O kilku zastosowaniach grup i pierścieni grupowych

Czesław BAGIŃSKI, Edmund R. PUCZYŁOWSKI, Białystok–Warszawa

Nierzadko zdarza się, że rozwiązanie elementarnie brzmiącego zadania, wymaga niestandardowych pomysłów. Niektóre z tych pomysłów odzwierciedlają własności pewnych abstrakcyjnych obiektów występujących w różnych działach matematyki wyższej. Przedstawimy tutaj kilka takich zadań i pokażemy jak można je dość prosto rozwiązać, gdy umiejętnie wykorzysta się pewne własności grup i algebr grupowych.

Kilkanaście lat temu w konkursie zadaniowym 'Kwanta' pojawiło się następujące zadanie:

1. *Na okręgu wypisano* 101 *liczb naturalnych, których suma jest równa* 300. *Wykazać, że suma pewnej ilości kolejnych z tych liczb wynosi* 200.

Można je łatwo rozwiązać, gdy się wie, że:

2. *Suma pewnej ilości kolejnych liczb wśród dowolnie zadanych liczb całkowitych $a_1, \ldots, a_n$ dzieli się przez n.*

Porównaj z przykładem na stronie 49 książki V. Bryant, *Aspekty kombinatoryki*, WN-T, Warszawa 1997.

Istotnie, ponumerujmy kolejno liczby na okręgu, zgodnie z ruchem wskazówek zegara, zaczynając od którejkolwiek z nich. Korzystając z **2** stwierdzamy, że suma pewnej ilości kolejnych, spośród liczb $a_1, \ldots, a_{100}$ dzieli się przez 100. Suma ta nie może być równa 0, bo sumujemy liczby naturalne, ani 300, bo a_{101} nie jest jej składnikiem. Zatem jest ona równa 100 lub 200. Jeśli jest równa 200, to właśnie ona realizuje tezę. Jeśli jest równa 100, to suma pozostałych liczb, które są kolejne dzięki temu, że mamy do czynienia z liczbami wypisanymi na okręgu, jest równa 200 i teraz ona realizuje tezę.

Aby rozwiązać zadanie **2**, oznaczmy przez $r_1, \ldots, r_n$ reszty z dzielenia przez n kolejnych liczb $a_1, \ldots, a_n$. Reszty te są elementami zbioru $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, który wraz z działaniem

$$a \oplus b = \text{reszta z dzielenia } a + b \text{ przez } n$$

tworzy grupę. Temu zadaniu można teraz nadać następującą postać:

Cz. Bagiński, E. R. Puczyłowski *O kilku twierdzeniach elementarnej teorii liczb, czyli o tym, skąd się biorą grupy*, Delta, sierpień 2003.

2'. *Udowodnić, że dla pewnych i, j $(0 \leqslant i < j \leqslant n)$, $r_{i+1} \oplus r_{i+2} \oplus \cdots \oplus r_j = 0$.*

Jest to szczególny przypadek znacznie ogólniejszej obserwacji dotyczącej dowolnej grupy skończonej.

3. *Jeśli $g_1, \ldots, g_n$ należą do n-elementowej grupy G, to dla pewnych i, j, $0 \leqslant i < j \leqslant n$, mamy $g_{i+1} \cdot g_{i+2} \cdot \ldots \cdot g_j = e$.*

Dla działania grupy stosujemy zapis multiplikatywny, e oznacza element neutralny grupy G.

Dla dowodu zauważmy, że elementy $h_0 = e, h_1 = g_1, h_2 = g_1 \cdot g_2, \ldots, h_n = g_1 \cdot g_2 \cdot \ldots \cdot g_n$ należą do grupy G. Ponieważ G ma n elementów, a ciąg przed chwilą utworzony ma $n+1$ wyrazów, więc na podstawie Szufladkowej Zasady Dirichleta, dla pewnych i, j $(0 \leqslant i < j \leqslant n)$, jest $h_i = h_j = h_i \cdot g_{i+1} \cdot g_{i+2} \cdot \ldots \cdot g_j$. Skracając obie strony tej równości przez h_i, otrzymujemy, że $g_{i+1} \cdot g_{i+2} \cdot \ldots \cdot g_j = e$.

Następne zadanie, które chcielibyśmy rozważyć, jest w sformułowaniu dość podobne do zadania drugiego.

