# Rozdział 1

# ALGEBRY GRUPOWE W TEORII KODÓW

Czesław Bagiński, Kamil Zabielski*

**Streszczenie** Rozwój teorii kodowania i teorii informacji jest pokłosiem realnej potrzeby usprawnienia komunikacji między urządzeniami technicznymi. Wzrost znaczenia informacji oraz rosnące zapotrzebowanie optymalizacji stosunku ilości przesyłanych informacji do zdolności korekcji i detekcji błędów jest nie do zignorowania. Odpowiedzią na te rosnące potrzeby jest algebraiczna teoria kodowania. Autorzy w pracy przedstawiają formalną konstrukcję kodów z wykorzystaniem języka teorii algebr grupowych, w szczególności z wykorzystaniem ideałów tych algebr. W pracy autorzy prezentują podstawy formalne, przedstawiają konstrukcję kodu Golay'a oraz kodu Reeda-Mullera, ostatecznie ilustrując w przykładach rachunki z wykorzystaniem systemu `GAP`.

**Słowa kluczowe:** algebry grupowe, teoria kodowania, kody, gap

## Wprowadzenie

Teoria kodowania narodziła się wraz z teorią informacji w latach 50-tych XX w. z potrzeby usprawnienia komunikacji między urządzeniami technicznymi oraz między człowiekiem a urządzeniem. Kody używane do tego celu stały się swego rodzaju językiem zrozumiałym dla komunikujących się stron. Wraz z rewolucją technologiczną oraz wyjątkowo szybkim rozwojem znaczenia informacji i jej przekazu, w odpowiedzi na gwałtownie rosnące zapotrzebowanie, sięgnięto do niezawodnego narzędzia, jakim jest matematyka. W efekcie powstała algebraiczna teoria kodowania, która z jednej strony uporządkowała dotychczasowe pomysły efektywnie działających kodów, z drugiej, dzięki abstrakcyjnym konstrukcjom, od dawna znanym w algebrze, stała się źródłem nowych kodów, których własności coraz lepiej spełniają wymagające oczekiwania. Jednym z tych wymagań, wynikającym z zawodności urządzeń przekazujących, jak również różnorodności warunków przekazu, jest potrzeba rozpoznawania błędów powstałych w przekazie i ich poprawiania przez odbiorcę, bez konieczności ponownego jej wysyłania, ponieważ bardzo często po-

* Wydział Informatyki, Politechnika Białostocka, Wiejska 45A, 15-351 Białystok, c.baginski@pb.edu.pl

DOI 10.24427/978-83-67185-18-9_1

wtórzenie przekazu nie jest po prostu możliwe. Spełnienie tych warunków wiąże się z wymuszeniem nadmiarowości przekazywanych informacji, co przy jej ogromie może oznaczać spowolnienie kodowania, jego przesyłu, procesu dekodowania i wreszcie reakcji na otrzymane wiadomości. W stopniu zadowalającym te warunki spełniają dobrze skonstruowane kody liniowe, znane od końca lat pięćdziesiątych dwudziestego wieku. Kody liniowe to w istocie konkretne podprzestrzenie przestrzeni liniowej $W = \mathbb{F}^n$, której wektory, przedstawione w standardowej bazie przestrzeni $W$, są wzajemnie jednoznacznie przyporządkowane jednostkom informacji, a ich postać pozwala na taki ich przesył między nadawcą i odbiorcą, że nawet w przypadku wystąpienia zakłóceń powodujących zniekształcenie przesyłanych informacji, odbiorca z dużym prawdopodobieństwem może precyzyjnie ją odtworzyć. Podstawowy, matematyczny opis własności kodów nie wymaga szczególnie głębokiej wiedzy matematycznej. Jest oparty na standardowym kursie algebry liniowej, kombinatoryki i rachunku prawdopodobieństwa. W końcu lat sześćdziesiątych odkryto, że niektórym z kodów liniowych można nadać bogatszą strukturę algebraiczną - ideałów algebr grupowych. Teoria algebr grupowych jest dalece zaawansowanym obszarem badań algebry abstrakcyjnej, wciąż intensywnie rozwijanym i coraz częściej dostarczającym interesujących przykładów zastosowań w teorii kodowania, zwłaszcza, że owa bogatsza struktura pozwala czasem na stworzenie szybszych algorytmów kodujących i dekodujących wiadomości.

Celem tego artykułu jest pokazanie na kilku przykładach jak można reprezentować kody w postaci ideałów algebry grupowej. Do zrozumienia materiału wystarczy podstawowy kurs algebry abstrakcyjnej, wykładany zwykle na drugim roku studiów matematycznych. W pierwszym rozdziale wprowadzimy podstawowe fakty z teorii algebr grupowych, a w drugim przedstawimy kilka wybranych kodów i przedstawimy je w języku teorii algebr. W niektórych przypadkach w obliczeniach posłużymy się systemem `GAP` - rozbudowanym pakietem do obliczeń symbolicznych stworzonych na potrzeby algebry abstrakcyjnej, zwłaszcza teorii grup. Współcześnie informatyka dostarcza całe mnóstwo systemów wspomagających obliczenia symboliczne oraz wnioskowanie matematyczne. Systemy algebry komputerowej (ang. Computer Algebra System) są powszechnie wykorzystywane jako wsparcie dowodu formalnego, poprzez ułatwienie wyszukiwania pewnych wzorców, jak również bywają podstawą dowodu. Na szczególną uwagę zasługuje właśnie `GAP` (p. GAP (2021)), ze względu na to, że jest żywo rozbudowywanym oprogramowaniem open source z zakresu obliczeniowej teorii grup i tylko nieznacznie odstaje od silnych komercyjnych programów z tego zakresu, jakimi są `CAYLEY` i `MAGMA`.

Nie wchodząc zbytnio w szczegóły techniczne, warto nadmienić, że `GAP` poza rdzennymi implementacjami standardowych obiektów algebraicznych, pozwala na proste i szerokie rozszerzanie bazowych funkcjonalności przez zastosowanie mechanizmu paczek. Na szczególną uwagę zasługują te, które są zaakceptowane; to znaczy takie, których kod źródłowy społeczność uważa za stabilny, a prezentowane wyniki za godne zaufania. Do badania kodów korekcyjnych, warto przyjrzeć się paczce

GUAVA, zaakceptowanej w lutym 2003 r. Wedderga, natomiast, jest to paczka, która okazuje się szczególnie przydatna przy badaniu półprostych algebr grupowych nad ciałami skończonymi z wykorzystaniem algorytmu rozkładu Weddeburna Broche i del Río (2007), Olteanu i del Río (2009), zaakceptowana w styczniu 2008 r.

## 1.1 Wprowadzenie do algebr grupowych

Wszystkie algebry i przestrzenie rozważane w tej pracy, są nad ciałami skończonymi. Na ogół są to ciała charakterystyki 2 lub ciała proste $\mathbb{Z}_p$, gdzie $p$ jest liczbą pierwszą. Podstawy teorii ciał skończonych można znaleźć np. w Kobliz (2006). Tu przytoczymy jedynie następujące twierdzenie.

**Twierdzenie 1.1.** Niech $p$ będzie liczbą pierwszą i $\mathbb{F}_q$ niech będzie ciałem o $q = p^k$ ($k \in \mathbb{N}$) elementach. Wówczas:

(a) Dla dowolnego $\alpha \in \mathbb{F}$ $f_q(\alpha) = 0$, gdzie $f_q(x) = x^q - x \in \mathbb{F}_q$, innymi słowy

$$f_q(x) = x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha).$$

(b) Wielomian $f_q(x)$ rozkłada się nad ciałem $\mathbb{F}_p = \mathbb{Z}_p$ na iloczyn wszystkich wielomianów nierozkładalnych nad $\mathbb{F}_p$, których stopnie są dzielnikami liczby $k$.

(c) Multyplikatywna grupa ciała $\mathbb{F}_q$ jest cykliczna, tzn. istnieje element $\omega \in \mathbb{F}_q$, taki że

$$\mathbb{F}_q^* = \mathbb{F}_q = \left\{ \omega, \omega^2, \omega^3, \ldots, \omega^{q-1} = 1 \right\}.$$

Niech $G$ będzie grupą skończoną z operacją o multyplikatywnym zapisie i $\mathbb{F}$ ciałem skończonym. Symbolem $\mathbb{F}[G]$ oznaczymy zbiór wszystkich formalnych kombinacji liniowych postaci:

$$\sum_{g \in G} a_g g, \quad a_g \in \mathbb{F}. \tag{1.1.1}$$

Zakładamy przy tym, że jeśli $\alpha = \sum_{g \in G} a_g g$ oraz $\beta = \sum_{g \in G} b_g g$, to $\alpha = \beta$ wtedy i tylko wtedy, gdy zachodzą równości $a_g = b_g$ dla wszystkich $g \in G$. W zbiorze $\mathbb{F}[G]$ definiujemy dodawanie elementów przyjmując, że dla określonych wyżej $\alpha$ i $\beta$ dane jest:

$$\alpha + \beta = \sum_{g \in G} a_g g + \sum_{g \in G} b_g g \stackrel{\text{def.}}{=} \sum_{g \in G} (a_g + b_g) g. \tag{1.1.2}$$

Wprowadzamy również operację mnożenia elementów zbioru $\mathbb{F}[G]$ przez elementy z ciała $\mathbb{F}$; mianowicie, jeśli $a \in \mathbb{F}$ i $\alpha \in \mathbb{F}[G]$ to

$$a\alpha = a \cdot \sum_{g \in G} a_g g \stackrel{\text{def.}}{=} \sum_{g \in G} (a a_g) g = \alpha a. \tag{1.1.3}$$

.

Te dwie operacje (1.1.2) (1.1.3) wprowadzają w zbiorze $\mathbb{F}[G]$ strukturę przestrzeni liniowej nad ciałem $\mathbb{F}$. Standardową bazą tej przestrzeni jest zbiór elementów grupy $G$. Do struktury przestrzeni liniowej dodajemy jeszcze strukturę pierścienia, wprowadzając mnożenie elementów tego zbioru (które, jak łatwo pokazać, jest rozdzielne względem dodawania (1.1.2) zdefiniowanego wyżej):

$$\alpha \cdot \beta = \left( \sum_{g \in G} a_g g \right) \cdot \left( \sum_{g \in G} b_g g \right) \stackrel{\text{def.}}{=} \sum_{g \in G} \left( \sum_{xy=g} a_x b_y \right) g. \tag{1.1.4}$$

Wszystkie te działania wprowadzają w $\mathbb{F}[G]$ strukturę algebry, którą nazywamy algebrą grupową grupy $G$ nad ciałem $\mathbb{F}$. Element neutralny mnożenia w ciele $\mathbb{F}$, czyli po prostu jedynka tego ciała, i element neutralny grupy $G$ zwykle oznacza się symbolem 1. Symbol ten ma, zatem, dwa znaczenia. W algebrze $\mathbb{F}[G]$ rozumiany jest jako skalar; w grupie jako element standardowej bazy tej algebry. Jeśli jednak przyjmiemy utożsamienie jedynki z ciała z jedynką w grupie, nie będzie to prowadzić do nieporozumień.

Struktura algebry grupowej jest silnie zależna od tego, czy $\operatorname{char}\mathbb{F}$ i $|G|$ są względnie pierwsze. Zajmiemy się najpierw przypadkiem, gdy $\operatorname{char}\mathbb{F} > 0$ nie dzieli rzędu grupy $G$.

**Twierdzenie 1.2.** Niech $\mathbb{F}$ będzie ciałem charakterystyki $p > 0$ i $G$ grupą, której rząd nie jest podzielny przez $p$. Wówczas istnieją liczby naturalne $n_1, n_2, \ldots, n_k$ oraz ciała $\mathbb{F}_1$, $\mathbb{F}_2$, ..., $\mathbb{F}_k$, będące rozszerzeniami ciała $\mathbb{F}$, takie że

$$\mathbb{F}[G] \cong M_{n_1}(\mathbb{F}_1) \oplus M_{n_2}(\mathbb{F}_2) \oplus \ldots \oplus M_{n_k}(\mathbb{F}_k), \tag{1.1.5}$$

gdzie $M_{n_i}(\mathbb{F}_i)$ jest algebrą macierzy kwadratowych nad ciałem $\mathbb{F}_i$, $i = 1, 2, \ldots, k$. Ponadto

$$|G| = \dim_{\mathbb{F}} \mathbb{F}[G] = n_1^2 \dim_{\mathbb{F}} \mathbb{F}_1 + n_2^2 \dim_{\mathbb{F}} \mathbb{F}_2 + \cdots + n_k^2 \dim_{\mathbb{F}} \mathbb{F}_k.$$

Do uzyskania rozkładu opisanego powyższym twierdzeniem należy wyznaczyć układ centralnych prymitywnych idempotentów tej algebry. Wcześniej, jeszcze jedno pojęcie; powiemy, że element $a$ algebry $\mathscr{A}$ anihiluje podzbiór $B$ tej algebry, jeśli dla dowolnego $b \in B$ zachodzi równość $ab = ba = 0$. Anihilatorem podzbioru $B$ nazywamy zbiór wszystkich elementów algebry anihilujących wszystkie elementy zbioru $B$:

$$Ann_{\mathscr{A}}(B) = \{a \in \mathscr{A} : \forall_{(b \in B)}\, ab = ba = 0\}$$

.

