0.1 Дејство групе на скуп

0.1.1 Дефиниција дејства и основни појмови

Дефиниција 0.1. Нека је G било која група и X непразан скуп. Дејство групе G на скуп X је свако пресликавање $\cdot : G \times X \to X$ за које важи: 1) $g \cdot (h \cdot x) = (gh) \cdot x$; 2) $e \cdot x = x$ за све $g, h \in G$, $x \in X$, при чему је e неутрал групе G.

Дефиниција 0.2. Нека је G било која група и X непразан скуп. Дејство групе G на скуп X је сваки хомоморфизам $\phi : G \to S_X$, где је S_X симетрична група скупа X (група свих пермутација скупа X).

Показаћемо да су ове две дефиниције еквивалентне.

Деф1 $\Rightarrow$ Деф2:
Ако је $\cdot$ једно дејство, како оно индукује хомоморфизам $\phi : G \to S_X$? -Сваком елементу $g \in G$ придружићемо пермутацију $\pi_g \in S_X$, одређену са $\pi_g(x) = g \cdot x$. За почетак треба проверити да смо заиста добили пермутацију, односно бијекцију скупа X: π_g је "1-1" јер $\pi_g(x) = \pi_g(y) \Leftrightarrow g \cdot x = g \cdot y \Leftrightarrow g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g \cdot y) \Leftrightarrow (g^{-1}g) \cdot x = (g^{-1} \cdot g) \cdot y \Leftrightarrow e \cdot x = e \cdot y \Leftrightarrow x = y$
π_g је "на" јер $y = \pi_g(x) \Leftrightarrow y = g \cdot x \Leftrightarrow g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) \Leftrightarrow g^{-1} \cdot y = (g^{-1}g) \cdot x \Leftrightarrow g^{-1} \cdot y = e \cdot x \Leftrightarrow x = g^{-1} \cdot y$ Дакле, за свако $g \in G$ пресликавање π_g је пермутација из S_X. Сада треба показати да је придруживање $\phi : G \to S_X$, $\phi(g) = \pi_g$ један хомоморфизам група G и S_X: $\phi(gh) = \pi_{gh} = \pi_g \circ \pi_h = \phi(g) \circ \phi(h)$ јер $\pi_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = \pi_g(\pi_h(x)) = (\pi_g \circ \pi_h)(x)$ за све $x \in X$.

Деф2 $\Rightarrow$ Деф1:
Нека је сада $\phi : G \to S_X$ један хомоморфизам група. Како да помоћу њега дефинишемо пресликавање $\cdot : G \times X \to X$ које задовољава услове 1) и 2) из прве дефиниције дејства? -Ставићемо $g \cdot x = \phi(g)(x)$. Проверавамо 1): $g \cdot (h \cdot x) = \phi(g)(\phi(h)(x)) = (\phi(g) \circ \phi(h))(x) = \phi(gh)(x) = gh \cdot x$ 2) $e \cdot x = \phi(e)(x) = Id_X(x) = x$

Свако дејство индукује две врсте подскупова, једне од X, а друге од G.

Дефиниција 0.3. Нека група G дејствује на непразном скупу X. Ако је x било који елемент (тачка) из X, *орбита* тачке x је

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

Из услова из дефиниције дејства одмах следи да је са

$$x \sim y \Leftrightarrow y \in \Omega_x$$

дефинисана једна релација еквиваленције:

рефлексивност: $x \sim x \Leftrightarrow x \in \Omega_x$, а ово је тачно јер $x = e \cdot x$
симетричност:$x \sim y \Leftrightarrow y \in \Omega_x \Leftrightarrow y = g \cdot x$ за неко $g \in G$, одакле је $x = g^{-1} \cdot y$, па $x \in \Omega_y$, тј. $y \sim x$

транзитивност: $x \sim y \ \wedge \ y \sim z \ \Leftrightarrow \ y \in \Omega_x \ \wedge \ z \in \Omega_y \ \Leftrightarrow \ y = g \cdot x \wedge z = h \cdot y$ за неке $g, h \in G$, а онда је $z = h \cdot (g \cdot x) = (hg) \cdot x$, па $z \in \Omega_x$, односно $x \sim z$
Класе ове еквиваленције су управо орбите:

$$C_x = \{y \in X : x \sim y\} = \{y \in X : y \in \Omega_x\} = \Omega_x.$$

Одавде следи веома важна особина орбита, коју ћемо користити више пута у наставку: различите орбите су дисјунктне и њихова унија је управо скуп X. Такође, за дејство кажемо да је *транзитивно* ако има тачно једну орбиту. То значи да за сваке две тачке $x, y \in X$ постоји $g \in G$ за које је $y = g \cdot x$.

Друга врста подскупова које придружујемо једном дејству налази се у G и за њих ће се испоставити да су и подгрупа.

Дефиниција 0.4. *Стабилизатор* елемента (тачке) $x \in X$ у односу на уочено дејство је

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

Поново користимо услове из дефиниције дејства да докажемо да је Σ_x подгрупа од G: из првог услова следи да ако $g, h \in \Sigma_x$, тј. $g \cdot x = x$ и $h \cdot x = x$, онда $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, односно $gh \in \Sigma_x$; из другог је $e \in \Sigma_x$ (јер $e \cdot x = x$) и на крају из $g \in \Sigma_x$, тј. $g \cdot x = x$ множењем са g^{-1} добијамо $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$, односно $(g^{-1}g) \cdot x = g^{-1} \cdot x$ или $x = g^{-1} \cdot x$, па $g^{-1} \in \Sigma_x$.

Теорема 0.1. *Ако је $\cdot : G \times X \to X$ било које дејство коначне групе G на скуп X, број елемената орбите произвољне тачке $x \in X$ је једнак индексу њеног стабилизатора у групи G:*

$$|\Omega_x| = [G : \Sigma_x]$$

Доказ. Знамо да је индекс неке подгрупе број њених левих (или десних) косета, односно $[G : \Sigma_x] = |G/\Sigma_x|$. Да би два скупа била истобројна, треба наћи бијекцију између њих. Из саме дефиниције орбите и косета, одмах имамо природно пресликавање $f : \Omega_x \to G/\Sigma_x$, дато са

$$f(g \cdot x) = g\Sigma_x.$$

Покажимо да је f инјективно: $f(g \cdot x) = f(h \cdot x) \ \Leftrightarrow \ g\Sigma_x = h\Sigma_x \ \Leftrightarrow \ g^{-1}h \in \Sigma_x \ \Leftrightarrow \ (g^{-1}h) \cdot x = x \ \Leftrightarrow \ g^{-1} \cdot (h \cdot x) = x \ \Leftrightarrow g \cdot x = h \cdot x$;

и сурјективно: ако је $g\Sigma_x \in G/\Sigma_x$ произвољан косет, за елемент g који га одређује је $f(g \cdot x) = g\Sigma_x$.