4. *Spośród dowolnych $2n-1$ liczb całkowitych można wybrać n liczb, których suma jest podzielna przez n.*

Nie żądamy tu, by wybrane liczby były kolejnymi. Chcemy natomiast, aby było ich dokładnie n. Okazuje się, że wykazanie, że jest to możliwe jest znacznie trudniejsze niż rozwiązanie zadania 2.

Najpierw zredukujemy zadanie do przypadku, gdy n jest liczbą pierwszą. W tym celu wystarczy wykazać, że jeśli $k, l > 1$ oraz spośród dowolnych $2k-1$ liczb całkowitych można wybrać k liczb, których suma jest podzielna przez k, a także spośród dowolnych $2l-1$ liczb całkowitych można wybrać l liczb, których suma jest podzielna przez l, to spośród dowolnych $2kl-1$ liczb całkowitych $a_1, a_2, \cdots, a_{kl}$ można wybrać kl liczb, których suma jest podzielna przez kl. Ponieważ $2kl-1 > 2k-1$, więc spośród naszych $2kl-1$ liczb możemy wybrać k, których suma s_1 jest podzielna przez k. Z pozostałych liczb znowu możemy wybrać k, których suma s_2 jest podzielna przez k. Postępowanie to kontynuujemy do momentu, gdy zostanie mniej niż $2k-1$ liczb. Zauważmy, że ponieważ $2kl-1 = k(2l-1)+k-1$, operację tę możemy powtórzyć $2l-1$ razy uzyskując sumy $s_1, s_2, \cdots, s_{2l-1}$ podzielne przez k. Spośród tych liczb możemy wybrać l, których suma jest podzielna przez l. Jasne jest, że ta suma jest podzielna przez kl i że jest sumą kl liczb wybranych spośród liczb $a_1, a_2, \cdots, a_{kl}$.

Rozwiązanie zadania **4** sprowadza się więc do wykazania, że:

4'. *Jeśli p jest liczbą pierwszą, to spośród $2p-1$ liczb całkowitych można wybrać p liczb, których suma jest podzielna przez p.*

W dowodzie tego faktu wykorzystamy pojęcie algebry grupowej.

Zacznijmy od ogólnej definicji. Niech G będzie dowolną grupą skończoną z działaniem o zapisie multiplikatywnym, mającą dokładnie n elementów, zaś K dowolnym ciałem. Przez $K[G]$ oznaczymy zbiór wszystkich formalnych wyrażeń postaci

Dla ustalenia uwagi można przyjąć, że K jest ciałem liczb wymiernych lub ciałem $\mathbb{Z}_p$ reszt modulo p, którego elementami są liczby $0, 1, \ldots, p-1$ z operacjami dodawania i mnożenia zdefiniowanymi równościami:

$a \oplus b =$ reszta z dzielenia $a+b$ przez p,

$a \odot b =$ reszta z dzielenia $a \cdot b$ przez p.

$$\sum_{g \in G} \alpha_g g, \tag{1}$$

gdzie $\alpha_g \in K$ i $g \in G$. Można przyjąć, że elementy zbioru $K[G]$ są wektorami o n współrzędnych numerowanych elementami grupy G. Zamiast $\sum_{g \in G} \alpha_g g$ piszemy też $\alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_n g_n$, gdzie $\alpha_1, \ldots, \alpha_n \in K$ oraz $\{g_1, \ldots, g_n\} = G$. Przyjmujemy przy tym, że

$$\alpha_1 g_1 + \alpha_2 g_2 + \cdots + \alpha_n g_n = \beta_1 g_1 + \beta_2 g_2 + \cdots + \beta_n g_n \tag{2}$$

wtedy i tylko wtedy, gdy $\alpha_i = \beta_i$, dla wszystkich $i = 1, \ldots, n$). Przy zapisie poszczególnych elementów w $K[G]$ pomijamy na ogół człony ze współczynnikami zero (gdy wszystkie współczynniki są równe zero, to piszemy zamiast $\sum_{g \in G} 0g$, lub $0g_1 + \cdots + 0g_n$, po prostu 0). W naturalny sposób wprowadzamy również inne uproszczenia notacji. I tak, zamiast $1g$ piszemy g, zamiast $(-\alpha)g$ piszemy $-\alpha g$, a element neutralny e grupy G oznaczamy symbolem 1 (tak jak element z ciała K) i będziemy go na ogół opuszczali przy zapisie elementów $K[G]$, tzn. zamiast $\alpha \cdot 1$ będziemy pisali α.