**Definicja 1.1.** Centralnym prymitywnym idempotentem algebry $A$ nazywamy element **e**, taki, że:

(i) $\mathbf{e}^2 = \mathbf{e}$;
(ii) $\mathbf{e}\alpha = \alpha\mathbf{e}$, dla dowolnego $\alpha \in A$;
(iii) nie istnieją $\mathbf{e}_1,\ \mathbf{e}_2$ spełniające warunki (i) i (ii), takie, że $\mathbf{e}_1 + \mathbf{e}_2 = \mathbf{e}$.

Centralność zapewnia (ii), a prymitywność (iii).

**Twierdzenie 1.3.** Niech $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_k\}$ będzie zbiorem wszystkich centralnych prymitywnych idempotentów algebry $\mathbb{F}[G]$. Wówczas:

(i) $\mathbf{e}_1 + \mathbf{e}_2 + \cdots + \mathbf{e}_k = 1$.
(ii) Każda składowa sumy prostej (1.1.5) ma postać $\mathbf{e}_i\mathbb{F}[G]$, tzn. jest ideałem głównym generowanym przez $\mathbf{e}_i$. Ponadto, każda taka składowa jest ideałem minimalnym.
(iii) Każdy ideał algebry $\mathbb{F}[G]$ jest sumą prostą ideałów minimalnych; dokładniej, jeśli $I$ jest ideałem, to $I = \mathbf{e}\mathbb{F}[G]$, gdzie $\mathbf{e} = \mathbf{e}_{i_1} + \mathbf{e}_{i_2} + \cdots + \mathbf{e}_{i_m}$, $1 \leqslant i_1 < i_2 < \ldots < i_m \leqslant k$, w szczególności liczba wszystkich ideałów jest równa $2^k$. Ponadto, jeśli $I = \mathbf{e}\mathbb{F}[G]$ jest ideałem, to $\mathrm{Ann}_{\mathbb{F}[G]}(I) = (1-\mathbf{e})\mathbb{F}[G]$.
(iv) Jeżeli każdy element grupy $G$ ma rząd dzielący $|\mathbb{F}| - 1$, to wszystkie ciała $\mathbb{F}_i$ ze sformułowania tw. 1.1.5 są izomorficzne z $\mathbb{F}$. Ponadto, liczba $k$ jest równa liczbie klas elementów sprzężonych grupy $G$.
(v) Jeśli $G$ jest grupą abelową, to $\mathbb{F}[G]$ jest sumą prostą ciał $\mathbb{F}_i$, a przy założeniach podpunktu (iv):

$$\mathbb{F}[G] \cong \underbrace{\mathbb{F} \oplus \ldots \oplus \mathbb{F}}_{|G|}.$$

Przykład 1.1. Niech $G = \langle g : g^3 = e\rangle = \{g, g^2, g^3 = 1\}$ będzie grupą cykliczną rzędu 3. Wówczas:

$$\mathbb{F}[G] = \{a + bg + cg^2 : a, b, c \in \mathbb{F}\}$$

jest przestrzenią trójwymiarową nad $\mathbb{F}$ z mnożeniem określonym wzorem:

$$\begin{aligned}&(ae + bg + cg^2)(a'e + b'g + c'g^2) = \\ &= (aa' + bc' + cb')e + (ab' + ba' + cc')g + (ac' + bb' + ca')g^2.\end{aligned}$$

Wewnętrzna struktura algebry, oprócz tego, że w oczywisty sposób zależy od $G$, jest zależna od ciała $\mathbb{F}$. Dla rozważanej grupy rzędu 3, jeżeli ciało $\mathbb{F}$ ma charakterystykę różną od 3, ale nie ma w niej pierwiastka trzeciego stopnia z 1, różnego od 1, to dla elementów:

$$\mathbf{e} = \frac{1}{3} + \frac{1}{3}g + \frac{1}{3}g^2 = \frac{1+g+g^2}{3} \ \text{ i } \ \mathbf{f} = 1 - \mathbf{e}$$

spełnione są warunki:

$$\mathbf{e}^2 = \mathbf{e},\ \ \mathbf{f}^2 = \mathbf{f},\ \ \mathbf{ef} = \mathbf{fe} = 0,\ \ \mathbf{e} + \mathbf{f} = 1.$$

Jeśli teraz $\alpha = a + bg + cg^2$ jest dowolnym elementem algebry $\mathbb{F}[G]$, to można go zapisać w postaci:

$$\alpha = \alpha \cdot 1 = \alpha(\mathbf{e} + \mathbf{f}) = \alpha\mathbf{e} + \alpha\mathbf{f} = \alpha_1 + \alpha_2$$

gdzie

$$\alpha_1 = (a+b+c)\mathbf{e}, \;\; \alpha_2 = ((a-c)+(b-c)g)\mathbf{f}$$

i oczywiście $\alpha_1 \cdot \alpha_2 = 0$. To pozwala patrzeć na $\mathbb{F}[G]$ jak na zbiór par postaci $(\alpha_1, \alpha_2)$, przy czym elementy stojące na pierwszym miejscu można traktować jak elementy ciała $\mathbb{F}$, a elementy stojące na drugim, jak elementy ciała $\mathbb{F}(\omega)$, gdzie $\omega$ jest pierwiastkiem trzeciego stopnia z 1. Algebra rozkłada się zatem na sumę prostą dwóch ciał:

$$\mathbb{F}[G] \cong \mathbb{F} \oplus \mathbb{F}(\omega).$$

Zauważmy, że ta algebra ma dokładnie dwa ideały właściwe. Jeśli $\mathbb{F} = GF(p)$ jest ciałem $p$-elementowym, takim, że $3 \nmid p-1$, to $\dim_{\mathbb{F}}\mathbb{F}(\omega) = 2$.

Niech teraz $\mathbb{F}$ będzie ciałem zawierającym element $\omega \neq 1$ taki, że $\omega^3 = 1$. Niech ponadto:

$$\mathbf{e}_1 = \frac{1+g+g^2}{3}, \;\; \mathbf{e}_2 = \frac{1+\omega g+\omega^2 g^2}{3}, \;\; \mathbf{e}_3 = \frac{1+\omega^2 g+\omega g^2}{3}.$$

Wówczas łatwo sprawdzić, że:

(a) $1 + \omega + \omega^2 = 0$,
(b) $\mathbf{e}_1$, $\mathbf{e}_2$ i $\mathbf{e}_3$ są liniowo niezależne i spełniają zależności:

$$\mathbf{e}_i^2 = \mathbf{e}_i, \;\; \mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3 = 1, \;\; e_i e_j = 0 \;\text{ dla } i \neq j.$$

(c) $\mathbf{e}_i\mathbb{F}[G] \cong \mathbb{F}$ dla $i = 1,2,3$ .

Rozważmy teraz przypadek bardziej ogólny.

Przykład 1.2. Niech $G = \langle g : g^r = e\rangle = \{g, g^2, \ldots, g^{r-1}, g^r = 1\}$ będzie grupą cykliczną rzędu $r$ i $\mathbb{F}$ ciałem, którego charakterystyka nie dzieli rzędu grupy. Wówczas:

$$\mathbb{F}[G] = \{a_0 + a_1 g + a_2 g^2 + \ldots a_{r-1} g^{r-1} : \; a_0, a_1, a_2, \ldots, a_{r-1} \in \mathbb{F}\}$$

z naturalnym dodawaniem tych wyrażeń i mnożeniem przez elementy z ciała $\mathbb{F}$ jest przestrzenią $r$-wymiarową nad $\mathbb{F}$. Z algebraicznego punktu widzenia ciekawszą jest struktura pierścienia (a zatem i algebry), którą uzyskujemy definiując w $\mathbb{F}[G]$ operację mnożenia. Mówiąc poglądowo, jest ono takie, jak mnożenie wielomianów zmiennej $g$, z uwzględnieniem równości $g^r = 1$, co pozwala na redukcję wykładników dla $g$ do zbioru reszt modulo $r$, $\mathbb{Z}_r$.

Mnożenie, zgodnie z definicją, jest więc określone wzorem

$$(a_0e + a_1g + a_2g^2 + \cdots + a_{r-1}g^{r-1})(b_0e + b_1g + b_2g^2 + \cdots + b_{r-1}g^{r-1}) =$$
$$= \left(\sum_{i+j\equiv 0} a_ib_j\right) + \left(\sum_{i+j\equiv 1} a_ib_j\right) g + \left(\sum_{i+j\equiv 2} a_ib_j\right) g^2 + \cdots + \left(\sum_{i+j\equiv -1} a_ib_j\right) g^{r-1} =$$
$$= \sum_{k=0}^{r-1} \left(\sum_{i+j\equiv k} \right) g^k,$$

gdzie przystawanie pod znakiem sumy, jest brane modulo $r$. Struktura ideałów tego pierścienia jest zależna od charakterystyki $p$ ciała $\mathbb{F}$ i zależności między $p$ i $r$. Przypadek $p = r$ jest algebraicznie bardziej skomplikowany. Zajmiemy się zatem przypadkiem $p \neq r$. Jeśli ciało $\mathbb{F}$ nie zawiera pierwiastków stopnia $r$ z jedynki, to stopień rozszerzenia ciała $|\mathbb{F}(\omega) : \mathbb{F}|$ jest dzielnikiem liczby $r-1$. Załóżmy najpierw, że ten stopień jest równy $r-1$, wówczas dla elementów:

$$\mathbf{e} = \frac{1 + g + g^2 + \cdots + g^{r-1}}{r}, \quad \mathbf{f} = 1 - \mathbf{e}, \tag{1.1.6}$$

spełnione są dwa warunki:

$$\mathbf{e}^2 = \mathbf{e}, \quad \mathbf{f}^2 = \mathbf{f}, \quad \mathbf{ef} = \mathbf{fe} = 0, \quad \mathbf{e} + \mathbf{f} = 1. \tag{1.1.7}$$

Ideały główne algebry, generowane przez te elementy, są jedynymi niezerowymi ideałami właściwymi, a ponadto

$$\mathbb{F}[G] = \mathbf{e}\mathbb{F}[G] \oplus \mathbf{f}\mathbb{F}[G],$$

przy czym ideał $\mathbf{e}\mathbb{F}[G]$ jest izomorficzny z ciałem $\mathbb{F}$, natomiast ideał $\mathbf{f}\mathbb{F}[G]$ jest izomorficzny z ciałem $\mathbb{F}(\omega)$, gdzie $\omega$ jest pierwiastkiem pierwotnym stopnia $r$ nad ciałem $\mathbb{F}$.

Załóżmy teraz drugi skrajny przypadek, innymi słowy załóżmy, że ciało $\mathbb{F}$ zawiera pierwiastek stopnia $r$ z 1, czyli $|\mathbb{F}(\omega) : \mathbb{F}| = 1$. Jeśli ciało jest skończone, to ma to miejsce wtedy i tylko wtedy, gdy $r$ jest dzielnikiem rzędu multyplikatywnej grupy ciała $\mathbb{F}$, tzn. gdy $r \mid (|\mathbb{F}| - 1)$. Oznaczmy, jak wyżej, ten pierwiastek przez $\omega$. Niech dalej:

$$\begin{aligned}
\mathbf{e}_0 &= \tfrac{1+g+g^2+\cdots+g^{r-1}}{r}, \\
\mathbf{e}_1 &= \tfrac{1+\omega g+\omega^2 g^2+\cdots+\omega^{r-1} g^{r-1}}{r}, \\
\mathbf{e}_2 &= \tfrac{1+\omega^2 g+\omega^4 g^2+\cdots+\omega^{2(r-1)} g^{r-1}}{r}, \\
\cdots &= \cdots\cdots\cdots\cdots\cdots\cdots, \\
\mathbf{e}_{r-1} &= \tfrac{1+\omega^{r-1} g+\omega^{2(r-1)} g^2+\cdots+\omega^{(r-1)^2} g^{r-1}}{r}.
\end{aligned} \tag{1.1.8}$$

Wówczas

$$\mathbf{e}_0+\mathbf{e}_1+\mathbf{e}_2+\cdots+\mathbf{e}_{r-1}=1,\ \mathbf{e}_i\mathbf{e}_j=\mathbf{e}_j\mathbf{e}_i=0\ \text{ dla }\ i\neq j,\ \mathbf{e}_i^2=\mathbf{e}_i,\ 0\leqslant i,j\leqslant r-1. \tag{1.1.9}$$

Wynika stąd, że

$$\mathbb{F}[G]=\mathbf{e}_0\mathbb{F}[G]\oplus\mathbf{e}_1\mathbb{F}[G]\oplus\ldots\oplus\mathbf{e}_{r-1}\mathbb{F}[G],$$

przy czym wszystkie ideały $\mathbf{e}_i\mathbb{F}[G]$ są jednowymiarowymi podprzestrzeniami przestrzeni $\mathbb{F}[G]$, które jako algebry są izomorficzne z ciałem $\mathbb{F}$.

Przypadek, gdy $1<|\mathbb{F}(\omega):\mathbb{F}|=k<r$ wymaga delikatniejszej analizy algebraicznej.