Дакле, f је бијекција и $|\Omega_x| = |G/\Sigma_x| = [G : \Sigma_x]$. Ово се може написати и као $|\Omega_x| = \frac{|G|}{|\Sigma_x|}$ или $|\Omega_x||\Sigma_x| = G|$. □

Бернсајдова лема

Следеће тврђење је основно средство за одређивање броја орбита дејства коначне групе на скуп.

Теорема 0.2. (Бернсајдова лема) *Нека је $\cdot : G \times X \to X$ дејство коначне групе G на коначан скуп X и нека је $Fix(g) = \{x \in X : g \cdot x = x\}$ скуп тачака које фиксира елемент $g \in G$. Означимо са X/G скуп свих орбита овог дејства. Тада је*

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

Доказ. Посматрајмо скуп $\{(x, g) : g \cdot x = x\}$. Њега можемо да пребројимо на два начина, "уздуж" и "попреко":

$$|\{(x, g) : g \cdot x = x\}| = \sum_{g \in G} |Fix(g)| = \sum_{x \in X} |\Sigma_x|.$$

Сада из $\sum_{g \in G} |Fix(g)| = \sum_{x \in X} |\Sigma_x|$ и претходне теореме добијамо

$$\sum_{g \in G} |Fix(g)| = \sum_{x \in X} \frac{|G|}{|\Omega_x|},$$

односно

$$\frac{1}{|G|} \sum_{g \in G} |Fix(g)| = \sum_{x \in X} \frac{1}{|\Omega_x|}.$$

Нека је Ω_x произвољна орбита. Она има $|\Omega_x|$ елемената, и разломак $\frac{1}{|\Omega_x|}$ се појављује у суми на десној страни претходне једнакости по једном за свако $x \in \Omega_x$, дакле $|\Omega_x|$ пута укупно. То значи да свака орбита тој суми дода јединицу, па је десна страна у ствари бројач орбита:

$$\sum_{x \in X} \frac{1}{|\Omega_x|} = \sum_{\Omega \in X/G} 1 = |X/G|.$$

Сада само изједначимо са левом страном и добијемо тражену формулу за број свих орбита уоченог дејства

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |Fix(g)|.$$

□

Примери дејстава

1) Нека је G група свих ротација еуклидске равни E око фиксиране тачке O (лако се провери да је G група, композиција две ротације око тачке O је ротација за збир њихових углова, идентитета је ротација за 0 степени, ротација инверзна ротацији за угао θ је ротација за $-\theta$). G дејствује на E тако што ротација ρ помери тачку A у $\rho(A)$. Опет се лако види да ротација за φ, па за θ, тачку A помера исто као ротација за $\varphi + \theta$, а идентитета фиксира све тачке, односно да су задовољени услови дејства. Шта су орбите и стабилизатори овог дејства? - Орбите су сви концентрични кругови са центром у O. Стабилизатор сваке тачке је id.

2) Нека је G група и H подгрупа групе G. Означимо са X количнички скуп G/H и посматрајмо пресликавање $\cdot : G \times X \to X$ одређено са $g \cdot (aH) = gaH$. Праволинијски следи да су испуњени услови из дефиниције дејства: $1) g \cdot (h \cdot (aH)) = g \cdot (haH) = ghaH = (gh) \cdot aH$; $2)$ $e \cdot aH = eaH = aH$. Тврдимо да је ово дејство транзитивно: ако је aH фиксиран косет и bH произвољан, онда $bH \in \Omega_{aH}$ јер једначина $ga = b$ има решење по g у групи G, па је $g \cdot aH = bH$. Дакле, постоји само једна орбита овог дејства, $\Omega_{aH} = G/H$.

3) Нека је $G = C_n = \{z \in \mathbb{C} : z^n = 1\}$ - група n-тих корена јединице $C_n = \{cos\frac{2k\pi}{n} + isin\frac{2k\pi}{n} : 0 \leq k < n\}$, па одмах следи да је C_n изоморфна цикличној групи C_n. G дејствује на комплексне бројеве на следећи начин: $g \cdot z = gz$ - множење два комплексна броја, па тривијално важе услови за дејство (геометријски ово је ротација око координатног почетка за угао $\frac{2k\pi}{n}$)

Ако је $z \neq 0$, $\Omega_z = \{z(cos\frac{2k\pi}{n} + isin\frac{2k\pi}{n}) : 0 \leq k < n\} = \{ze^{\frac{2k\pi}{n}} : 0 \leq k < n\}$, а $\Omega_0 = 0$. Орбите тачака $z \neq 0$ су n-точлане, па су по теореми о орбити и стабилизатору, стабилизатори једночлани, $\Sigma_z = 1$, $z \neq 0$, док је орбита нуле једночлана, па је њен стабилизатор цела група G, $\Sigma_0 = C_n$.

-Још један важан пример дејства је дејство групе на саму себе, конјугацијом.

0.1.2 Конјугација и једначина класа

Нека је G произвољна група. За $X = G$ посматрајмо пресликавање $\cdot : G \times X \to X$ дато са $g \cdot x = gxg^{-1}$, $g, x \in G$. Проверимо да је ово заиста једно дејство: $1)$ $g \cdot (h \cdot x) = g \cdot (hxh^{-1}) = ghxh^{-1}g^{-1} = (gh)x(gh)^{-1} = (gh) \cdot x$ $2)$ $e \cdot x = exe^{-1} = x$.

Ово дејство зовемо дејство групе на саму себе конјугацијом.

Хајде да нађемо орбите и стабилизаторе овог дејства.

$\Omega_x = \{g \cdot x : g \in G\} = \{gxg^{-1} : g \in G\} = K_x$ - класа конјугације елемента x у групи G. Приметимо да оно што знамо да важи за орбите овде има за последицу да су две различите класе конјугације и дисјунктне и да је група G унија класа конјугације њених елемената.

$\Sigma_x = \{g \in G : g \cdot x = x\} = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = C_x$ - централизатор елемента x у групи G

Ако је група G коначна, из теореме о орбити и стабилизатору знамо да $|\Omega_x| \mid |G|$. Питамо се шта значи да је орбита неке тачке при овом дејству једночлана:

$|\Omega_x| = 1 \Leftrightarrow |K_x| = 1 \Leftrightarrow gxg^{-1} = x, \forall g \in G \Leftrightarrow gx = xg, \forall g \in G \Leftrightarrow x \in C_G = Z(G)$

Дакле, класа конјугације елемента x је једночлана акко је тај елемент у центру групе G, па је број једночланих класа конјугације управо ред центра групе. Даље, знамо да је сваки скуп на који нека група дејствује, унија дисјунктних орбита тог дејства, па је $G = \bigsqcup \Omega_x = \bigsqcup K_x$ што имплицира да је ред групе G збир бројева елемената па дисјунктним класама конјугације:

$$|G| = \sum |K_x| = \sum_{|K_x|=1} |K_x| + \sum_{|K_x|>1} |K_x| = |C_G| + \sum_{|K_x|>1} |K_x|.$$

Додатно важи да број елемената у свакој орбити дели ред групе G (јер је једнак индексу стабилизатора одговарајуће тачке): $|\Omega_x| = |K_x| \mid |G|$, па је друга сума не само по бројевима већим од 1, него по неким делиоцима $|G|$ већим од 1. Овим смо доказали тврђење које има посебан назив и доста примена у наставку:

Теорема 0.3. (Једначина класа) *Ако је G коначна група, C_G њен центар и K_x њене класе конјугације са бар по два елемента, онда $|K_x| \mid |G|$ и*

$$|G| = |C_G| + \sum_{|K_x|>1} |K_x|.$$

Пример 0.1. Ако је G група чији је ред p^n, где је p прост, а n природан број, онда њен центар није тривијалан, $C_G \neq \{e\}$.