Przy skróconej notacji (1), równość (2) ma postać $\sum_{g \in G} \alpha_g g = \sum_{g \in G} \beta_g g$, i zachodzi wtedy i tylko wtedy, gdy $\alpha_g = \beta_g$ dla wszystkich $g \in G$.

W zbiorze $K[G]$ wprowadzamy działania dodawania i mnożenia przez skalary (czyli elementy ciała), tak jak czyni się to z wektorami:
dodawanie:

$$(\alpha_1 g_1 + \cdots + \alpha_n g_n) + (\beta_1 g_1 + \cdots + \beta_n g_n) = (\alpha_1 + \beta_1) g_1 + \cdots + (\alpha_n + \beta_n) g_n;$$

mnożenie przez skalary:

$$\alpha \cdot (\beta_1 g_1 + \cdots + \beta_n g_n) = (\alpha\beta_1) g_1 + \cdots + (\alpha\beta_n) g_n.$$

Wprowadzamy jeszcze jedną operację, którą jednak wygodniej zapisać w skrótowej postaci. Jest to operacja mnożenia:

$$\Big(\sum_{g \in G} \alpha_g g\Big) \cdot \Big(\sum_{g \in G} \beta_g g\Big) = \sum_{x \in G} \gamma_x x,$$

gdzie $\gamma_x = \sum_{gh=x} \alpha_g \beta_h$.

Jak zatem widać, najbardziej skomplikowane jest mnożenie. Ono także w decydującym stopniu wpływa na wewnętrzną strukturę algebry $K[G]$, dlatego przyjrzyjmy się mu jeszcze przez chwilę. Mnożąc element $\alpha_1 g_1 + \cdots + \alpha_n g_n$ przez

$\beta_1 g_1 + \cdots + \beta_n g_n$, postępujemy dokładnie tak samo, jak przy mnożeniu wyrażeń algebraicznych, czyli wszystkie składniki $\alpha_i g_i$ pierwszej sumy mnożymy po kolei przez wszystkie składniki $\beta_j g_j$ drugiej, wedle wzoru

$$\alpha_i g_i \cdot \beta_j g_j = (\alpha_i \beta_j)(g_i g_j).$$

Następnie sumujemy otrzymane wyniki i redukujemy wyrazy podobne.

Działania określone w $K[G]$ mają prawie wszystkie własności podstawowych działań na liczbach i na wektorach. Jedynie czego nie można oczekiwać, to istnienie odwrotności dla dowolnego elementu różnego od zera i przemienności mnożenia, jeśli G nie jest grupą przemienną.

W przypadku pewnych grup o mało skomplikowanej strukturze, ich algebry grupowe można opisać w nieco inny, może bardziej elementarny, sposób.

Niech G będzie cykliczną grupą rzędu n, tzn. $G = \{x, x^2, \ldots, x^{n-1}, x^n = 1\}$. Elementy grupy G możemy traktować jak jednomiany zmiennej x, które mnożymy wedle powszechnie znanych reguł, ale dodatkowo upraszczamy zapis wynikający z faktu, iż $x^n = 1$. I tak na przykład, $x^2 \cdot x^{n-1} = x^{n+1} = x^n \cdot x = x$. Elementy algebry $K[G]$ możemy więc traktować jak wielomiany zmiennej x, których stopień nie przekracza $n-1$:

$$\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}.$$

Mnożenie elementów tej algebry wykonujemy dokładnie tak, jak mnożenie wielomianów, pamiętając przy tym, że $x^n = 1$. Mamy zatem:

$$\begin{aligned}
&(\alpha_0 + \alpha_1 x + \cdots + \alpha_{n-1} x^{n-1}) \cdot (\beta_0 + \beta_1 x + \cdots + \beta_{n-1} x^{n-1}) = \\
&\quad = \alpha_0\beta_0 + \alpha_0\beta_1 x + \cdots + \alpha_0\beta_{n-2} x^{n-2} + \alpha_0\beta_{n-1} x^{n-1} + \\
&\qquad + \alpha_1\beta_0 x + \alpha_1\beta_1 x^2 + \cdots + \alpha_1\beta_{n-2} x^{n-1} + \alpha_1\beta_{n-1} + \\
&\qquad + \alpha_2\beta_0 x^2 + \alpha_2\beta_1 x^3 + \cdots + \alpha_2\beta_{n-2} + \alpha_2\beta_{n-1} x + \\
&\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\qquad + \alpha_{n-1}\beta_0 x^{n-1} + \alpha_{n-1}\beta_1 + \cdots + \alpha_{n-1}\beta_{n-2} x^{n-3} + \alpha_{n-1}\beta_{n-1} x^{n-2} = \\
&\quad = (\alpha_0\beta_0 + \alpha_1\beta_{n-1} + \cdots + \alpha_{n-2}\beta_2 + \alpha_{n-1}\beta_1) + \\
&\qquad + (\alpha_0\beta_1 + \alpha_1\beta_0 + \cdots + \alpha_{n-2}\beta_3 + \alpha_{n-1}\beta_2) x + \\
&\qquad + (\alpha_0\beta_2 + \alpha_1\beta_1 + \cdots + \alpha_{n-2}\beta_4 + \alpha_{n-1}\beta_3) x^2 + \\
&\qquad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\qquad + (\alpha_0\beta_{n-1} + \alpha_1\beta_{n-2} + \cdots + \alpha_{n-2}\beta_1 + \alpha_{n-1}\beta_0) x^{n-1}.
\end{aligned}$$

Nietrudno sprawdzić, że tak określone mnożenie można zdefiniować analogicznie, jak mnożenie modulo n. Otóż, elementy omawianej algebry $K[G]$ można traktować jak reszty z dzielenia wielomianów zmiennej x o współczynnikach z K przez wielomian $x^n - 1$. Jeśli teraz mamy dwa dowolne elementy (reszty), to ich iloczyn w $K[G]$ jest po prostu resztą z dzielenia przez $x^n - 1$ zwykłego iloczynu tych elementów, traktowanych jak wielomiany.

Niech teraz G będzie iloczynem kartezjańskim dwóch kopii grupy cyklicznej $\{1, g, g^2, \ldots, g^{p-1}\}$ rzędu p. Można ją interpretować jako zbiór wszystkich jednomianów zmiennych x, y postaci $x^k y^l$, gdzie $1 \leqslant k, l \leqslant p-1$, których mnożenie wykonujemy tak, jak zwykłe mnożenie jednomianów przemiennych zmiennych x i y, pamiętając przy tym, że $x^p = y^p = 1$. Niech ponadto $K = \mathbb{Z}_p$. W algebrze $K[G]$ rozważmy zbiór $\omega(G) = \{\sum_{g \in G} \alpha_g (g-1) \mid \alpha_g \in K\}$. Zauważmy, że jeśli $g = x^k y^l$, to

$$\begin{aligned}
g - 1 &= x^k y^l - 1 = (x^k - 1) y^l + y^l - 1 = \\
&= (x-1)(1 + x + x^2 + \cdots + x^{k-1}) y^l + (y-1)(1 + y + y^2 + \cdots + y^{l-1}) = \\
&= (x-1)a + (y-1)b
\end{aligned}$$

dla odpowiednich $a, b \in K[G]$. Wynika stąd, że jeśli $a_1, \ldots, a_n \in \omega(G)$, to $a_1 \cdot \ldots \cdot a_n$ jest sumą elementów postaci $(x-1)^m (y-1)^r c$, gdzie m, r są liczbami całkowitymi nieujemnymi takimi, że $m + r = n$ oraz $c \in K[G]$. Zauważmy także, że $(x-1)^p = x^p - 1^p = 0 = (y-1)^p$, a zatem jeśli $m \geqslant p$, to $(x-1)^m = (y-1)^m = 0$. Jeśli teraz $a_1, \ldots, a_{2p-1} \in \omega(G)$, to

$$a_1 \cdot a_2 \cdot \ldots \cdot a_{2p-1} = 0. \tag{3}$$

Rzeczywiście, po uwzględnieniu postaci czynników i ich wymnożeniu, iloczyn po lewej stronie tej równości stanie się sumą elementów postaci $(x-1)^m(y-1)^r c$, gdzie $m+r=2p-1$. Zatem każdy składnik tej sumy jest równy zero.