Niech $k=r-1$. Nie wdając się w szczegóły, rozważmy grupę Galois rozszerzenia $Gal(\mathbb{F}(\omega)/\mathbb{F})$. Jej rząd jest równy stopniowi rozszerzenia $|\mathbb{F}(\omega):\mathbb{F}|$. Działanie tej grupy na $\mathbb{F}(\omega)$ można w naturalny sposób rozszerzyć na działanie na algebrze $\mathbb{F}(\omega)[G]$. Bezpośrednio sprawdza się, że automorfizmy zachowują zbiór $\{\mathbf{e}_1,\ \mathbf{e}_2,\ \ldots,\ \mathbf{e}_{r-1}\}$. Bez zmniejszenia ogólności można przyjąć, że orbitami tego działania są zbiory $\{\mathbf{e}_1,\mathbf{e}_2,\ldots,\mathbf{e}_k\},\{\mathbf{e}_{k+1},\mathbf{e}_{k+2},\ldots,\mathbf{e}_{2k}\},\ldots,\{\mathbf{e}_{(l-1)k+1},\mathbf{e}_{(l-1)k+2},\ldots,\mathbf{e}_{lk}\}$. Niech

$$\begin{aligned}\mathbf{f}_1&=\mathbf{e}_1+\mathbf{e}_2+\cdots+\mathbf{e}_k,\\ \mathbf{f}_2&=\mathbf{e}_{k+1}+\mathbf{e}_{k+2}+\cdots+\mathbf{e}_{2k},\\ \cdots&=\cdots,\\ \mathbf{f}_l&=\mathbf{e}_{(l-1)k+1}+\mathbf{e}_{(l-1)k+2}+\cdots+\mathbf{e}_{lk}.\end{aligned}$$

Wówczas dla każdego $i$, $1\leqslant i\leqslant l$, $\mathbf{f}_i\in\mathbb{F}[G]$ oraz

$$\mathbf{f}_i^2=\mathbf{f}_i,\ \mathbf{f}_i\mathbf{f}_j=0\ \text{ dla }\ i\neq j,\ \sum_{i=1}^{l}\mathbf{f}_i=1-\mathbf{e}_0. \tag{1.1.10}$$

Ponadto dla dowolnego $i$, $\mathbf{f}_i\mathbb{F}[G]\cong\mathbb{F}(\omega)$. Zatem

$$\mathbb{F}[G]\cong\mathbb{F}\oplus\underbrace{\mathbb{F}(\omega)\oplus\cdots\oplus\mathbb{F}(\omega)}_{l}. \tag{1.1.11}$$

Dla ilustracji wcześniejszych, ogólnych rozważań rozpatrzmy przypadek, gdzie $r=5$ i $\mathbb{F}=\mathbb{Z}_p$, gdzie $p\in\{11,13,19\}$. Niech najpierw $\mathbb{F}=\mathbb{Z}_{11}$ i $\omega=3$. Wtedy

$$\omega^1=3,\ \omega^2=9,\ \omega^3=5,\ \omega^4=4,\omega^5=1,$$

a wobec tego, że $r^{-1}=5^{-1}=9$:

$$\begin{aligned}
\mathbf{e}_0 &= \tfrac{1+g+g^2+g^3+g^4}{5} &&= 9(1+g+g^2+g^3+g^4) &&= 9+9g+9g^2+9g^3+9g^4,\\
\mathbf{e}_1 &= \tfrac{1+3g+9g^2+5g^3+4g^4}{5} &&= 9(1+3g+9g^2+5g^3+4g^4) &&= 9+5g+4g^2+g^3+3g^4,\\
\mathbf{e}_2 &= \tfrac{1+9g+4g^2+3g^3+5g^4}{5} &&= 9(1+9g+4g^2+3g^3+5g^4) &&= 9+4g+3g^2+5g^3+g^4,\\
\mathbf{e}_3 &= \tfrac{1+5g+3g^2+4g^3+9g^4}{5} &&= 9(1+5g+3g^2+4g^3+9g^4) &&= 9+g+5g^2+3g^3+4g^4,\\
\mathbf{e}_4 &= \tfrac{1+4g+5g^2+9g^3+3g^4}{5} &&= 9(1+4g+5g^2+9g^3+3g^4) &&= 9+3g+g^2+4g^3+5g^4,
\end{aligned}$$

co oznacza, że dla $i = 0,1,2,3,4$ mamy $\mathbf{e}_i\mathbb{F}[G] \cong \mathbb{F}$, czyli $\mathbb{F}[G] \cong \mathbb{F}\oplus\mathbb{F}\oplus\mathbb{F}\oplus\mathbb{F}\oplus\mathbb{F}$.

Niech teraz $\mathbb{F} = \mathbb{Z}_{13}$. Najmniejszym ciałem charakterystyki 13 zawierającym pierwiastek stopnia 5 z 1 jest ciało o $13^4$ elementach ($13^4 \equiv 1 \pmod 5$ i dla $k < 4$, $13^k \not\equiv 1 \pmod 5$), więc w algebrze $\mathbb{F}[G]$ mamy sytuację opisaną wzorami (1.1.6) i (1.1.7). Zatem:

$$\mathbb{F}[G] \cong \mathbb{F}\oplus\mathbb{F}(\omega).$$

Rozważmy na koniec przypadek $\mathbb{F} = \mathbb{Z}_{19}$. Ponieważ $19^2 \equiv 1 \pmod 5$, więc $|\mathbb{F}(\omega) : \mathbb{F}| = 2$, a jedyny nietożsamościowy automorfizm rozszerzenia $\mathbb{F}(\omega)/\mathbb{F}$ jest indukowany przez przyporządkowanie $\omega \to \omega^{-1}$. Orbitami działania na elementach $\mathbf{e}_i$ (patrz (1.1.8) są $\{\mathbf{e}_1,\mathbf{e}_4\}$ oraz $\{\mathbf{e}_2,\mathbf{e}_3\}$. Stąd

$$\begin{aligned}
\mathbf{f}_1 &= \mathbf{e}_1+\mathbf{e}_4 = \tfrac{2+(\omega+\omega^4)(g+g^4)+(\omega^2+\omega^3)(g^2+g^3)}{5},\\
\mathbf{f}_2 &= \mathbf{e}_2+\mathbf{e}_3 = \tfrac{2+(\omega^2+\omega^3)(g+g^4)+(\omega+\omega^4)(g^2+g^3)}{5}.
\end{aligned}$$

Jednakże $1+\omega+\omega^2+\omega^3+\omega^4 = 0$, zatem dla $t = \omega+\omega^4$ mamy $t^2+t-1 = 0$, a ponieważ nad ciałem $\mathbb{Z}_{19}$ mamy $t^2+t-1 = (t-4)(t+5)$, możemy przyjąć, że $t = \omega+\omega^4 = 4$ i w konsekwencji $\omega^2+\omega^3 = t^2-2 = 14$. Ostatecznie zatem

$$\begin{aligned}
\mathbf{f}_1 &= \mathbf{e}_1+\mathbf{e}_4 = \tfrac{2+4(g+g^4)+14(g^2+g^3)}{5} = 8-3g-g^2-g^3-3g^4,\\
\mathbf{f}_2 &= \mathbf{e}_2+\mathbf{e}_3 = \tfrac{2+14(g+g^4)+4(g^2+g^3)}{5} = 8-g-3g^2-3g^3-g^4,
\end{aligned}$$

$\mathbf{f}_1\mathbb{F}[G] \cong \mathbf{f}_2\mathbb{F}[G] \cong \mathbb{F}(\omega)$ i $\mathbb{F}[G] \cong \mathbb{F}\oplus\mathbb{F}(\omega)\oplus\mathbb{F}(\omega)$.

Bazując na powyższym przykładzie można analogicznie rozważyć przypadek, gdy $G$ jest grupą cykliczną rzędu będącego potęgą liczby pierwszej $r$. W następstwie, korzystając z zasadniczego twierdzenia o strukturze dowolnej grupy abelowej oraz tego, że

$$\mathbb{F}[G\times H] = \mathbb{F}[G]\otimes_{\mathbb{F}}\mathbb{F}[H],$$

można uzyskać strukturalny rozkład algebry $\mathbb{F}[G]$ na sumę prostą ciał, będących rozszerzeniami ciała $\mathbb{F}$ o stosowne pierwiastki z 1.

Przykład 1.3. Na koniec tej części zademonstrujemy na przykładzie wynik obliczeń wykonanych w GAP-ie dla grupy cyklicznej rzędu 17 i ciała 2-elementowego.

```
gap> G := CyclicGroup(17);
<pc group of size 17 with 1 generators>
gap> F := GF(2);
gap> FG := GroupRing(F, G);
<algebra-with-one over GF(2), with 1 generators>
gap> FGe :=
   ↪ PrimitiveCentralIdempotentsByCharacterTable(FG)
   ↪ ;;
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f1^2+(
   ↪ Z(2)^0)*f1^3+(Z(2)^0)*f1^4+(Z(2)^0)*f1^5+(Z(2)
   ↪ ^0)*f1^6+(Z(2)^0)*f1^7+(Z(2)^0)*f1^8+(Z(2)^0)*f1
   ↪ ^9+(Z(2)^0)*f1^10+(Z(2)^0)*f1^11+(Z(2)^0)*f1
   ↪ ^12+(Z(2)^0)*f1^13+(Z(2)^0)*f1^14+(Z(2)^0)*f1
   ↪ ^15+(Z(2)^0)*f1^16
(Z(2)^0)*f1+(Z(2)^0)*f1^2+(Z(2)^0)*f1^4+(Z(2)^0)*f1
   ↪ ^8+(Z(2)^0)*f1^9+(Z(2)^0)*f1^13+(Z(2)^0)*f1^15+(
   ↪ Z(2)^0)*f1^16
(Z(2)^0)*f1^3+(Z(2)^0)*f1^5+(Z(2)^0)*f1^6+(Z(2)^0)*f1
   ↪ ^7+(Z(2)^0)*f1^10+(Z(2)^0)*f1^11+(Z(2)^0)*f1
   ↪ ^12+(Z(2)^0)*f1^14
```

W przetłumaczeniu na bardziej przejrzystą postać idempotenty wyznaczone przez GAP są następujące:

$$\begin{aligned}
\mathbf{e}_0 &= 1+x+x^2+x^3+\ldots+x^{16},\\
\mathbf{e}_1 &= x+x^2+x^4+x^8+x^9+x^{13}+x^{15}+x^{16},\\
\mathbf{e}_2 &= x^3+x^5+x^6+x^7+x^{10}+x^{11}+x^{12}+x^{14},
\end{aligned}$$

Podany rozkład algebry jest szczególnym przypadkiem sytuacji ogólnej.

Przykład 1.4. Niech $G$ będzie grupą dihedralną rzędu $2r$, gdzie $r$ jest liczbą pierwszą:

$$G = \langle x,y |\ x^r = 1,\ y^2 = 1,\ yxy = x^{-1}\rangle. \tag{1.1.12}$$

Załóżmy, że $p \nmid 2r$, gdzie $p = \mathrm{char}\mathbb{F}$. Niech także $|\mathbb{F}(\omega) : \mathbb{F}| = k$. Niech najpierw $k = r-1$. Wówczas idempotenty algebry $\mathbb{F}[\langle x\rangle]$ opisane wzorami (1.1.6) są przemienne z $y$ i tym samym algebra $\mathbb{F}[G]$ rozpada się na sumę prostą

$$\mathbb{F}[G] = \mathbf{e}_0\mathbb{F}[G] \oplus \mathbf{e}_1\mathbb{F}[G].$$

Pierwsza składowa ma wymiar dwa, bo jest rozpięta nad $\mathbb{F}$ na zbiorze $\{\mathbf{e}_0,\ \mathbf{e}_0 y\}$ i rozpada się na sumę prostą jednowymiarowych składowych.

$$\mathbf{e}_0\mathbb{F}[G] = \mathbf{f}_{00}\mathbb{F}[G] \oplus \mathbf{f}_{01}\mathbb{F}[G],$$

gdzie $\mathbf{f}_{00} = \mathbf{e}_0 \cdot \frac{1+y}{2}$ i $\mathbf{f}_{01} = \mathbf{e}_0 \cdot \frac{1-y}{2}$.

