АЛГЕБРА 2

ЗОРАН ПЕТРОВИЋ

Предавања за школску 2014/15 годину

Групе

Дејства група

Започнимо ову лекцију следећом дефиницијом.

Дефиниција 1 Нека је G група и X непразан скуп. Под дејством групе G на скупу X подразумевамо хомоморфизам $\varphi: G \to S_X$.

Дакле, овај појам и није непознат читаоцима. Већ смо у претходној лекцији користили овакве хомоморфизме у појединим примерима. Постоји други, еквивалентан начин, задавања дејства групе на скупу.

Дефиниција 2 Нека је G група и X непразан скуп. Под дејством групе G на скупу X подразумевамо функцију $\Theta: G \times X \to X$ за коју важи:

а) $\Theta(e, x) = x$, за све $x \in X$;

б) $\Theta(g, \Theta(h, x)) = \Theta(gh, x)$ за све $x \in X$ и $g, h \in G$.

Није тешко уверити се да су ове дефиниције еквивалентне. Наиме, ако је $\varphi: G \to S_X$ задат хомоморфизам, функцију $\Theta: G \times X \to X$, која задовољава тражене услове задајемо са

$$\Theta(g, x) := \varphi(g)(x).$$

Како је φ хомоморфизам, то је $\varphi(e) = id_X$, па је

$$\Theta(e, x) = \varphi(e)(x) = id_X(x) = x.$$

Такође је

$$\Theta(gh, x) = \varphi(gh)(x) = (\varphi(g) \circ \varphi(h))(x) = \varphi(g)(\varphi(h)(x)) =$$

$$= \varphi(g)(\Theta(h, x)) = \Theta(g, \Theta(h, x)).$$

Обратно, ако је задата функција $\Theta: G \times X \to X$, која има наведена својства, хомоморфизам $\varphi: G \to S_X$ дефинише се са

$$\varphi(g)(x) := \Theta(g, x).$$

Остављамо читаоцима да провере да је тако заиста добијен један хомоморфизам $\varphi: G \to S_X$.

Уместо $\Theta(g, x)$ често ћемо писати $g \cdot x$. Својства функције Θ се тада записују овако:

а) $e \cdot x = x$, за све $x \in X$;

б) $(gh) \cdot x = g \cdot (h \cdot x)$, за све $g, h \in G$ и $x \in X$.

Наравно, не треба „мешати“ ову ознаку са ознаком операције у групи G (операцију у групи често нећемо ни писати, као што смо и до сада радили у многим случајевима). У вези са дејством групе појављују се два значајна појма.

Дефиниција 3 Нека група G дејствује на непразном скупу X. Орбита елемента $x \in X$, у ознаци $\Omega(x)$, дефинише се са:

$$\Omega(x) := \{g \cdot x : g \in G\}.$$

Стабилизатор елемента $x \in X$, у ознаци G_x, дефинише се са:

$$G_x := \{g \in G : g \cdot x = x\}.$$

Наведимо неке примере дејства групе на скупу.

Пример 4 Нека је $X = \mathbb{R}^2$, а $G = \mathbb{Z}_2$. Тада је дејство групе G на скупу X задато са:

$$0 \cdot (x_1, x_2) = (x_1, x_2), \quad 1 \cdot (x_1, x_2) = (-x_1, -x_2).$$

Орбита елемента $(x_1, x_2) \in \mathbb{R}^2$ је

$$\Omega(((x_1, x_2)) = \{(x_1, x_2), (-x_1, -x_2)\}.$$

Приметимо да је једино орбита елемента $(0, 0)$ једночлана, док су све остале двочлане. ♣

Пример 5 Нека је $X = \mathbb{C}$, а $G = \mathbb{C}_n$ (где је $n \geq 2$). Тада је дејство групе G на X задато са:

$$g \cdot x := gx.$$

Подсетимо се да је $\mathbb{C}_n = \{z \in \mathbb{C} : z^n = 1\}$. Дакле, $\mathbb{C}_n \subseteq \mathbb{C}$ и наведено дејство заиста јесте дефинисано. Орбита сваког комплексног броја $z \neq 0$ је

$$\Omega(z) = \left\{ e^{\frac{2k\pi i}{n}} z : 0 \leq k < n \right\},$$

док је

$$\Omega(0) = \{0\}.$$

Дакле, свака орбита има или n елемената, или 1 елемент. ♣

Пример 6 Нека је G произвољна група и H нека њена подгрупа. Тада је задато дејство G на G/H са:

$$g \cdot (aH) := (ga)H.$$

У овом случају орбита ма ког елемента једнака је целом скупу X. За дејство које има само једну орбиту кажемо да је транзитивно. ♣

Пример 7 Нека је G произвољна група и H нека њена подгрупа. Дејство групе H на скупу G задато је са:

$$h \cdot x := hx.$$

Јасно је да је орбита елемента $x \in G$ једнака десном косету Hx. ♣

Пример 8 Нека је G било која група и $X = G$. Дејство G на G задато је са:

$$g \cdot x = gxg^{-1}.$$

Приметимо да се у овом случају орбите поклапају са класама конјугације, док се стабилизатори елемената из G поклапају са централизаторима тих елемената. ♣

Већ је из дефиниције, а посебно из ових примера, јасно да се природно може увести релација еквиваленције на скупу на коме дејствује нека група тако да се класе еквиваленције поклапају са орбитама. Између осталог добијамо да је X дисјунктна унија различитих орбита.

Следећи став повезује орбиту неког елемента и његов стабилизатор.

Став 9 Нека је X непразан скуп и нека група G дејствује на X. Тада је $G_x \leq G$ за свако $x \in X$. Осим тога, постоји бијекција између G/G_x и $\Omega(x)$.

Доказ. Како је $e \cdot x = x$, видимо да $e \in G_x$. Уколико $g \in G_x$, то је $g \cdot x = x$. Тада је и

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x,$$

па закључујемо да и g^{-1} припада стабилизатору елемента x. Ако су $g, h \in G_x$, то је

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x,$$

па $gh \in G_x$. Тако смо показали да је $G_x \leq G$.

Бијекцију $f \colon G/G_x \to \Omega(x)$ задајемо са

$$f(g\,G_x) := g \cdot x.$$

Проверимо најпре добру дефинисаност функције f.

$$\begin{aligned} g\,G_x = h\,G_x &\implies h^{-1}g \in G_x \\ &\implies (h^{-1}g) \cdot x = x \\ &\implies h^{-1} \cdot (g \cdot x) = x \\ &\implies h \cdot (h^{-1} \cdot (g \cdot x)) = h \cdot x \\ &\implies (hh^{-1}) \cdot (g \cdot x) = h \cdot x \\ &\implies e \cdot (g \cdot x) = h \cdot x \\ &\implies g \cdot x = h \cdot x. \end{aligned}$$

Јасно је да је f „на“. Остаје само да се провери да је f „1–1“.

$$g \cdot x = h \cdot x \implies h^{-1} \cdot (g \cdot x) = h^{-1} \cdot (h \cdot x)$$

$$
\begin{aligned}
&\implies (h^{-1}g)\cdot x = (h^{-1}h)\cdot x\\
&\implies (h^{-1}g)\cdot x = e\cdot x\\
&\implies (h^{-1}g)\cdot x = x\\
&\implies h^{-1}g \in G_x\\
&\implies g\,G_x = h\,G_x.
\end{aligned}
$$

□

Применом овог резултата у случају коначне групе, добијамо следећу последицу.

Последица 10 Уколико коначна група G дејствује на непразном скупу X, онда ред орбите ма ког елемента дели ред групе G. □

Искористимо до сада добијене резултате за доказ Кошијеве теореме.

Доказ Кошијеве теореме. Дакле, нека је G коначна група и p прост број који дели ред групе G. Треба доказати да у G постоји елемент реда p. У ту сврху, нека је $H = \langle a\rangle$ нека циклична група реда p и

$$X = \{(x_1, x_2, \ldots, x_p) \in G^p : x_1x_2\cdots x_p = e\}.$$

Приметимо пре свега да је $|X| = |G|^{p-1}$. Наиме, $x_1, \ldots, x_{p-1}$ могу бити ма који елементи групе G, а тада је $x_p = (x_1\cdots x_{p-1})^{-1}$. Стога $p \mid |X|$. Дејство групе H на X задато је са:

$$a\cdot(x_1, x_2, \ldots, x_p) := (x_2, \ldots, x_p, x_1).$$

Дакле, дејство одговара цикличном пермутовању дате p-торке. Приметимо да је довољно задати дејство генератора пошто је H циклична група (зашто?). Како ред орбите ма ког елемента дели ред групе H, закључујемо да је ред ма које орбите или 1 или p. Приметимо да је орбита елемента $(e, e, \ldots, e)$ једночлана. Како је X дисјунктна унија различитих орбита, тј.

$$X = \Omega_1 \sqcup \Omega_2 \sqcup \cdots \sqcup \Omega_k,$$

за неке орбите $\Omega_1, \ldots, \Omega_k$, и како постоји бар једна једночлана орбита закључујемо да мора постојати бар још једна таква. Наиме, уколико је нпр. Ω_1 једина једночлана орбита, добили бисмо једнакост

$$|G|^{p-1} = 1 + p(k-1).$$

Но, ово није могуће пошто $p \mid |G|$. Нека је $\Omega_2 = \{(x_1, x_2, \ldots, x_p)\}$ једночлана орбита различита од $\{(e, e, \ldots, e)\}$. Тада мора бити

$$a\cdot(x_1, x_2, \ldots, x_p) = (x_1, x_2, \ldots, x_p),$$

тј.

$$(x_2, \ldots, x_p, x_1) = (x_1, x_2, \ldots, x_p).$$

Добијамо да је $x_1 = x_2 = \cdots = x_p$. Означимо тај елемент са g. По претпоставци, $g \neq e$, а осим тога, како $(g, g, \ldots, g) \in X$, мора бити $g^p = e$. Закључујемо да је g тражени елемент реда p. □

Видели смо да је број елемената у орбити неког елемента једнак индексу стабилизатора. Да ли постоји веза између стабилизатора два елемента из исте орбите? Важи следећи став.

Став 11 Нека група G дејствује скупу X. Ако су елементи x и y из исте орбите, онда су њихови стабилизатори конјуговане подгрупе.

Доказ. По претпоставци постоји елемент $g \in G$ такав да је $y = g \cdot x$. Покажимо да је

$$G_y = g\, G_x\, g^{-1}.$$

$\subseteq$: Нека је $h \in G_y$. Како је $y = g \cdot x$, то је $x = g^{-1} \cdot y$. Добијамо

$$(g^{-1}hg) \cdot x = g^{-1} \cdot (h \cdot (g \cdot x)) = g^{-1} \cdot (h \cdot y) = g^{-1} \cdot y = x.$$

Дакле, $g^{-1}hg \in G_x$, па $h \in g\, G_x\, g^{-1}$.

$\supseteq$: Нека је $h \in G_x$. Тада је

$$(ghg^{-1}) \cdot y = g \cdot (h \cdot (g^{-1} \cdot y)) = g \cdot (h \cdot x) = g \cdot x = y.$$

Дакле, $g\, G_x\, g^{-1} \subseteq G_y$. □

Нека G дејствује на X и нека је g елемент из G. Скуп свих фиксних тачака елемента g, у ознаци X^g задаје се са:

$$X^g := \{x \in X : g \cdot x = x\}.$$

Приметимо да важи следеће:

$$x \in X^g \iff g \in G_x.$$

Став 12 Нека G дејствује на X. Ако су елементи g и h конјуговани, онда постоји бијекција између скупова X^g и X^h.

Доказ. Нека је $g = khk^{-1}$. Дефинишимо функцију $f\colon X \to X$ са $f(x) = k \cdot x$. Покажимо да f успоставља бијекцију између X^h и X^g.

$$x \in X^h \Rightarrow h \cdot x = x \Rightarrow g \cdot f(x) = g \cdot (k \cdot x) = k \cdot (h \cdot (k^{-1} \cdot (k \cdot x)))$$

$$= k \cdot (h \cdot ((k^{-1}k) \cdot x)) = k \cdot (h \cdot (e \cdot x)) = k \cdot (h \cdot x) = k \cdot x = f(x).$$

Дакле, $f\left[X^h\right] \subseteq X^g$. Но, ако $y \in X^g$, није тешко проверити да $k^{-1} \cdot y \in X^h$ (проверите!), док је очигледно $f(k^{-1} \cdot y) = y$. Стога добијамо да f заиста успоставља тражену бијекцију. □

Формула која одређује број различитих орбита је веома корисна у разним применама. Дајемо је у оквиру наредне теореме.

Теорема 13 Нека коначна група G дејствује на коначном скупу X. Тада је број различитих орбита једнак броју

$$\frac{1}{|G|}\sum_{g\in G}|X^g|\,.$$

Доказ. Означимо тражени број различитих орбита са k. Дакле,

$$X=\Omega_1\sqcup\cdots\sqcup\Omega_k,$$

где су Ω_i различите орбите. Посматрајмо скуп E задат са

$$E=\{(g,x)\in G\times X : g\cdot x=x\}.$$

„Пребројаћемо“ елементе у E на два начина. Приметимо најпре да је

$$E=\bigsqcup_{g\in G}\{g\}\times X^g.$$

Дакле,

$$|E|=\sum_{g\in G}|X^g|\,. \tag{1}$$

С друге стране,

$$E=\bigsqcup_{x\in X}G_x\times\{x\}.$$

Према томе,

$$|E|=\sum_{x\in X}G_x=\sum_{i=1}^{k}\sum_{x\in\Omega_i}|G_x|.$$

Како елементи из исте орбите имају конјуговане стабилизаторе, то је $|G_x|=|G_y|$ уколико су x и y у истој орбити. Изаберимо по један елемент x_i из сваке од орбита Ω_i. Добијамо

$$|E|=\sum_{i=1}^{k}\sum_{x\in\Omega_i}|G_{x_i}|=\sum_{i=1}^{k}|\Omega_i||G_{x_i}|=\sum_{i=1}^{k}[G:G_{x_i}]|G_{x_i}|=\sum_{i=1}^{k}|G|=k|G|. \tag{2}$$

Из (1) и (2) тражени резултат следи. □

За крај наводимо један пример примене управо доказане формуле.

Пример 14 Темена, средишта ивица и тежишта страна правилног тетраедра треба обележети коришћењем три боје. Показати да има укупно 400707 начина на који се то може извести.

Ово заправо уопште није тешко показати, ма колико то у почетку изгледало. Размотримо најпре проблем мало пажљивије. Рецимо да желимо да темена тетраедра обележимо са две боје, нпр. плавом и

црвеном, али тако да је једно теме обележено плавом бојом, а остала црвеном. Јасно је да је то могуће урадити на само један начин. Наиме, треба имати у виду да темена немају никакве додатне ознаке. Према томе, било које од њих обележимо плавом бојом, а онда сва остала црвеном. Ако бисмо наш тетраедар заротирали, добили бисмо само другачији распоред темена, али то је тај исти тетраедар!

Ево како ћемо поступити при решавању задатка. Означимо сва темена бројевима $1, 2, 3$ и 4. Означимо ивицу чија су крајња темена a и b са $[a, b]$ (при чему је $a < b$). На крају, означимо страну на којој су темена a, b и c са $[a, b, c]$ (при чему је $a < b < c$). Дакле, укупно имамо $4 + 6 + 4$ тачке које желимо да обележимо са три боје. Нека је X скуп свих могућих обележених тетраедара (са овако означеним теменима, ивицама и странама) са три боје као у условима примера. Видимо да је $|X| = 3^{14}$. То наравно није тражени одговор. Наиме, многи од ових обележених тетраедара са означеним теменима, ивицама и странама, заправо представљају један те исти обележени тетраедар, само посматран из различитих углова (да се тако изразимо).

У нашем поједностављеном примеру обележавања темена са две боје тако да је једно теме обележено плавом, а остала црвеном, добили бисмо 4 различита означена тетраедра (у зависности од тога које од означених темена смо обележили плавом бојом), а заправо постоји само једно бојење, пошто темена нису означена у поставци задатка. Сваки од овако обележених тетраедара се ротацијом може превести у било који други. Тако поступамо и при решавању постављеног задатка. Наиме, посматрамо дејство групе ротација тетраедра на скупу X и интересује нас број различитих орбита, пошто су тетраедри из исте орбите само различити положаји једног те истог обележеног тетраедра.