-Из једначине класа имамо $|G| = |C_G| + \sum_{|K_x|>1} |K_x|$, при чему бројеви $|K_x|$ деле $|G|$. Овде је $|G| = p^n$, па су и сви $|K_x|$ облика p^k за $1 \leq k$. Дакле, $p \mid \sum_{|K_x|>1} |K_x|$, а свакако $p \mid |G|$, па онда $p \mid |G| - \sum_{|K_x|>1} |K_x|$, што је управо ред центра. То значи да ред центра није 1, и да је дељив са p.

Дефиниција 0.5. Група чији је ред степен простог броја p зове се p-група.

- На пример, група реда 49 је 7-група, а група реда 125 је 5-група.

Пример 0.2. Свака група реда p^2, где је p прост број, је комутативна.
-Из Лагранжове теореме имамо да ред центра дели ред групе, а из претходног примера следи да ред центра ове групе није 1. Остају две могућности: ред центра је p или ред центра је p^2. Прва отпада јер ако би ред центра био p, онда би и његов индекс у групи G био p, а знамо од раније да "индекс центра није прост број". Дакле, ред центра је исто p^2, па је $C_G = G$, а самим тим је и цела G комутативна.

Такође, према теореми о класификацији комутативних група, можемо у потпуности да опишемо овакве групе: оне су или цикличне или директни производи две цикличне групе:

$$|G| = p^2 \;\Rightarrow\; G \cong Z_{p^2} \;\vee\; G \cong Z_p \times Z_p.$$

Пример 0.3. Број различитих конјугата подгрупе H у коначној групи G једнак је индексу њеног нормализатора у тој групи.
-Да се подсетимо шта је нормализатор неког скупа S у групи G, $S \subset G$: $N_S = \{g \in G : gS = Sg\}$. То је увек подгрупа групе G (проверите ако нисте до сада). Посебно, за S можемо да узмемо неку подгрупу и онда добијамо нормализатор подгрупе $N_H = \{g \in G : gH = Hg\}$. То је подгрупа групе G која садржи H и заправо је највећа подгрупа групе G у којој је H нормална, јер се дефиниција нормализатора може написати и овако: $N_H = \{g \in G : gHg^{-1} = H\}$.

Вратимо се сада на наш пример. Уочићемо дејство групе G на скуп X свих подгрупа групе G: $X = \{H : H \leq G\}$, дато са $g \cdot H = gHg^{-1}$, $g \in G$, $H \in X$ (провера да је ово дејство је иста као код дејства конјугацијом на елементе). Јасно је да су у орбити тачке (тј. подгрупе) H сви њени конјугати, па је број елемената у орбити једнак броју различитих конјугата подгрупе H. Шта је стабилизатор тачке H?

$\Sigma_H = \{g \in G : g \cdot H = H\} = \{g \in G : gHg^{-1} = H\} = \{g \in G : gH = Hg\} = N_H$ - нормализатор подгрупе H у групи G.

Из теореме о орбити и стабилизатору следи да је број елемената у орбити једнак индексу стабилизатора, а код нас то тачно значи да је број различитих конјугата подгрупе H једнак индексу њеног нормализатора у групи G.

0.1.3 Кошијева лема

Из Лагранжове теореме знамо да ред елемента у коначној групи G дели ред саме групе. Обрнуто, наравно, не важи: за сваки број k који дели $|G|$, у G не мора да постоји елемент реда k. Међутим, ако је k прост, то ће важити.

Теорема 0.4. (Кошијева лема) *Ако је ред коначне групе G дељив простим бројем p, онда у G постоји елемент реда p.*

Доказ. Пре свега, приметимо да је елемент g реда p, где је p прост, акко је $g \neq e$ и $g^p = e$ (ово следи из $g^k = e \;\Rightarrow\; \omega(g) \mid k$). Нека је $C_p = \langle a \rangle$ циклична група реда p. Посматраћемо скуп X оних p-торки са компонентама из G чији је производ једнак неутралу e групе G,

$$X = \{(g_1, g_2, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = e\}$$

и пресликавање $\cdot : C_p \times X \to X$ дато на генератору са $a \cdot (g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1)$ (односно на било ком елементу a^i са $a^i \cdot (g_1, g_2, \ldots, g_p) = (g_{i+1}, g_{i+2}, \ldots, g_p, g_1, \ldots, g_i)$.) Пре свега треба проверити да смо овим цикличним померањем компонената дате p-торке остали у скупу X, односно да из $g_1 g_2 \cdots g_p = e$ следи $g_2 g_3 \cdots g_p g_1 = e$. Ово је тачно јер множењем прве једнакости слева са g_1^{-1} добијамо $g_2 \cdots g_p = g_1^{-1}$, а када ову једнакост помножимо са g_1 здесна добијамо управо $g_2 g_3 \cdots g_p g_1 = e$. Даље, множењем ове једнакости са g_2^{-1} добили бисмо $g_3 \cdots g_p g_1 g_2 = e$ итд.

Јасно је да је ово пресликавање једно дејство цикличне групе C_p на X (множење са a^i помери првих i компонената p-торке на крај, а даље множење са a^j пребаци следећих j елемената иза оних i - ефекат је исти као да смо множили са a^{i+j}; такође, $e = a^p$ помери циклично p-торку за p места, односно она остаје иста).

Приметимо да лако можемо да одредимо број елемената у скупу X - у $(g_1, g_2, \ldots, g_p)$ за коју је $g_1 g_2 \cdots g_p = e$ можемо произвољно да изаберемо $g_1, g_2, \ldots, g_{p-1}$, а онда је g_p одређено са $g_p = (g_1 g_2 \cdots g_{p-1})^{-1}$. За сваки од првих $p-1$ елемената имамо $|G|$ могућности, па је $|X| = |G|^{p-1}$. Посебно, пошто $p \mid |G|$, следи да $p \mid |X|$ (штавише, $p^{p-1} \mid |X|$).