Druga składowa zawiera $\frac{r-1}{2}$-wymiarowe centrum rozpięte na zbiorze $\{\mathbf{e}_1 \cdot \frac{x^i+x^{-i}}{2} : i = 1,2,\ldots,\frac{r-1}{2}\}$ i można dowieść, że jest ono izomorficzne z ciałem $\mathbb{F}(\omega+\omega^{-1})$, którego stopień rozszerzenia nad $\mathbb{F}$ jest równy $\frac{r-1}{2}$. Z tego faktu, na podstawie twierdzenia 1.2, wynika, że

$$\mathbf{e}_1\mathbb{F}[G] \cong M_2\left(\mathbb{F}\left(\omega+\omega^{-1}\right)\right).$$

Załóżmy teraz, że $k = 1$. Wówczas idempotenty zdefiniowane wzorami (1.1.8) nie są centralnymi idempotentami w $\mathbb{F}[G]$, ale są nimi elementy:

$$\mathbf{f}_1 = \mathbf{e}_1 + \mathbf{e}_{r-1},\ \mathbf{f}_2 = \mathbf{e}_2 + \mathbf{e}_{r-2},\ldots,\ \mathbf{f}_{(r-1)/2} = \mathbf{e}_{(r-1)/2} + \mathbf{e}_{(r+1)/2}.$$

Ponadto, każda z podalgebr $\mathbf{f}_i\mathbb{F}[G]$ jest izomorficzna z algebrą macierzy $M_2(\mathbb{F})$. Mamy zatem:

$$\mathbb{F}[G] \cong \mathbb{F} \oplus \mathbb{F} \oplus \underbrace{M_2(\mathbb{F}) \oplus \ldots \oplus M_2(\mathbb{F})}_{(r-1)/2}.$$

Przykład 1.5. Niech $G = A_4$ będzie grupą permutacji parzystych stopnia 4. Można ją opisać w następujący sposób:

$$G = \langle x_1, x_2, y |\ x_1^2 = x_2^2 = 1,\ x_1x_2 = x_2x_1,\ y^3 = 1,\ yx_1y^{-1} = x_2,\ yx_2y^{-1} = x_1x_2\rangle.$$

Załóżmy najpierw, że ciało $\mathbb{F}$ zawiera pierwiastek pierwotny $\omega$ trzeciego stopnia z 1. Wtedy elementy:

$$\begin{aligned}
\mathbf{e}_0 &= \tfrac{(1+x_1+x_2+x_1x_2)(1+y+y^2)}{12},\\
\mathbf{e}_1 &= \tfrac{(1+x_1+x_2+x_1x_2)(1+\omega y+\omega^2y^2)}{12},\\
\mathbf{e}_2 &= \tfrac{(1+x_1+x_2+x_1x_2)(1+\omega^2 y+\omega y^2)}{12},
\end{aligned}$$

wyznaczają trzy jednowymiarowe składowe z rozkładu $\mathbb{F}[G]$, a zatem składowe izomorficzne z ciałem $\mathbb{F}$. Grupa $A_4$ ma dokładnie 4 klasy elementów sprzężonych, zatem oprócz wymienionych jest jeszcze jedna składowa, której wymiar na $\mathbb{F}$ wynosi 9. Na podstawie twierdzenia 1.2, jest to zatem składowa izomorficzna z $M_3(\mathbb{F})$. Idempotent, który tę składową generuje, może być wyznaczony ze wzoru

$$\mathbf{f} = 1 - (\mathbf{e}_1 + \mathbf{e}_2 + \mathbf{e}_3).$$

Jeżeli ciało $\mathbb{F}$ nie zawiera pierwiastka trzeciego stopnia z 1, to algebra $\mathbb{F}[G]$ rozkłada się na sumę trzech składowych, które są wyznaczone przez idempotenty:

$$\mathbf{e}_0, \mathbf{e}_1 + \mathbf{e}_2 = \frac{(1+x_1+x_2+x_1x_2)\left(2-y-y^2\right)}{12}, \mathbf{f}.$$

Przykład 1.6. Na koniec zilustrujemy przypadek, gdy char$\mathbb{F}=2$ i $G$ jest grupą nieparzystego rzędu. Najmniejszą nieabelową grupą rzędu nieparzystego jest grupa rzędu 21 postaci:

$$G=\langle x,y|\ x^7=1,\ y^3=1,\ y^{-1}xy=x^2\rangle. \tag{1.1.13}$$

Załóżmy najpierw, że ciało $\mathbb{F}$ zawiera pierwiastki z jedynki stopni 3 i 7. Najmniejszym takim ciałem jest $GF(2^6)$, którego jedynymi podciałami są $\mathbb{Z}_2$, $GF(2^2)$ i $GF(2^3)$. Algebra grupowa $\mathbb{F}[G]$ rozkłada się na sumę prostą pięciu ideałów minimalnych, z czego trzy są izomorficzne z ciałem $\mathbb{F}$. Ponieważ suma wymiarów składowych jest równa 21, a pozostałe składowe nie są przemienne, więc stanowią sumę dwóch egzemplarzy algebry $M_3(\mathbb{F})$. Można sprawdzić, że idempotentami wyznaczającymi te składowe są:

$$\begin{aligned}
\mathbf{e}_1 &= (1+y+y^2)(1+x+x^2+x^3+x^4+x^5+x^6),\\
\mathbf{e}_2 &= (1+\omega y+\omega^2 y^2)(1+x+x^2+x^3+x^4+x^5+x^6),\\
\mathbf{e}_3 &= (1+\omega^2 y+\omega y^2)(1+x+x^2+x^3+x^4+x^5+x^6),\\
\mathbf{e}_4 &= 1+x+x^2+x^4,\\
\mathbf{e}_5 &= 1+x^3+x^5+x^6,
\end{aligned}$$

gdzie $\omega$ jest pierwiastkiem trzeciego stopnia z 1. Zauważmy dalej, że elementy $\mathbf{e}_1$, $\mathbf{e}_4$ i $\mathbf{e}_5$ niezależnie od tego, jakim ciałem jest $\mathbb{F}$, są idempotentami algebry $\mathbb{F}[G]$. To oznacza, że oprócz sytuacji opisanej wyżej mamy taką, gdy ciało $\mathbb{F}$ nie zawiera pierwiastka trzeciego stopnia z 1 i wtedy idempotenty

$$\mathbf{e}_1, \mathbf{e}_2+\mathbf{e}_3,\ \mathbf{e}_4,\ \mathbf{e}_5$$

wyznaczają cztery składowe sumy prostej, którymi są kolejno $\mathbb{F}$, $\mathbb{F}(\omega)$, a dwa ostatnie są izomorficzne z $M_3(\mathbb{F})$. Potwierdzają to rachunki wykonane w GAP.

```
gap> G := OneSmallGroup( 21, IsAbelian, false );;;
gap> F := GF(2);;
gap> FG := GroupRing(F, G);;
gap> FGe :=
   ↪ PrimitiveCentralIdempotentsByCharacterTable(FG);
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f1+(Z(2)^0)*f2+(Z
   ↪ (2)^0)*f1^2+(Z(2)^0)*f1*f2+(Z(2)^0)*f2^2+(Z(2)
   ↪ ^0)*f1^2*f2+(Z(2)^0)*f1*f2^2+(Z(2)^0)*f2^3+(Z(2)
   ↪ ^0)*f1^2*f2^2+(Z(2)^0)*f1*f2^3+(Z(2)^0)*f2^4+(Z
   ↪ (2)^0)*f1^2*f2^3+(Z(2)^0)*f1*f2^4+(Z(2)^0)*f2
   ↪ ^5+(Z(2)^0)*f1^2*f2^4+(Z(2)^0)*f1*f2^5+(Z(2)^0)*
   ↪ f2^6+(Z(2)^0)*f1^2*f2^5+(Z(2)^0)*f1*f2^6+(Z(2)
   ↪ ^0)*f1^2*f2^6
(Z(2)^0)*f1+(Z(2)^0)*f1^2+(Z(2)^0)*f1*f2+(Z(2)^0)*f1
   ↪ ^2*f2+(Z(2)^0)*f1*f2^2+(Z(2)^0)*f1^2*f2^2+(Z(2)
   ↪ ^0)*f1*f2^3+(Z(2)^0)*f1^2*f2^3+(Z(2)^0)*f1*f2
```

```
    ↪ ^4+(Z(2)^0)*f1^2*f2^4+(Z(2)^0)*f1*f2^5+(Z(2)^0)*
    ↪ f1^2*f2^5+(Z(2)^0)*f1*f2^6+(Z(2)^0)*f1^2*f2^6
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f2^3+(Z(2)^0)*f2
    ↪ ^5+(Z(2)^0)*f2^6
(Z(2)^0)*<identity> of ...+(Z(2)^0)*f2+(Z(2)^0)*f2^2+(
    ↪ Z(2)^0)*f2^4
```

Kolejne idempotenty wskazane w powyższej tabeli są następujące:

$$\begin{aligned}
\mathbf{e}_0 &= (1+y+y^2)(1+x+x^2+x^3+x^4+x^5+x^6) = \mathbf{f}_1,\\
\mathbf{e}_2+\mathbf{e}_3 &= (y+y^2)(1+x+x^2+x^3+x^4+x^5+x^6) \quad = \mathbf{f}_2,\\
\mathbf{e}_4 &= 1+x^3+x^5+x^6 \quad = \mathbf{f}_3,\\
\mathbf{e}_5 &= 1+x+x^2+x^4 \quad = \mathbf{f}_4.
\end{aligned}$$

Wśród wszystkich ideałów algebry grupowej $\mathbb{F}[G]$, na szczególną uwagę zasługuje ideał augmentacyjny, który będziemy oznaczać symbolem $A(\mathbb{F}[G])$. Ideał augmentacyjny $A(\mathbb{F}[G])$ jest jądrem homomorfizmu $\phi : \mathbb{F}[G] \to \mathbb{F}$:

$$\phi(\sum_{g\in G} a_g g) = \sum_{g\in G} a_g.$$

Zauważamy, że jeśli tylko $\alpha = \sum_{g\in G} a_g g$ oraz $\phi(\alpha) = 0$, to:

$$\phi(\alpha) = \sum_{g\in G} a_g = 0,$$

$$\alpha = \sum_{g\in G} a_g g - \sum_{g\in G} a_g = \sum_{g\in G} a_g (g-1).$$

Z powyższego, wszystkie elementy postaci $g-1$ należą do $\ker\phi$, a zatem ideał augmentacyjny algebry grupowej generowany jest przez wszystkie elementy postaci $g-1$, gdzie $g \in G$:

$$A(\mathbb{F}[G]) = \langle g-1 :\ g\in G\rangle = \sum_{g\in G}(g-1)\mathbb{F}[G] = \{\sum_{g\in G} a_g g \in \mathbb{F}[G] :\ \sum_{g\in G} a_g = 0\}.$$

Zauważmy jeszcze, że algebra ilorazowa $\mathbb{F}[G]/A(\mathbb{F}[G])$ jest izomorficzna z ciałem $\mathbb{F}$.

W przypadku, gdy char$\mathbb{F}$ nie dzieli $|G|$, ideał augmentacyjny, jak każdy ideał algebry $\mathbb{F}[G]$, jest generowany przez idempotent tej algebry. Niech zatem:

$$\mathbf{e}_0 = \frac{\sum_{g\in G} g}{|G|}.$$

Wówczas, jak wiemy, $\mathbf{e}_0\mathbb{F}[G] \cong \mathbb{F}$. Ponadto, dla dowolnego $g \in G$ mamy

$$\mathbf{e}_0 (g-1) = 0,$$

co oznacza, że

$$\mathbb{F}[G] = e_0\mathbb{F}[G] \oplus A(\mathbb{F}[G]),$$

a stąd

$$A(\mathbb{F}[G]) = (1-e_0)\mathbb{F}[G].$$

Jeśli $G = \langle x : \ x^n = e \rangle$ jest grupą cykliczną rzędu $n$, to:

$$A(\mathbb{F}[G]) = (x-1)\mathbb{F}[G], \tag{1.1.14}$$

tzn. jest ideałem głównym generowanym przez element $x-1$, bowiem każdy element $g \in G$ ma postać $x^i$, $i = 0, 1, \ldots, n-1$, a zatem

$$(g-1)\mathbb{F}[G] = (x^i-1)\mathbb{F}[G] = (x-1)(x^{i-1}+\ldots+x+1)\mathbb{F}[G] \subseteq (x-1)\mathbb{F}[G].$$

Stąd

$$A(\mathbb{F}[G]) = \sum_{g\in G} (g-1)\mathbb{F}[G] \subseteq (x-1)\mathbb{F}[G].$$

Równość (1.1.14) domyka inkluzja w stronę przeciwną, która wydaje się oczywista.

Jeżeli charakterystyka ciała $\mathbb{F}$ jest równa $p$, zaś $G$ jest skończoną $p$-grupą, tzn. $|G| = p^k$, dla pewnej liczby całkowitej $k$, to $\mathscr{A} = A(\mathbb{F}[G])$ jest ideałem największym algebry $\mathbb{F}[G]$, tzn. każdy ideał tej algebry jest zawarty w jej ideale augmentacyjnym. Ponadto ideał ten jest nilpotentny, tzn. istnieje liczba naturalna $m$, taka że iloczyn dowolnych $m$ elementów ideału augmentacyjnego jest równy zero. Ten fakt z jednej strony oznacza ogromną różnorodność ideałów zawartych w $\mathscr{A}$ i tym samym duży rezerwuar kodów, z drugiej jednak, skomplikowana struktura tego ideału wymusza dużą pracochłonność opisu tych kodów/ideałów. By nieco przybliżyć tę strukturę rozważmy dwa przypadki grup abelowych, w pewnym sensie skrajnych z punktu widzenia ich struktury. Niech najpierw $G = \langle x : \ x^{p^n} = 1 \rangle$ będzie grupą cykliczną rzędu $p^n$. Wówczas, oprócz standardowej bazy algebry $\mathbb{F}[G]$, złożonej z elementów grupy $G$ mamy bazę złożoną z potęg elementu $(x-1)$:

$$1,\ (x-1),\ (x-1)^2,\ \ldots,\ (x-1)^{p^n-1}.$$

Zaletą tej bazy jest to, że jej kolejne elementy generują wszystkie ideały. Są one potęgami ideału augmentacyjnego:

$$\mathbb{F}[G] \supset (x-1)\mathbb{F}[G] \supset (x-1)^2\mathbb{F}[G] \supset \ldots \supset (x-1)^{p^n-1}\mathbb{F}[G] \supset \{0\},$$

przy czym ilorazy dwóch kolejnych są jednowymiarowe.