Група ротација правилног тетраедра је група A_4. По формули изведеној у претходној теореми, број различитих орбита је

$$\frac{1}{|A_4|} \sum_{\pi \in A_4} |X^\pi|.$$

Присетимо се да је $|X^g| = |X^h|$ уколико су елементи g и h конјуговани. Дакле, довољно је при примени горње формуле посматрати само по један елемент из сваке класе конјугације. Како су класе конјугације у групи A_4:

$$\{(123), (124), (134), (234)\};$$
$$\{(132), (142), (143), (243)\};$$
$$\{(12)(34), (13)(24), (14)(23)\};$$
$$\{(1)\},$$

то добијамо да је број различитих орбита једнак

$$\frac{1}{12}\left(|X^{(123)}| \cdot 4 + |X^{(132)}| \cdot 4 + |X^{(12)(34)}| \cdot 3 + |X^{(1)}| \cdot 1\right).$$

Одредимо $|X^{(123)}|$. Теме 4 може бити обележено било којом бојом. Ако је теме 1 обележено неком бојом, онда том бојом мора бити обележено и теме 2 и теме 3 пошто наведена ротација тетраедра преводи теме 1 у теме 2, теме 2 у теме 3, а теме 3 у теме 1, а ми посматрамо скуп фиксних тачака при дејству (123). Слично, ако је средиште ивице $[1,2]$ обележена неком бојом, онда том истом бојом мора бити обележено и средиште ивице $[2,3]$ и средиште ивице $[1,3]$. Исто то важи и за ивице $[1,4]$, $[2,4]$ и $[3,4]$. Тежиште стране $[1,2,3]$ може бити обележено ма којом бојом, али тежишта страна $[1,2,4]$, $[1,3,4]$ и $[2,3,4]$ морају бити обележена истом бојом. Добијамо да је

$$|X^{(123)}| = \underbrace{3}_{\text{теме } 4} \cdot \underbrace{3}_{\text{темена } 1,2,3} \cdot \underbrace{3}_{\text{ивице } [1,2],[1,3],[2,3]} \cdot \underbrace{3}_{\text{ивице } [1,4],[2,4],[3,4]} \cdot$$

$$\cdot \underbrace{3}_{\text{страна } [1,2,3]} \cdot \underbrace{3}_{\text{стране } [1,2,4],[1,3,4],[2,3,4]} = 3^6.$$

Потпуно аналогно добијамо да је $|X^{(132)}| = 3^6$. С обзиром да је $X^{(1)} = X$, одредимо још и $|X^{(12)(34)}|$. У овом случају, темена 1 и 2 морају бити обележена истом бојом, као и темена 3 и 4. Средиште ивице $[1,2]$, као и ивице $[3,4]$ може бити обележено ма којој бојом, док средишта ивица $[1,4]$ и $[2,3]$ морају бити обележена истом бојом, као и средишта ивица $[1,3]$ и $[2,4]$. Тежишта страна $[1,2,3]$ и $[1,2,4]$ морају бити обележена истом бојом, као и средишта страна $[1,3,4]$ и $[2,3,4]$. Добијамо да је

$$|X^{(12)(34)}| = \underbrace{3}_{\text{темена } 1,2} \cdot \underbrace{3}_{\text{темена } 3,4} \cdot \underbrace{3}_{\text{ивица } [1,2]} \cdot \underbrace{3}_{\text{ивица } [3,4]} \cdot$$

$$\cdot \underbrace{3}_{\text{ивице}[1,4],[2,3]} \cdot \underbrace{3}_{\text{ивице } [1,3],[2,4]} \cdot \underbrace{3}_{\text{стране } [1,2,3],[1,2,4]} \cdot \underbrace{3}_{\text{стране } [1,3,4],[2,3,4]} = 3^8.$$

Дакле, број различитих орбита је

$$\frac{1}{12}\left(3^6 \cdot 4 + 3^6 \cdot 4 + 3^8 \cdot 3 + 3^{14} \cdot 1\right) = 400707.$$

♣

Теореме Силова

Нека је G група и H нека њена подгрупа. Уочимо скуп X свих подгрупа од G конјугованих са H.

$$X = \{gHg^{-1} : g \in G\}.$$

На овом скупу G дејствује конјуговањем:

$$g \cdot (xHx^{-1}) := (gx)H(gx)^{-1}.$$

Јасно је да је ово дејство транзитивно (има само једну орбиту), док је стабилизатор подгрупе H подгрупа од G, која се зове нормализатор подгрупе H и означава са $N(H)$:

$$N(H) = \{g \in G : gHg^{-1} = H\}.$$

Својства нормализатора дата су у следећем ставу.

Став 15 1. $H \triangleleft N(H)$.

2. Ако је $K \leq G$ и $H \triangleleft K$, онда је $K \subseteq N(H)$.

3. Ако је $K \leq N(H)$, онда је $KH \leq G$, $H \triangleleft KH$ и $KH/H \cong K/(H \cap K)$.

Доказ. 1. Ово директно следи из дефиниције нормализатора.

2. Претпоставимо да је K подгрупа од G таква да је $H \triangleleft K$ и $k \in K$. Како је $H \triangleleft K$, то је $kHk^{-1} = H$, а то управо значи да је $k \in N(H)$. Дакле, $K \subseteq N(H)$.

3. Јасно је да $e \in KH$. Нека $x, y \in KH$. То значи да је $x = kh$ и $y = k_1h_1$, за неке $k, k_1 \in K$ и $h, h_1 \in H$. Тада је

$$x^{-1}y = (kh)^{-1}(k_1h_1) = h^{-1}k^{-1}k_1h_1.$$

Како је $zHz^{-1} = H$ за све $z \in K$, то значи да је и $Hz = zH$ за све $z \in K$. Посебно: $h^{-1}(k^{-1}k_1) = (k^{-1}k_1)h'$ за неки $h' \in H$. Стога је $x^{-1}y = (k^{-1}k_1)(h'h_1)$, па $x^{-1}y \in KH$. Закључујемо да је KH заиста подгрупа од G. Но, H је очигледно садржана у KH и лако је проверити да је H нормална подгрупа од KH. Нека $k \in K$ и $h \in H$. Тада:

$$\begin{aligned}(kh)H(kh)^{-1} &= k(hHh^{-1})k^{-1} \\ &= kHk^{-1} \text{ (јер је } hH = H = Hh^{-1}) \\ &= H \text{ (јер } k \in N(H)).\end{aligned}$$

Изоморфизам $KH/H \cong K/(H \cap K)$ доказује се на исти начин на који се доказује такав изоморфизам у доказу друге теореме о изоморфизму (ово је заправо једна општија формулација те теореме). □

Сваку коначну групу чији је ред степен простог броја p зовемо p-група. Сетимо се да смо раније доказали да свака нетривијална p група има нетривијалан центар. То ћемо користити у даљем раду.

Сада ћемо дати неке теореме које више говори о структури коначних група, но што су то дали досадашњи резултати. Подсетимо се Кошијеве теореме: уколико $p \mid |G|$, где је p прост број, онда у G постоји елемент реда p. Заправо можемо закључити доста више од тога о постојању p-подгрупа у групи G уколико p дели ред те групе.

Дефиниција 16 Нека је група G реда n. Уколико је $n = p^r m$, где p не дели m (дакле, уколико је p^r највећи степен броја p који дели ред групе G), онда подгрупу групе G реда p^r (уколико она постоји) зовемо Силовљевом p-подгрупом групе G.

Испоставља се да Силовљева p-подгрупа увек постоји. То је садржај следеће теореме.

Теорема 17 Нека је G коначна група. За сваки прост број p који дели ред групе G постоји Силовљева p-подгрупа те групе.

Доказ. Нека је p прост број и нека $p \mid |G|$. Уколико је $|G| = p$, резултат је тривијалан. Доказ изводимо индукцијом по $|G|$. Базу индукције смо урадили. Претпоставимо да је $|G| = n$ и да је тврђење тачно за све групе са мање од n елемената. Разматрамо два случаја.

1. У G постоји права подгрупа H чији индекс није дељив са p. Како је $|H| < |G|$, то постоји Силовљева p-подгрупа од H. Но, највећи степен од p који дели ред групе G исти је као и највећи степен од p који дели $|H|$: $|G| = |H|[G : H]$, а p не дели $[G : H]$. Стога је Силовљева p-подгрупа од H заправо и Силовљева p-подгрупа од G. Дакле, у овом случају она постоји.

2. Претпоставимо сада да p дели индекс сваке праве подгрупе од G. Уколико G дејствује на самој себи конјуговањем, онда су орбите при том дејству класе коњугованости елемената из G, а унија једночланих орбита једнака је центру те групе (подсетите се доказа нетривијалности центра p-групе, који је урађен у Алгебри 1):

$$|G| = |Z(G)| + |C_1| + \cdots + |C_k|,$$

при чему је $C_i = \Omega(x_i) = [G : G_{x_i}]$. Како p по претпоставци дели индекс сваке праве подгрупе, добијамо да $p \mid |C_i|$ за све i. Закључујемо да $p \mid |Z(G)|$ (посебно: $Z(G) \neq \{e\}$). Према Кошијевој теореми, у $Z(G)$ постоји елемент реда p. Означимо га са x. Подгрупа $H = \langle x \rangle$ је нормална у G пошто $x \in Z(G)$, па комутира са свим елементима из G. Тада је $|G/H| = \frac{n}{p} < n = |G|$. По индуктивној хипотези у G/H постоји Силовљева p-подгрупа. Означимо је са K'. Уочимо канонски епиморфизам $\pi : G \to G/H$, $\pi(g) = gH$. Није тешко проверити да је $K = \pi^{-1}[K']$ подгрупа од G (проверите!). Но, K садржи H (зашто?) и заправо је $K/H = K'$ (уколико K/H видимо као подскуп од G/H). Стога је $|K| = p|K'|$ и како је и $|G| = p|G/H|$, а K' је Силовљева p-подгрупа од G/H, то је K Силовљева p-подгрупа од G. □

Напомена 1. У овом доказу смо користили Кошијеву теорему. Но, заправо смо могли и без ње. Наиме, једино нам је био потребан резултат да свака коначна Абелова група чији је ред дељив са p (радило се о центру групе G) садржи елемент реда p. А та се чињеница лако доказује помоћу класификације коначних Абелових група, коју смо урадили у Алгебри 1.

Дакле, показали смо да Силовљеве p-подгрупе увек постоје. Пре него што наставимо, докажимо једну техничку лему.

Лема 18 Нека p-група H дејствује на коначном скупу X. Тада је

$$|X^G| \equiv |X| \pmod{p},$$

где је са X^G означен скуп фиксних тачака од G:

$$X^G := \{x \in X : (\forall g \in G)(g \cdot x = x)\}.$$

Доказ. Како је ред орбите једнак индексу стабилизатора елемента те орбите, и како је група која дејствује једна p-група, то је број елемената у свакој неједночланој орбити дељив са p. Унија једночланих орбита је заправо скуп фиксних тачака X^G. Дакле,

$$|X| = |X^G| + |\Omega_1| + \cdots + |\Omega_k|$$

. где $p \mid |\Omega_i|$ за све $i = \overline{1,k}$. Следи да је $|X| - |X^G|$ заиста дељиво са p.□

Теорема 19 Нека је G коначна група.

1. Свака p-подгрупа од G садржана је у некој Силовљевој p-подгрупи од G.
2. Све Силовљеве p-подгрупе од G су међусобно конјуговане.
3. Број Силовљевих p-подгрупа од G конгруентан је са 1 по модулу p.
4. Број Силовљевих подгрупа дели ред групе G.

Доказ. 1. Нека је H нека p-подгрупа од G и P Силовљева p-подгрупа. Размотримо најпре случај када је $H \subseteq N(P)$. Према доказаном ставу добијамо да је HP подгрупа од G (заправо је HP подгрупа од $N(P)$ – размислите зашто) и $[HP : P] = [H : H \cap P]$. Уколико је $[H : H \cap P] \neq 1$, с обзиром да је H једна p-подгрупа, добијамо да је и HP једна p-подгрупа и да је $|HP| > |P|$, што није могуће с обзиром да је P Силовљева p-подгрупа. Закључујемо да је $[H : H \cap P] = 1$, те је $H = H \cap P$, па је $H \subseteq P$. Дакле, у овом случају смо добили тражени резултат.

Посматрамо сада скуп S свих конјугата од P. Нека G дејствује на S конјуговањем. Добијамо да је $|S| = [G : N(P)]$ (погледајте почетак предавања и присетите се да је број елемената у орбити индекс стабилизатора). Како је $P \subseteq N(P)$ и P је Силовљева p-подгрупа, то $[G : N(P)]$ није дељиво са P (уколико $H \subseteq K \subseteq G$, то је $[G : H] = [G : K] \cdot [K : H]$ за коначну групу G и њене подгрупе K и H – доказ касније!), те ни $|S|$ није дељиво са p.

Нека сада H дејствује на S конјуговањем. На основу леме, $|S| \equiv |S^H| \pmod{p}$. Како p не дели $|S|$, то p не дели ни $|S^H|$. То посебно значи да $S^H \neq \emptyset$. Нека је $Q \in S^H$. То значи да је $hQh^{-1} = Q$, па је $H \subseteq N(Q)$. На основу првог дела доказа, закључујемо да је $H \subseteq Q$. Како је Q подгрупа конјугована подгрупи P, она је и сама Силовљева p-подгрупа (има исти број елемената као и P), а то значи да је заиста p-подгрупа H садржана у некој Силовљевој p-подгрупи Q.

2. Ово смо заправо већ доказали. Наиме, ако у претходном доказу за H узмемо неку Силовљеву p-подгрупу, видимо да смо доказали да

је $H \subseteq Q(= xPx^{-1})$. Како је $|H| = |P|$, то добијамо да је $H = xPx^{-1}$. Дакле, S је заправо скуп свих Силовљевих p-подгрупа.

3. Нека је поново H нека Силовљева p-подгрупа, која дејствује на S конјугованьем. Свакако $H \in S^H$. Претпоставимо да $K \in S^H$. То значи да је $hKh^{-1} = K$ за све $k \in H$, па је $H \subseteq N(K)$. На основу првог дела доказа добијамо да је $H \subseteq K$, па мора бити $H = K$. Дакле, $S^H = \{H\}$. Тада, помоћу леме, добијамо да је $|S| \equiv 1 \pmod{p}$ што и завршава доказ.

4. Број Силовљевих подгрупа једнак је индексу нормализатора било које од њих, те стога дели ред групе G. □

Напомена 2. У доказу смо користили следећи резултат. Ако је K подгрупа од H коначног индекса $[H : K]$ и H подгрупа од G коначног индекса $[G : H]$, онда је

$$[G : K] = [G : H] \cdot [H : K].$$

Докажимо га.

Пре свега, нека је $[G : H] = m$ и $[H : K] = n$. Показаћемо да је $[G : K] = mn$. Како је $[G : H] = m$, то постоје елементи $g_1, g_2, \ldots, g_m \in G$ такви да је

$$G = g_1H \sqcup g_2H \sqcup \ldots \sqcup g_mH. \tag{3}$$

Такође постоје и елементи $h_1, h_2, \ldots, h_n \in H$ за које је

$$H = h_1K \sqcup h_2K \sqcup \ldots \sqcup h_nK. \tag{4}$$

Заменом (4) у (3), добијамо

$$G = g_1h_1K \cup g_1h_2K \cup \ldots \cup g_1h_nK \cup \ldots \cup g_mh_1K \cup g_mh_2K \cup \ldots \cup g_mh_nK. \tag{5}$$

Ако покажемо да су скупови у наведеној унији различити (подсетимо се да су различити косети обавезно дисјунктни), доказ ће бити завршен. Но, заиста је тако. Наиме, претпоставимо да је

$$g_ih_jK = g_kh_lK, \tag{6}$$

за неке индексе i, j, k, l. Тада је и

$$g_ih_jKH = g_kh_lKH,$$

а како је $KH = H$ (зашто?), то мора бити

$$g_ih_jH = g_kh_lH,$$

па је

$$g_iH = g_kH.$$

Но, то је могуће једино ако је $i = k$. Множењем (6) слева са g_i^{-1} добијамо

$$h_jK = h_lK,$$

но то је могуће једино ако је $j = l$.

Напомена 3. Нека је $|G| = p^r m$, где p не дели m. Ако са s_p означимо број Силовљевих p-подгрупа, онда, на основу претходне теореме, знамо да је $s_p \equiv 1 \pmod{p}$ и да $s_p \mid |G|$. Но, из чињенице $s_p \equiv 1 \pmod{p}$ следи да $s_p \mid m$.

Решиве групе

Пажљив читалац би могао да примети да смо за сада доказали постојање Силовљевих p-подгрупа, као и подгрупа реда p (уколико прост број p дели ред групе G). Но, мада смо ми причали о свим p-подгрупама дате групе, ипак нисмо експлицитно показали да постоје p-подгрупе свих могућих редова. Нпр. ако је $|G| = p^5 m$, где p не дели m, ми знамо да у G постоје подгрупе реда p и реда p^5. Али, да ли заиста постоје подгрупе реда p^2, p^3 и p^4? Одговор је наравно потврдан, а доказаћемо и више од тога.

Пре свега, уведимо неке неопходне појмове.

За опадајући низ подгрупа

$$G = G_0 \supset G_1 \supset \cdots \supset G_m,$$

групе G кажемо да је нормалан низ уколико је $G_{i+1} \triangleleft G_i$ за све $i = \overline{0, m-1}$. Овај низ је Абелов уколико је нормалан и уколико је G_i/G_{i+1} Абелова група за све $i = \overline{0, m-1}$. Он је цикличан уколико је нормалан и уколико је G_i/G_{i+1} циклична група за све $i = \overline{0, m-1}$.

Дефиниција 20 Група G је решива уколико постоји Абелов низ

$$G = G_0 \supset G_1 \supset \cdots \supset G_m,$$

за који је $G_m = \{e\}$.

Приметимо да је решива група једна генерализација Абелове групе. Профињење низа

$$G = G_0 \supset G_1 \supset \cdots \supset G_m,$$

је низ који се добија „уметањем" нових подгрупа између већ постојећих у низу. Важи следећи став.

Став 21 Нека је G коначна група. Тада за сваки Абелов низ

$$G = G_0 \supset G_1 \supset \cdots \supset G_m,$$

постоји профињење, које је цикличан низ.

Доказ. Ово заправо није тешко доказати. Све се своди на следеће. Нека је G група и H њена нормална подгрупа тако да је G/H коначна комутативна група. Тада постоји цикличан низ подгрупа

$$G = G_0 \supset H_1 \supset \cdots \supset H_k = H. \qquad (*)$$

Уметањем оваквих низова између сваке две групе у почетном низу, добија се тражено циклично профињење.

Докажимо егзистенцију наведеног цикличног низа. Заправо доказујемо да постоји цикличан низ који почиње групом $G' = G/H$ и завршава се тривијалном групом. „Подизањем" овог низа до групе G завршавамо доказ. Радимо индукцијом по реду групе G'. Узмимо ма који елемент $x' \in G'$. Уколико је $G' = \langle x' \rangle$, доказ је готов. У супротном, група $G'/\langle x' \rangle$ је коначна комутативна група мањег реда од G'. По индуктивној претпоставци, постоји цикличан низ

$$G'/\langle x' \rangle = K_0'' \supset K_1'' \supset \cdots \supset K_l'',$$

при чему је $K_l' = \{\langle x' \rangle\}$ тривијална подгрупа од $G'/\langle x' \rangle$ (шта је неутрал у количничкој групи?). Налажењем инверзних слика подгрупа овог низа при канонском епиморфизму $p : G' \to G'/\langle x' \rangle$, добијамо нормалан низ

$$G/H = G' = K_0' \supset K_1' \supset \cdots \supset K_l', \qquad (**)$$

за који је $K_i'/K_{i+1}' \cong K_i''/K_{i+1}''$, а то су све цикличне групе. Наравно, група K_l' је циклична са генератором $x'(= xH)$. Налажењем инверзних слика при канонском епиморфизму $\pi : G \to G/H(= G')$ подгрупа у низу $(**)$ добијамо тражени цикличан низ $(*)$. □

Напомена. У овом доказу користимо следећи резултат: ако је $f\colon K \to L$ епиморфизам група и ако су L_1 и L_2 подгрупе од L при чему је $L_1 \triangleleft L_2$, онда је и $f^{-1}[L_1] \triangleleft f^{-1}[L_2]$ и $f^{-1}[L_2]/f^{-1}[L_1] \cong L_2/L_1$. Докажимо га.

