რიცხვთა ველში. მაგრამ აქვს ფესვი $\sqrt{2}$ ნამდვილ რიცხვთა ველში.

s^n პოლინომის წარმოებულს განსაზღვრავენ როგორც ns^{n-1}-ს. თუ მოვითხოვთ რომ წარმოებულს უნდა ჰქონდეს წრფივობის თვისება, მაშინ $f = a_0 s^n n + a_1 s^{n-1} + \cdots + a_n$ პოლინომის წარმოებული უნდა იყოს

$$f' = na_0 s^{n-1} + (n-l)a_1 s^{n-2} + \cdots + a_{n-1}.$$

ეს სუფთა ალგებრული ოპერაციაა. უნდა აღინიშნოს, რომ იგი აკამყოფილებს ლაიბნიცის წესს:

$$(fg)' = f'g + fg'.$$

წარმოებულის ერთი მნიშვნელობა ალგებრაში არის ის რომ იგი საშუალებას იძლევა გავარკვიოთ თო როდის აქვს პოლინომს ჯერადი ფესვები.

Lemma 3 *F იყოს ველი, და $f \in F[s]$ იყოს პოლინომი. ვთქვათ $x \in F$ არის f-ს ფესვი. მაშინ x არის ჯერადი ფესვი, ანუ $(s-x)^2$ ყოფს f-ს, მაშინ და მხოლოდ მაშინ როცა იგი არის ფესვი აგრეთვე f-ის წარმოებულისა.*

Proof. რადგან x არის ფესვი f პოლინომისა, $s - x$ ყოფს მას: $f = (s-x)g$. x არის ჯერადი ფესვი მაშინ და მხოლოდ მაშინ , როცა იგი ფესვია g პოლინომისა. ლაიბნიცის წესის თანახმად,

$$f' = (s-x)g' + g.$$

თუ ჩავსვამთ $s = x$ დავინახავთ, რომ $f'(x) = 0$ მაშინ და მხოლოდ მაშინ როცა $g(x) = 0$.

□

Lemma 4 *ვთქვათ F არის ველი, და ვთქვათ p არის დაუყვანადი პოლინომი $F[s]$-ში. მაშინ რგოლი $K = F[s]/(p)$ არის F-ის გაფართოება, და s-ს ნაშთთა კლასი არის p პოლინომის ფესვი K-ში.*

Proposition 5 *. ვთქვათ F არის ველი, და ვთქვათ f არის დადებითი ხარისხის პოლინომი $F[s]$-ში. არსებობს სასრული გაფართოება K/F ისეთი რომ f იშლება წრფივ მამრავლებად K-ზე.*

Proof. ლემის ძალით არსებობს გაფართოება, სადაც f-ს აქვს ფესვი. ეს ფესვი ავღნიშნოთ a-თი, და თვითონ გაფართოება ავღნიშნოთF_1-ით. პოლინომთა $F_1[s]$ რგოლში გვექნება დაშლა $f = (s-a)g$, სადაც g არის პოლინომი კოეფიციენტებით F_1-ში. იგივე ლემის გამოყენებით, შეგვიძლია ავაგოთ F_1-ის გაფართოება F_2 რომელშიც g პოლინომს გააჩნია ფესვი. და ა.შ.

□

Definition ვთქვათ f არის პოლინომი კოეფიციენტებით F ველში. ამბობენ, რომ E/F გაფართოება არის f-ის დაშლის ველი თუ კი ის არის ყველაზე პატარა გაფართოება, რომელიც შეიცავს f-ს ყველა ფესვს.

Proposition 6 *ყოველ პოლინომს $f \in F[s]$ აქვს დაშლის ველი.*

ამბობენ, რომ F ველი არის ალგებრულად ჩაკეტილი თუ ყოველ დადებითი ხარისხის პოლინომს $f \in F[s]$ აქვს ფესვი F-ში. მაგ. კომპლექსუ რიცხვთა ველი $\mathbb{C}$ არის ალგებრულად ჩაკეტილი. ამ ფაქტს ჰქვია *ალგებრის ფუნდამენტური თეორემა*.

Theorem 14 *ყოველ არამუდმივ პოლინომს კომპლექსური კოეფიციენტებით აქვს კომპლექსური ფესვი.*

შემდეგი თეორემა მტკიცდება ცორნის ლემის მეშვეობით.

Theorem 15 *ყოველ F ველს გააჩნია ალგებრული ჩაკეტვა. და თუ K_1 და K_2 ორი ალგებრული ჩაკეტვაა F, მაშინ არსებობს იზომორფიზმი $\phi : K_1 \to K_2$ რომელიც ადგილზე ტოვებს F-ს.*

ამრგიგად, ალგებრული ჩაკეტვა არსებობს და არსებითად ერთია.

ვთვათ L/K არის ველების გაფართოება. მაშინ L შეგვიძლია განვიხილოთ როგორც ვექტორული სივრცე K-ზე. როგორც ასეთს მას აქვს განზომილება, და ეს განზომილება იწოდება გაფართოების ხარისხად და აღინიშნება $[L : K]$ სიმბოლოთი.