Inną, bardziej skomplikowaną sytuację mamy w przypadku elementarnej abelowej $p$-grupy. Niech zatem $G$ będzie taką grupą, tzn.

$$G = \langle x_1, x_2, \ldots, x_k : \ x_i^p = e, \ x_i x_j = x_j x_i, \ i, j \in \{1, 2, \ldots, k\} \rangle.$$

Dla dowolnych $\alpha, \beta \in \mathbb{F}[G]$ zachodzi równość

$$\alpha\beta - 1 = (\alpha - 1)(\beta - 1) + (\alpha - 1) + (\beta - 1), \tag{1.1.15}$$

a każdy element grupy $G$ ma postać $g = x_1^{m_1} x_2^{m_2} \ldots x_k^{m_k}$, $0 \leq m_j < p$. Zatem wielokrotnie korzystając z tej tożsamości, dowolny element ideału $\mathscr{A}$ możemy przedstawić w postaci kombinacji liniowej elementów:

$$(x_1 - 1)^{m_1} (x_2 - 1)^{m_2} \ldots (x_k - 1)^{m_k}, \ \ 0 \leq m_j < p. \tag{1.1.16}$$

Wynika stąd w szczególności, że dla dowolnego $\alpha \in \mathscr{A}$ mamy $\alpha^p = 0$, co oznacza między innymi, że 0 jest jedynym idempotentem w $\mathscr{A}$. Łatwą indukcją można również dowieść, że ideał $\mathscr{A}^m$ jest rozpięty na elementach postaci (1.1.16), dla których zachodzi nierówność $m_1 + m_2 + \ldots + m_k \geq m$. Przy maksymalnych wartościach wszystkich $m_j$ (równych $p-1$) dostajemy element $(x_1 - 1)^{p-1}(x_2 - 1)^{p-1} \ldots (x_k - 1)^{p-1} = \sum_{x \in G} x$. Oznacza to po pierwsze, że $\mathscr{A}^{m(p-1)}$ jest rozpięty na tym elemencie, czyli ma wymiar 1, a po drugie, wobec faktu iż ten element anihiluje $\mathscr{A}$, dostajemy równość

$$\mathscr{A}^{m(p-1)+1} = 0.$$

Można także dowieść, że anihilatorem ideału $\mathscr{A}^j$ jest ideał $\mathscr{A}^i$, gdzie $i = m(p-1) + 1 - j$. Wyczerpujący opis najważniejszych własności ideału $\mathscr{A}$ można znaleźć w monografiach Passman (1977) i Sehgal (1978).

## 1.2 Kody i ich realizacja z pomocą algebr grupowych

Dla celów tworzenia kodów będziemy interpretować zbiór $\mathbb{F}_q$, z zachowaniem własności przedstawionych w powyższym rozdziale, jako alfabet, którego symbole posłużą do zapisania dowolnej informacji. Jednostkami informacji są ciągi elementów ciała $\mathbb{F}_q$, o ustalonej długości $m \in \mathbb{N}$. Zbiór wszystkich jednostek informacji można więc utożsamiać z przestrzenią liniową $\mathbb{F}_q^m$. Do kodowania informacji posłuży przestrzeń $\mathbb{F}_q^n$, gdzie $n > m$. Dowolna podprzestrzeń $\mathscr{C}$ wymiaru $m$ tej przestrzeni nazywamy kodem długości $n$. Elementy podprzestrzeni $\mathscr{C}$ nazywamy słowami kodowymi. Macierz różnowartościowego przekształcenia liniowego $\psi : \mathbb{F}_q^m \to C$ z przestrzeni informacji $\mathbb{F}_q^m$ na kod $\mathscr{C} \subseteq \mathbb{F}_q^n$ nazywamy macierzą generującą.

Niech $\mathscr{C} \subset \mathbb{F}_q^n$ będzie kodem. Kod $\mathscr{C}$ nazwiemy liniowym, jeśli, jak wyżej, możemy przedstawić go w postaci podprzestrzeni liniowej $\mathbb{F}_q^m \subseteq \mathbb{F}_q^n$.

Niech $C_0, C_1 \in \mathscr{C}$ będą słowami kodowymi. Odległością Hamminga między słowami kodowymi $C_0$ i $C_1$ nazwiemy liczbę współrzędnych, na których $C_0$ różni się od $C_1$ i oznaczać będziemy przez $\mathrm{d}(C_0, C_1)$. Łatwo wykazać, że odległość Hamminga jest metryką na $\mathscr{C}$.

Wagą Hamminga słowa kodowego $C$ nazwiemy liczbę niezerowych współrzędnych w tym słowie i oznaczać będziemy przez $\mathrm{wt}(C)$. Formalnie, wagę Hamminga słowa kodowego definiować można również jako odległość Hamminga tego słowa od wektora zerowego. W dalszej części pracy pisać będziemy skrótowo – odległość oraz waga.

Odległością minimalną $\mathrm{d}(\mathscr{C})$ kodu $\mathscr{C}$ nazwiemy minimalną odległość Hamminga między dwoma różnymi słowami kodowymi lub równoważnie, minimalną wagę niezerowego słowa kodowego.

**Twierdzenie 1.4.** Niech dany będzie liniowy kod $\mathscr{C}$; niech $\mathrm{d}(\mathscr{C}) = d$, wtedy:

(i) Liniowy kod $\mathscr{C}$ może wykrywać $d-1$ błędów.
(ii) Liniowy kod $\mathscr{C}$ może korygować $\kappa$ błędów, gdzie $\kappa$ dane jest wzorem

$$\kappa = \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Kod liniowy $\mathscr{C}$ długości $n$, wymiaru $k$ oraz średnicy $d$ nazywany jest $(n,k,d)$-kodem.

Szczególnym przypadkiem kodów liniowych są kody cykliczne. Powiemy, że liniowy kod $\mathscr{C}$ jest kodem cyklicznym jeśli dla dowolnego słowa kodowego $C_0 = (c_1, c_2, \ldots, c_{n-1}, c_n)$, słowo $C_1 = (c_n, c_1, \ldots, c_{n-2}, c_{n-1})$ także jest słowem kodowym. Innymi słowy, jeśli $G = C_n = \langle g \mid g^n = 1 \rangle$ jest grupą cykliczną rzędu $n$, której działanie na $\mathbb{F}_q^n$ jest realizowane przez operację mnożenia przez macierz

$$M_g = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 1 & 0 \end{pmatrix},$$

to kod $\mathscr{C}$ jest cykliczny, jeśli z faktu, że $v \in \mathscr{C}$ jest słowem kodowym, wynika, że $gv \in \mathscr{C}$ również jest słowem kodowym:

$$v \in \mathscr{C} \implies gv \in \mathscr{C}.$$

W poniższych przykładach podamy realizacje wybranych kodów cyklicznych w postaci ideałów algebr grupowych.

Przykład 1.7. Jednym z najmniej skomplikowanych kodów cyklicznych jest kod binarny długości $n$ i wymiaru $n-1$, którego słowa kodowe zawierają cyfrę kontroli parzystości (powiedzmy, że jest to pierwsza współrzędna słowa kodowego). Niech $n>1$ będzie ustaloną liczbą nieparzystą i $\mathbb{F}=GF(2)=\mathbb{Z}_2$. Nasz kod można określić w następujący sposób:

$$\mathscr{C}=\left\{(c_0,c_1,\ldots,c_{n-1})\in\mathbb{F}^n:\ \sum_{i=0}^{n-1}c_i=0\right\}.$$

Zgodnie z obserwacjami poczynionymi w końcu poprzedniego rozdziału, ideał augmentacyjny algebry $\mathbb{F}[G]$ składa się ze wszystkich elementów postaci: $a_0+a_1x+a_2x^2+\ldots+a_{n-1}x^{n-1}$, takich że $a_0+a_1+a_2+\ldots+a_{n-1}=0$. Jeśli zatem $\varphi\colon\mathbb{F}[G]\to\mathbb{F}^n$ jest wzajemnie jednoznacznym odwzorowaniem określonym wzorem:

$$\varphi\left(\sum_{i=0}^{n-1}a_ix^i\right)=(a_0,a_1,\ldots,a_n),$$

to $\varphi(A(\mathbb{F}[G]))=\mathscr{C}$.

Ideał augmentacyjny algebry grupowej grupy cyklicznej generowanej przez element $x$ jest ideałem głównym generowanym przez element $x-1$. Jego anihilatorem jest ideał generowany przez element

$$\varepsilon=1+x+x^2+\ldots+x^{n-1},$$

a zatem może służyć do algebraicznego testowania, czy dany element algebry grupowej należy do $\mathbb{A}(\mathbb{F}[G])$ (czy jest słowem kodowym):

$$\alpha\in A(G)\Leftrightarrow\alpha\cdot\varepsilon=0.$$

Zamieńmy teraz rolami elementy $\varepsilon$ i $(x-1)$: niech kodem będzie ideał generowany przez $\varepsilon$, a $x-1$ posłuży nam do algebraicznego testowania, jaki element jest słowem kodowym. Bezpośrednio z postaci $\varepsilon$ wynika, że jest to przestrzeń jednowymiarowa, której elementami są 0 i $\varepsilon$, co przy innym zapisie odpowiada kodowi powtórzeniowemu oznaczanemu symbolem $(n,2,n)$, czyli kodowi

$$\mathscr{C}=\{(\underbrace{0,0,\ldots,0}_{n}),\ (\underbrace{1,1,\ldots,1}_{n})\}.$$

Pójdźmy dalej, niech $H$ będzie podgrupą grupy $G$ rzędu $k$, $n=km$, generowaną przez element $y=x^m$ i niech

$$\eta=1+y+y^2+\ldots+y^{k-1}=\sum_{h\in H}h.$$

Niech ponadto $T$ będzie zbiorem reprezentantów warstw grupy $G$ względem $H$. Wówczas zbiór

$$I = \{\eta t \mid t \in T\}$$

jest bazą ideału $\eta\mathbb{F}[G]$ jako przestrzeni liniowej nad $\mathbb{F}$. Łatwo dostrzec, że wszystkie elementy ideału $I$ są postaci

$$\alpha = \sum_{t\in T} a_t t\eta,$$

co oznacza, że gdyby zapisać je w standardowej bazie $G$ nad $\mathbb{F}$, to wszystkie współczynniki przy elementach postaci $th$, dla ustalonego $t \in T$ i dowolnego $h \in H$ byłyby takie same, a kod jest algebro-grupową realizacją kodu powtórzeniowego, zdefiniowanego następująco:

Niech $W = \mathbb{F}^k$ i $V = \mathbb{F}^{km} = W^m$, wówczas przez $(k,m)$-powtórzeniowy kod rozumiemy podprzestrzeń, której elementami są ciągi

$$(\underbrace{w,w,\ldots,w}_{m}) \text{ , gdzie } w \in W.$$

Dla ilustracji ostatniego stwierdzenia rozważmy przykład grupy $G$ rzędu $n = 9$ i podgrupy $H$ rzędu $k = 3$ ($k = 3 = m$). Niech przy tym $T = 1,x,x^2$. Jeśli $\alpha = a_0 + a_1x + a_2x^2 + a_3x^3 + a_4x^4 + a_5x^5 + a_6x^6 + a_7x^7 + a_8x^8 \in \mathbb{F}G$ jest dowolnym elementem algebry (który odpowiada wektorowi $(a_0,a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8) \in \mathbb{F}^9$), to wobec równości

$$\begin{aligned}
\eta = x^3\eta = x^6\eta &= 1 + x^3 + x^6 \leftrightarrow (1,0,0,1,0,0,1,0,0)\\
x\eta = x^4\eta = x^7\eta &= x + x^4 + x^7 \leftrightarrow (0,1,0,0,1,0,0,1,0)\\
x^2 = x^5\eta = x^8\eta &= x^2 + x^5 + x^8 \leftrightarrow (0,0,1,0,0,1,0,0,1)
\end{aligned}$$

otrzymujemy postać dowolnego elementu ideału $\eta\mathbb{F}[G]$

$$\eta\alpha = (a_0 + a_3 + a_6)\eta + (a_1 + a_4 + a_7)x\eta + (a_2 + a_5 + a_8)x^2\eta,$$

który przy podstawieniu $b_0 = a_0 + a_3 + a_6$, $b_1 = a_1 + a_4 + a_7$, $b_2 = a_2 + a_5 + a_8$ odpowiada wektorowi $(b_0,b_1,b_2,b_0,b_1,b_2,b_0,b_1,b_2)$, ten zaś możemy zapisać w postaci $(w,w,w)$ dla $w = (b_0,b_1,b_2) \in \mathbb{F}^3$.

Powyższe rozumowanie można przenieść na ogólny przypadek, gdy $\mathbb{F}$ jest dowolnym ciałem skończonym, $G$ jest dowolną grupą skończoną, zaś $H$ – jej podgrupą normalną. Wtedy przyjmujemy, że $\eta = \sum_{h\in H} h$ i gdy charakterystyka ciała nie dzieli $|G|$ możemy $\eta$ zastąpić idempotentem $\mathbf{e} = \frac{\eta}{|H|}$. To pozwala na uzyskanie łatwego kryterium rozpoznawania słów kodowych: $\alpha \in \mathbb{F}[G]$ jest słowem kodowym wtedy i tylko wtedy $\alpha(1-\mathbf{e}) = 0$.

W następnych przykładach, odnosząc się czasem do przykładów omówionych w poprzednim rozdziale, przedstawimy kody zrealizowane w tam wskazanych algebrach grupowych z pomocą programu GAP. Na potrzeby skrócenia pracy, część kodu, która w sposób naturalny powtarza się między kolejnymi przykładami zastąpiono `[...]`.