Кад смо одредили $|X|$ идемо на сумирање по дисјунктним орбитама:

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

$$|X| = |\Omega_1| + |\Omega_2| + \cdots + |\Omega_n|.$$

Знамо да је број елемената у орбити једнак индексу стабилизатора одговарајуће тачке, што значи да дели ред групе која дејствује. Како је код нас то група C_p, следи да $|\Omega_i| \in \{1, p\}$ за свако $1 \leq i \leq n$. Једну једночлану орбиту сигурно имамо, то је $\Omega_{(e,e,\ldots,e)}$. Тврдимо да мора постојати бар још једна једночлана орбита, јер бисмо у супротном имали:

$$|X| = 1 + (n-1)p,$$

али $p \mid |X|$, па би следило да $p \mid 1$, контрадикција! Дакле, и орбита неке тачке $(g_1, g_2, \ldots, g_p)$ је једночлана. Шта то значи?

$$a \cdot (g_1, g_2, \ldots, g_p) = (g_1, g_2, \ldots, g_p) \;\Rightarrow\; (g_1, g_2, \ldots, g_p) = (g_2, g_3, \ldots, g_p, g_1),$$

а ово даје да је $g_1 = g_2 = \cdots = g_p \ (= g)$. Дакле, све компоненте те тачке су међусобно једнаке (и различите од e јер је то друга тачка чија је орбита једночлана). Сада из тога да та тачка припада скупу X имамо $g \cdot g \cdots g = e$, $g \neq e$, односно $g^p = e$ и $g \neq e$. Према првој реченици у доказу, g је елемент реда p. □

0.1.4 Теорема о факторијелу

Теорема 0.5. (Теорема о факторијелу) *Нека је H подгрупа групе G коначног индекса n. Тада постоји нормална подгрупа N групе G која је садржана у H и за чији индекс у групи G важи:*

$$[G : N] \mid n!.$$

Доказ. Нека је $X = G/H$. Јасно је да је $\mid X \mid = [G : H] = n$. Имали смо код примера дејстава да је пресликавање $\cdot : G \times X \to X$ дефинисано са $g \cdot (aH) = gaH$ једно дејство групе G на скуп X. Сетимо се друге дефиниције дејства - ово је еквивалентно томе да је $\phi : G \to S_X$ дато са $\phi(g)(aH) = gaH$ хомоморфизам група. Језгро овог хомоморфизма је нормална подгрупа од G. Тврдимо да је она садржана у H:
нека $g \in Ker\phi$, то значи да је $\phi(g) = Id_X \ \Leftrightarrow \ \phi(g)(aH) = aH$ за свако $a \in G$, односно $gaH = aH$ за свако $a \in G$. Посебно, $gH = H$, а одавде $g \in H$, што даје $Ker\phi \subset H$.
Сада применимо Прву теорему о изоморфизмима група: $G/Ker\phi \cong Im\phi$, али $Im\phi \leq S_X = S_n$, па $|Im\phi| \mid |S_n| = n!$, односно $|G/Ker\phi| \mid n!$ или еквивалентно $[G : Ker\phi] \mid n!$.

Дакле, $Ker\phi$ је тражена нормална подгрупа - садржана је у H и коначног је индекса. □

Испоставља се да је $Ker\phi = CoreH$, где је $CoreH$ дефинисана као пресек свих конјугата подгрупе H: $CoreH = \bigcap_{a \in G} aHa^{-1}$ - карактеризација ове подгрупе је да је то највећа подгрупа од H која је нормална у G! $(\star)$

$Ker\phi = CoreH$:
$\subseteq$: $Ker\phi$ је подгрупа од H која је нормална у G, а $CoreH$ је највећа таква, па $Ker\phi \subseteq CoreH$
$\supseteq$: нека $g \in CoreH$, онда $g \in aHa^{-1}, \forall a \in G \ \Leftrightarrow \ ga \in aH, \forall a \in G \ \Leftrightarrow \ gaH = aH, \forall a \in G \ \Leftrightarrow \ \phi(g) = Id_X \ \Rightarrow \ g \in Ker\phi$

$\star$: Нека је $H \leq G$ и $CoreH = \bigcap_{a \in G} aHa^{-1}$. Пре свега, $CoreH$ је подгрупа од G као пресек неких подгрупа (конјугати подгрупе су подгрупе; пресек произвољне фамилије подгрупа је опет подгрупа). $CoreH \subseteq H$ јер је и H међу подгрупама чији је $CoreH$ пресек. Даље, $CoreH \lhd G$: узмимо произвољно $b \in G$ и посматрајмо $bCoreHb^{-1}$,

$$bCoreHb^{-1} = b(\bigcap_{a \in G} aHa^{-1})b^{-1} = \bigcap_{a \in G} baH(ba)^{-1} = CoreH.$$

Последња једнакост следи из тога што је множење у групи бијекција, па кад a "прође" цело G исто се деси и са ba за фиксирано $b \in G$. На крају, ако је K нормална подгрупа од G садржана у H, тада је за свако $a \in G$, $K = aKa^{-1} \subseteq aHa^{-1}$, па је онда K садржана

и у пресеку свих конјугата од H, а то је тачно $CoreH$, $K \subseteq CoreH$. Дакле, $CoreH$ је највећа подгрупа од H која је нормална у G.

Пример 0.4. Нека је H подгрупа групе G чији је индекс p најмањи прост број који дели $|G|$. Тада је H нормална подгрупа групе G.

-Применимо $n!$-теорему: $[G : CoreH] \mid p!$. Број $[G : CoreH]$ има своју факторизацију облика $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, где су сви $p_i \geq p$ због услова да је p најмањи прост број који дели $|G|$, а $[G : CoreH]$ је један делилац броја $|G|$. Одавде следи да за свако i, $p_i \mid p!$. С друге стране, у $p!$ се не појављују прости бројеви већи од p, што даје $p_i = p$ за све i. Закључујемо да је $[G : CoreH] = p^\alpha$, а онда из $p^\alpha \mid p!$ добијамо $\alpha = 1$. Дакле, $[G : CoreH] = p$, што упоређено са $[G : H] = p$ и $CoreH \subseteq H$ коначно даје $H = CoreH$, а самим тим је и H нормална подгрупа од G.

Примена $n!$-факторијел теореме иде у два правца: некада показујемо да је $H = CoreH$ чиме добијамо да је H нормална, а некада само тражимо праву нормалну подгрупу од G (то ће бити $CoreH$) да бисмо показали да G није проста. У сваком случају за H бирамо подгрупу малог индекса.

0.2 Теореме Силова

На основу Лагранжове теореме, ако је H подгрупа коначне групе G, тада $|H| \mid |G|$. Обрат овог тврђења не важи у општем случају: ако неки број дели ред групе G, G не мора да има подгрупу тог реда (видели смо да ово нпр. важи код цикличних група). Ипак, подгрупе одређених редова (који су прости бројеви или степени простих бројева) постоје у свакој коначној групи. Више информација о њима дају нам теореме Силова.