Да бисмо поједноставили запис, уведимо ознаке $K_i = f^{-1}[L_i]$. Нека су $x \in K_2$ и $y \in K_1$ произвољни елементи. Треба проверити да $xyx^{-1} \in K_1 = f^{-1}[L_1]$. Но, $f(xyx^{-1}) = f(x)f(y)f(x)^{-1}$. Како $y \in K_1 = f^{-1}[L_1]$, то $f(y) \in L_1$, а како је $L_1 \triangleleft L_2$, то и $f(x)f(y)f(x)^{-1} \in L_1$, што је и требало показати. Приметимо да овде нисмо користили чињеницу да је f „на".

За доказ траженог изоморфизма $K_2/K_1 \cong L_2/L_1$, посматрајмо композицију рестрикције хомоморфизма f на K_2 и природног епиморфизма $p\colon L_2 \to L_2/L_1$:

$$K_2 \xrightarrow{f|_{K_2}} L_2 \xrightarrow{p} L_2/L_1.$$

Означимо је са g. Јасно је да је g „на" (пошто су оба хомоморфизма у композицији таква), док је такође лако проверити да је $\mathrm{Ker}(g) = K_1$. Прва теорема о изоморфизму завршава доказ. ◇

Следећи став разрешава претходно споменута неразјашњена питања.

Став 22 Свака p-група је решива.

Доказ. Нека је G једна p-група. Радимо индукцијом по реду групе. Свака p-група има нетривијалан центар. Група $G/Z(G)$ је такође p-група и њен ред је мањи од реда групе G. По индуктивној хипотези, постоји Абелов низ подгрупа

$$G/Z(G) = G_0' \supset G_1' \supset \cdots \supset G_m' = \{Z(G)\}.$$

Подизањем овог низа помоћу канонског епиморфизма добијамо Абелов низ

$$G = G_0 \supset G_1 \supset \cdots \supset G_m = Z(G).$$

Како је $Z(G)$ Абелова група, то можемо додати тривијалну групу на крај, што показује да је група G решива. □

Зашто овај став разрешава раније постављена питања? Како је свака p-група решива, то свака p-група има и цикличан низ. Но, свака циклична група има (тачно) једну подгрупу за сваки делилац реда те групе. То значи да заправо за сваку p-групу G постоји опадајући низ нормалних подгрупа

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset \{e\}.$$

при чему је G_i/G_{i+1} циклична група реда p (размислите зашто). Но, тада следи да, ако је $|G| = p^n$, онда је $|G_i| = p^{n-i}$, те у p-групи постоје подгрупе свих могућих редова. Резултат за произвољну коначну групу добијамо применом чињенице да Силовљева p-подгрупа увек постоји.

Следећи став је веома важан у применама теорије група на проблем решивости алгебарских једначина.

Став 23 Група $\mathbb{S}_n$ није решива ако је $n \geq 5$.

Доказ. Подсетимо се два позната резултата:

1. $[\mathbb{S}_n, \mathbb{S}_n] = A_n$
2. Ако је H нормална подгрупа групе G и G/H комутативна, онда је $[G, G] \subseteq H$.

Претпоставимо да је $n \geq 5$ и да је $\mathbb{S}_n$ решива група. Посебно, то значи да постоји нормална подгрупа H од $\mathbb{S}_n$ таква да је $\mathbb{S}_n/H$ Абелова. Но, према 2. то значи да $[S_n, S_n] \subseteq H$, а према 1. да је $A_n \subseteq H$. Дакле, ако је $\mathbb{S}_n/H$ нетривијална, мора бити $H = A_n$.

Докажимо да је за $n \geq 5$: $[A_n, A_n] = A_n$. Ово заправо није тешко доказати. Наиме,

$$(abc)(cde)(abc)^{-1}(cde)^{-1} = (adc),$$

где су a, b, c, d, e међусобно различити. Дакле, сваки 3-цикл можемо добити као комутатор нека друга два 3-цикла, па, како је A_n генерисано 3-циклима, добијамо да је $[A_n, A_n] = A_n$.

Сада је јасно зашто $\mathbb{S}_n$ не може бити решива. Наиме, Абелов низ почиње са: $\mathbb{S}_n \supset A_n$ и поставља се питање како га наставити. Ако је K нормална подгрупа од A_n таква да је A_n/K Абелова група, онда $[A_n, A_n] \subseteq K$, но, како је $[A_n, A_n] = A_n$, то мора бити $K = A_n$ и не можемо наставити наш низ. Како A_n није комутативна, добијамо да $\mathbb{S}_n$ није решива група. □

Групе $\mathbb{S}_n$ за $n \leq 4$ јесу решиве. Уколико је $n = 4$, онда је Абелов низ дат са: $\mathbb{S}_4 \supset A_4 \supset V \supset \{(1)\}$, пошто је Клајнова група V Абелова. Остали случајеви су још лакши. Чињеница да су ове групе решиве омогућава решавање једначина другог, трећег и четвртог степена „у радикалима“, али то је прича за касније.

Урадимо за крај неколико примера.

Пример 24 Свака група реда pq, где су p и q прости бројеви, је решива.

Решење. Наравно, једино је занимљив случај када је $p \neq q$ (зашто?). Но, и он је лак. Нека је $|G| = pq$ и $p < q$. На основу Кошијеве теореме, у групи G постоји елемент x реда q. Ако је H подгрупа генерисана са x, онда је $[G : H] = p$, а како је p најмањи прост број који дели ред групе G, H мора бити нормална. Стога Абелов (заправо и цикличан) низ: $G \supset H \supset \{e\}$ показује да је група G решива. ♣

Пример 25 Свака група реда p^2q, где су p и q прости бројеви, је решива.

Решење. И овде имамо нешто ново само ако је $p \neq q$.

1. $p > q$. Ако са s_p означимо број Силовљевих p-подгрупа од G, онда знамо да је $s_p \equiv 1 \pmod{p}$ и да $s_p \mid q$. Но, ако је $s_p = q$, онда $p \mid (q-1)$, што није могуће, јер је $p > q$. Стога је $s_p = 1$ и једина Силовљева p-подгрупа је нормална. Ако је означимо са H, добијамо Абелов низ: $G \supset H \supset \{e\}$. Наиме, G/H је реда q, па је циклична, а H је, као група реда p^2 комутативна.

2. $p < q$. Знамо да је $s_q \equiv 1 \pmod{q}$ и да $s_q \mid p^2$. Уколико је $s_q = 1$, поступамо као у претходном случају. Претпоставимо да је $s_q \neq 1$.

а) $s_q = p$. Тада $q \mid (p-1)$, што није могуће, јер је $q > p$.

б) $s_q = p^2$. То значи да $q \mid (p^2-1)$, тј. $q \mid (p-1)(p+1)$. Како је q прост број, то $q \mid (p-1)$, или $q \mid (p+1)$. Пошто је $q > p$, мора бити $q \mid (p+1)$, али и то је могуће једино у случају да је $q = p+1$. С обзиром да су p и q прости бројеви, мора бити $p = 2$, $q = 3$. Дакле, наша група G је реда 12. Осим тога, $s_3 = 4$. Уколико је $s_2 = 1$, добијамо Абелов низ, стога претпостављамо да је $s_2 = 3$. Нека су H_1, H_2, H_3, H_4 Силовљеве 3-подгрупе. Како је $H_i \cap H_j = \{e\}$, за $i \neq j$, то добијамо да је $|H_1 \cup H_2 \cup H_3 \cup H_4| = 4 \cdot 2 + 1 = 9$. Нека су K_1, K_2, K_3 Силовљеве

2-подгрупе. С обзиром да је $|K_i| = 4$, то у $K_1 \cup K_2$, сем неутрала, има бар још $4+4-2 = 6$ елемената. Тако смо добили да у нашој групи има бар 15 елемената. Како је она реда 12, то смо дошли до контрадикције и тиме је доказ завршен. ♣

Пример 26 Свака група реда $2pq$, где су p и q прости бројеви, је решива.

Решење. Јасно је да имамо нешто ново само уколико су p и q различити непарни прости бројеви. Нека је $p < q$.

Уколико је $s_p = 1$, или $s_q = 1$, све је јасно. Наиме, тада је једна од Силовљевих подгрупа нормална, те је и производ те Силовљеве подгрупе и Силовљеве подгрупе, која одговара другом простом броју такође подгрупа, а како је индекса 2, та подгрупа је нормална. Тако добијамо Абелов низ: $G \supset HK \supset H \supset \{e\}$ (где смо са H и K означили одговарајуће Силовљеве подгрупе). Дакле, у даљем претпостављамо да је $s_p \neq 1$ и $s_q \neq 1$. Како је $p < q$, мора бити $s_q = 2p$ (зашто?). Нека су $H_1, \ldots, H_{2p}$ Силовљеве q-подгрупе. У њиховом унији има (сем неутрала) $2p(q-1)$ елемената. Како је $s_p > 1$ по претпоставци, то има бар q Силовљевих p-подгрупа. Означимо их са $K_1, \ldots, K_q$. У њима сем неутрала има $q(p-1)$ елемената. Закључујемо да у унији $H_1 \cup \ldots \cup H_{2p} \cup K_1 \ldots \cup K_q$ има $2p(q-1)+q(p-1)+1$ елемената. Остављамо читаоцима за вежбу да докажу да је $2p(q-1)+q(p-1)+1 > 2pq$, те смо тако добили контрадикцију. ♣

Комутативни прстени са јединицом

Идеали и хомоморфизми

Као што у теорији група имамо појам подгрупе неке групе, тако и у теорији комутативних прстена са јединицом имамо појам потпрстена са јединицом.

Дефиниција 27 Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ комутативни прстени са јединицом при чему је $B \subseteq A$. Уколико је за све $x, y \in B$ испуњено:

$$x + y = x +' y, \quad x \cdot y = x \cdot' y$$

и $1_A = 1_B$, онда је B један потпрстен са јединицом прстена A.

Приметимо да такође важи и $0_A = 0_B$, но та се чињеница може извести из преосталих, што није тачно за једнакост $1_A = 1_B$. На пример, нека је $A = \{(0,0), (0,1), (1,0), (1,1)\}$ и $B = \{(0,0), (1,0)\}$, где су операције дефинисане по координатама, а на свакој координати су сабирање, односно множење по модулу 2. Тада B јесте комутативан прстен са јединицом, но јединица у B је елемент $(1,0)$, а јединица у A је $(1,1)$. Стога B није потпрстен са јединицом прстена A.

Важнији од појма потпрстена је појам идеала.

Дефиниција 28 Нека је A комутативан прстен са јединицом и I непразан подскуп од A. Тада је I идеал у A уколико

1. за све $x, y \in I$: $x + y \in I$;
2. за све $a \in A$ и $x \in I$: $a \cdot x \in I$.

Приметимо да $0 \in I$ за сваки идеал I. Наиме, како је I непразан, то постоји $x \in I$. Но, тада је и $0 = 0 \cdot x \in I$. Ознака $I \triangleleft A$ означава да је I идеал у A.

Са идеалима се могу вршити операције сабирања и множења као и са елементима.

Дефиниција 29 Нека су I и J идеали прстена A.

1. $I + J := \{x + y : x \in I, y \in J\}$;
2. $I \cdot J := \{x_1 y_1 + \cdots + x_n y_n : x_i \in I$ за све $i = \overline{1,n}, y_j \in J$ за све $j = \overline{1,n}$, и све $n \geq 1\}$.

Директна провера показује да су $I + J$ и $I \cdot J$ заиста идеали у прстену A. Идеал $I + J$ је најмањи идеал, који садржи (као своје подскупове) идеале I и J, док је $I \cdot J$ заправо најмањи идеал који садржи све могуће производе елемената из I са елементима из J.

Као и у случају подгрупа, пресек два идеала $I \cap J$ јесте идеал, док је њихова унија $I \cup J$ идеал ако и само ако је један од тих идеала садржан у другом. Заправо, ако посматрамо само операцију сабирања, приметимо да су идеали подгрупе групе $(A, +)$, а знамо да из чињенице да је унија две подгрупе подгрупа, следи да је једна од њих садржана у другој. Други смер се лако проверава.

Наведимо неке примере.

Пример 30 Ако је A комутативан прстен са јединицом и $a \in A$ произвољан елемент, онда је

$$\langle a \rangle := \{r \cdot a : r \in A\},$$

идеал. Овај идеал се назива главни идеал генерисан елементом a.

Како је $r \cdot a + s \cdot a = (r + s) \cdot a$, као и $s \cdot (r \cdot a) = (sr) \cdot a$, видимо да је $\langle a \rangle$ заиста идеал у прстену A. ♣

Пример 31 Сваки идеал у $\mathbb{Z}$ је облика $\langle m \rangle$ за неки природан број m.

Нека је $I \lhd \mathbb{Z}$. Како је $(I, +)$ подгрупа групе $(\mathbb{Z}, +)$, то на основу претходног знања о подгрупама групе $\mathbb{Z}$, добијамо да је $I = \langle m \rangle$. ♣

Напомена. Идеал $\langle m \rangle$ означава се и са $m\mathbb{Z}$ (скуп свих целобројних умножака броја m).

Пример 32 Нека су m и n позитивни цели бројеви. Одредити:

$$\langle m \rangle \cdot \langle n \rangle, \quad \langle m \rangle + \langle n \rangle, \quad \langle m \rangle \cap \langle n \rangle.$$

Пре свега, $\langle a \rangle \cdot \langle b \rangle = \langle ab \rangle$ важи у сваком прстену и за све елементе a и b (проверите!). Стога је $\langle m \rangle \cdot \langle n \rangle = \langle mn \rangle$. На основу дефиниције:

$$\langle m \rangle + \langle n \rangle = \{mx + ny : x, y \in \mathbb{Z}\}.$$

Како ми знамо да је $\langle m \rangle + \langle n \rangle$ сигурно главни идеал, потребно је само одредити који је његов генератор. Но, није потребно много размишљати о томе. Из горње једнакости се просто намеће да је

$$\langle m \rangle + \langle n \rangle = \langle d \rangle,$$

где је $d = \mathrm{NZD}(m, n)$. Пре свега, добро нам је познато да увек постоје $p, q \in \mathbb{Z}$ за које је $mp + nq = d$. Стога, $d \in \langle m \rangle + \langle n \rangle$, па мора бити и $\langle d \rangle \subseteq \langle m \rangle + \langle n \rangle$. Но, како $d \mid m$ и $d \mid n$, то постоје m_1 и n_1 такви да је $m = dm_1$ и $n = dn_1$. Уколико је $mx + ny$ произвољан елемент из $\langle m \rangle + \langle n \rangle$ добијамо:

$$mx + ny = dm_1x + dn_1y = d(m_1x + n_1y),$$

те закључујемо да $mx + ny \in \langle d \rangle$

Одредимо још и $\langle m \rangle \cap \langle n \rangle$. Приметимо да $x \in \langle m \rangle \cap \langle n \rangle$ ако и само ако $m \mid x$ и $n \mid x$. Но, то управо значи да је $\langle m \rangle \cap \langle n \rangle = \langle \mathrm{NZS}(m, n) \rangle$. ♣

Пример 33 У прстену $\mathbb{Z}[X]$ постоји идеал који није главни.

Посматрајмо идеал I генерисан са два елемента 2 и X, $I = \langle 2, X\rangle$ (ознака $\langle S\rangle$ означава најмањи идеал (који увек постоји јер је пресек ма које колекције идеала идеал) који садржи скуп S; у случају да је $S = \{x_1, \ldots, x_n\}$ пишемо $\langle x_1, \ldots, x_n\rangle$, уместо $\langle\{x_1, \ldots, x_n\}\rangle$). Овај идеал сигурно није главни. Наиме, претпоставимо да је

$$\langle 2, X\rangle = \langle a(X)\rangle,$$

за неки полином $a(X)$. Како је $2 \in \langle a(X)\rangle$, то мора бити $2 = a(X) \cdot b(X)$ за неки полином $b(X)$. То значи да је $a(X)$ константан полином. Но, из чињенице да $X \in \langle a(X)\rangle$, следи да $a(X) \mid X$, па мора бити $a(X) = 1$, или $a(X) = -1$. То би значило да је $1 = 2p(X) + Xq(X)$ за неке полиноме $p(X), q(X) \in \mathbb{Z}[X]$. Но, заменом 0 уместо X добијамо да је тада $1 = 2p(0)$, те би следило да $\frac{1}{2} \in \mathbb{Z}$. Закључујемо да наведени идеал није главни. ♣

Пример 34 Нека је K ма које поље. Тада је сваки идеал у прстену $K[X]$ главни.

У доказу ћемо користити чињеницу да за полиноме $a(X)$ и $b(X)$ из $K[X]$ за које је $b(X) \neq 0$ постоје и једнозначно су одређени полиноми, $q(X)$ и $r(X)$ такви да је

$$a(X) = q(X)b(X) + r(X), \quad r(X) = 0 \text{ или } \deg r(X) < \deg b(X).$$

Ово је познато еуклидско дељење полинома, или дељење са остатком, са којим смо упознати у средњој школи (додуше само за реалне, односно комплексне полиноме, али лако се види да се овакво дељење може извести у ма ком пољу).

Нека је $I \triangleleft K[X]$. Уколико је $I = \{0\}$, јасно је да је I главни идеал генерисан елементом 0. Претпоставимо стога да је $I \neq \{0\}$. Нека је μ моничан полином најмањег степена који се налази у I. Тај полином сигурно постоји пошто је I идеал. Докажимо да је $I = \langle\mu\rangle$. Посматрајмо произвољни елемент $a \in I$. На основу резултата наведеног горе, постоје полиноми q и r (читалац сигурно примећује да понекад полиноме означавамо са $a(X)$, а понекад и само са a, као и да производ два елемента у прстену понекад пишемо без ознаке операције множења) такви да је $a = q\mu + r$, при чему је степен полинома r мањи од степена полинома μ, или је $r = 0$. Како $a, \mu \in I$, добијамо да је $r = a - q\mu$ такође из I. Но, уколико је $r \neq 0$, множењем инверзом водећег коефицијента од r добили бисмо да се у I налази моничан полином степена мањег од степена полинома μ што противречи избору полинома μ. Закључујемо да мора бити $r = 0$, тј. да $\mu \mid a$, те да $a \in \langle\mu\rangle$, чиме је доказ завршен. ♣

Пример 35 Нека је K поље и $I \triangleleft K$. Тада је $I = \{0\}$, или је $I = K$.