Wyposażeni w tę wiedzę możemy już nietrudno wykazać **4'** (chociaż w pewnym sensie właśnie teraz pojawia się najistotniejszy pomysł). Załóżmy więc, że $n_1, n_2, \cdots, n_{2p-1}$ są danymi liczbami całkowitymi. Możemy je oczywiście zastąpić przez ich reszty modulo p i w efekcie założyć, że są to liczby nieujemne nie większe od $p-1$. Niech, jak wyżej, G będzie grupą, która jest iloczynem kartezjańskim dwóch kopii grupy cyklicznej $\{1, g, \ldots, g^{p-1}\}$ rzędu p, $K = Z_p$ i niech $g_1 = x^{n_1}y^{n_1+1}, g_2 = x^{n_2}y^{n_2+1}, \ldots, g_{2p-1} = x^{n_{2p-1}}y^{n_{2p-1}+1}$. Oczywiście $g_1 - 1, g_2 - 1, \cdots, g_{2p-1} - 1 \in \omega(G)$. Zatem $(g_1-1)(g_2-1)\cdots(g_{2p-1}-1) = 0$. Po rozwinięciu lewej strony tej równości otrzymamy wyrażenie, które jest sumą -1 oraz wyrażeń $\pm g_{i_1}g_{i_2}\cdots g_{i_k}$, gdzie $k \leqslant 2p-1$. Oczywiście -1 musi się zredukować z pewnym takim wyrażeniem. Wynika stąd, że dla pewnego k oraz $i_1, i_2, \cdots, i_k$ takich, że $1 \leqslant k, i_1, i_2, \cdots, i_k \leqslant 2p-1$, mamy $g_{i_1}g_{i_2}\cdots g_{i_k} = 1$. To zaś oznacza, że $x^{n_{i_1}+n_{i_2}+\cdots+n_{i_k}}y^{n_{i_1}+n_{i_2}+\cdots+n_{i_k}+k} = 1$. W efekcie $x^{n_{i_1}+n_{i_2}+\cdots+n_{i_k}} = 1$ oraz $y^k = 1$. Z tych równości wynika, że k oraz $n_{i_1} + n_{i_2} + \cdots + n_{i_k}$ są podzielne przez p. Ponieważ jednak $1 \leqslant k \leqslant 2p-1$, więc $k = p$. Zatem suma p spośród liczb $n_1, n_2, \cdots, n_{2p-1}$ jest podzielna przez p i zadanie jest rozwiązane.

Zajmiemy się teraz innym zadaniem z elementarnej teorii liczb. Przy odrobinie ciekawości można opisaną w nim własność odkryć bawiąc się potęgami elementu $1-x$ należącego do rozpatrywanej wyżej algebry grupowej grupy rzędu p nad ciałem $\mathbb{Z}_p$. Załóżmy najpierw, że $p = 2$. Jak wiemy, w tej algebrze $(1-x)^2 = 1 - 2x + x^2 = 2 - 2x = 0$, a więc dla dowolnej liczby naturalnej $n \geqslant p$ także mamy równość $(1-x)^n = 0$. Z rozwinięcia lewej strony tego wyrażenia oraz równości $x^2 = 1$ otrzymujemy

$$0 = \sum_{k=0}^{n}(-1)^k\tbinom{n}{k}x^k = \sum_{0\leqslant 2k\leqslant n}\tbinom{n}{2k} - \sum_{1\leqslant 2k+1\leqslant n}\tbinom{n}{2k+1}x.$$

Zatem obie liczby $\sum\limits_{0\leqslant 2k\leqslant n}\tbinom{n}{2k}$ i $\sum\limits_{1\leqslant 2k+1\leqslant n}\tbinom{n}{2k+1}$ są podzielne przez 2, ponieważ traktowane, jako elementy ciała $\mathbb{Z}_2$ są równe 0. Rozważmy jeszcze jeden szczególny przypadek $p = 3$. Tu analogicznie, dla $n \geqslant 3$ zachodzi równość $(1-x)^n = 0$, a po rozwinięciu lewej strony i uwzględnieniu równości $x^3 = 1$, dostajemy

$$\begin{aligned} 0 &= \sum_{k=0}^{n}(-1)^k\tbinom{n}{k}x^k = \\ &= \sum_{0\leqslant 3k\leqslant n}(-1)^k\tbinom{n}{3k} + \sum_{1\leqslant 3k+1\leqslant n}(-1)^{k+1}\tbinom{n}{3k+1}x + \sum_{1\leqslant 3k+2\leqslant n}(-1)^k\tbinom{n}{3k+2}x^2. \end{aligned}$$