0.2.1 Прва теорема Силова

Теорема 0.6. (Прва теорема Силова) *Нека је G група чији је ред $|G| = p^r m$, где је p прост број, m и r природни, и m није дељив са p. Тада група G има подгрупу реда p^r.*

Доказ. Доказ изводимо индукцијом по реду групе G, односно и по r и по m. База индукције су случајеви $r = 1$ или $m = 1$. Ако је $r = 1$, тврђење следи из Кошијеве леме, док је за $m = 1$ сама група G тражена подгрупа. Претпоставимо сада да тврђење важи за све групе реда $p^s n$ при чему је или $1 \leq s < r$ или $1 \leq n < m$ и наравно p не дели n.

Разликујемо два случаја:

1) У G постоји права подгрупа H таква да p не дели индекс $[G : H]$.

Из Лагранжове теореме је $|G| = |H|[G : H] = p^r m$, па пошто p не дели $[G : H]$, биће $|H| = p^r n$, где n није дељив са p и $n < m$. На основу индуктивне претпоставке, H има подгрупу реда p^r, што је онда и тражена подгрупа групе G.

2) p дели индекс сваке праве подгрупе групе G.

Овде примењујемо 3 тврђења која знамо од раније.

-Прво је једначина класа: $|G| = |C_G| + \sum_{|K_x|>1} |K_x|$, при чему су бројеви $|K_x| = |\Omega_x|$ па су једнаки индексима одговарајућих стабилизатора $[G : \Sigma_x]$. Сви ови индекси су дељиви са p, из чега следи да је и ред центра $|C_G|$ дељив са p.

-Даље, на основу Кошијеве леме постоји елемент x из центра чији је ред баш p. Посматрајмо подгрупу $H = \langle x \rangle$ која је такође реда p. Штавише, она је и нормална подгрупа групе G, јер x припада центру, па комутира са свим елементима из G. Дакле, имамо $|G/H| = p^{r-1} m$ и онда можемо применити индуктивну претпоставку: G/H има подгрупу $\mathcal{K}$ реда p^{r-1}

-На крају, примењујемо Трећу теорему о изоморфизмима која каже да $\mathcal{K}$ мора бити облика $\mathcal{K} = K/H$, где је K подгрупа групе G која садржи H ($K = \{a \in G : aH \in \mathcal{K}\}$ или $K = \pi^{-1}(\mathcal{K})$, где је $\pi : G \to G/H$ природни епиморфизам). Онда је

$$|K| = |H||K/H| = |H||\mathcal{K}| = pp^{r-1} = p^r$$

и K је подгрупа групе G коју смо тражили. □

Дефиниција 0.6. Ако је G група чији је ред $|G| = p^r m$, где је p прост број, $r \geq 1$ и m природан број који није дељив са p, тада сваку подгрупу од G реда p^r зовемо *Силовљева p-подгрупа групе G* или краће *S_p-подгрупа групе G*.

Дакле, претходна теорема тврди да Силовљеве p-подгрупе групе G постоје за сваки прост број p који дели ред групе G.

0.2.2 Друга теорема Силова

Теорема 0.7. (Друга теорема Силова) *Нека је G група чији је ред $|G| = p^r m$, где је p прост број, m и r природни, и m није дељив са p. Тада:*
1) Свака p-подгрупа групе G садржана је у некој Силовљевој p-подгрупи групе G.
2) Све Силовљеве p-подгрупе групе G су међусобно конјуговане.
3) Број свих Силовљевих p-подгрупа дели $|G|$.

Доказ. Нека су H и K произвољне подгрупе групе G и $X = G/K$. Пресликавање $H \times X \to X$ дефинисано са $(h, aK) \mapsto haK$ је једно дејство (имали смо код примера дејстава - косет дејство, G делује на скуп косета неке њене подгрупе). Пошто ово важи за било које две подгрупе, сада ћемо сукцесивно бирати H и K тако да добијемо жељена тврђења.
-Прво узимамо да је K нека Силовљева p-подгрупа групе G. Пошто је K реда p^r, скуп X има $|X| = |G/K| = \frac{|G|}{|K|} = \frac{p^r m}{p^r} = m$ елемената. Пребројмо сада X по дисјунктним орбитама уоченог дејства:

$$m = |X| = |\Omega_1| + |\Omega_2| + \cdots + |\Omega_n|.$$

Из услова да p не дели m добијамо да број елемената у бар једној орбити није дељив са p, нека је то орбита неке тачке aK, $|\Omega_{aK}|$ није дељив са p.
-Даље узмемо да је H p-подгрупа, $|H| = p^k$. На основу теореме о орбити и стабилизатору $|H| = p^k = |\Omega_{aK}||\Sigma_{aK}|$, где је aK косет из претходне реченице. Одавде имамо да број $|\Omega_{aK}|$ није дељив са p, а дели p^k, из чега закључујемо да он мора да буде 1: $|\Omega_{aK}| = 1$, односно да је $\Omega_{aK} = \{aK\}$. То даље значи да је $haK = aK$, $\forall h \in H$. Пошто aK није подгрупа, помножићемо са a^{-1} да добијемо подгрупу: $haKa^{-1} = aKa^{-1}$, $\forall h \in H$. Дакле, за подгрупу $\tilde{K} = aKa^{-1}$ је $h\tilde{K} = \tilde{K}$ за свако $h \in H$, односно $H\tilde{K} = \tilde{K}$, што повлачи да је $H \subset \tilde{K}$. Међутим, $|\tilde{K}| = |aKa^{-1}| = |K| = p^r$, па је и $\tilde{K}$ Силовљева p подгрупа.
Тиме смо показалаи да је произвољна p-подгрупа H садржана у некој Силовљевој p-подгрупи $\tilde{K}$.
-На крају ћемо узети да је и H Силовљева p-подгрупа. Сада из $H \subseteq \tilde{K}$ и $|H| = |\tilde{K}|$ следи да је $H = \tilde{K}$, тј. $H = aKa^{-1}$, односно H и K су конјуговане. То показује да су сваке две Силовљеве p-подгрупе међусобно конјуговане.

Дакле, укупан број Силовљевих p-подгрупа је једнак броју свих различитих конјугата било које од њих. Имали смо већ да је број конјугата неке подгрупе једнак индексу њеног нормализатора, што повлачи да тај број дели ред групе G, и тиме је доказано и последње тврђење ове теореме. □

Ако са $\mathcal{S}_p$ означимо скуп свих Силовљевих p-подгрупа и са $s_p = |\mathcal{S}_p|$, за сада имамо $s_p||G|$.

Желимо да докажемо да је број s_p конгруентан са 1 по модулу p. За то нам најпре треба следеће помоћно тврђење.
За било које дејство $\cdot : G \times X \to X$, означимо са

$$X^G = \{x \in X : g \cdot x = x,\ \forall g \in G\}$$

скуп његових фиксних тачака.