Претпоставимо да је I идеал у K и да је $I \neq \{0\}$. То значи да идеал I садржи неки елемент $x \neq 0$. Уколико је a ма који елемент из K, добијамо да и a припада идеалу I. Наиме, како је I идеал, а $x \neq 0$, то постоји x^{-1} и елемент $(ax^{-1}) \cdot x$ мора припадати идеалу I, а јасно је да је тај елемент једнак елементу a. ♣

Пример 36 Нека је A ма који комутативан прстен са јединицом и $u \in U(A)$. Тада је $\langle u \rangle = A$.

Доказ се изводи на исти начин као у претходном примеру. ♣

Пређимо сада на појам хомоморфизма прстена.

Дефиниција 37 Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ два комутативна прстена са јединицом. Функција $f\colon A \to B$ је хомоморфизам прстена уколико је $f(1_A) = 1_B$ и уколико за све $x, y \in A$ важи:

$$f(x + y) = f(x) +' f(y) \quad \text{и} \quad f(x \cdot y) = f(x) \cdot' f(y).$$

Пример 38 Функција $\rho_n\colon \mathbb{Z} \to \mathbb{Z}_n$ задата са $\rho_n(x) := \rho(x, n)$, где је са $\rho(x, n)$ означен остатак при дељењу x са n, је један хомоморфизам прстена.

Овај хомоморфизам ћемо искористити да опишемо идеале у прстенима $\mathbb{Z}_n$, но пре тога ћемо навести неке опште резултате о хомоморфизмима.

Дефиниција 39 Нека је $f\colon A \to B$ хомоморфизам комутативних прстена са јединицом. Језгро хомоморфизма f, у ознаци $\mathrm{Ker}(f)$ дефинише се са:

$$\mathrm{Ker}(f) := \{x \in A : f(x) = 0_B\}.$$

Став 40 Нека је $f\colon A \to B$ хомоморфизам комутативних прстена са јединицом. Тада важи:

а) $\mathrm{Ker}(f) \lhd A$;

б) ако је $J \lhd B$ онда је $f^{-1}[J] \lhd A$;

в) ако је $I \lhd A$ и f „на“, онда је $f[I] \lhd B$.

Доказ.

а) Нека $x, y \in \mathrm{Ker}(f)$. Тада је

$$f(x + y) = f(x) +' f(y) = 0_B +' 0_B = 0_B,$$

па $x + y \in \mathrm{Ker}(f)$.

Уколико је $x \in \mathrm{Ker}(f)$ и $a \in A$:

$$f(a \cdot x) = f(a) \cdot' f(x) = f(a) \cdot' 0_B = 0_B,$$

те $a \cdot x \in \mathrm{Ker}(f)$.

б) Нека је J идеал у B и $x, y \in f^{-1}[J]$. То значи да је $f(x) \in J$ и $f(y) \in J$. Како је J идеал, закључујемо да и $f(x+y) = f(x) +' f(y) \in J$. Дакле, $x + y \in f^{-1}[J]$.

Такође, уколико је $x \in f^{-1}[J]$ и $a \in A$, добијамо да је $f(a \cdot x) = f(a) \cdot' f(x) \in J$, пошто $f(x) \in J$, а J је идеал.

в) Нека су $u, v \in f[I]$. То значи да је $u = f(x)$ и $v = f(y)$ за неке $x, y \in I$. Како је I идеал, то је $x + y \in I$, а како је $u +' v = f(x) +' f(y) = f(x+y)$, закључујемо да је $u +' v \in f[I]$.

Уколико је $u \in f[I]$, а $b \in B$, с обзиром да је по претпоставци f „на“, добијамо да постоји $a \in A$ тако да је $b = f(a)$. Осим тога је $u = f(x)$ за неко $x \in I$. Како је I идеал, $a \cdot x$ припада I, па је $b \cdot' u = f(a) \cdot f(x) = f(a \cdot x)$ из $f[I]$. □

Приметимо да је, као и у случају хомоморфизма група, $\mathrm{Ker}(f) = \{0\}$ ако и само ако је хомоморфизам инјективан.

У општем случају директна слика идеала не мора бити идеал. На пример, јасно је да функција $i\colon \mathbb{Z} \to \mathbb{Q}$ дефинисана са $i(x) = x$ за све $x \in \mathbb{Z}$, јесте хомоморфизам (то је инклузија прстена целих бројева у поље рационалних бројева). Но,

$$i[\langle 2 \rangle] = \{2m : m \in \mathbb{Z}\},$$

а то очигледно није идеал у $\mathbb{Q}$, пошто су, на основу раније доказаног, једини идеали у $\mathbb{Q}$: $\{0\}$ и $\mathbb{Q}$.

Пример 41 Нека је $n \geq 2$ цео број. Тада је сваки идеал у $\mathbb{Z}_n$ главни.

Искористићемо хомоморфизам $\rho_n\colon \mathbb{Z} \to \mathbb{Z}_n$, који је и „на“. Нека је $J \lhd \mathbb{Z}_n$. Тада је $\rho_n^{-1}[J] \lhd \mathbb{Z}$. На основу структуре идеала прстена $\mathbb{Z}$, знамо да постоји $m \geq 0$ такав да је $\rho_n^{-1}[J] = \langle m \rangle$. Но, тада је

$$J = \rho_n[\rho_n^{-1}[J]] = \rho_n[\langle m \rangle] = \langle \rho_n(m) \rangle.$$

Приметимо да једнакост $J = \rho_n[\rho_n^{-1}[J]]$ следи из чињенице да је ρ_n „на“, док је јасно да је $f[\langle a \rangle] = \langle f(a) \rangle$ за сваки епиморфизам (хомоморфизам који је „на“) f и сваки елемент a (покажите да је ово тачно!). ♣

Напомена. Можда је читалац приметио да смо овај резултат могли да докажемо као и у случају прстена целих бројева. Наиме, сваки идеал у $\mathbb{Z}_n$ је и подгрупа цикличне групе, па је тиме и сама циклична. А знамо како изгледају цикличне подгрупе групе $\mathbb{Z}_n$. У овом доказу само треба обратити пажњу на чињеницу да је свака подгрупа од $\mathbb{Z}_n$ заиста идеал (у случају прстена $\mathbb{Z}$, то је тривијално испуњено, пошто се множење елементима из $\mathbb{Z}$ заправо своди на сабирање (уз евентуално множење са -1 које одговара тражењу супротног елемента). Чињеница да је то испуњено и за $\mathbb{Z}_n$ захтева мали доказ. Размислите мало о томе.

Пример 42 Навести пример комутативног прстена са јединицом и подгрупе адитивне групе тог прстена, која није идеал.

Посматрамо прстен $A = \mathbb{Z}_2 \times \mathbb{Z}_2$. Овде су операције дефинисане по координатама и заправо је A директан производ прстена $\mathbb{Z}_2$ и $\mathbb{Z}_2$ (поновите појам директног производа алгебри). Скуп $\{(0,0),(1,1)\}$ је подгрупа адитивне групе тог прстена, али није идеал пошто елемент $(1,0)\cdot(1,1) = (1,0)$ не припада том скупу, а $(1,1)$ му припада. ♣

Пример 43 Наћи све идеале у прстену $\mathbb{Z}_{12}$.

Знамо да су сви идеали у овом прстену главни. Такође знамо да је сваки елемент у $\mathbb{Z}_{12}$ или делитељ нуле или инвертибилан. Како сваки инвертибилан елемент генерише, према једном од раније наведених примера, цео прстен, остаје да се види које идеале генеришу делитељи нуле. Приметимо да је $m \in Z_{12}$ делитељ нуле ако и само ако $2 \mid m$ или $3 \mid m$ (зашто?). Стога је

$$Z(\mathbb{Z}_{12}) = \{0,2,3,4,6,8,9,10\}.$$

Приметимо да, пошто је $5 \in U(\mathbb{Z}_{12})$ и $10 = 5 \cdot_{12} 2$ имамо да је $\langle 10\rangle = \langle 2\rangle$ (размислите како се ово може генерализати). Такође је $9 = -3 = (-1)\cdot 3$, па је и $\langle 9\rangle = \langle 3\rangle$. Добијамо да је и $\langle 8\rangle = \langle 4\rangle$.

С друге стране, $\langle 2\rangle \neq \langle 4\rangle$. Наиме, претпоставимо да $2 \in \langle 4\rangle$. Тада би постојао $m \in Z_{12}$ такав да је $2 = 4 \cdot_{12} m$. То би значило да постоји цео број q такав да је $2 = 4m + 12q$. Дељењем са 2 добили бисмо да је $1 = 2m + 6q$ за неке целе бројеве m и q што свакако није могуће. Како је очигледно $4 \in \langle 2\rangle$, то добијамо да је $\langle 4\rangle \subset \langle 2\rangle$ (идеал генерисан са 4 је прави подскуп идеала генерисаног са 2). На сличан начин се добија да је $\langle 6\rangle \subset \langle 3\rangle$. Читаоцима остављамо да се увере да су сви различити идеали прстена $\mathbb{Z}_{12}$ следећи:

$$\langle 0\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle, \mathbb{Z}_{12}.$$

Хомоморфизми и количнички прстени

Од сада претпостављамо да су сви идеали са којима радимо прави, тј. да нису једнаки целом прстену.

Дефиниција 44 Нека је $I \triangleleft A$. На A дефинишемо релацију конгруенције по модулу I са:

$$a \equiv b \pmod{I} \quad \textbf{акко} \quad a - b \in I.$$

Проверимо да је ова релација заиста конгруенција.

Рефлексивност. Како је $a - a = 0 \in I$, то је заиста $a \equiv a \pmod{I}$ за све $a \in A$.

Симетричност. Нека је $a \equiv b \pmod{I}$. То значи да $a - b \in I$, но, множењем са (-1) добијамо да и $b - a = (-1)(a - b)$ припада I.

Транзитивност. Нека је $a \equiv b \pmod{I}$ и $b \equiv c \pmod{I}$. Дакле, $a-b \in I$ и $b-c \in I$. Но, тада је и

$$a - c = (a - b) + (b - c) \in I.$$

Слагање са $+$. Нека је $a \equiv a' \pmod{I}$ и $b \equiv b' \pmod{I}$. Дакле, $a-a' \in I$ и $b-b' \in I$. Добијамо да је

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I.$$

Слагање са $\cdot$. Нека је $a \equiv a' \pmod{I}$ и $b \equiv b' \pmod{I}$. Дакле, $a-a' \in I$ и $b-b' \in I$. Добијамо да је

$$a \cdot b - a' \cdot b' = (a \cdot b - a' \cdot b) + (a' \cdot b - a' \cdot b') = (a - a') \cdot b + a' \cdot (b - b') \in I.$$

Приметимо да је класа еквиваленције елемента a заправо скуп

$$a + I = \{a + x : x \in I\}.$$

Скуп класа еквиваленције означавамо са A/I. На основу претходног добијамо да је структура $(A/I, +, \cdot)$ један комутативан прстен са јединицом где су операције $+$ и $\cdot$ дефинисане са:

$$(a + I) + (b + I) := (a + b) + I, \quad (a + I) \cdot (b + I) := (a \cdot b) + I.$$

Наравно да неке од ових заграда нећемо увек записивати.

Као и у случају група, важе и теореме о изоморфизмима за прстене. Навешћемо само прву.

Теорема 45 *(*Теорема о изоморфизмима за прстене*)* Нека је $f\colon A \to B$ хомоморфизам комутативних прстена са јединицом. Тада је $\tilde{f}\colon A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ задато са:

$$\tilde{f}(a + \mathrm{Ker}(f)) := f(a)$$

изоморфизам комутативних прстена са јединицом.

Доказ. Проверимо најпре да је $\tilde{f}$ добро дефинисано. У ту сврху, нека је $a+\mathrm{Ker}(f) = b+\mathrm{Ker}(f)$. То значи да $a-b \in \mathrm{Ker}(f)$, тј. да је $f(a) = f(b)$. Закључујемо да је $\tilde{f}$ заиста добро дефинисано.

Проверимо да је $\tilde{f}$ хомоморфизам.

$$\tilde{f}((a + \mathrm{Ker}(f)) + (b + \mathrm{Ker}(f))) = \tilde{f}((a + b) + \mathrm{Ker}(f)) = f(a + b) =$$

$$= f(a) + f(b) = \tilde{f}(a + \mathrm{Ker}(f)) + \tilde{f}(b + \mathrm{Ker}(f)).$$

$$\tilde{f}((a + \mathrm{Ker}(f)) \cdot (b + \mathrm{Ker}(f))) = \tilde{f}((a \cdot b) + \mathrm{Ker}(f)) = f(a \cdot b) =$$

$$= f(a) \cdot f(b) = \tilde{f}(a + \mathrm{Ker}(f)) \cdot \tilde{f}(b + \mathrm{Ker}(f)).$$

Јасно је да је $\tilde{f}$ „на“. Остаје да се провери да је $\tilde{f}$ „1–1“.

$$\begin{aligned}\tilde{f}(a+\mathrm{Ker}(f)) = \tilde{f}(b+\mathrm{Ker}(f)) &\implies f(a)=f(b)\\ &\implies f(a-b)=0\\ &\implies a-b\in\mathrm{Ker}(f)\\ &\implies a+\mathrm{Ker}(f)=b+\mathrm{Ker}(f).\end{aligned}$$

Проверимо још и да $\tilde{f}$ слика јединицу прстена у јединицу прстена:

$$\tilde{f}(1_A+\mathrm{Ker}(f)=f(1_A)=1_B.$$

Закључујемо да је $\tilde{f}$ заиста један изоморфизам комутативних прстена са јединицом. □

Пример 46 Нека је $I\triangleleft A$. Тада је $p\colon A\to A/I$ један епиморфизам. ♣

Пример 47 За све $n\geq 1$ важи: $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$.

Хомоморфизам $\rho_n\colon\mathbb{Z}\to\mathbb{Z}_n$, дат раније, је „на“, а осим тога $\mathrm{Ker}(\rho_n)=n\mathbb{Z}$, те резултат следи. ♣

Већ смо у претходној лекцији навели појам директног производа два прстена, а и познат нам је општи појам директног производа алгебри, но ипак дајмо и ту дефиницију.

Дефиниција 48 Нека су $(A_1,+^1,\cdot^1),\dots(A_n,+^n,\cdot^n)$ комутативни прстени са јединицом. На Декартовом производу

$$A=A_1\times\cdots\times A_n,$$

задајемо структуру комутативног прстена са јединицом са:

$$(a_1,\dots,a_n)+(b_1,\dots,b_n):=(a_1+^1b_1,\dots,a_n+^nb_n)$$

$$(a_1,\dots,a_n)\cdot(b_1,\dots,b_n):=(a_1\cdot^1b_1,\dots,a_n\cdot^nb_n)$$

Приметимо да је $0_A=(0_1,\dots,0_n)$ и $1_A=(1_1,\dots,1_n)$.

Став 49 Нека су $m_1,\dots,m_n$ позитивни цели бројеви за које важи: $\mathrm{NZD}(m_i,m_j)=1$ за све $i\neq j$. Тада је

$$\mathbb{Z}/(m_1\cdots m_n)\mathbb{Z}\cong(\mathbb{Z}/m_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/m_n\mathbb{Z}).$$

Доказ. Дефинишимо хомоморфизам

$$f\colon\mathbb{Z}\to(\mathbb{Z}/m_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/m_n\mathbb{Z})$$

са:

$$f(x)=(x+m_1\mathbb{Z},\dots,x+m_n\mathbb{Z}).$$

Остављамо читаоцима да провере да је f заиста хомоморфизам. Одредимо језгро овог хомоморфизма. Нека је $x \in \mathrm{Ker}(f)$. То значи да је $f(x) = (m_1\mathbb{Z}, \ldots, m_n\mathbb{Z})$, тј. то значи да $x \in m_1\mathbb{Z}$, $\ldots$, $x \in m_n\mathbb{Z}$. Дакле, у језгру се налазе они цели бројеви, који су дељиви свим бројевима $m_1, \ldots, m_n$. Како су m_i узајамно прости то језгро чине умношци од $m_1 \cdots m_n$, тј.

$$\mathrm{Ker}(f) = (m_1 \cdots m_n)\mathbb{Z}.$$

Добијамо да је

$$\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z} \cong \mathrm{Im}(f).$$

Но, како је $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$, то је

$$|\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z}| = m_1 \cdots m_n = |(\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})|.$$

Закључујемо да f мора бити „на“. Тиме смо добили тражени изоморфизам. □

Последица 50 *(*Кинеска теорема о остацима*)* Нека су $m_1, \ldots, m_n$ позитивни цели бројеви који су пар по пар узајамно прости и $x_1, \ldots, x_n$ произвољни цели бројеви. Тада постоји цео број x такав да је

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \\ &\cdots\cdots\cdots\cdots \\ x &\equiv x_n \pmod{m_n} \end{aligned}$$

Ако је x' неки други цео број који задовољава наведени систем конгруенција, онда је

$$x \equiv x' \pmod{m_1 \cdots m_n}.$$

Доказ. Посматрајмо елемент

$$(x_1 + m_1\mathbb{Z}, \ldots, x_n + m_n\mathbb{Z}) \in (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z}).$$

Како је хомоморфизам f, из доказа претходне теореме, „на“, то постоји $x \in \mathbb{Z}$ који се слика у наведени елемент, тј. постоји $x \in \mathbb{Z}$ за који је

$$x + m_1\mathbb{Z} = x_1 + m_1\mathbb{Z}, \quad \ldots \quad , x + m_n\mathbb{Z} = x_n + m_n\mathbb{Z},$$

но, то управо значи да је

$$x \equiv x_1 \pmod{m_1}, \quad \ldots \quad , x \equiv x_n \pmod{m_n}.$$

Уколико је x' други цео број који задовољава наведене конгруенције, то значи да је $f(x) = f(x')$, тј.

$$x - x' \in \mathrm{Ker}(f) = (m_1 \cdots m_n)\mathbb{Z},$$

као што је и тврђено. □

Заправо, у произвољном прстену важи одговарајућа теорема, коју такође називамо Кинеском теоремом о остацима. Потребна нам је најпре једна дефиниција.