Analogicznie, jak poprzednio otrzymujemy zatem, że każda z liczb

$$\sum_{0\leqslant 3k\leqslant n}(-1)^k\tbinom{n}{3k}, \quad \sum_{1\leqslant 3k+1\leqslant n}(-1)^k\tbinom{n}{3k+1}, \quad \sum_{1\leqslant 3k+2\leqslant n}(-1)^k\tbinom{n}{3k+2}$$

dzieli się przez 3. Na bazie tych szczególnych przypadków sformułujmy zadanie ogólne, którego rozwiązanie pozostawiamy Czytelnikowi.

5. *Niech p będzie dowolną liczbą pierwszą, $p > 2$, i m liczbą całkowitą z przedziału $\langle 0; p-1\rangle$. Wówczas dla dowolnej liczby naturalnej $n \geqslant p$, liczba*

$$\sum_{1\leqslant pk+m\leqslant n}(-1)^k\tbinom{n}{pk+m}$$

dzieli się przez p.

Na zakończenie zaproponujemy do rozwiązania w liczbach całkowitych następujący układ równań.

$$\text{(4)} \qquad \begin{cases} a^2 + 2bc = pa \\ b^2 + 2ac = pc \\ c^2 + 2ab = pb \end{cases}$$

Jego rozwiązanie metodami tradycyjnymi nie jest może szczególnie trudne, ale za to jest dość żmudne. Tymczasem okazuje się, że wykorzystanie algebr grupowych i ich klasycznych własności daje odpowiedź natychmiast. Niech $G = \{1, g, g^2\}$ będzie grupą cykliczną rzędu 3 oraz $\mathbb{Q}[G]$ algebrą grupową tej grupy nad ciałem $\mathbb{Q}$ liczb wymiernych. W algebrze tej rozważmy podzbiór $\mathbb{Z}[G] = \{a + bg + cg^2 |\ a, b, c \in \mathbb{Z}\}$, gdzie $\mathbb{Z}$ oznacza zbiór liczb całkowitych. Zauważmy, że rozwiązanie układu (4) jest równoważne z wyznaczeniem wszystkich elementów $\xi = a + bg + cg^2 \in \mathbb{Z}[G]$, które dla ustalonej liczby p spełniają równanie

$$\xi^2 = p\xi. \tag{5}$$

Podstawienie $\xi = a + bg + cg^2$ prowadzi właśnie do układu (4). Dzieląc równanie (5) obustronnie przez p^2 otrzymujemy równanie w algebrze $\mathbb{Q}[G]$

$$\eta^2 = \eta, \tag{6}$$

gdzie $\eta = \frac{\xi}{p}$. Ze znanych od ponad 100 lat strukturalnych własności algebr grupowych wiadomo, że w naszej sytuacji, ostatnie z równań ma cztery rozwiązania: $0,\ 1,\ \frac{1+g+g^2}{3},\ 1 - \frac{1+g+g^2}{3} = \frac{2-g-g^2}{3}$. To oznacza, że $p = 3$ i układ (4) ma cztery rozwiązania:

1) $a = b = c = 0$
2) $a = 3,\ b = 0,\ c = 0$
3) $a = b = c = 1$
4) $a = 2,\ b = c = -1$

Wzorując się na powyższym przykładzie można ułożyć całą serię układów równań nieliniowych, niełatwych do rozwiązania metodami elementarnymi.

Owe strukturalne własności algebr grupowych, na które powołaliśmy się przy rozwiązaniu układu (4) znane są dla znacznie ogólniejszego przypadku grup, niż tylko grupy cykliczne. Na początku dwudziestego wieku opisano rozwiązania równań postaci (6) również w przypadku grup nieabelowych tzn. takich, w których działanie nie jest przemienne. Od takich rozważań zaczął się m.in. jeden z bardzo ważnych i obszernych działów współczesnej algebry – teoria reprezentacji grup skończonych. O niej i zagadnieniach pokrewnych opowiemy przy innej okazji.