Лема 0.1. *Ако је G p-група и X коначан скуп, онда је*

$$|X^G| \equiv_p |X|.$$

Доказ. Као и раније, број елемената у скупу X једнак је збиру по дисјунктним орбитама: $|X| = |\Omega_1| + |\Omega_2| + \cdots + |\Omega_n| = \sum_{|\Omega_x|=1} |\Omega_x| + \sum_{|\Omega_x|>1} |\Omega_x|$. Приметимо одмах да су бројеви елемената у вишечланим орбитама дељиви са p јер је $|\Omega_x| = [G : \Sigma_x] = \frac{p^n}{|\Sigma_x|}$, па $1 < |\Omega_x| \mid p^n$ повлачи $p \mid |\Omega_x|$. С друге стране, $|\Omega_x| = 1 \ \Leftrightarrow\ g \cdot x = x,\ \forall g \in G \ \Leftrightarrow\ x \in X^G$. То управо значи да је скуп свих фиксних тачака унија једночланих орбита, па почетна једнакост постаје $|X| = |X^G| + p(\ldots)$ из чега следи $p \mid |X| - |X^G|$ што је еквивалентно са $|X^G| \equiv_p |X|$. □

Теорема 0.8. *Нека је G група чији је ред $|G| = p^r m$, где је p прост број који не дели m. Број Силовљевих p-подгрупа од G конгруентан је са 1 по модулу p:*

$$s_p \equiv_p 1.$$

Доказ. Нека је $X = \mathcal{S}_p$ скуп свих Силовљевих p-подгрупа групе G. Узмимо једну Силовљеву p-подгрупу, $H \in \mathcal{S}_p$, и посматрајмо њено дејство на X конјуговањем:
$\cdot : H \times X \to X$, $h \cdot K = hKh^{-1}$ (имали смо већ да је конјугација дејство, а $H \in \mathcal{S}_p \ \Rightarrow\ hKh^{-1} \in \mathcal{S}_p$).
Показаћемо да је скуп фиксних тачака овог дејства једночлан, $X^H = \{H\}$. Јасно је да $H \in X^H$, јер је $h \cdot H = hHh^{-1} = H$ за свако $h \in H$. Нека сада $K \in X^H$. То значи да је $h \cdot K = hKh^{-1} = K$, за свако $h \in H$, односно $hK = Kh$, за свако $h \in H$, или $HK = KH$ што знамо да је еквивалентно томе да је $HK \leq G$. Успут смо из $hKh^{-1} = K$, за свако $h \in H$, добили да је H садржана у нормализатору од K, $H \subseteq N_K$. Сада из $H \subseteq N_K$ и $K \subseteq N_K$ следи $HK \subseteq N_K$, па је посебно $K \lhd HK$. Примењујемо Другу теорему о изоморфизмима група: $HK/K \cong H/H \cap K$, односно $[HK : K] = [H : H \cap K]$. Међутим, $|HK| \mid |H||K|$, што повлачи да је HK p-подгрупа групе G, али $|H| \leq |HK| \leq p^r$, па је $|HK| = p^r$. То даље имплицира да је $[HK : K] = 1$, односно $[H : H \cap K] = 1$, тј. $H = H \cap K$. Ово значи да је $H \subseteq K$, и још су истих редова, па је коначно $H = K$.
Дакле, $X^H = \{H\}$, па је према претходној леми $|X| = |\mathcal{S}_p| \equiv_p |X^H| = 1$, односно

$$s_p \equiv_p 1.$$

□

Пошто смо већ доказали да $s_p||G|$, сада из $s_p|p^r m$ и $s_p \equiv_p 1$ следи $s_p|m$. Дакле, за број Силовљевих p-подгрупа групе G реда $p^r m$ важи $s_p|m$ и $s_p \equiv_p 1$. То нам омогућава да сузимо број могућих вредности за s_p и у неким случајевима добијемо само $s_p = 1$.

Зашто је ово важно? По делу 2) Друге теореме Силова, све Силовљеве p-подгрупе су међусобно конјуговане, па је s_p број уствари број конјугата било које од њих. Ако је $s_p = 1$, онда је та (јединствена) Силовљева подгрупа и нормална у групи G!

Такође, ако за неку групу и све просте бројеве који деле њен ред важи да су одговарајуће Силовљеве подгрупе јединствене, а тиме и нормалне, добијамо разлагање те групе у директан производ њених Силовљевих подгрупа.

Тврђење 0.9. *Коначна група је директан производ својих Силовљевих подгрупа ако и само ако су те подгрупе и нормалне.*

Доказ. Ако је група G директан производ својих Силовљевих подгрупа, оне су свакако нормалне.
Нека су сада све Силовљеве подгрупе групе G и нормалне и нека је ред те групе $|G| = n = p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}$. Бројеви $p_i^{r_i}$ су наравно узајамно прости, али приметимо да су и бројеви $m_i = \frac{n}{p_i^{r_i}}$ узајамно прости, у смислу да је њихов највећи заједнички делилац 1: $(m_1, m_2, \ldots, m_k) = 1$. За два природна броја смо имали да онда постоји њихова "линеарна комбинација" са целобројним коефицијентима која је једнака 1. Индукцијом се лако показује да то важи и за ових k бројева (НЗД од m_1 и НЗД-а од $m_2, \ldots, m_k$ је такође 1, па кренемо од те комбинације и она нам даје комбинацију свих $m_1, m_2, \ldots, m_k$ чија је вредност 1). Дакле, постоје цели бројеви $n_1, n_2, \ldots, n_k$ за које је