Przykład 1.8. Zaczniemy od algebry grupowej grupy cyklicznej rzędu 17 opisanej w przykładzie 1.3. W poniższych przykładach konstruujemy algebrę grupową, a następnie z kolejnych centralnych prymitywnych idempotentów oraz ich sum, tworzymy lewostronne ideały w tej algebrze, na podstawie których generujemy kolejne kody.

```
gap> G := CyclicGroup(17);; S := AsSet(G);;
gap> F := GF(2);;;
gap> FG := GroupRing(F, G);
<algebra-with-one over GF(2), with 1 generators>
gap>
```

```
gap> I := LeftIdealByGenerators(FG,[FGe[1]]);;
gap> V := VectorSpace(F,CodeByLeftIdeal(F,G,S,I));;
gap> B := Basis(V);;
gap> C1 := GeneratorMatCode(B,F);
a linear [17,1,17]8 code defined by generator matrix
   ↪ over GF(2)
gap>
```

```
gap> I := LeftIdealByGenerators(FG,[FGe[2]]);;
[...]
gap> C2 := GeneratorMatCode(B,F);
a linear [17,8,1..6]3..7 code defined by generator
   ↪ matrix over GF(2)
gap>
```

Zauważamy, że kod $\mathscr{C}_1$ jest kodem powtórzeniowym, natomiast kod $\mathscr{C}_2$ jest kodem cyklicznym; kod wygenerowany przez ostatni z idempotentów - $\mathscr{C}_3$ jest kodem tożsamym z $\mathscr{C}_2$.

Kody powstałe jako ideał generowany przez sumę idempotentów, to znaczy – kod $\mathscr{C}_{12}$ dany jest jako suma idempotentów $\mathbf{e}_1, \mathbf{e}_2$ dane są jak niżej.

```
gap> I := LeftIdealByGenerators(FG,[FGe[1] + FGe[2]])
   ↪ ;;
[...]
gap> C12 := GeneratorMatCode(B,F);
a linear [17,9,1..5]3..4 code defined by generator
   ↪ matrix over GF(2)
gap>
```

```
gap> I := LeftIdealByGenerators(FG,[FGe[1] + FGe[3]])
   ↪ ;;
[...]
gap> C13 := GeneratorMatCode(B,F);
a linear [17,9,1..5]3..4 code defined by generator
   ↪ matrix over GF(2)
gap>
```

```
gap> I := LeftIdealByGenerators(FG,[FGe[2] + FGe[3]])
   ↪ ;;
[...]
gap> C23 := GeneratorMatCode(B,F);
a linear [17,16,1..2]1 code defined by generator
   ↪ matrix over GF(2)
gap>
```

Wagi oraz wymiary powyższych kodów to odpowiednio

```
gap> List([C1, C2, C3, C12, C13, C23], MinimumWeight);
[ 17, 6, 6, 5, 5, 2 ]
gap>
```

```
gap> List([C1, C2, C3, C12, C13, C23], Dimension);
[ 1, 8, 8, 9, 9, 16 ]
gap>
```

Niech $\mathscr{C}$ będzie dowolnym kodem cyklicznym długości $n$ nad ciałem $\mathbb{F}$. Bezpośrednio z definicji wynika, że jako przestrzeń liniowa, $\mathscr{C}$ jest $G$-modułem, gdzie $G = \langle x : x^n = e \rangle$, co oznacza, że jest określone naturalne mnożenie elementów z $\mathscr{C}$ przez elementy z algebry grupowej $\mathbb{F}[G]$, jak swego rodzaju uogólnione skalary. Jeżeli $\mathrm{char}\,\mathbb{F}$ nie dzieli rzędu grupy, to $\mathbb{F}[G]$ jest algebrą półprostą (patrz [1.2,1.3]), co z kolei oznacza, że każdy $G$-moduł jest sumą prostą podmodułów prostych, te zaś są izomorficzne z minimalnymi ideałami algebry $\mathbb{F}[G]$, jako modułami nad $\mathbb{F}[G]$. Podsumowując, każdy kod cykliczny można zrealizować jako sumę prostą kodów, z których każdy jest izomorficzny (jako $G$-moduł) z ideałem minimalnym algebry $\mathbb{F}[G]$.

Przykład 1.9. Pokażemy teraz konstrukcję kodu na podstawie przykładu 1.6. Skonstruujmy algebrę grupową nad ciałem charakterystyki dwa oraz jedyną nieabelową grupą rzędu 21, a następnie weźmy układ centralnych prymitywnych idempotentów tej algebry (patrz przykład 1.6).

Kolejno, utworzymy kody $\mathscr{C}_1, \mathscr{C}_2, \mathscr{C}_3, \mathscr{C}_4$, które odpowiadają lewostronnym ideałom w tej algebrze generowanym przez idempotenty $\mathbf{f}_1, \mathbf{f}_2, \mathbf{f}_3, \mathbf{f}_4$.

```
gap> I := LeftIdealByGenerators(FG,[FGe[1]]);;
gap> V := VectorSpace(F,CodeByLeftIdeal(F,G,S,I));;
gap> B := Basis(V);;
gap> C1 := GeneratorMatCode(B,F);
a linear [21,1,21]10 code defined by generator matrix
   ↪ over GF(2)
gap>
```

```
gap> I := LeftIdealByGenerators(FG,[FGe[3]]);;
gap> V := VectorSpace(F,CodeByLeftIdeal(F,G,S,I));;
gap> B := Basis(V);;
gap> C3 := GeneratorMatCode(B,F);
a linear [21,9,1..4]4..10 code defined by generator
   ↪ matrix over GF(2)
gap>
```

Kody $\mathscr{C}_2, \mathscr{C}_4$, które utworzone zostały z idempotentów $\mathbf{f}_2, \mathbf{f}_4$, są równoważne kodom $\mathscr{C}_1, \mathscr{C}_3$ odpowiednio.

```
gap> IsEquivalent(C1, C2);
true
gap> IsEquivalent(C3, C4);
true
gap> IsEquivalent(C1, C3);
false
gap>
```

Zatem wystarczy tylko podać opis kodów $\mathscr{C}_1$ i $\mathscr{C}_3$. W szczególności, minimalne wagi Hamminga dla obu kodów przedstawiają się następująco:

```
gap> MinimumWeight(C1);
14
gap> MinimumWeight(C3);
4
gap>
```

Następny przykład jest ilustracją realizacji kodu niecyklicznego za pomocą algebry grupowej elementarnej grupy abelowej rzędu 8 nad ciałem $\mathbb{F}_8$ (Wolfmann (1991)). Mamy tu do czynienia z sytuacją, gdy charakterystyka ciała dzieli rząd grupy. Jak wiemy, struktura tych algebr jest opisana w znacznie mniej wyczerpującym stopniu.

Przykład 1.10. Rozważmy rozszerzony kod Golay'a, binarny kod o wymiarze 12, korygujący trzy lub mniej błędów, którym posługiwała się między innymi sonda kosmiczna Voyager, w latach osiemdziesiątych XX w. Za jego pomocą kodowała między innymi zdjęcia przesyłane z kosmosu.

Niech

$$B = \begin{bmatrix} 1&1&0&1&1&1&0&0&0&1&0&1 \\ 1&0&1&1&1&0&0&0&1&0&1&1 \\ 0&1&1&1&0&0&0&1&0&1&1&1 \\ 1&1&1&0&0&0&1&0&1&1&0&1 \\ 1&1&0&0&0&1&0&1&1&0&1&1 \\ 1&0&0&0&1&0&1&1&0&1&1&1 \\ 0&0&0&1&0&1&1&0&1&1&1&1 \\ 0&0&1&0&1&1&0&1&1&1&0&1 \\ 0&1&0&1&1&0&1&1&1&0&0&1 \\ 1&0&1&1&0&1&1&1&0&0&0&1 \\ 0&1&1&0&1&1&1&0&0&0&1&1 \\ 1&1&1&1&1&1&1&1&1&1&1&0 \end{bmatrix}$$

będzie macierzą nad ciałem $\mathbb{F}_2$ i niech $M = [I;B]$ będzie $12 \times 24$-macierzą nad tym ciałem, gdzie $I$ jest macierzą jednostkową stopnia 12. Macierz $M$ jest macierzą generującą tego kodu, tzn. przestrzeń informacji $W$ jest 12-wymiarową przestrzenią nad ciałem $\mathbb{F}_2$, a słowa kodowe stanowią podprzestrzeń przestrzeni 24-wymiarowej, które otrzymujemy mnożąc wektory przestrzeni $W$ przez macierz $M$. Ten kod oznaczymy symbolem $\mathscr{C}_{24}$. W literaturze określa się go również jako kod Golay'a $(24,12,8)$ Wolfmann (1991).

Kod Golay'a ma następujące własności:

1. Kod $\mathscr{C}_{24}$ ma długość 24 wymiar 12 i średnicę 8;
2. Macierzą sprawdzającą kodu jest $[I;B]^T$;
3. Kod $\mathscr{C}_{24}$ koryguje co najwyżej 3 błędy.

Niech $\mathbb{F}_8$ będzie ciałem 8-elementowym. Niech $\alpha$ będzie generatorem multyplikatywnej grupy tego ciała, tzn. $\alpha \neq 1$ i $\alpha^7 = 1$. Stąd:

$$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 = 0,$$

a ponieważ

$$1 + \alpha + \alpha^2 + \alpha^3 + \alpha^4 + \alpha^5 + \alpha^6 = \left(1 + \alpha + \alpha^3\right)\left(1 + \alpha^2 + \alpha^3\right),$$

więc możemy przyjąć, że $1 + \alpha + \alpha^3 = 0$, tzn. $\alpha^3 = 1 + \alpha$. Pozostałymi pierwiastkami wielomianu $f(x) = 1 + x + x^3 \in \mathbb{F}_2[x]$ są $\alpha^2$ i $\alpha^4$.
Istotnie $f(\alpha^2) = (1 + \alpha + \alpha^3)^2 = 0$ i $f(\alpha^4) = (1 + \alpha + \alpha^3)^4 = 0$. Elementy $\alpha^3$, $\alpha^5$ i $\alpha^6$ są pierwiastkami wielomianu $g(x) = 1 + x^2 + x^3 \in \mathbb{F}_2[x]$. Niech teraz $G$ będzie addytywną grupą ciała $\mathbb{F}_8$. Ze względu na dwoistość ról elementów, wprowadzimy dla elementów grupy addytywnej oznaczenia zgodnie z następującym przyporządkowaniem. Dla $\beta \in \mathbb{F}_8$ przez $X^\beta$ oznaczymy ten sam element $\beta$, ale jako element

bazy przestrzeni $\mathbb{F}_8[G]$. Przy czym, addytywne działanie w $\mathbb{F}_8$ zostanie zastąpione działaniem multyplikatywnym zgodnie ze wzorem:

$$X^{\beta}X^{\gamma} = X^{\beta+\gamma}.$$

W szczególności zatem, elementy $X^0 = 1, X^{\alpha}, X^{\alpha^2}, X^{\alpha^4}$ tworzą podgrupę rzędu 4 w grupie $G$. Rzeczywiście, skoro $1+\alpha = \alpha^3$, więc $\alpha+\alpha^2 = \alpha^4$ i tym samym

$$X^{\alpha}X^{\alpha^2} = X^{\alpha+\alpha^2} = X^{\alpha^4},$$

skąd już łatwo wyprowadzić pozostałe zależności.

Niech teraz

$$y = 1 + X\left(1 + \alpha X^{\alpha} + \alpha^2 X^{\alpha^2} + \alpha^4 X^{\alpha^4}\right).$$

**Lemat 1.1.** Ideał $I$ algebry $\mathbb{F}_8[G]$ generowany przez element $y$ spełnia następujące warunki:
(i) $I^2 = 0$;
(ii) $\dim_{\mathbb{F}_8} I = 4$.