Proposition 7 *ვთქვათ $K(\alpha)/K$ არის მარტივი გაფართოება. თუ α ტრანსცენდენტულია K-ზე, მაშინ გაფართოება არის უსასრულო. თუ α ალგებრულია K-ზე და p არის მისი მინიმალური პოლინომი, მაშინ*

$$[K(\alpha) : K] = \deg p.$$

ელემენტები $1, \alpha, \ldots \alpha^{d-1}$, სადაც $d = \deg p$, არის ბაზისი.

Proposition 8 (კოშკის წესი) *ვთქვათ, გვაქვს გაფართოებათა კოშკი $M/L/K$. მაშინ $[M : K] = [M : L][L : K]$.*

Definition. თუ E/F არის ველების გაფართოება, მაშინ მისი გალუას ჯგუფი, რომელიც აღინიშნება $Gal(E/F)$ სიმბოლოთი, არის სიმრავლე E-ს F-ავტომორფიზმებისა.

Example. თუ $E = \mathbb{Q}(2^{1/3})$, მაშინ $Gal(E/Q) = \{1\}$.

Definition. L/K გაფართოებას ჰქვია გალუას გაფართოება თუ $Gal(L/K)$-ს უძრავი ველი ემთხვევა K-ს.

შემდეგი წინადადება იძლევა გალუას გაფართოებების რიცხობრივ დახასიათებას. ის ამბობს რომ გალუას გაფართოებები ეს ის გაფართოებებია რომელთა გალუას ჯგუფი იმდენად დიდია რამდენადაც ეს შესაძლებელია.

Proposition 9 *თუ L/K სასრული გაფართოებააა, მაშინ $|Gal(L/K)| \leq [L : K]$. თოლობას ადგილი აქვს მაშინ ა მხოლოდ მაშინ როცა L/K არის გალუას გაფართოება.*

Definition. ვთქვათ E/F არის სასრული გაფართოება და $G = Gal(E/F)$ ამ გაფართოების გალუას ჯგუფი. თუ H არის ქვეჯგუფი G-ში, მისი უძრავი ველი არის სიმრავლე E^H იმ ელემენტებისა რომლებსაც H-ის ყოველი ავტომორფიზმი უძრავად ტოვებს; ანუ

$$E^H = \{x \in E | \sigma(x) = x \text{ for all } \sigma \in H\}.$$

არსებობს შესანიშნავი კავშირი ველების თეორიასა და ჯგუფების თეორიას შორის. გალუას თეორია სწავლობს სწორედ ამ კავშირს.

Theorem 16 *ვთქვათ L/K არის გალუას სასრული გაფართოება. არსებობს ურთიერთცალსახა თანადობა $Gal(L/K)$-ს ქვეჯგუფებსა და L/K გაფართოების ქვეველებს შორის. ასახვა*

$$H \mapsto L^H$$

ამყარებს ამ თანადობას.

Example. განვიხილოთ $F = \mathbb{Q}(i, \sqrt{5})/\mathbb{Q}$ გაფართოება. მას აქვს ოთხი $\mathbb{Q}$-ავტომორფიზმი, რომლებიც მოიცემიან შემდეგნაირად:

$$\sigma_1 : \quad i \mapsto i, \ \sqrt{5} \mapsto \sqrt{5},$$
$$\sigma_2 : \quad i \mapsto -i, \ \sqrt{5} \mapsto \sqrt{5},$$
$$\sigma_3 : \quad i \mapsto i, \ \sqrt{5} \mapsto -\sqrt{5},$$
$$\sigma_4 : \quad i \mapsto -i, \ \sqrt{5} \mapsto -\sqrt{5}$$

(საკმარისია აღვწეროთ მოქმედება i-სა და $\sqrt{5}$-ზე.) ამრიგად

$$Gal(F/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}.$$

$Gal(E/Q)$ ჯგუფის საკუთრივი ქვეჯგუფებია

$$\{\sigma_1\}, \{\sigma_1, \sigma_2\}, \{\sigma_1, \sigma_3\}, \{\sigma_1, \sigma_4\}$$

და მათი შესაბამისი ქვეველებია

$$F, \mathbb{Q}(\sqrt{5}), \mathbb{Q}(i), \mathbb{Q}(i\sqrt{5}).$$

$s^n - 1$ მრავალწევრის დაშლის ველს Q-ზე ჰქვია n-ური რიგის ციკლოტომური გაფართოება. პოლინომს

$$\Phi_n = \prod_{i=1}^{\phi(n)} (s - \alpha_i),$$

სადაც a_i აღნიშნავენ n-ური რიგის პრიმიტიულ ფესვებს ერთიანიდან, ჰქვია n რიგის ციკლოტომური პოლინომი.

Example. მე-8 რიგის ერთერთი პირველადი ფესვი ერთიანიდან არის

$$\zeta = cos(2\pi/n) + isin(2\pi/n) = cos(\pi/4) + isin(\pi/4) = (1+i)/\sqrt{2}.$$

ყველა სხვა პირველადი ფესვებია $\zeta, \zeta^3, \zeta^5, \zeta^7$. ასე რომ

$$\Phi_8 = (s-\zeta)(s-\zeta^3)(s-\zeta^5)(s-\zeta^7).$$

ადვილი გამოსათვლელია, რომ $\Phi_8 = s^4 + 1$.

Proposition 10 *n-ური რიგის ციკლოტომური გაფართოების გალუას ჯგუფი იზომორფულია $\mathbb{Z}/n\mathbb{Z}$ რგოლის მულტიპლიკაციური ჯგუფისა.*