$$m_1n_1 + m_2n_2 + \cdots m_kn_k = 1.$$

Подсетимо се да смо ову јединицу у задацима са редовима елемената често користили да неки елемент групе G "разбијемо" у производ два или више елемената. Тако ћемо урадити и сада. Нека је $g \in G$ произвољан. Из $g = g^1 = g^{m_1n_1+m_2n_2+\cdots m_kn_k}$ добијамо да је $g = g^{m_1n_1}g^{m_2n_2}\cdots g^{m_kn_k}$, односно $g = g_1g_2\cdots g_k$ где је $g_i = g^{m_in_i}$. Приметимо сада да кад сваки g_i степенујемо са $p_i^{r_i}$ добијамо $g_i^{p_i^{r_i}} = g^{m_in_ip_i^{r_i}} = g^{\frac{n}{p_i^{r_i}}n_ip_i^{r_i}} = g^{nn_i} = (g^n)^{n_i} = e^{n_i} = e$. То значи да ред елемента g_i дели $p_i^{r_i}$, па је он у некој Силовљевој p_i-подгрупи групе G. Али, по претпоставци, те подгрупе су јединствене. Дакле, g_i припада H_i, где је H_i јединствена Силовљева подгрупа реда $p_i^{r_i}$ за све $i \in \{1, 2, \ldots, n\}$, и сваки елемент $g \in G$ је производ $g = g_1g_2\cdots g_k$. Одавде је $G = H_1H_2\cdots H_k$. Услов $H_i \lhd G$ већ имамо, па остаје да се провери још само трећи услов за разложивост групе G у директан производ подгрупа $H_1, H_2, \ldots H_k$, који гласи $(H_1H_2\cdots H_l)\cap H_{l+1} = \{e\}$ за свако $1 \leq l \leq k-1$. Узмимо произвољно $g = g_1g_2\ldots g_l \in H_1H_2\cdots H_l$. Редови подгрупа H_i су узајамно прости и све оне су нормалне, па осим тога што су пресеци две по две тривијални, оне ће комутирати члан по члан (важи: $H, K \lhd G$ и $(|H|, |K|) = 1$ повлачи $H \cap K = \{e\}$ и $hk = kh$ за свако $h \in H$, $k \in K$: за пресек је лако, а за комутирање посматрамо $hkh^{-1}k^{-1}$ - он припада и једној и другој јер $hkh^{-1} \in K$, $k^{-1} \in K$, па и производ припада K, а такође $h \in H$, $kh^{-1}k^{-1} \in H$, па и производ припада H; дакле, $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, а $hkh^{-1}k^{-1} = e \Leftrightarrow hk = kh$). То значи да је $g^{p_1^{r_1}p_2^{r_2}\cdots p_l^{r_l}} = (g_1g_2\ldots g_l)^{p_1^{r_1}p_2^{r_2}\cdots p_l^{r_l}} = (g_1^{p_1^{r_1}})^{p_2^{r_2}\cdots p_l^{r_l}}\cdots(g_l^{p_l^{r_l}})^{p_1^{r_1}\cdots p_{l-1}^{r_{l-1}}} = e$, па ред елемента g дели $p_1^{r_1}p_2^{r_2}\cdots p_l^{r_l}$. С друге стране, $g \in H_{l+1}$, па његов ред мора да дели $p_{l+1}^{r_{l+1}}$. Међутим, бројеви $p_1^{r_1}p_2^{r_2}\cdots p_l^{r_l}$ и $p_{l+1}^{r_{l+1}}$ су узајамно прости, па је тај ред 1, односно $(H_1H_2\cdots H_l)\cap H_{l+1} = \{e\}$.
Дакле, испуњена су сва три услова и важи $G \cong H_1 \times H_2 \times \cdots \times H_k$. □

0.3 Прстени

0.3.1 Дефиниција и основне особине прстена

Дефиниција 0.7. *Прстен* је алгебарска структура $(R, +, \cdot)$, где је R непразан скуп, а $+$ и $\cdot$ две бинарне операције, која задовољава услове

1) $(R, +)$ је Абелова група:

- за све $a, b, c \in R$ важи $(a + b) + c = a + (b + c)$
- постоји елемент $0 \in R$ такав да за све $a \in R$ важи $a + 0 = 0 + a = a$
- за свако $a \in R$ постоји $-a \in R$ такав да је $a + (-a) = (-a) + a = 0$
- за све $a, b \in R$ важи $a + b = b + a$

2) $(R, \cdot)$ је семигрупа:

- за све $a, b, c \in R$ важи $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

3) Операција $\cdot$ је дистрибутивна према $+$

- за све $a, b, c \in R$ важи $a \cdot (b + c) = a \cdot b + a \cdot c$ и $(b + c) \cdot a = b \cdot a + c \cdot a$.

Напомена 0.5. У дефиницији прстена уместо $(R, \cdot)$ је семигрупа може да стоји $(R, \cdot)$ је моноид, и у том случају не разликујемо прстене са јединицом и без јединице.

Дефиниција 0.8. Прстен $(R, +, \cdot)$ у коме постоји елемент 1 такав да за све $a \in R$ важи $a \cdot 1 = 1 \cdot a = a$ назива се *прстен са јединицом.*

Пример 0.6. Структура $(5\mathbb{Z}, +, \cdot)$ где су $+$ и $\cdot$ сабирање и множење целих бројева, задовољава све аксиоме прстена, али нема јединицу. Ово је пример прстена без јединице.

У наставку ћемо се бавити скоро искључиво прстенима са јединицом.

Иако нам је већина појмова у вези прстена позната од раније, рећи ћемо пар речи о ознакама и терминологији. Операције прстена најчешће означавамо са $+$ и $\cdot$ и зовемо *сабирање* и *множење*. Не наглашавамо их ако се подразумевају, па кажемо само *прстен* R уместо *прстен* $(R, +, \cdot)$. Групу $(R, +)$ зовемо *адитивна група* прстена R. Њен неутрал ћемо звати *нула прстена* R. Инверз елемента $a \in R$ ћемо, као и до сада кад је операција означена адитивно, звати *супротан елемент* елемента a (да бисмо га разликовали од инверза у односу на множење).
Семигрупу $(R, \cdot)$ зовемо *мултипликативна семигрупа* прстена R. Ако је у питању прстен са јединицом, одговарајући моноид $(R, \cdot, 1)$ је *мултипликативни моноид* прстена R, а као што смо већ дефинисали, његов неутрал је *јединица прстена* R. За прстен кажемо да је *комутативан* ако је његово множење комутативно (јер сабирање свакако јесте), односно ако је $ab = ba$ за све $a, b \in R$. Даље, за елемент a кажемо да је *инверзибилан* у прстену са јединицом R, ако је инверзибилан у његовом мултипликативном моноиду, односно ако постоји $a^{-1} \in R$ за које је $a \cdot a^{-1} = a^{-1} \cdot a = 1$. У комутативном прстену

инверз елемента a означавамо и са $a^{-1} = \frac{1}{a}$ јер је онда без забуне $a^{-1} \cdot b = b \cdot a^{-1} = \frac{b}{a}$. Скуп инверзибилних елемената моноида $(R, \cdot, 1)$ зваћемо скуп инверзибилних елемената прстена R и као и раније означавати са R^* (знамо да је R^* група у односу на множење, јер је $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ и $(a^{-1})^{-1} = a$). Такође, за елемент a кажемо да је *регуларан* у прстену R ако је регуларан у његовој мултипликативној семигрупи $(R, \cdot)$, односно ако допушта крађење (*регуларан слева* ако $a \cdot x = a \cdot y \ \Rightarrow \ x = y$, *регуларан здесна* ако $x \cdot a = y \cdot a \ \Rightarrow \ x = y$; регуларан ако је регуларан и слева и здесна).

Закључак који се намеће је да особине прстену даје множење (јер за сабирање већ важи све што може да важи).