Дефиниција 51 Идеали I и J комутативног прстена са јединицом A су копрости (узајамно прости) уколико је $I + J = A$.

Теорема 52 (Кинеска теорема о остацима) Нека су идеали $I_1, \ldots, I_n$ комутативног прстена са јединицом A пар по пар узајамно прости. Тада важи изоморфизам:

$$A/(I_1 \cap \ldots \cap I_n) \cong A/I_1 \times \cdots \times A/I_n.$$

Доказ. Доказ је нешто тежи него у случају прстема целих бројева. Посматрамо хомоморфизам $f\colon A \to A_1 \times \cdots \times A_n$ дефинисан са:

$$f(x) = (x + I_1, \ldots, x + I_n).$$

Није тешко проверити да је ова функција заиста један хомоморфизам (проверите то).

Јасно је да је језгро овог хомоморфизма пресек свих идеала. Једино треба проверити да је f „на".

Приметимо да важи следећи резултат. Ако су I и J копрости, а такође и I и K, онда су и I и JK такође копрости. Наиме, како су I и J копрости следи да је $I + J = A$. Посебно, постоји $x_1 \in I$ и $y \in J$ такви да је $x_1 + y = 1$. Слично, постоји $x_2 \in I$ и $z \in K$ тако да је $x_2 + z = 1$. Множењем ове две једнакости добијамо

$$(x_1x_2 + x_1z + x_2y) + yz = 1.$$

Како $x_1x_2 + x_1z + x_2y \in I$, а $yz \in JK$ (зашто?), то $1 \in I + JK$, те мора бити $I + JK = A$ (зашто?), па су I и JK узајамно прости. Из овог резултата следи да је за свако $i = \overline{1,n}$ испуњено:

$$I_i \text{ и } \prod_{j \neq i} I_j \text{ су копрости.}$$

Наравно са $\prod_{j\neq i} I_j$ смо означили производ свих идеала I_j за $j \neq i$.

Дакле, за $i = \overline{1,n}$, постоје $a_i \in I_i$ и $b_i \in \prod_{j\neq i} I_j$ такви да је $a_i + b_i = 1$. То посебно значи да је $b_i \equiv 1 \pmod{I_i}$ и $b_i \equiv 0 \pmod{I_j}$, за све $j \neq i$ (зашто?).

Докажимо сада да је f „на". Нека је $(x_1 + I_1, \ldots, x_n + I_n)$ произвољни елемент из $A/I_1 \times \cdots \times A/I_n$. Уочимо елемент $x = b_1x_1 + \cdots + b_nx_n$, где су b_i претходно изабрани елементи. Тада је, за све i:

$$x = b_1x_1 + \cdots + b_ix_i + \cdots + b_nx_n \equiv 0 \cdot x_1 + \cdots + 1 \cdot x_i + \cdots + 0 \cdot x_n \pmod{I_i}.$$

Дакле, за све $i = \overline{1,n}$: $x \equiv x_i \pmod{I_i}$, а то управо значи да је

$$f(x) = (x_1 + I_1, \ldots, x_n + I_n).$$

Закључујемо да је f заиста „на". □

Напомена. Приметимо да за копросте идеале I и J важи следећа једнакост: $I \cdot J = I \cap J$.

Доказ. Увек је $I \cdot J \subseteq I \cap J$ (зашто?). Дакле, потребно је доказати само обратну инклузију. Како су I и J копрости, то постоје $x \in I$ и $y \in J$ тако да важи $x + y = 1$. Нека је $z \in I \cap J$ произвољан елемент. Тада је

$$z = z \cdot 1 = z \cdot (x + y) = z \cdot x + z \cdot y.$$

Како $x \in I$ и $z \in J$, то је $z \cdot x \in I \cdot J$ (радимо са комутативним прстенима, па је $z \cdot x = x \cdot z$. Такође и $z \cdot y \in I \cdot J$, па закључујемо да и z припада пресеку $I \cap J$. □

Питање: Чему одговара резултат из напомене у случају целих бројева?

Јасно је да се претходни резултат генералише на произвољан коначан производ идеала. Размислите како се претходна Кинеска теорема за комутативне прстене може формулисати имајући у виду претходно доказано.

Прости и максимални идеали

Започнимо ову лекцију следећим ставом

Став 53 Нека је A комутативан прстен са јединицом и $P \lhd A$ ($P \neq A$). Следећи услови су еквивалентни.

1. За $I, J \lhd A$ важи: ако је $I \cdot J \subseteq P$, онда $I \subseteq P$ или $J \subseteq P$.
2. За $a, b \in A$ важи: ако $ab \in P$, онда $a \in P$ или $b \in P$.
3. Прстен A/P је област целих.

Доказ. Подсетимо се најпре да се област целих дефинише као комутативан прстен са јединицом у коме нема правих делитеља нуле, тј. у коме важи: ако је $ab = 0$, онда је $a = 0$ или $b = 0$.

$1 \Longrightarrow 2$. Уочимо идеале $I = \langle a \rangle$, $J = \langle b \rangle$. Како је $I \cdot J = \langle ab \rangle$ и $ab \in P$, то $I \cdot J \subseteq P$. На основу 1. следи да $I \subseteq P$, или $J \subseteq P$, тј. $a \in P$, или $b \in P$.

$2 \Longrightarrow 3$. Претпоставимо да за елементе $x, y \in A/P$ важи: $xy = 0$. Како су то елементи из количничког прстена, то постоје $a, b \in A$ такви да је $x = a + P$ и $y = b + P$ и да важи: $(a + P)(b + P) = P$. Ова једнакост се своди на $ab + P = P$, тј. на $ab \in P$. На основу 2. добијамо да $a \in P$, или $b \in P$, односно $a + P = P$ или $b + P = P$, тј. $x = 0$, или $y = 0$.

$3 \Longrightarrow 1$. Нека су идеали I, J прстена A такви да је $I \cdot J \subseteq P$, а да $I \not\subseteq P$ и $J \not\subseteq P$. То значи да постоји $a \in I \setminus P$ и $b \in J \setminus P$. Но, $ab \in I \cdot J \subseteq P$, па је $(a + P)(b + P) = ab + P = P$. Како је A/P област целих, следи да $a \in P$, или $b \in P$. Ова контрадикција завршава доказ. □

Дефиниција 54 Идеал $P \lhd A$ је прост уколико испуњава неко од претходна три еквивалентна својства.

Приметимо да, уколико је P прост идеал, а $a_1, \ldots, a_n \in A$, онда из $a_1 \cdots a_n \in P$ следи да $a_i \in P$ за неко $i \in \{1, \ldots, n\}$ (што се лако доказује индукцијом по n).

У основној школи смо научили да је природан број прост уколико нема других делилаца сем 1 и њега самог (ово такође важи и за број 1, али се он не сматра простим бројем). Но, у произвољној области целих разликује се појам простог и нерастављивог елемента. Подсетимо се да са $U(A)$ означавамо скуп свих инвертибилних елемената у прстену A.

Дефиниција 55 Нека је A област целих. Елемент $p \in A \setminus (U(A) \cup \{0\})$ је

- прост, уколико за $a, b \in A$ важи: ако $p \mid ab$, онда $p \mid a$, или $p \mid b$;
- нерастављив уколико за $a, b \in A$ важи: ако је $p = ab$, онда је $a \in U(A)$, или $b \in U(A)$.

Веза између простих и нерастављивих елемената у произвољном прстену дата је следећим ставом.

Став 56 Сваки прост елемент (у области целих) је нерастављив.

Доказ. Претпоставимо да је p прост и да је $p = ab$. Посебно то значи да p дели производ ab. Како је p прост, то $p \mid a$, или $p \mid b$. Нека, на пример, $p \mid a$. То значи да постоји $c \in A$ за који је $a = pc$. Како је $p = ab$, то је $p = pcb$, тј. $p(1 - cb) = 0$, па мора бити $1 - cb = 0$, пошто је A област целих. Дакле, $cb = 1$, те је елемент b инвертибилан. □

У произвољној области целих, прости и нерастављиви елементи се разликују. Размотримо следећи пример.

Пример 57 У прстену $\mathbb{Z}\left[\sqrt{-5}\right]$ елемент 3 је нерастављив, али није прост.

Пре свега,

$$\mathbb{Z}\left[\sqrt{-5}\right] := \{p(\sqrt{-5}) : p \in \mathbb{Z}[X]\}.$$

Но, није тешко уверити се да из дефиниције следи да је

$$\mathbb{Z}\left[\sqrt{-5}\right] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

Уверимо се најпре да је 3 нерастављив. Претпоставимо да је $3 = uv$. Уведимо ознаку $N(z) := z\overline{z}$, за $z \in \mathbb{Z}\left[\sqrt{-5}\right]$ (наравно да је $N(z)$ квадрат модула комплексног броја z). Јасно је да је $N(z_1 z_2) = N(z_1)N(z_2)$ за све z_1, z_2. Добијамо да је $N(3) = N(u)N(v)$, односно $9 = N(u)N(v)$. Ово је факторизација природног броја 9 у скупу природних бројева, то имамо две могућности:

1) један од $N(u)$, $N(v)$ једнак је 1, а други 9;

2) $N(u) = N(v) = 3$.

1) Претпоставимо, на пример, да је $N(u) = 1$. Уколико је $u = a + b\sqrt{-5}$, добијамо да је $1 = N(u) = u\overline{u} = (a + b\sqrt{-5})(a - b\sqrt{-5}) = a^2 + 5b^2$.

С обзиром да $a, b \in \mathbb{Z}$, ово је могуће једино ако је $b = 0$ и $a \in \{-1, 1\}$, тј. $u \in \{-1, 1\}$, те следи да је u инвертибилан (било би добро да читаоци сами покажу, за вежбу, да је $U(\mathbb{Z}\left[\sqrt{-5}\right] = \{-1, 1\}$ користећи функцију N).

2) Поступамо на сличан начин. Уколико је $u = a + b\sqrt{-5}$, добијамо да је $3 = N(u) = a^2 + 5b^2$. С обзиром да $a, b \in \mathbb{Z}$, мора бити $b = 0$ и добијамо да је $3 = a^2$, за неко $a \in \mathbb{Z}$. Ово наравно није могуће, те закључујемо да се слуцај 2) и не појављује.

Дакле, из чињенице да је $3 = uv$, добијамо да је један од фактора инвертибилан, а то заправо значи да је 3 нерастављив.

Остаје да покажемо да 3 није прост. посматрајмо факторизацију броја 9 у $\mathbb{Z}\left[\sqrt{-5}\right]$:

$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Како је $9 = 3 \cdot 3$, то

$$3 \mid (2 + \sqrt{-5})(2 - \sqrt{-5}).$$

Покажимо да 3 не дели ниједан од ових фактора. Из те чињенице ће следити да 3 није прост.

Нека $3 \mid 2 + \sqrt{-5}$ (аналогно се разматра и други случај). Дакле, за неки елемент $u \in \mathbb{Z}\left[\sqrt{-5}\right]$:

$$3 \cdot u = 2 + \sqrt{-5}.$$

Применом функције N добијамо

$$9 \cdot N(u) = 9.$$

Добијамо да је $N(u) = 1$, те је $u \in \{-1, 1\}$, тј. $3 = 2 + \sqrt{-5}$, или $3 = -(2 + \sqrt{-5})$. Ова контрадикција нам показује да 3 не дели $2 + \sqrt{-5}$, тј. 3 заиста није прост. ♣

Напомена 58 Приметимо да једнакост $3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ даје две различите факторизације броја 9 у производ нерастављивих. То је нешто са чиме се нисмо срели у случају целих бројева. Више ћемо о овоме рећи у наредним предавањима.

Пример 59 У прстену тригонометријских полинома $A = \mathbb{R}[\sin x, \cos x]$ наћи пример неједнозначне факторизације на нерастављиве елементе.

Читаоци би требало да буду упознати са овим прстеном из курса Анализе 2 (Фуријеови редови и сл.). Заправо, није тешко показати да је сваки елемент из A облика $a_0 + \sum_{k=1}^{n}(a_k \cos kx + b_k \sin kx)$ (по дефиницији је $A = \{p(\sin x, \cos x) : p \in \mathbb{R}[X, Y]\}$). Познати идентитет $\sin^2 x + \cos^2 x = 1$ даје тражене факторизације:

$$\cos x \cdot \cos x = (1 - \sin x)(1 + \sin x).$$

Остављамо читаоцима за вежбу да покажу нерастављивост функција које се појављују у овој факторизацији (знање Анализе 2 може бити корисно за ово, али није и неопходно – довољно је знање адиционих формула и једноставно рачунање интеграла функција облика $\sin kx$ и $\cos kx$) .

Следећи став је помало и очекиван.

Став 60 Елемент је прост ако и само ако је идеал генерисан тим елементом прост идеал.

Доказ. Нека је p прост елемент у прстену A и $\langle p\rangle$ идеал генерисан тим елементом. Уколико $ab \in \langle p\rangle$, онда је $ab = pc$ за неки $c \in A$, тј. $p \mid ab$. Како је елемент p прост, то $p \mid a$, или $p \mid b$, односно, $a \in \langle p\rangle$, или $b \in \langle p\rangle$, те закључујемо да је $\langle p\rangle$ прост идеал.

Обратно, претпоставимо да је $\langle p\rangle$ прост идеал и нека $p \mid ab$. То значи да $ab \in \langle p\rangle$, те следи да $a \in \langle p\rangle$, или $b \in \langle p\rangle$, односно $p \mid a$, или $p \mid b$. □

За крај ове приче о простим идеалима, наведимо једну интересантну теорему.

Теорема 61 (Теорема о избегавању простих идеала) Нека су $P_1, \ldots, P_n$ прости идеали прстена A и $I \triangleleft A$. Ако је $I \subseteq P_1 \cup \ldots \cup P_n$, онда је $I \subseteq P_i$ за неко $i \in \{1, \ldots, n\}$.

Доказ. Изводимо доказ индукцијом по n. Случај $n = 1$ је тривијалан. Претпоставимо да је $n > 1$ и да је тврђење тачно уколико је I садржан у унији мање од n простих идеала. Нека је $I \subseteq P_1 \cup \ldots \cup P_n$, при чему су сви ови прости. Уколико је I садржано у некој од унија $\cup_{j\neq i} P_j$ (за неко i), онда резултат следи на основу индуктивне хипотезе. Претпоставимо, стога, да $I \not\subseteq \cup_{j\neq i} P_j$ за све $i = \overline{1,n}$. Дакле, постоје елементи $x_i \in I \setminus \cup_{j\neq i} P_j$. Посматрамо елемент $x = x_1 + x_2 \cdots x_n$. Како је $x_i \in I \setminus \cup_{j\neq i} P_j$, а $I \subseteq P_1 \cup \ldots \cup P_n$, то $x_i \in P_i$. Поставља се питање где се налази елемент x. Уколико $x \in P_1$, онда $x_2 \cdots x_n \in P_1$ (јер $x_1 \in P_1$), те из чињенице да је P_1 прост, следи да $x_j \in P_1$ за неко $j \neq i$, што није тачно. Дакле, $x \notin P_1$. Следи да $x \in P_j$ за неко $j \neq 1$. Како и $x_j \in P_j$, то и производ $x_2 \cdots x_n$ припада P_j, те следи да и $x_1 = x - x_2 \cdots x_n \in P_j$. Ова контрадикција завршава доказ. □

Пређимо сада на појам максималног идеала.

Дефиниција 62 Идеал M прстена A је максималан, уколико не постоји идеал I прстена A за који важи: $M \subset I \subset A$.

Дакле, максималан идеал је прави идеал за који не постоји прави идеал, различит од њега, који га садржи као свој подскуп.

Став 63 Нека је M прави идеал прстена A. Тада је M максималан идеал ако и само ако је A/M поље.

Доказ. Претпоставимо да је M максималан идеал и $a+M \neq M$. Треба показати да $a+M$ има инверз у прстену A/M. Посматрамо идеал $\langle a\rangle + M$. Како $a \notin M$, то је M прави подскуп од $\langle a\rangle + M$. Но, с обзиром да је M максималан идеал, мора бити $\langle a\rangle + M = A$. То значи да постоје $b \in A$ и $m \in M$ за које је $ab + m = 1$. Дакле, $ab - 1 = m \in M$, па је $ab + M = 1 + M$, те је $b + M$ тражени инверз елемента $a + M \in M$.

Обратно, претпоставимо да је A/M поље. Нека је M прави подскуп идеала I. Дакле, постоји $a \in I \setminus M$. Стога је $a + M \neq M$ у количничком прстену A/M. Како је овај прстен по претпоставци поље, то постоји $b \in M$ тако да је $(a+M)(b+M) = 1+M$, односно, $ab-1 \in M$. Дакле, за неко $m \in M$ важи: $ab - 1 = m$, тј. $1 \in ab - m$. Како и a и m припадају идеалу I, то и $1 \in I$, па мора бити $I = A$. Закључујемо да је M заиста максималан идеал у A. □

Напомена 64 Видимо да из овог става следи да је сваки максималан идеал уједно и прост идеал, пошто у пољу нема правих делитеља нуле.

Веза између нерастављивих елемената и максималних идеала дата је следећим ставом.

Став 65 Елемент $a \in A$ је нерастављив ако и само ако је идеал $\langle a\rangle$ максималан у скупу свих главних идеала прстена A.

Доказ. Претпоставимо да је $a \in A$ нерастављив и нека је $\langle a\rangle \subseteq \langle b\rangle$. Треба да покажемо да је $\langle a\rangle = \langle b\rangle$ или $\langle b\rangle = A$. Како је $\langle a\rangle \subseteq \langle b\rangle$, то $a \in \langle b\rangle$, па постоји $c \in A$ тако да је $a = bc$. Како је a нерастављив, то $b \in U(A)$, или $c \in U(A)$. Уколико $b \in U(A)$, онда је $\langle b\rangle = A$, а ако $c \in U(A)$, онда је $\langle a\rangle = \langle b\rangle$.

Обратно, претпоставимо да је $\langle a\rangle$ максималан у скупу свих главних идеала прстена A. Нека је $a = bc$ и претпоставимо да $c \notin U(A)$. То значи да је $a \in \langle b\rangle$, али да $b \notin \langle a\rangle$ (зашто?), тј. да је $\langle a\rangle$ прави подскуп идеала $\langle b\rangle$. Како је $\langle a\rangle$ максималан у скупу свих главних идеала, то мора бити $\langle b\rangle = A$, тј. постоји $c \in A$ тако да је $bc = 1$, те закључујемо да је b инвертибилан. □

Максималан идеал у сваком комутативном прстену са јединицом постоји. Заправо, важи следећа теорема, коју нећемо доказивати.