Dowód. (i) Ponieważ algebra jest przemienna, więc wystarczy zauważyć, że $y^2 = 0$. Istotnie, w ciele $\mathbb{Z}_2$ mamy $1+1=0$, zatem $X^2 = X^{1+1} = X^0 = 1$ i dalej

$$\begin{aligned} y^2 &= (1+X(1+\alpha X^{\alpha}+\alpha^2 X^{\alpha^2}+\alpha^4 X^{\alpha^4}))^2 &&= \\ &= 1^2 + X^2(1^2+\alpha^2 X^{2\alpha}+\alpha^4 X^{2\alpha^2}+\alpha X^{2\alpha^4}) &&= \\ &= \alpha^2+\alpha^4+\alpha = \alpha(1+\alpha+\alpha^3) &&= 0. \end{aligned}$$

(ii) Dowód tej części jest dość kłopotliwy, dlatego wskażemy tylko jego zarys. Korzystając z tego, że grupa $G$, w zapisie formalnym z wykorzystaniem notacji $X^{\beta}$, jest generowana przez elementy $X, X^{\alpha}, X^{\alpha^2}$. Zatem element $y$ można zapisać w postaci

$$\begin{aligned} y &= 1+X+\alpha X^{\alpha+1}+\alpha^2 X^{\alpha^2+1}+\alpha^4 X^{\alpha^4+1} &&= \\ &= 1+X+\alpha X^{\alpha^3}+\alpha^4 X^{\alpha^5}+\alpha^2 X^{\alpha^6} &&= \\ &= (X+1)+\alpha(X\cdot X^{\alpha}+1)+\alpha^4(X\cdot X^{\alpha}\cdot X^{\alpha^2}+1)+\alpha^2(X\cdot X^{\alpha^2}+1). \end{aligned}$$

Następnie korzystając z tożsamości 1.1.15, która dla algebry nad ciałem 2–elementowym przyjmuje postać

$$ab+1 = (a+1)(b+1)+(a+1)+(b+1)$$

oraz jej iteracji

$$\begin{aligned} abc+1 = {} & (a+1)(b+1)(c+1)+(a+1)(b+1)+(a+1)(c+1)+(b+1)(c+1)+ \\ & +(a+1)+(b+1)+(c+1) \end{aligned}$$

dostajemy postać

$$\begin{aligned} y = {} & \alpha^4(X+1)(X^{\alpha}+1)(X^{\alpha^2}+1)+ \\ & + \alpha^2(X+1)(X^{\alpha}+1)+\alpha(X+1)(X^{\alpha^1}+1)+\alpha^4(X^{\alpha}+1)(X^{\alpha^2}+1)+ \\ & + (X+1)+\alpha^2(X^{\alpha}+1)+\alpha(X^{\alpha^2}+1). \end{aligned} \tag{1.2.1}$$

Ideał augmentacyjny $A = A(\mathbb{F}_8[G])$ algebry $\mathbb{F}_8[G]$, który, jak wiadomo, jest jej największym ideałem, jest podprzestrzenią rozpiętą nad $\mathbb{F}_8$ na elementach:

$$\begin{gathered} X+1,\ X^{\alpha}+1,\ X^{\alpha^2}+1, \\ (X+1)(X^{\alpha}+1),\ (X+1)(X^{\alpha^2}+1),\ (X^{\alpha}+1)(X^{\alpha^2}+1), \\ (X+1)(X^{\alpha}+1)(X^{\alpha^2}+1), \end{gathered} \tag{1.2.2}$$

przy czym $A^2$ jest podprzestrzenią rozpiętą na elementach z drugiego i trzeciego wiersza ostatniej listy (ma więc wymiar 4), natomiast $A^3$ jest jednowymiarową przestrzenią rozpiętą na elemencie z ostatniego wiersza.

Łatwo teraz zauważyć, że ideał generowany przez $y$ jest rozpięty na elementach:

$$\begin{aligned} & y, \\ & \alpha^2(X+1)(X^{\alpha}+1)+\alpha(X+1)(X^{\alpha^2}+1), \\ & (X+1)(X^{\alpha}+1)+\alpha(X^{\alpha}+1)(X^{\alpha^2}+1), \\ & (X+1)(X^{\alpha^2}+1)+\alpha^2(X^{\alpha}+1)(X^{\alpha^2}+1), \\ & \alpha^4(X+1)(X^{\alpha}+1)(X^{\alpha^2}+1). \end{aligned}$$

Element $y$ jest jedynym elementem, który nie należy do $A^2$, zatem jest on liniowo niezależny od pozostałych. Ponadto,

$$y(X+1)+\alpha^2 y(X^{\alpha}+1)+\alpha y(X^{\alpha^2}+1) = \alpha^2(X+1)(X^{\alpha}+1)(X^{\alpha^2}+1),$$

co oznacza, że cztery pozostałe elementy są liniowo zależne. Jednocześnie, nietrudno zauważyć, że jeśli pominiemy jeden z nich, drugi, trzeci lub czwarty, pozostałe trzy są liniowo niezależne. To kończy dowód lematu.

Dowód poniższego lematu w części wynika z poprzedniego, w części zaś jest nieskomplikowaną obserwacją, którą możemy przeprowadzić na bazie poprzedniego dowodu.

**Lemat 1.2.** Anihilatorem ideału $I$ jest ideał $I$; innymi słowy $I^2 = 0$ oraz dla dowolnego $r \in \mathbb{R}_8[G] - I$ zachodzi nierówność $r \cdot y \neq 0$.

Ciało $\mathbb{F}_8$ jest przestrzenią liniową wymiaru 3 nad ciałem $\mathbb{F}_2 = \{0, 1\}$. Rozważmy bazę tej przestrzeni złożonej z elementów:

$$u_1 = \alpha^3,\ u_2 = \alpha^6,\ u_3 = \alpha^5.$$

Każdy element ciała odpowiada zatem trójwyrazowemu binarnemu ciągowi współczynników kombinacji liniowej dającej dany element:

$$\begin{array}{ll}
0 & \leftrightarrow (0,0,0);\\
1 = u_1 + u_2 + u_3 & \leftrightarrow (1,1,1);\\
\alpha = u_2 + u_3 & \leftrightarrow (0,1,1);\\
\alpha^2 = u_1 + u_3 & \leftrightarrow (1,0,1);\\
\alpha^3 = u_1 & \leftrightarrow (1,0,0);\\
\alpha^4 = u_1 + u_2 & \leftrightarrow (1,1,0);\\
\alpha^5 = u_3 & \leftrightarrow (0,0,1);\\
\alpha^6 = u_2 & \leftrightarrow (0,1,0).
\end{array}$$

Oto kilka przykładowych obliczeń:

$$1 = \alpha^7 = \alpha^4\alpha^3 = \alpha^3\alpha(1+\alpha) = \alpha^3(\alpha+\alpha^2) = \alpha^3(1+\alpha^3+\alpha^2) = \alpha^3+\alpha^6+\alpha^5$$
$$\alpha = 1+\alpha^3 = (\alpha^3+\alpha^6+\alpha^5)+\alpha^3 = \alpha^6+\alpha^5$$

Rozważmy elementy:

$$\begin{aligned}
x_1 &= y = 1+X(1+\alpha X^{\alpha}+\alpha^2 X^{\alpha^2}+\alpha^4 X^{\alpha^4}) = 1+X+\alpha X^{\alpha^3}+\alpha^2 X^{\alpha^6}+\alpha^4 X^{\alpha^5} =\\
&= 1+X+\alpha X^{\alpha^3}+\alpha^4 X^{\alpha^5}+\alpha^2 X^{\alpha^6},\\
x_2 &= X^{\alpha} y = X^{\alpha}+X^{\alpha+1}+\alpha X^{\alpha+\alpha^3}+\alpha^2 X^{\alpha+\alpha^6}+\alpha^4 X^{\alpha+\alpha^5} =\\
&= X^{\alpha}+X^{\alpha^3}+\alpha X+\alpha^2 X^{\alpha^5}+\alpha^4 X^{\alpha^6}\\
&= \alpha X+X^{\alpha}+X^{\alpha^3}+\alpha^2 X^{\alpha^5}+\alpha^4 X^{\alpha^6},\\
x_3 &= X^{\alpha^2} y = X^{\alpha^2}+X^{\alpha^2+1}+\alpha X^{\alpha^2+\alpha^3}+\alpha^2 X^{\alpha^2+\alpha^6}+\alpha^4 X^{\alpha^2+\alpha^5} =\\
&= X^{\alpha^2}+X^{\alpha^6}+\alpha X^{\alpha^5}+\alpha^2 X+\alpha^4 X^{\alpha^3}\\
&= \alpha^2 X+X^{\alpha^2}+\alpha^4 X^{\alpha^3}+\alpha X^{\alpha^5}+X^{\alpha^6},\\
x_4 &= X^{\alpha^4} y = X^{\alpha^4}+X^{\alpha^4+1}+\alpha X^{\alpha^4+\alpha^3}+\alpha^2 X^{\alpha^4+\alpha^6}+\alpha^4 X^{\alpha^4+\alpha^5} =\\
&= \alpha^4 X+\alpha^2 X^{\alpha^3}+X^{\alpha^4}+X^{\alpha^5}+\alpha X^{\alpha^6}.
\end{aligned}$$

Tworzą one bazę ideału $I$ jako przestrzeni liniowej nad ciałem $\mathbb{F}_8$. Ze względu na to, że $\mathbb{F}_8$ jest przestrzenią liniową nad $\mathbb{F} = \mathbb{Z}_2$, można ideał I traktować, jako 12-wymiarową podprzestrzeń algebry $\mathbb{F}[G]$. Nie jest to jednak ideał tej algebry, zatem poza algebraiczną prezentacją oraz możliwością algebraicznego testowania, czy dany element reprezentuje słowo kodowe, nie daje dodatkowych korzyści w postaci alternatywnych algorytmów dekodowania.

W nieco ogólniejszym ujęciu wygląda to następująco: rozważmy podprzestrzeń algebry $\mathbb{F}_8[G]$ z ustaloną bazą $\{v_1, v_2, \ldots, v_k\}$ nad ciałem $\mathbb{F}_8$. Binarnym przekształceniem ze względu na bazę $\{u_1, u_2, u_3\}$ ciała $\mathbb{F}_8$ nad ciałem $\mathbb{F}_2$ nazywamy funkcję, która każdej kombinacji liniowej $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_k v_k$ przyporządkowuje ciąg binarny powstały z ciągu $(\alpha_1, \alpha_2, \ldots, \alpha_k)$ przez zastąpienie wyrazów $\alpha_i$ ciągami binarnych współczynników $(a_{i1}, a_{i2}, a_{i3})$ i opuszczeniu nawiasów, gdzie
$\alpha_i = a_{i1}u_1 + a_{i2}u_2 + a_{i3}u_3$.

**Twierdzenie 1.5.** Binarny obraz ideału $I$ w przestrzeni $\mathbb{F}_2^{24}$, ze względu na bazę $\{u_1, u_2, u_3\}$ jest $(24, 12, 8)$-kodem Golay'a.

Przykład 1.11. Innym przykładem kodów, które mogą być zrealizowane w języku algebr grupowych jest rodzina kodów Reeda-Mullera zaproponowana przez Mullera w 1954 r. Istnieje wiele sposobów ich opisu, patrz np. Hoffman i in. (1991). Tu przedstawimy standardową definicję opartą na pojęciu funkcji boolowskiej. Jeśli $X$ jest dowolnym ustalonym zbiorem, to przez funkcję boolowską określoną na $X$ rozumiemy dowolną funkcję $f\colon X \to \mathbb{Z}_2$. Każda funkcja boolowska może być utożsamiana z funkcją charakterystyczną podzbioru $A = \{x \in X : \ f(x) = 1\}$.

Niech

$$X_m = \{(a_1, a_2, \ldots, a_m) : \ a_i \in \{0,1\}\} = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{m}$$

będzie zbiorem wszystkich ciągów binarnych długości $m$. Jest jasne, że $|X_m| = 2^m$. Rozważmy zbiór wszystkich funkcji boolowskich określonych na zbiorze $X_m$. Ma on $2^{2^m}$ elementów i można go w naturalny sposób traktować, jako algebrę nad ciałem $\mathbb{F} = \mathbb{Z}_2$

$$\mathbb{A}_m = \underbrace{\mathbb{Z}_2 \times \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2}_{2^m}.$$

z naturalnymi operacjami dodawania i mnożenia oraz mnożenia przez skalary. Przestawimy konstrukcję kodów Reeda-Mullera jako podprzestrzeni tej przestrzeni. Niech $T_1,\ T_2,\ \ldots, T_m$ będą przemiennymi zmiennymi. Aby wskazać te podprzestrzenie wprowadźmy najpierw przyporządkowanie

$$\begin{aligned}
T_0 &\leftrightarrow (1,1,1,1,1,1,1,1,\ldots,1,1,1,1) = t_0\\
T_1 &\leftrightarrow (0,1,0,1,0,1,0,1,\ldots,0,1,0,1) = t_1\\
T_2 &\leftrightarrow (0,0,1,1,0,0,1,1,\ldots,0,0,1,1) = t_2\\
&\ldots\ldots\ldots\ldots\\
T_{m-1} &\leftrightarrow (\underbrace{0,0,\ldots,0}_{2^{m-2}},\underbrace{1,1,\ldots,1}_{2^{m-2}},\underbrace{0,0,\ldots,0}_{2^{m-2}},\underbrace{1,1,\ldots,1}_{2^{m-2}}) = t_{m-1}\\
T_m &\leftrightarrow (\underbrace{0,0,\ldots,0}_{2^{m-1}},\underbrace{1,1,\ldots,1}_{2^{m-1}}) = t_m
\end{aligned}$$

Zauważmy, że powyższe przyporządkowanie w naturalny sposób przedłuża się do epimorfizmu algebry wielomianów $\mathbb{Z}_2[T_0, T_1, \ldots, T_{m-1}]$ na $\mathbb{A}$. Jądrem tego odwzorowania jest ideał generowany przez wielomiany $T_i^2 = T_i$, $i = 0, 1, \ldots, m-1$. Ponadto, nietrudno dowieść, że nasz epimorfizm działa wzajemnie jednoznacznie na podprzestrzeni rozpiętej na zbiorze wszystkich jednomianów postaci

$$T_1^{\varepsilon_1} T_2^{\varepsilon_2} \ldots T_m^{\varepsilon_m}, \;\; \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_m \in \{0, 1\}.$$

Przez stopień takiego jednomianu rozumiemy $\sum_{1 \leq i \leq m} \varepsilon_i$, a przez stopień ich kombinacji liniowej – największą z wartości stopni jednomianów, które wchodzą do kombinacji z niezerowym współczynnikiem.

Kodem Reeda-Mullera $RM(r,m)$ nazywamy podprzestrzeń przestrzeni $\mathbb{A}_m$, która jest obrazem podprzestrzeni rozpiętej na wszystkich jednomianach stopnia $\leq r$.