Теорема 66 Нека је I прави идеал у комутативном прстену са јединицом A. Тада постоји максималан идеал M за који је $I \subseteq M$.

Посебно је занимљив случај прстена у којима постоји тачно један максимални идеал.

Став 67 У комутативном прстену са јединицом A постоји тачно један максималан идеал ако и само ако је $A \setminus U(A)$ идеал.

Доказ. Претпоставимо да је прстену постоји тачно један максималан идеал M. Доказаћемо да је заправо $M = A \setminus U(A)$. Пре свега, ниједан

елемент у M не може бити инвертибилан пошто је M прави идеал (идеал генерисан инвертибилним елементом једнак је целом прстену). Дакле, $M \subseteq A \setminus U(A)$. Обратно, нека је $a \in A \setminus U(A)$. Како a није инвертибилан, то је идеал $\langle a \rangle$ прави идеал, па је по претходној теореми садржан у неком максималном идеалу. Но, како је M једини максималан идеал, то $a \in M$. Добили смо да је $A \setminus U(A) = M$, па је $A \setminus U(A)$ заиста идеал.

Обратно, нека у прстену A сви неинвертибилни елементи чине идеал M. Јасно је да тај идеал мора бити максималан. Наиме, ако је M прави подскуп идеала I у I постоји неки елемент који није у M. Тај елемент је нужно инвертибилан (пошто су у M сви неинвертибилни), те генерише цео прстен и следи да је и $I = A$. Дакле, M је максималан идеал. Претпоставимо да је M' неки други максималан идеал и нека је $M \neq M'$. Како је M' максималан то $M' \not\subseteq M$, па постоји елемент $x \in M' \setminus M$. Но, то значи да је x инвертибилан, па је $M' = A$ и M' није прави идеал, а то противречи претпоставци да је он максималан. Закључујемо да је M једини максималан идеал у A. □

Следећи пример је само специјалан случај важне конструкције, коју ћемо подробније анализирати када се будемо бавили пољима.

Пример 68 Показати да је $\mathbb{R}[X]/\langle X^2+1\rangle \cong \mathbb{C}$.

Користићемо теорему о изоморфизмима за прстене. Нека је $f\colon \mathbb{R}[X] \to \mathbb{C}$ дефинисана са: $f(p) = p(i)$ (i је наравно имагинарна јединица). Јасно је да је f хомоморфизам: $f(pq) = (pq)(i) = p(i)q(i)$, $f(p+q) = (p+q(i) = p(i)+q(i)$. Осим, тога, f је „на": $f(a+bX) = a+bi$ за $a, b \in \mathbb{R}$. Потребно је само да одредимо језгро хомоморфизма f. Јасно је да је $X^2+1 \in \mathrm{Ker}(f)$, пошто је $i^2 + 1 = 0$. Стога је $\langle X^2+1\rangle \subseteq \mathrm{Ker}(f)$. Претпоставимо да $p(X) \in \mathrm{Ker}(f)$. То значи да је $p(i) = 0$. Поделимо $p(X)$ полиномом X^2+1. Добијамо да је, за неке $a, b \in \mathbb{R}$

$$p(X) = q(X)(X^2+1) + a + bX.$$

Како је $p(i) = 0$, добијамо да је $0 = a+bi$. Како су a и b реални бројеви, то је могуће једино ако је $a = b = 0$, те закључујемо да $(X^2+1) \mid p(X)$. Стога је заиста $\mathrm{Ker}(f) = \langle X^2+1\rangle$. Теорема о изоморфизмима за прстене даје нам тражени резултат. ♣

На потпуно аналогни начин доказује се да је

$$\mathbb{Q}[X]/\langle X^2-2\rangle \cong \mathbb{Q}[\sqrt{2}],$$

при чему је $\mathbb{Q}[\sqrt{2}] := \{p(\sqrt{2}) : p \in \mathbb{Q}[X]\}$. Како је полином $X^2-2 \in \mathbb{Q}[X]$ нерастављив, добијамо да је заправо $\mathbb{Q}[\sqrt{2}]$ поље. О примерима овог типа биће више речи када будемо изучавали поља.

Факторизација; локализација

Подсетимо се да је област целих (домен) комутативан прстен са јединицом у коме нема правих делитеља нуле, тј. у којима важи: за све $a, b \in A$ из $ab = 0$ следи $a = 0$, или $b = 0$. Сви прстени којима ћемо се бавити у овој лекцији биће домени.

Дефиниција 69 Два елемента $a, b \in A$ су придружена уколико постоји $u \in U(A)$ такав да је $a = ub$.

Јасно је да је придруженост елемената једна релација еквиваленције. Приметимо да ако је p нерастављив онда је то и сваки њему придружен елемент. Исто то важи и за просте елементе у домену.

Дефиниција 70 Домен A је домен за једнозначном факторизацијом уколико за сваки елемент из $a \in A \setminus (U(A) \cup \{0\})$ постоје нерастављиви елементи $p_1, \ldots, p_r$ такви да је $a = p_1 p_2 \cdots p_r$. Осим тога ако је за нерастављиве елемента p_i, q_j:

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

онда је $r = s$ и постоји пермутација $\sigma \in \mathbb{S}_r$ тако да је за све $i = \overline{1, r}$ елемент p_i придружен елементу $q_{\sigma(i)}$.

Другим речима у домену са једнозначном факторизацијом, сваки елемент може се на јединствен начин, до на придруженост и редослед фактора, приказати у облику производа нерастављивих елемената.

Став 71 Домен A је домен са једнозначном факторизацијом акко се сваки елемент $a \in A \setminus (U(A) \cup \{0\})$ може приказати у облику производа простих елемената. Посебно, то значи да је сваки нерастављив елемент прост.

Доказ. Претпоставимо да се сваки неинвертибилан, ненула елемент може приказати у облику производа простих. Како су прости нерастављиви, потребно је само доказати да је приказ у облику производа јединствен (у горенаведеном смислу). Докажимо најпре да је, у овом случају, сваки нерастављив елемент прост.

Нека је q нерастављив елемент. По претпоставци, он се може написати у облику производа простих елемената: $q = p_1 \cdots p_r$, где су p_i прости. Но, како је q нерастављив, мора бити $r = 1$, тј. и сам q је прост.

Докажимо сада јединственост разлагања у облику производа нерастављивих елемената. Нека је

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

Доказ изводимо индукцијом по r. Случај $r = 1$ је тривијалан (зашто?). Претпоставимо да је у горњој једнакости $r > 1$ и да су су p_i, q_j нерастављиви. Према доказаном, p_1 је прост, па постоји $j_1 \in \{1, \ldots, s\}$ тако

да $p_1 \mid q_{j_1}$. Како је q_{j_1} нерастављив, добијамо да су p_1 и q_{j_1} придружени, тј. да постоји $u_1 \in U(A)$ за који је $q_{j_1} = u_1 p_1$. Горњу једнакост можемо поделити са p_1 и добијамо

$$p_2 \cdots p_r = q_2' q_3 \cdots q_s,$$

где је $q_2' = q_2 u_1$ и он је такође нерастављив. Индуктивна хипотеза завршава доказ.

Обратно, претпоставимо да је A домен за једнозначном факторизацијом. Довољно је показати да је сваки нерастављив елемент прост. Нека је p нерастављив и нека $p \mid ab$. Треба показати да $p \mid a$, или $p \mid b$. Претпоставимо да p не дели ни a ни b. Нека је $a = p_1 \cdots p_r$ факторизација a на нерастављиве елементе и $b = q_1 \cdots q_s$ факторизација b на нерастављиве. Тада је

$$ab = p_1 \cdots p_r q_1 \cdots q_s$$

факторизација ab на нерастављиве. Како p дели ab, то је $ab = pc$ за неко c. И c има факторизацију на нерастављиве елементе, па је $c = z_1 \cdots z_l$ за неке нерастављиве $z_1, \ldots, z_l$. Добијамо да је

$$p_1 \cdots p_r q_1 \cdots q_s = p z_1 \cdots z_l,$$

где су сви p_i, q_j, z_k и p нерастављиви. Како је, по претпоставци, A домен са једнозначном факторизацијом, то је p придружен неком од елемената из скупа $\{p_1, \ldots, p_r, q_1, \ldots, q_s\}$. Уколико је p придружен елементу p_i (за неко i), добијамо да $p \mid a$, а ако је p придружен неком q_j онда $p \mid b$. Наиме, лако се показује да важи следеће: ако је p придружен елементу q и ако $q \mid c$, онда и $p \mid c$ (докажите то!). Овим је доказ завршен. □

Подсетимо се да је прстен главноидеалски уколико је сваки идеал у њему главни. Раније смо закључили да су $\mathbb{Z}$ и $K[X]$, за произвољно поље K, главноидеалски домени. Показаћемо да је сваки главноидеалски домен уједно и домен са једнозначном факторизацијом.

Став 72 Доказати да у сваком главноидеалском домену за свака два елемента постоји њихов највећи заједнички делилац.

Доказ. Нека A један главноидеалски домен и $a, b \in A$. Посматрајмо идеал $\langle a, b \rangle$ генерисан елементима a и b. Како је у A сваки идеал главни, то је и $\langle a, b \rangle = \langle d \rangle$, за неки $d \in A$. Докажимо да је d један највећи заједнички делилац елемената a и b (највећи заједнички делилац није једнозначно одређен, али су свака два највећа заједничка делиоца придружени један другом).

Најпре, $a, b \in \langle d \rangle$. То значи да постоје a_1, b_1 за које је $a = da_1$ и $b = db_1$, тј. $d \mid a$ и $d \mid b$, те d јесте заједнички делилац од a и b.

Претпоставимо да $d_1 \mid a$ и $d_1 \mid b$, тј. да је d_1 неки заједнички делилац од a и b. Треба доказати да $d_1 \mid d$. Како $d_1 \mid a$ и $d_1 \mid b$, то постоје a_1

и b_1 тако да је $a = d_1a_1$ и $b = d_1b_1$. С обзиром да $d \in \langle a, b\rangle$, постоје p, q такви да је $d = ap + bq$. Добијамо да је $d = d_1a_1p + d_1b_1q = d_1(a_1p + b_1q)$, те следи да $d_1 \mid d$. □

Заправо је у овом ставу доказано не само да свака два елемента a и b имају највећи заједнички делилац d, но и да постоје p и q за које је $d = ap + bq$ (Безуова релација). Из ове релације се, на стандардан начин, изводи следеће својство: ако $a \mid bc$ и ако је $\mathrm{NZD}(a, b)$ придружен јединици, онда $a \mid c$ (наравно, уместо да пишемо да је $\mathrm{NZD}(a, b)$ придружен јединици, писаћемо да је $\mathrm{NZD}(a, b) = 1$, имајући на уму шта то значи). Нека читаоци ово сами докажу.

Теорема 73 Сваки главноидеалски домен је и домен са јединственом факторизацијом.

Доказ. Нека је A главноидеалски домен. Докажимо најпре да је сваки нерастављив елемент у A прост. Нека је q нерастављив и нека $q \mid ab$. Уколико q не дели a, мора бити $\mathrm{NZD}(q, a) = 1$. Наиме, ако је $d = \mathrm{NZD}(q, a)$, то значи да је $q = dz$ за неко z. Како је q нерастављив, мора бити $d \in U(A)$, или $z \in U(A)$. Но, ако је $z \in U(A)$, онда из чињенице да $d \mid a$ следи да и $q \mid a$ (зашто?), што противречи претпоставци. Закључујемо да $d \in U(A)$, тј. $\mathrm{NZD}(q, a) = 1$ (погледајте ранију напомену у загради). Но, тада из горенаведеног својства следи да $q \mid b$, те закључујемо да је q прост.

Да бисмо доказали да је A домен са јединственом факторизацијом, остаје само да покажемо да се сваки елемент из $A \setminus (U(A) \cup \{0\})$ може приказати у облику производа нерастављивих елемената (видети став 71).

Докажимо најпре да сваки непразан скуп идеала у A има максималан елемент. Претпоставимо да то није тако и нека је $\mathcal{I}$ неки непразан скуп идеала који не садржи максималан елемент. Нека је $I_1 \in \mathcal{I}$ произвољан идеал из $\mathcal{I}$. Како он није максималан у $\mathcal{I}$, то постоји $I_2 \in \mathcal{I}$ за који је $I_1 \subset I_2$. Слично, постоји и $I_3 \in \mathcal{I}$ такав да је $I_2 \subset I_3$. Заправо добијамо стриктно растући ланац идеала

$$I_1 \subset I_2 \subset I_3 \subset \cdots$$

из $\mathcal{I}$. Унија $J = \cup_{i=1}^{\infty} I_i$ је идеал као што се лако може проверити (проверите!). Но, с обзиром да је A главноидеалски, то је $J = \langle x\rangle$ за неки $x \in A$. Како је $x \in \cup_{i=1}^{\infty} I_i$, то $x \in I_{i_0}$ за неки i_0. Но, одавде следи да је $J = I_{i_0}$, па је и $I_i = I_{i_0}$ за све $i \geq i_0$, те бесконачан стриктно растући ланац идеала и не постоји. Закључујемо да у $\mathcal{I}$ постоји максималан елемент.

Претпоставимо да у $A \setminus (U(A) \cup \{0\})$ има елемената који немају факторизацију на нерастављиве елементе. Уочимо скуп идеала $\mathcal{J}$ задат са:

$$\mathcal{J} = \{\langle a\rangle : a \in A \setminus (U(A) \cup \{0\}) \text{ и } a \text{ нема факторизацију на нерастављиве}\}.$$

Према управо доказаном резултату, у $\mathcal{J}$ постоји максималан елемент $\langle x\rangle$. Како x нема факторизацију на нерастављиве, то он сам није нерастављив, па постоје a, b такви да је $x = ab$, при чему $a, b \in A\setminus(U(A)\cup\{0\})$. Стога је $\langle x\rangle \subset \langle a\rangle$ и $\langle x\rangle \subset \langle b\rangle$ (зашто?), па a и b имају факторизацију на нерастављиве ($\langle x\rangle$ је максималан елемент у $\mathcal{J}$). Но, ако су то факторизације $a = p_1\cdots p_r$ и $b = q_1\cdots q_s$, онда је $x = ab = p_1\cdots p_r q_1\cdots q_s$ једна факторизација x на нерастављиве, што противречи избору елемента x. Ова контрадикција завршава доказ. □

Може се показати (али ми то нећемо) да из чињенице да је A домен са једнозначном факторизацијом следи да је и $A[X]$ домен са једнозначном факторизацијом. Дакле, $\mathbb{Z}[X]$ је један пример домена са једнозначном факторизацијом, који није главноидеалски домен.

Дакле, домен са једнозначном факторизацијом се карактерише тиме да се у њему прости и нерастављиви елементи подударају и да се сваки ненула, неинвертибилан елемент a може представити у облику

$$a = up_1^{\alpha_1}\cdots p_k^{\alpha_k}, \tag{7}$$

где је u инвертибилан елемент и p_i нерастављиви, при чему за $i \neq j$ елементи p_i и p_j нису придружени, док је $\alpha_i \in \mathbb{N}$. Осим тога, ако је

$$a = vq_1^{\beta_1}\cdots q_l^{\beta_l},$$

где је v инвертибилан, q_j нерастављиви и q_i, q_j нису придружени за $i \neq j$, онда је $k = l$ и за неку пермутацију $\sigma \in \mathbb{S}_k$ $\alpha_i = \beta_{\sigma(i)}$ и p_i је придружен елементу $q_{\sigma(i)}$.

Напомена 74 Читалац се можда пита зашто се појављује инвертибилан елемент u у представљању елемента a у облику производа, када се тако нешто не појављује у самој дефиницији домена са једнозначном факторизацијом. Разлог лежи у томе што нерастављиви елементи p_i нису међусобно придружени и онда је неопходно издвојити инвертибилан елемент u. На пример, елемент $-36 \in \mathbb{Z}$ се може записати у облику $-36 = (-1)2^2 3^2$, или у облику $-36 = (-1)2^2(-3)^2$, али се (-1) мора појавити у овим записима. Презентација $-36 = 2(-2)3^2$ не задовољава услов да за различите индексе прости елементи нису придружени.

На основу једнакости (7), лако се показује да свака два елемента из домена са једнозначном факторизацијом имају највећи заједнички делилац (како се то показује?), но Безуова релација ипак не мора важити. Довољно је посматрати пример прстена $\mathbb{Z}[X]$ и елемената 2 и X, који јесу узајамно прости, али за које не постоје полиноми $p(X)$ и $q(X)$ тако да је $2p(X) + Xq(X) = 1$ (зашто?).

Пређимо сада на важан метод локализације којим се од датог домена прелази на нови домен, а у коме су неки изабрани елементи из почетног домена инвертибилни у новом домену. Почнимо следећом дефиницијом.

Дефиниција 75 Нека је A домен и $S \subseteq A \setminus \{0\}$. За S кажемо да је мултипликативан ако $1 \in S$ и ако из $s, t \in S$ следи да $st \in S$.

Пример 76 Следећи подскупови од $A \setminus \{0\}$ су мултипликативни:

1. $A \setminus \{0\}$;
2. $\{f^n : n \in \mathbb{N}\}$, за ма који елемент $f \in A \setminus \{0\}$;
3. $A \setminus P$ за ма који прост идеал $P \lhd A$.

1. Ово је јасно.

2. Подсетимо се да $0 \in \mathbb{N}$, па $1 \in S$. Осим тога, како је $f^m f^n = f^{m+n}$ и други услов је испуњен.

3. Јасно је да $1 \in A \setminus P$. Осим тога, ако $a \notin P$ и $b \notin P$, онда и $ab \notin P$, пошто је P прост идеал (појасните себи ово!). ♣

Нека је A домен и S ма који мултипликативан подскуп од A. На скупу $A \times S$ дефинишемо релацију $\sim$ са:

$$(a, s) \sim (b, t) \overset{\text{def}}{\iff} ta = sb.$$

Докажимо да је $\sim$ једна релација еквиваленције.

Рефлексивност. Ово је јасно пошто је $sa = sa$, па је $(a, s) \sim (a, s)$.

Симетричност. И ово је јасно, јер из $(a, s) \sim (b, t)$, следи да је $ta = sb$, тј, $sb = ta$, а то управо значи да је $(b, t) \sim (a, s)$.

Транзитивност. Нека је $(a, s) \sim (b, t)$ и $(b, t) \sim (c, r)$. То значи да је $ta = sb$ и $rb = tc$. Добијамо да је

$$rta = rsb = stc.$$

Како је A домен, то је $ra = sc$, па је $(a, s) \sim (c, r)$.

Са $S^{-1}A$ означавамо скуп свих класа еквиваленције, а са $\frac{a}{s}$ класу еквиваленције елемента (a, s). Дефинишемо операције $+$ и $\cdot$ на $S^{-1}A$ са:

$$\frac{a}{s} + \frac{b}{t} := \frac{ta + sb}{st};$$
$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

Како је скуп S мултипликативан, то за $s, t \in S$ и $st \in S$, па ови записи имају смисла. Треба још да проверимо да су ове операције добро дефинисане.

Нека је $\frac{a}{s} = \frac{a'}{s'}$ и $\frac{b}{t} = \frac{b'}{t'}$. То заправо значи да је $(a, s) \sim (a', s')$ и $(b, t) \sim (b', t')$. Треба проверити да је $(ta + sb, st) \sim (t'a' + s'b', s't')$ и $(ab, st) \sim (a'b', s't')$. Рачунамо:

$$s't'(ta + sb) = s't'ta + s't'sb = t'tsa' + s'stb' = st(t'a' + s'b'),$$

па је заиста $(ta+sb, st) \sim (t'a'+s'b', s't')$. На сличан начин се проверава и добра дефинисаност операције множења.

Није тешко проверити да је структура $(S^{-1}A, +, \cdot)$ један комутативан прстен са јединицом (урадите то за вежбу: $0_{S^{-1}A} = \frac{0}{1}$, $1_{S^{-1}A} = \frac{1}{1}$). Овај прстен назива се локализација домена A у односу на мултипликативан скуп S. Основно својство локализације дато је следећим ставом.

Став 77 Нека је A домен и S неки мултипликативан подскуп од A.

а) Са $i(a) = \frac{a}{1}$ задат је један мономорфизам $i: A \to S^{-1}A$,

б) Ако је B ма који комутативан прстен и $f: A \to B$ хомоморфизам такав да за све $s \in S$ важи: $f(s) \in U(B)$, онда постоји тачно један хомоморфизам $\widetilde{f}: S^{-1}A \to B$ за који је $\widetilde{f} \circ i = f$.

Доказ.

а) Како је $i(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i(a) + i(b)$ и $i(ab) = \frac{ab}{1} = \frac{a}{1}\frac{b}{1}$, то је i заиста хомоморфизам. Но, $a \in \mathrm{Ker}(i)$ ако и само ако је $\frac{a}{1} = \frac{0}{1}$, што је еквивалентно са $a = 0$, па је i мономорфизам.

б) Тражени хоморфизам $\widetilde{f}$ дефинишемо са: $\widetilde{f}(\frac{a}{s}) = f(a)f(s)^{-1}$. Како је, за све $s \in S$, $f(s)$ инвертибилан, ова дефиниција има смисла. Остављамо читаоцима да провере да је ово заиста један добро дефинисан хомоморфизам и да важи: $\widetilde{f} \circ i = f$. □

Уколико је $S = A \backslash P$ за неки прост идеал P, онда се уместо $(A \backslash P)^{-1}A$ краће пише: A_P. Важи следећа теорема.

Теорема 78 За сваки прост идеал $P \lhd A$, прстен A_P је локални прстен.

Доказ. Доказаћемо да је скуп свих неинвертибилних елемената идеал. Одредимо најпре $U(A_P)$:

$$\frac{a}{s} \in U(A_P) \text{ акко постоје } b \in A \text{ и } t \in A \setminus P \text{ тако да је } \frac{a}{s} \cdot \frac{b}{t} = \frac{1}{1}.$$

Другим речима, $\frac{a}{s}$ је инвертибилан акко постоји $b \in A$ и $t \notin P$ за које је $ab = st$. Уколико $a \in P$, онда и $st = ab \in P$, па како је P прост идеал, следи да $s \in P$, или $t \in P$, што није могуће на основу избора s и t. А уколико $a \notin P$, онда је $\frac{s}{a} (\in A_P)$ инверз елемента $\frac{a}{s}$. Дакле,

$$A_P \setminus U(A_P) = \left\{ \frac{a}{s} \in A_P : a \in p \right\}.$$

Уверимо се да је ово заиста идеал у A_P.

Нека су x, y неинвертибилни елементи из A_P. То значи да постоје елементи $a, b \in p$ и $s, t \notin P$ за које је $x = \frac{a}{s}$ и $y = \frac{b}{t}$. Тада је $x + y = \frac{a}{s} + \frac{b}{t} = \frac{ta+sb}{st}$, но, како је P идеал, $ta + sb \in P$, па је заиста и елемент $x + y$ неинвертибилан. На сличан начин се показује да ако $x \in A_P$ нема инверз и ако је $z \in A_P$ произвољан, ни елемент zx нема инверз. Закључујемо да је $A_P \setminus U(A_P)$ заиста идеал, па је и прстен A_P локални прстен. □

За крај напоменимо да, уколико је $S = A \setminus \{0\}$, у прстену $S^{-1}A$ је сваки елемент различит од нуле инвертибилан, те је, у овом случају, $S^{-1}A$ једно поље. Ово поље се назива поље разломака домена A и означава са $Q(A)$. На овај начин смо показали да се сваки домен може утопити у неко поље. Као што видимо, ова је конструкција у потпуности аналогна конструкцији рационалних бројева као разломака над целим бројевима.

Поља

Раширења и коренска поља полинома

У једној од претходних лекција показано је да је

$$\mathbb{R}[X]/\langle X^2+1\rangle \cong \mathbb{C}(=\mathbb{R}[i])$$

и

$$\mathbb{Q}[X]/\langle X^2-2\rangle \cong \mathbb{Q}[\sqrt{2}].$$

У овој лекцији позабавићемо се озбиљније овим конструкцијама. Започнимо лекцију следећом важном теоремом.

Теорема 79 Нека је F поље и $a(X) \in F[X] \setminus \{0\}$ нерастављив полином.

а) $E = F[X]/\langle a(X)\rangle$ је поље.

б) Поље E садржи потпоље изоморфно пољу F.

в) Полином $a(X)$ има бар једну нулу у пољу E.

г) На основу а) можемо сматрати да је $F \subset E$. Тада се E може видети и као векторски простор над пољем F и димензија тог простора једнака је степену полинома $a(X)$.

Доказ. а) Како је $a(X)$ нерастављив, то је идеал $I = \langle a(X)\rangle$ максималан у скупу свих главних идеала. Но, у прстену $F[X]$ је сваки идеал главни, те је I максималан идеал. Стога је E поље.

б) Дефинишимо хомоморфизам $f\colon F \to E$ са $f(\alpha) = \alpha + I$ за све $\alpha \in F$. Како су једини идеали у ма ком пољу $\{0\}$ и цело поље, то закључујемо да је $\mathrm{Ker}(f) = \{0\}$ (језгро је увек идеал, али не може бити једнако целом пољу пошто се при хомоморфизму јединица слика у јединицу, а не у нулу). Дакле, хомоморфизам f успоставља изоморфизам између F и слике од f, која је потпоље од E. У даљем идентификујемо F и слику $f[F]$, ради једноставнијег писања, тако да ћемо, између осталог, уместо $a + I$, за $a \in F$ писати само a.

в) Уочимо елемент $X + I$ у E. Означимо га са $\widetilde{X}$. Уколико је $a(X) = a_0 + a_1X + \cdots + a_nX^n$, добијамо да је

$$a(\widetilde{X}) = a_0 + a_1\widetilde{X} + a_2\widetilde{X}^2 + \cdots + a_n\widetilde{X}^n = a_0 + a_1(X+I) + a_2(X+I)^2 + \cdots + a_n(X+I)^n,$$

$$= (a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) + I = a(X) + I = I,$$

те добијамо да $\widetilde{X}$ заиста анулира полином $a(X)$.

г) Како E садржи потпоље F' изоморфно са F, заиста са алгебарске тачке можемо сматрати да је $F \subset E$. У овом случају кажемо и да је

поље E једно проширење поља F. Наравно да елементе поља E можемо сабирати, али, с обзиром да је $F \subset E$, можемо их и множити елементима из F. На основу својстава операција у пољу E добијамо да је E заиста векторски простор над F. Димензију тог простора зовемо и степен проширења поља E над F и означавамо са $[E : F]$. Наш задатак је да докажемо да је $[E : F] = \deg a(X)$. Доказаћемо заправо да је

$$[1 + I, X + I, \ldots, X^{n-1} + I]$$

једна база простора E уколико је полином $a(X)$ степена n.

$\{1 + I, X + I, \ldots, X^{n-1} + I\}$ је генератриса. Уочимо ма који елемент $p(X) + I \in E$. Тада је

$$p(X) = q(X)a(X) + r(X),$$

где је $r(X) = 0$, или је $\deg r(X) < \deg a(X) = n$. Дакле,

$$r(X) = r_0 + r_1X + \cdots + r_{n-1}X^{n-1},$$

где наравно неки, па и сви, коефицијенти $r_i \in F$ могу бити једнаки 0. Но, тада је

$$p(X) + I = (q(X) + I)(a(X) + I) + (r(X) + I),$$

те је

$$p(X) + I = r_0(1 + I) + r_1(X + I) + \cdots + r_{n-1}(X^{n-1} + I).$$

Закључујемо да $1 + I, \ldots, X^{n-1} + I$ заиста генеришу E.

Линеарна независност. Нека је

$$c_0(1 + I) + c_1(X + I) + \cdots + c_{n-1}(X^{n-1} + I) = 0 + I,$$

за неке $c_i \in F$. Тада је

$$(c_0 + c_1X + \cdots + c_{n-1}X^{n-1}) + I = I,$$

те

$$c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in I = \langle a(X) \rangle.$$

Но, полином $a(X)$ је степена n и он може да дели полином $c_0+c_1X+\cdots+c_{n-1}X^{n-1}$ једино ако је $c_0+c_1X+\cdots+c_{n-1}X^{n-1} = 0$. Но, то управо значи да је $c_0 = c_1 = \cdots = c_{n-1} = 0$, те закључујемо да су $1 + I, \ldots, X^{n-1} + I$ заиста линеарно независни. □

Искористимо управо доказану теорему да конструишемо поље од 4 елемента. Приметимо да $\mathbb{Z}_4$ јесте комутативан прстен, али наравно да да није поље пошто у $\mathbb{Z}_4$ важи: $2 \cdot 2 = 0$, а $2 \neq 0$.

Пример 80 Конструисати поље, које има тачно 4 елемента.

Како ово извести? Пре свега, ми знамо да је $\mathbb{Z}_2$ поље и да има 2 елемента. Претходна теорема нам каже да ако нађемо нерастављив полином $a(X) \in \mathbb{Z}_2[X]$, који је степена n онда ће $\mathbb{Z}_2[X]/\langle a(X)\rangle$ бити поље, које је истовремено векторски простор над $\mathbb{Z}_2$ димензије n. Дакле, то поље је као векторски простор над $\mathbb{Z}_2$ изоморфно $\mathbb{Z}_2^n$, те има 2^n елемената. Нама је потребно поље са 4 елемента, тј. потребан нам је нерастављив полином из $\mathbb{Z}_2[X]$ степена 2. Такав полином наравно није тешко наћи. То је полином $a(X) = 1 + X + X^2$. Како је то полином другог степена, он је нерастављив ако и само ако нема ниједну нулу у $\mathbb{Z}_2$, а како је $a(0) = 1$ и $a(1) = 1$, то је заиста испуњено. Дакле, наше поље F_4 је дато са

$$F_4 = \mathbb{Z}_2[X]/\langle X^2 + X + 1\rangle.$$

Означимо са η елемент $X + \langle X^2 + X + 1\rangle$ у овом пољу. Добијамо да је

$$F_4 = \{0, 1, \eta, 1 + \eta\}.$$

Како у пољу F_4 важи: $\eta^2 = 1 + \eta$ (зашто?), можемо написати и таблице сабирања и множења у том пољу.

$+$	0	1	η	$1+\eta$
0	0	1	η	$1+\eta$
1	1	0	$1+\eta$	η
η	η	$1+\eta$	0	1
$1+\eta$	$1+\eta$	η	1	0

$\cdot$	0	1	η	$1+\eta$
0	0	0	0	0
1	0	1	η	$1+\eta$
η	0	η	$1+\eta$	1
$1+\eta$	0	$1+\eta$	1	η

♣

Вратимо се поново на теорему. Претпоставимо да нам је дат неки полином $a(X) \in F[X]$ где је F неко поље. Тај полином наравно не мора имати линеарну факторизацију над пољем F. Поставља се питање: да ли постоји неко поље E које садржи поље F и у коме се полином $a(X)$ факторише на линеарне факторе? То заиста јесте тачно и претходна теорема нам показује и пут доказа.

Последица 81 Нека је F поље и $a(X) \in F[X]$. Тада постоји раширење E поља F у коме се полином $a(X)$ факторише на линеарне факторе.

Доказ. Јасно је да можемо да претпоставимо да је полином $a(X)$ нерастављив, пошто бисмо у супротном његову факторизацију добили тако што бисмо нашли раширење у коме сви његови фактори имају линеарну факторизацију.

На основу доказане теореме, постоји поље E', које је раширење поља F, а у коме полином $a(X)$ има бар једну нулу, назовимо је α. То значи да у $E'[X]$ важи факторизација

$$a(X) = (X - \alpha)b(X),$$

где је $b(X) \in E'[X]$ и $\deg b(X) = n-1$. Уколико сада $b(X)$ раставимо на нерастављиве факторе у $E'[X]$, на њих можемо применити претходно закључивање. Тако процес настављамо све док не дођемо до линеарне факторизације. Јасно је да се процес мора завршити пошто у сваком кораку добијамо бар једну нову нулу почетног полинома, а он ни у једном пољу не може имати више од n нула. □

Сва поља, која ћемо у даљем разматрати ће бити такозвана бројевна поља, тј. потпоља од $\mathbb{C}$. Приметимо да свако такво поље обавезно садржи као своје потпоље поље $\mathbb{Q}$. Најмање раширење поља F у коме се дати полином из $F[X]$ факторише на линеарне факторе назива се коренско поље тог полинома.

У претходном је коришћена ознака $\mathbb{Q}[\sqrt{2}]$. Овде је $\mathbb{Q}$ наравно поље, док је $\sqrt{2}$ елемент који није у том пољу. Његовим „додавањем" добијамо структуру, која је поље. Позабавимо се мало општијим разматрањем.

Нека је B комутативни прстен са јединицом, A његов потпрстен (са јединицом наравно) и $b \in B \setminus A$. Како одредити најмањи потпрстен од B који садржи и A (као подскуп) и b као елемент? Очигледно је да такав прстен мора да садржи и све степене од b, као и све елементе облика $a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n$ где $a_i \in A$. Дакле, мора да садржи све елементе облика $p(b)$, где $p(X) \in A[X]$. Но, то је заправо и довољно, тј. тражени најмањи потпрстен је

$$A[b] := \{p(b) : p(X) \in A[X]\}.$$

Наиме, $A[b]$, овако дефинисан, је заиста потпрстен од B (очигледно је да је $A \subset A[b]$ и $b \in A[b]$):

$$\begin{aligned} p(b), q(b) \in A[b] &\implies p(b) - q(b) = (p-q)(b) \in A[b]; \\ p(b), q(b) \in A[b] &\implies p(b)q(b) = (pq)(b) \in A[b]. \end{aligned}$$

Уколико је F поље и $\alpha \in \mathbb{C} \setminus F$, онда са $F[\alpha]$ означавамо најмањи потпрстен који садржи F и α, а са $F(\alpha)$ најмање потпоље које садржи (као своје потпоље) F и α (као свој елемент). Поставља се природно питање: када је $F[\alpha] = F(\alpha)$? Другим речима, интересује нас у ком је случају прстен $F[\alpha]$ поље. Није тешко наћи један потребан услов за то. Наиме, како је

$$F[\alpha] = \{p(\alpha) : p(X) \in F[X]\},$$

а сваки елемент поља, који је различит од нуле има инверз, то и елемент $\alpha \in F[\alpha]$ има инверз у $F[\alpha]$, тј. постоји $a(\alpha) \in F[X]$ такав да је $\alpha \cdot a(\alpha) = 1$. Ако је $a(X) = a_0 + a_1 X + \cdots + a_n X^n$, то добијамо да је

$$a_n \alpha^{n+1} + \cdots + a_1 \alpha^2 + a_0 \alpha - 1 = 0,$$

тј. постоји полином $p(X) \in F[X]$ такав да је $p(\alpha) = 0$.

Дефиниција 82 Нека је F потпоље од $\mathbb{C}$ и $\alpha \in \mathbb{C}$. Тада је α алгебарски над F уколико постоји полином $p(X) \in F[X]$ за који је $p(\alpha) = 0$.

Дакле, видели смо да је потребан услов да прстен $F[\alpha]$ буде поље да је α алгебарски над F. Но, то је и довољан услов.

Став 83 Нека је F потпоље од $\mathbb{C}$ и $\alpha \in \mathbb{C}$. Тада је $F[\alpha]$ поље ако и само ако је α алгебарски над F.

Доказ. Један смер смо већ доказали. Остало је да се покаже да из чињенице да је α алгебарски над F следи да је $F[\alpha]$ поље. Како је α алгебарски над F, посматрајмо идеал $I \lhd F[X]$ дефинисан са:

$$I = \{a(X) \in F[X] : a(\alpha) = 0\}.$$

Није тешко проверити да је I заиста идеал. Како је сваки идеал у $F[X]$ главни, то постоји моничан полином $\mu_\alpha(X)$ за који је $I = \langle \mu_\alpha \rangle$.