**Twierdzenie 1.6.** Kod Reeda-Mullera $\mathscr{C} = RM(r,m)$ ma następujące własności:

(i) Długość kodu $\mathscr{C}$ jest równa $2^m$.
(ii) Wymiar kodu jest równy $dim_{\mathbb{F}} \mathscr{C} = 1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r}$.
(iii) Średnica kodu jest równa $2^{m-r}$, wykrywa $2^{m-r} - 1$ błędów i koryguje $2^{m-r-1} - 1$ z nich.
(iv) Macierz generująca kodu $\mathscr{C}$ jest równa $[I;B]$, gdzie

$$B = [t_0; t_1; \ldots; t_m; t_1 t_2; \ldots; t_{m-1} t_m; \ldots]^T,$$

czyli jest macierzą, której kolejne wiersze odpowiadają jednomianom stopnia $\leq r$ uporządkowanym leksykograficznie.

Przejdźmy teraz do demonstracji tego kodu jako ideału algebry grupowej. Niech $G$ będzie elementarną grupą abelową rzędu $2^m$, tzn.

$$G = \langle x_1, x_2, \ldots, x_m : \; x_i^2 = e, \; x_i x_j = x_j x_i, \; i, j = 1, 2, \ldots, m \rangle$$

i $\mathbb{F} = \mathbb{Z}_2$. Niech dalej, $\mathscr{A}$ będzie ideałem augmentacyjnym algebry $\mathbb{F}[G]$ oraz dla dowolnego podzbioru $Y$ grupy $G$ przez $\overline{Y}$ będziemy rozumieć element algebry $\mathbb{F}[G]$ postaci $\sum_{y \in Y} y$. Z opisu własności ideału $\mathscr{A}$ podanego na końcu rozdziału 1.1 wynika, że

$$\mathscr{A}^m = \mathrm{lin}((x_1 + 1)(x_2 + 1) \ldots (x_m + 1)) \;\; \text{i} \;\; \mathscr{A}^{m+1} = 0.$$

Zauważmy, że jeśli $\{x_{i_1}, x_{i_2}, \ldots, x_{i_k}\}$ jest $k$-elementowym podzbiorem zbioru $\{x_1, x_2, \ldots, x_m\}$, to

$$(x_{i_1} + 1)(x_{i_2} + 1) \ldots (x_{i_k} + 1) = \overline{\langle x_{i_1}, x_{i_2}, \ldots, x_{i_k} \rangle}.$$

Wynika z tego, że ideał $\mathscr{A}^j$, $j = 1, 2, \ldots, m$ jest rozpięty, jako przestrzeń liniowa, na elementach postaci $\overline{\langle Y \rangle}$, gdzie $Y$ przebiega wszystkie podzbiory zbioru $\{x_1, x_2, \ldots, x_m\}$,

których moc jest nie mniejsza niż $j$. Liczba takich podzbiorów jest równa

$$\binom{m}{j}+\binom{m}{j+1}+\ldots+\binom{m}{m}=\binom{m}{0}+\binom{m}{1}+\ldots+\binom{m}{m-j},$$

co oznacza, że $\mathscr{A}^j$ ma wymiar taki, jak kod Reeda-Mullera $RM(m-j,m)$. Dowodzi się, że w standardowej bazie algebry $\mathbb{F}[G]$ ideał $A^j$ zachowuje wszystkie cechy tego kodu. Jednocześnie $A^j$ jako ideał algebry $\mathbb{F}[G]$ ma dodatkowe zalety, które pozwalają na zaproponowanie algorytmu dekodowania. Na podstawie Landrock i Manz (1992) zilustrujemy to w przypadku, gdy $m=5, j=4$. Takich parametrów użyto w kodzie Reeda-Mullera, wykorzystanego do przekazu zdjęć wykonanych w ramach misji statku kosmicznego Mariner w 1969 r.

Niech

$$G=\langle x_1,x_2,x_3,x_4,x_5:\ x_i^2=e,\ x_ix_j=x_jx_i,\ i,j\in\{1,2,3,4,5\}\rangle.$$

Wówczas

| Ideał $\mathscr{A}^i$ | generatory $\mathscr{A}^i$ modulo $\mathscr{A}^{i+1}$ | $\dim\mathscr{A}^i/\mathscr{A}^{i+1}$ |
|---|---|---|
| $\mathscr{A}^0=\mathbb{F}[G]$ | $1$ | $\binom{5}{0}=1$ |
| $\mathscr{A}$ | $(x_1+1),\ (x_2+1),\ (x_3+1),\ (x_4+1),\ (x_5+1)$ | $\binom{5}{1}=5$ |
| $\mathscr{A}^2$ | $(x_i+1)(x_j+1),\ \ i<j,\ \ i,j\in\{1,2,3,4,5\}$ | $\binom{5}{2}=10$ |
| $\mathscr{A}^3$ | $(x_i+1)(x_j+1)(x_k+1),\ \ i<j<k,\ \ i,j,k\in\{1,2,3,4,5\}$ | $\binom{5}{3}=10$ |
| $\mathscr{A}^4$ | $(x_i+1)(x_j+1)(x_k+1)(x_l+1),\ \ i<j<k<l,\ \ i,j,k,l\in\{1,2,3,4,5\}$ | $\binom{5}{4}=5$ |
| $\mathscr{A}^5$ | $(x_1+1)(x_2+1)(x_3+1)(x_4+1)(x_5+1)$ | $\binom{5}{5}=1$ |

Podane parametry oznaczają, że kodem $RM(4,5)$ jest ideał $\mathscr{A}^4$. Jako przestrzeń liniowa jest on rozpięty na elementach z ostatnich dwóch wierszy powyższej tabeli, a więc ma wymiar 6 i tym samym, liczba słów kodowych jest równa $2^6=64$.

Ostatni element jest równy $\eta=\sum_{x\in G}x$, a zatem jego waga Hamminga $\mathrm{wt}(\eta)=32$. Waga Hamminga pozostałych elementów jest równa 16. Dokładniej, jeśli $G_i$, $i=1,2,3,4,5$ jest podgrupą grupy $G$ generowaną przez elementy $x_j$, gdzie $i\neq j$, to bazą kodu jest układ:

$$\begin{aligned}
\gamma_0&=\textstyle\sum_{x\in G}x=(x_1+1)(x_2+1)(x_3+1)(x_4+1)(x_5+1),\\
\gamma_1&=\textstyle\sum_{x\in G_1}x=(x_2+1)(x_3+1)(x_4+1)(x_5+1),\\
\gamma_2&=\textstyle\sum_{x\in G_2}x=(x_1+1)(x_3+1)(x_4+1)(x_5+1),\\
\gamma_3&=\textstyle\sum_{x\in G_3}x=(x_1+1)(x_2+1)(x_4+1)(x_5+1),\\
\gamma_4&=\textstyle\sum_{x\in G_4}x=(x_1+1)(x_2+1)(x_3+1)(x_5+1),\\
\gamma_5&=\textstyle\sum_{x\in G_5}x=(x_1+1)(x_2+1)(x_3+1)(x_4+1).
\end{aligned}$$

Dla sprawdzenia, czy dany element $\alpha$ algebry reprezentuje słowo kodowe, wystarczy sprawdzić, czy jest anihilowane przez elementy postaci $(x_i+1)(x_j+1)$, $i<j$. Jeśli $\alpha$ reprezentuje słowo kodowe, tzn.

$$\alpha = a_0\gamma_0 + a_1\gamma_1 + a_2\gamma_2 + a_3\gamma_3 + a_4\gamma_4 + a_5\gamma_6,$$

to dla $i = 1,2,3,4,5$, zachodzi równość $\alpha\cdot(x_i+1) = a_i\gamma_0$, co automatycznie wyznacza skalary $a_1,a_2,a_3,a_4$. To z kolei pozwala wyznaczyć $a_0$.

Załóżmy teraz, że w wyniku transmisji danych, po wysłaniu słowa reprezentowanego przez element $\alpha$ otrzymano słowo reprezentowane przez $\beta$. Z własności kodu wiadomo, że koryguje błędy, jeśli ich liczba nie przekracza liczby 7. Jeśli więc słowo $\beta$ różni się od $\alpha$ na nie więcej niż 7 pozycjach, to $\alpha = \beta+\varepsilon$, gdzie $\varepsilon$ ma wagę Hamminga nieprzekraczającą tej liczby. To oznacza, że każde ze słów reprezentowanych przez $\varepsilon\cdot(x_i+1)$ ma wagę Hamminga nie przekraczającą liczby 14. Dla wyznaczenia wysłanego słowa $\alpha$ na podstawie $\beta$ i przedstawienia go w postaci kombinacji liniowej elementów $\gamma_i$, $i = 0,1,2,3,4,5$ wystarczy zauważyć, że

$$\begin{aligned}\beta(x_i+1) &= (\alpha+\varepsilon)(x_i+1)\\ &= \alpha(x_i+1)+\varepsilon(x_i+1)\\ &= a_i\gamma_0+\varepsilon(x_i+1).\end{aligned}$$

Wobec tego, że $\mathrm{wt}(\gamma_0) = 32$ i $\mathrm{wt}(\varepsilon(x_i+1)) \leqslant 14$, $a_i = 0$ wtedy i tylko wtedy, gdy $\mathrm{wt}(\beta(x_i+1)) \leqslant 14$. Ta obserwacja pozwala wyznaczyć współczynniki $a_1,a_2,a_3,a_4$. Do wyznaczenia $a_0$ wystarczy zauważyć, że $a_0 = 0$ wtedy i tylko wtedy, gdy waga Hamminga elementu $a_1\gamma_1+a_2\gamma_2+a_3\gamma_3+a_4\gamma_4+a_5\gamma_5+\beta$ nie przekracza 7.

## Podsumowanie

Czytelnika zainteresowanego tym obszarem badawczym odsyłamy do dwóch publikacji przeglądowych, a mianowicie Milies (2019) oraz Guerreiro (2016). Obie cytują po kilkadziesiąt artykułów, w większości opublikowanych po roku 2000. Liczne, szczegółowe wyniki przywoływane w tych pracach, odnoszą się do przypadku, gdy charakterystyka ciała nie dzieli rzędu grupy, te zaś są albo abelowe, albo bliskie abelowym. Algebraiczny opis rozważanych kodów jest oparty na dobrze znanej strukturze półprostych algebr grupowych. Tymczasem, jak widzieliśmy w przykładach kodów Golay'a i Reeda-Müllera, bardzo obiecujące wyniki uzyskano wcześniej dla algebr modularnych, tzn. takich, gdy charakterystyka ciała dzieli rząd grupy, a nawet dla $p$-grup. Struktura algebr grupowych $p$-grup nad ciałami charakterystyki $p$ jest bardzo skomplikowana i daleko do uzyskania jej zadowalającego opisu, co może

być elementem zniechęcającym do poszukiwań w tych obszarach. Jednakże, wiele wiadomo dla bardzo konkretnych klas grup, które nie były badane pod kątem ich przydatności dla teorii kodowania. Dotyczy to w szczególności $p$-grup abelowych lub $p$-grup, które są w jakimś sensie bliskie abelowym. Na szczególną uwagę zasługuje zbadanie własności ideałów generowanych przez elementy centralne w algebrach grupowych 2-grup bliskim grupom dihedralnym (patrz Bagiński i Konovalov (2004) i Bagiński i Kurdics (2014)).

## Bibliografia


Bagiński, C., i Kurdics, J. (2014, January). On the center of the modular group algebra of a finite $p$-group. Journal of Algebra and Its Applications, 13(04), 1350127. doi: 10.1142/s0219498813501272

Bagiński, C., i Konovalov, A. (2004, July). On 2-groups of almost maximal class. Publicationes Mathematicae, 65.

Broche, O., i del Río, A. (2007). Wedderburn decomposition of finite group algebras. Finite Fields and Their Applications, 13(1), 71-79. doi: 10.1016/j.ffa.2005.08.002

Gap – groups, algorithms, and programming, version 4.11.1 [Computer software manual]. (2021).

Guerreiro, M. (2016, May). Group algebras and coding theory. São Paulo Journal of Mathematical Sciences, 10(2), 346–371. doi: 10.1007/s40863-016-0040-x

Hoffman, D. G., Wal, Leonard, D. A., Lidner, C. C., Phelps, K. T. i Rodger, C. A. (1991). Coding theory: The essentials. USA: Marcel Dekker, Inc.

Kobliz, N. (2006). Wykład z teorii liczb i kryptografii. Warszawa: WNT.

Landrock, P., i Manz, O. (1992, September). Classical codes as ideals in group algebras. Des. Codes Cryptography, 2(3), 273–285. doi: 10.1007/BF00141972

Milies, C. (2019, April). Group algebras and coding theory: a short survey. Revista Integración, 37, 153-166. doi: 10.18273/revint.v37n1-2019008

Olteanu, G., i del Río, A. (2009, May). An algorithm to compute the wedderburn decomposition of semisimple group algebras implemented in the gap package wedderga. J. Symb. Comput., 44(5), 507–516. doi: 10.1016/j.jsc.2007.07.019

Passman, D. S. (1977). The algebraic structure of group rings [Book]. Wiley New York.

Sehgal, S. K. (1978). Topics in group rings ( 50). Marcel Dekker Incorporated.

Wolfmann, J. (1991, May). A new construction of the binary golay code (24, 12, 8) using a group algebra over a finite field. Discrete Math., 31(3), 337–338. doi: 10.1016/0012-365X(80)90147-8