Приметимо да је полином $\mu_\alpha(X)$ нерастављив. У супротном, нека је $\mu_\alpha(X) = a(X)b(X)$ за неке неконстантне полиноме $a(X), b(X)$ из $F[X]$. Но, тада је $a(\alpha)b(\alpha) = \mu_\alpha(\alpha) = 0$, па следи да је $a(\alpha) = 0$ или $b(\alpha) = 0$. Уколико је нпр. $a(\alpha) = 0$, добили бисмо да $a(X) \in I$, па $\mu_\alpha(X) \mid a(X)$, што није могуће јер је $a(X)$ полином степена мањег од степена полинома $\mu_\alpha(X)$. Слично се добија и у случају да је $b(\alpha) = 0$.

Сада, као и у ранијим примерима, посматрамо хомоморфизам

$$f\colon F[X] \to F[\alpha]$$

дефинисан са $f(p(X)) = p(\alpha)$. Хомоморфизам f је очигледно „на", а $\mathrm{Ker}(f) = I$. Стога добијамо да је

$$F[X]/I \cong F[\alpha].$$

Но, како је $\mu_\alpha(X)$ нерастављив полином, $F[X]/I$ је поље, па је и $F[\alpha]$ такође поље. □

Приметимо да смо у оквиру доказа овог става добили и да је

$$[F(\alpha) : F] = \deg \mu_\alpha(X).$$

Полином $\mu_\alpha(X)$ из овог става зове се и минимални полином елемента α. Базу за $F(\alpha)$ над F чине елементи $1, \alpha, \ldots, \alpha^{n-1}$ уколико је $n = \deg \mu_\alpha(X)$.

Пример 84 Нека је $\alpha = \sqrt{2} + \sqrt{3}$.

а) Показати да је α алгебарски над $\mathbb{Q}$.

б) Наћи минимални полином за α над $\mathbb{Q}$.

в) Одредити $\frac{1}{\alpha+3}$ у облику $p(\alpha)$ за неки полином $p(X) \in \mathbb{Q}[X]$.

а) Нађимо полином који елемент α анулира. Како је $\alpha - \sqrt{2} = \sqrt{3}$, то је

$$\begin{aligned}(\alpha - \sqrt{2})^2 &= 3\\ \alpha^2 - 2\alpha\sqrt{2} + 2 &= 3\\ \alpha^2 - 1 &= 2\alpha\sqrt{2}\\ (\alpha^2 - 1)^2 &= (2\alpha\sqrt{2})^2\\ \alpha^4 - 2\alpha^2 + 1 &= 8\alpha^2\\ \alpha^4 - 10\alpha^2 + 1 &= 0.\end{aligned}$$

б) Покажимо да је минимални полином елемента α заиста полином $X^4 - 10X^2 + 1$. Означимо га са $\mu(X)$. Једино треба доказати је овај полином нерастављив над $\mathbb{Q}$. Како се ради о полиному четвртог степена, уколико је он растављив, он се растаља или на производ полинома првог степена и полинома трећег степена, или на производ два полинома другог степена.

$\mu(X)$ је производ полинома првог степена и полинома трећег степена над пољем $\mathbb{Q}$. То значи да $\mu_(X)$ има нулу у $\mathbb{Q}$. Но, ако полином

$$a_n X^n + \cdots + a_1 X + a_0$$

има рационалну нулу r/s (где је r/s нескратив разломак) онда $r \mid a_0$ и $s \mid a_n$. Како је у нашем случају $a_n = a_4 = 1$, то је $s = 1$, а како је $a_0 = 1$, то r може бити само 1 или -1. Но, ни 1 ни -1 нису нуле полинома $\mu(X)$.

$\mu(X)$ је производ два полинома другог степена. Дакле,

$$\mu(X) = (X^2 + aX + b)(X^2 + cX + d)$$

(како је $\mu(X)$ можемо претпоставити да су и ти полиноми монични). Добијамо (изједначавањем одговарајућих коефицијената)

$$\begin{aligned}a + c &= 0 &(8)\\ b + ac + d &= -10 &(9)\\ ad + bc &= 0 &(10)\\ bd &= 1 &(11)\end{aligned}$$

Из (8) добијамо да је $c = -a$. Тада из (10) следи да је $a(d - b) = 0$. Размотримо два случаја.

$a = 0$. Тада је и $c = 0$ и добијамо да се систем своди на две једначине

$$\begin{aligned}b + d &= -10 &(12)\\ bd &= 1 &(13)\end{aligned}$$

Из (13) следи да је $d = 1/b$ (сигурно ни b ни d нису једнаки нули). Заменом у (12) и сређивањем добијамо квадратну једначину

$$b^2 + 10b + 1 = 0.$$

Решења ове једначине су дата са:

$$b_{1,2} = \frac{-10 + \sqrt{96}}{2}$$

По претпоставци $b \in \mathbb{Q}$. Како је $\sqrt{96} = 4\sqrt{6}$, добили бисмо да је $\sqrt{6} \in \mathbb{Q}$. Остављамо читаоцима да покажу да ово није могуће.

$a \neq 0$. У овом случају је $b = d$. Из једначине (11) добијамо да је $b \in \{1, -1\}$. Заменом у (10) (узимајући у обзир да је $c = -a$) добијамо да је $a^2 = 12$ или $a^2 = 8$. По претпоставци је $a \in \mathbb{Q}$ па би из $a^2 = 12$ следило да $\sqrt{3} \in \mathbb{Q}$, а из $a^2 = 8$ да је $\sqrt{2} \in \mathbb{Q}$. Како ни једно ни друго није тачно закључујемо да је $\mu(X)$ нерастављив.

в) За налажење $\frac{1}{\alpha+3}$ можемо користити метод неодређених коефицијената. Наиме, знамо да постоје a, b, c, d такви да је

$$\frac{1}{\alpha + 3} = a + b\alpha + c\alpha^2 + d\alpha^3. \tag{14}$$

Потребно је одредити коефицијенте a, b, c, d. Из (14), множењем обе стране са $\alpha + 3$, добијамо

$$1 = (\alpha + 3)(a + b\alpha + c\alpha^2 + d\alpha^3). \tag{15}$$

Узимајући у обзир да је $\alpha^4 = 10\alpha^2 - 1$ и да су $1, \alpha, \alpha^2, \alpha^3$ линеарно независни над $\mathbb{Q}$, добијамо

$$\begin{array}{rrrrcl} 3a & & & -d & = & 1 \\ a & +3b & & & = & 0 \\ & b & +3c & +10d & = & 0 \\ & & c & +3d & = & 0 \end{array}$$

Препуштамо читаоцима да реше овај систем једначина. ♣

Алгебарска раширења; примитивни елемент

Видели смо да су од посебног значаја за теорију раширења поља они елементи који су алгебарски над датим пољем.

Дефиниција 85 За раширење E поља F кажемо да је алгебарско раширење ако је сваки елемент из E алгебарски над F.

За раширење E поља F кажемо да је коначно раширење уколико је E коначно димензионални простор над F.

Став 86 Свако коначно раширење је алгебарско.

Доказ. Нека је $[E : F] = n$. То значи да је E n-димензионални простор над пољем F. Узмимо произвољни елемент $\alpha \in E$ и покажимо да је он алгебарски над F. Како је димензија простора једнака n, то је скуп од $n+1$ вектора $\{1, \alpha, \ldots, \alpha^n\}$ сигурно линеарно зависан скуп вектора, тј. постоје $a_0, \ldots, a_n \in E$ такви да је

$$a_0 1 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

но, то управо значи да је $p(\alpha) = 0$, где је $p(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$. Дакле, елемент α је алгебарски над F. □

Уколико је E_1 коначно раширење поља F, а E_2 коначно раширење поља E_1, онда је наравно E_2 и једно раширење поља F.

Став 87 Ако су F, E_1 и E_2 поља као у претходној реченици, онда је E_2 коначно раширење поља F и важи

$$[E_2 : F] = [E_2 : E_1][E_1 : F].$$

Доказ. Нека је $[E_1 : F] = n$ и $[E_2 : E_1] = m$. Како је димензија E_1 као векторског простора над пољем F једнака n, то постоји нека база $[\alpha_1, \ldots, \alpha_n]$. Слично, нека је $[\beta_1, \ldots, \beta_m]$ база векторског простора E_2 над пољем E_1. Докажимо да производи $\alpha_i\beta_j$, $i = \overline{1,n}$, $j = \overline{1,m}$ чине базу простора E_2 над пољем F.
Линеарна независност. Претпоставимо да је

$$\sum_{j=1}^{m}\sum_{i=1}^{n} c_{ij}\alpha_i\beta_j = 0,$$

за неке $c_{ij} \in F$. Нека је $d_j = \sum_{i=1}^{n} c_{ij}\alpha_i$, $j = \overline{1,m}$. Елементи d_j су из поља E_1 и за њих важи:

$$\sum_{j=1}^{m} d_j\beta_j = 0.$$

Како је $[\beta_1, \ldots, \beta_m]$ база за E_2 над E_1, то мора бити $d_j = 0$ за све $j \in \{1, \ldots, m\}$. Но, како је $[\alpha_1, \ldots, \alpha_n]$ база за E_1 над пољем F, то из $\sum_{i=1}^{n} c_{ij}\alpha_i = 0$, за $j = \overline{1,m}$ следи да је $c_{ij} = 0$ за $i = \overline{1,n}$, $j = \overline{1,m}$.

Генератриса. Нека је $\gamma \in E_2$. Како је $[\beta_1, \ldots, \beta_m]$ база за E_2 над E_1, то постоје $r_j \in E_1$ такви да је

$$\gamma = \sum_{j=1}^{m} r_j\beta_j.$$

Но, како је $[\alpha_1, \ldots, \alpha_n]$ база за E_1 над F то за свако $j \in \{1, \ldots, m\}$ постоје s_{ij} за које је

$$r_j = \sum_{i=1}^{n} s_{ij}\alpha_i.$$

Коначно добијамо да је

$$\gamma = \sum_{j=1}^{m} \sum_{i=1}^{n} s_{ij} \alpha_i \beta_j.$$

□

У примерима из претходне лекције доказивали смо да су неки елементи алгебарски над датим пољем тако што смо налазили полиноме, које они поништавају, тј. користили смо директно дефиницију. То понекад није лако. Потражите уосталом сами полином, који поништава елемент $i\sqrt{3} + \sqrt[3]{2}$. Заправо, то се може избећи. А ево и како.

Већ смо се упознали са проширењима облика $E(\alpha)$. Но, ако $\beta \notin E(\alpha)$, може се формирати и проширење $E(\alpha)(\beta)$, које се краће означава са $E(\alpha, \beta)$. Уколико су α и β алгебарски над E, онда су степени проширења $[E(\alpha) : E]$ и $E(\beta) : E]$ коначни, а такав мора бити и $E(\alpha, \beta) : E(\alpha)]$ (зашто?). Стога је, на основу претходног става, $[E(\alpha, \beta) : E]$ коначан број, те је проширење $E(\alpha, \beta)$ поља E алгебарско, те је сваки елемент из $E(\alpha, \beta)$, алгебарски над E. Посебно, то су и елементи $\alpha + \beta$, $\alpha \cdot \beta$ и слично.

Општије, имамо и проширења $E(\alpha_1, \ldots, \alpha_n)$. Но, веома је занимљив следећи резултат који нам каже да у случају алгебарских проширења поља $\mathbb{Q}$ ситуација није толико компликована колико изгледа.

Теорема 88 (Теорема о примитивном елементу за бројевна поља) Свако коначно проширење E поља $\mathbb{Q}$ је облика $\mathbb{Q}(\alpha)$, за неко $\alpha \in E$.

Елемент α је тај примитивни елемент проширења E. Ову теорему нећемо доказивати, урадићемо неке примере. Но, пре тих примера, докажимо одговарајући резултат за коначна поља.

Теорема 89 (Теорема о примитивном елементу за коначна поља) Свако коначно проширење E коначног поља F је облика $F(\alpha)$, за неко $\alpha \in E$.

Доказ. Како је поље F коначно и E је коначно проширење поља F, то је и поље E коначно (зашто?). Но, ми знамо да је тада група $(E \setminus \{0\}, \cdot)$ циклична (зашто?), тј. постоји елемент $\alpha \in E$ такав да је $E \setminus \{0\} = \{\alpha^k : k \geq 0\}$. Но, јасно је да је тада и $E = F(\alpha)$. □

Пример 90 Наћи примитивни елемент коренског поља полинома $X^4 - X^2 - 2 \in \mathbb{Q}[X]$.

Другим речима, треба наћи коренско поље K датог полинома и елемент $\alpha \in K$ за који је $K = \mathbb{Q}(\alpha)$. Факторишимо наш полином над $\mathbb{Q}$ коришћењем метода комплетирања квадрата:

$$X^4 - X^2 - 2 = \left(X^2 - \frac{1}{2}\right)^2 - \frac{1}{4} - 2 = \left(X^2 - \frac{1}{2}\right)^2 - \left(\frac{3}{2}\right)^2 =$$

$$= \left(X^2 - \frac{1}{2} - \frac{3}{2}\right)\left(X^2 - \frac{1}{2} + \frac{3}{2}\right) = \left(X^2 - 2\right)\left(X^2 + 1\right) =$$
$$= (X - \sqrt{2})(X + \sqrt{2})(X - i)(X + i),$$

где је i наравно имагинарна јединица. Дакле, коренско поље K је поље $K = \mathbb{Q}(\sqrt{2}, i)$. Ми треба да нађемо α за које је $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\alpha)$. Покушајмо да докажемо да се за α може узети елемент $\alpha = \sqrt{2} + i$. Јасно је да је $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Обратна инклузија је нетривијална. Наравно, довољно је да докажемо да нпр. $\sqrt{2} \in \mathbb{Q}(\alpha)$, пошто из тога непосредно следи да и $i \in \mathbb{Q}(\alpha)$, а тиме и тражено. Једнакост

$$\alpha = \sqrt{2} + i,$$

„подигнимо" на трећи степен. Добијамо

$$\alpha^3 = 2\sqrt{2} + 6i - 3\sqrt{2} - i = -\sqrt{2} + 5i = 5(\sqrt{2} + i) - 6\sqrt{2}.$$

Дакле,

$$\alpha^3 - 5\alpha = 6\sqrt{2},$$

па је

$$\sqrt{2} = \frac{1}{6}(\alpha^3 - 5\alpha) \in \mathbb{Q}(\alpha).$$

♣

Пример 91 Нека је K коренско поље полинома $X^4 - 24X^2 + 4 \in \mathbb{Q}[X]$.
а) Показати да је $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.
б) Одредити $\alpha \in \mathbb{C}$ тако да је $K = \mathbb{Q}(\alpha)$.

Поступимо као у претходном примеру.

$$\begin{aligned} X^4 - 24X^2 + 4 &= (X^2 - 12)^2 - 144 + 4 \\ &= (X^2 - 12)^2 - 140 \\ &= (X^2 - 12)^2 - (2\sqrt{35})^2 \\ &= (X^2 - 12 - 2\sqrt{35})(X^2 - 12 + 2\sqrt{35}) \\ &= (X^2 - (12 + 2\sqrt{35})(X^2 - (12 - 2\sqrt{35}), \end{aligned}$$

те добијамо $X^4 - 24X^2 + 4 = (X - \sqrt{12 + 2\sqrt{35}})(X + \sqrt{12 + 2\sqrt{35}})(X - \sqrt{12 - 2\sqrt{35}})(X + \sqrt{12 - 2\sqrt{35}})$. Према томе, добијамо да је

$$K = \mathbb{Q}\left(\sqrt{12 + 2\sqrt{35}}, \sqrt{12 - 2\sqrt{35}}\right).$$

Један савет: увек када добијете овакав резултат, није лоше помножити ова два корена и видети шта се добија. Применимо тај савет у овом случају.

$$\sqrt{12 + 2\sqrt{35}} \cdot \sqrt{12 - 2\sqrt{35}} = \sqrt{144 - 140} = \sqrt{4} = 2.$$

Дакле, можемо да закључимо да, ако је $\alpha = \sqrt{12 + 2\sqrt{35}}$, а $\beta = \sqrt{12 - 2\sqrt{35}}$, онда је $\alpha \cdot \beta = 2$, па је $\beta = \frac{2}{\alpha} \in \mathbb{Q}(\alpha)$. Закључујемо да је $K = \mathbb{Q}(\alpha)$. Тако смо нашли примитивни елемент и урадили пример под б)!

Други савет: када имате корен попут овога: $\sqrt{12 + 2\sqrt{35}}$, проверите да можда не можете да га „препознате". Шта то значи? У овом случају, појављује се корен из броја облика $p + q\sqrt{s}$ где су p, q, s цели бројеви. Да ли је можда тај корен збир (или разлика) два корена из неких целих бројева? Како је $35 = 5 \cdot 7$, намеће се да израчунамо колико је $(\sqrt{5} + \sqrt{7})^2$. Добијамо

$$(\sqrt{5} + \sqrt{7})^2 = 5 + 2\sqrt{35} + 7 = 12 + 2\sqrt{35},$$

тј. баш оно што имамо. Дакле, $\alpha = \sqrt{5} + \sqrt{7}$ (приметимо да је $\beta = \sqrt{7} - \sqrt{5}$), те је $K = \mathbb{Q}\left(\sqrt{5} + \sqrt{7}\right)$. Ми треба да покажемо да је $K = \mathbb{Q}\left(\sqrt{5}, \sqrt{7}\right)$. То није тешко, поступићемо као у претходном примеру.

$$\begin{aligned}
\alpha &= \sqrt{5} + \sqrt{7} \\
\alpha^3 &= 5\sqrt{5} + 15\sqrt{7} + 21\sqrt{5} + 7\sqrt{7} \\
\alpha^3 &= 26\sqrt{5} + 22\sqrt{7} \\
22\alpha &= 22\sqrt{5} + 22\sqrt{7} \\
\alpha^3 - 22\alpha &= 4\sqrt{5} \\
\sqrt{5} &= \frac{\alpha^3 - 22\alpha}{4} \in \mathbb{Q}(\alpha) \\
\sqrt{7} &= \alpha - \sqrt{5} \\
\sqrt{7} &= \frac{26\alpha - \alpha^3}{4} \in \mathbb{Q}(\alpha).
\end{aligned}$$

Наравно, могли смо то да урадимо и другачије. Пошто смо већ препознали да је $\beta = \sqrt{7} - \sqrt{5}$, онда само треба показати да је

$$\mathbb{Q}\left(\sqrt{5} + \sqrt{7}, \sqrt{7} - \sqrt{5}\right) = \mathbb{Q}\left(\sqrt{5}, \sqrt{7}\right),$$

а то је наравно врло једноставно.