Последице аксиома или правила рачунања у прстену

Нека је $(R, +, \cdot)$ прстен. Све што од раније знамо да важи за комутативне групе, важиће у групи $(R, +)$, па и у самом прстену R. Исто то се односи на све особине семигрупе или моноида $(R, \cdot)$. Такође, ове две операције су повезане дистрибутивним законом. Као и код векторских простора, он се може лако уопштити на коначно елемената прстена:

- $(a_1 + a_2 + \cdots + a_m) \cdot b = a_1 \cdot b + a_2 \cdot b + \cdots + a_m \cdot b$ (доказује се индукцијом по m - означимо са $a = a_1$, а са $c = a_2 + \cdots a_m$), па следи из $(a + c) \cdot b = a \cdot b + c \cdot b$)
- $a \cdot (b_1 + b_2 + \cdots + b_n) = a \cdot b_1 + a \cdot b_2 + \cdots + a \cdot b_n$ (индукцијом по n)
- $(a_1 + a_2 + \cdots + a_m) \cdot (b_1 + b_2 + \cdots + b_n) = \sum_{i,j} a_i \cdot b_j$

Тврђење 0.10. *У прстену R важи:*
1) $a \cdot 0 = 0$; $0 \cdot a = 0$
2) $(-a) \cdot b = -(a \cdot b)$; $a \cdot (-b) = -(a \cdot b)$

Доказ. 1) Нула прстена је његов неутрал за сабирање и зато није аксиомама повезана са множењем. Искористићемо дистрибутивност да је повежемо са множењем, а кренућемо од тачне једнакости $0 + 0 = 0$. Помножимо ову једнакост слева елементом a: $a \cdot (0 + 0) = a \cdot 0$, искористимо дистрибутивност: $a \cdot 0 + a \cdot 0 = a \cdot 0$. Сада је ово једнакост у адитивној групи $(R, +)$, а у њој можемо лако да рачунамо: $x + x = x$, где смо означили $x = a \cdot 0$, нам после додавања $-x$ на обе стране даје $((-x) + x) + x = (-x) + x$, односно $0 + x = 0$, тј. $x = 0$. За $0 \cdot a = 0$ опет крећемо од $0 + 0 = 0$, само што множимо са a с десне стране. 2) Овде крећемо од дефинишуће релације елемента $(-a)$: то је елемент који сабран са a даје нулу прстена, $(-a) + a = 0$. Помножимо ово здесна са b: $((-a) + a) \cdot b = 0 \cdot b$ и искористимо дистрибутивност: $(-a) \cdot b + a \cdot b = 0 \cdot b$. Из 1) је $0 \cdot b = 0$, па имамо $(-a) \cdot b + a \cdot b = 0$. Ово је опет дефинишућа релација супротног елемента за елемент $a \cdot b$: "нешто" плус $a \cdot b$ је нула значи да је то "нешто" управо $-(a \cdot b)$, односно $(-a) \cdot b = -(a \cdot b)$. За другу релацију множимо $b + (-b) = 0$ слева са a. □

У семигрупи смо увели n-ти степен елемента, где је $n \in \mathbb{N}$, па тако и у прстену можемо да говоримо о $a^n = a \cdot a \cdot \cdots \cdot a$. Онда би $(ab)^n$ био производ $(ab) \cdot (ab) \cdot \cdots \cdot (ab)$ n пута. Ако је прстен комутативан, овај производ ће бити $a^n b^n$:

$$ab = ba \ \Rightarrow \ (ab)^n = a^n b^n.$$

Од раније знамо да и степен збира два реална или цела броја можемо лепо да запишемо. Приметимо да смо за то (неприметно) користили комутативност њиховог множења. И у сваком комутативном прстену ће важити биномна формула, која се доказује индукцијом:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

Такође, важи и следећа формула коју смо имали за реалне бројеве:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + a^2b^{n-3} + ab^{n-2} + b^{n-1}),$$

а за непарно n и

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots + a^2b^{n-3} - ab^{n-2} + b^{n-1}),$$

Приметимо да претходне формуле важе и у некомутативном прстену ако елементи a и b комутирају, то јест ако је $ab = ba$.

Примери прстена

1) Скуп целих бројева у односу на сабирање и множење, $(\mathbb{Z}, +, \cdot)$, је комутативан прстен са јединицом. Инверзибилни елементи овог прстена су

$$\mathbb{Z}^* = \{1, -1\}$$

2) Скуп остатака при еуклидском дељењу са n, $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$ је прстен у односу на сабирање и множење по модулу n:

$$r +_n s = rest(r+s, n), \quad r \cdot_n s = rest(r \cdot s, n).$$

$(\mathbb{Z}_n, +_n, \cdot_n)$ је такође комутативан прстен са јединицом. Његови инверзибилни елементи су они r мањи од n који су узајамно прости са n: $\mathbb{Z}_n^* = \{r \in \mathbb{Z}_n : (r, n) = 1\}$.

3) Скуп свих реалних квадратних матрица реда n је прстен у односу на сабирање и множење матрица, $(M_n(\mathbb{R}), +, \cdot)$. Ово је прстен са јединицом (то је E_n - јединична матрица реда n), који није комутативан. Његови инверзибилни елементи су све матрице ранга n, односно детерминанте различите од нуле: $M_n(\mathbb{R})^* = \{A \in M_n(\mathbb{R}) : detA \neq 0\}$. Такође, уместо $\mathbb{R}$ овде може да стоји било који прстен R. Јединица некомутативног прстена $M_n(\mathbb{R})$ у том случају је дијагонална матрица која на дијагонали има јединице прстена R, а његови инверзибилни елементи су све матрице чија је детерминанта инверзибилна у прстену R: $M_n(R)^* = \{A \in M_n(R) : detA \in R^*\}$.

4) Скуп полинома са реалним коефицијентима је прстен у односу на сабирање и множење полинома, $(\mathbb{R}[X], +, \cdot)$. То је комутативан прстен са јединицом, чији су инверзибилни елементи само скалари (константни полиноми) различити од нуле: $\mathbb{R}[X]^* = \{a \in \mathbb{R} : a \neq 0\}$. И овде можемо уместо поља $\mathbb{R}$ ставити било који прстен R, добићемо опет комутативан прстен са јединицом, чији су инверзибилни елементи само инверзибилни скалари $R[X]^* = R^*$.

Напомена: И у овом и у претходном примеру, прстени који добијемо се разликују ако је R само прстен од оних где је R и поље. Разлика ће бити видљивија у наставку. У задацима и примерима ће, као и до сада, матрице и полиноми бити углавном над пољем реалних бројева.

5) За прстене $(R_1, +_1, \cdot_1)$ и $(R_2, +_2, \cdot_2)$, на скупу $R_1 \times R_2$ имамо структуру прстена у односу на операције $+$ и $\cdot$ дате са

$$(x_1, x_2) + (y_1, y_2) = (x_1 +_1 y_1,\ x_2 +_2 y_2)$$

и

$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 \cdot_1 y_1,\ x_2 \cdot_2 y_2),$$

за све $x_1, y_1 \in R_1$ и све $x_2, y_2 \in R_2$, чија је нула $(0_{R_1}, 0_{R_2})$ и јединица $(1_{R_1}, 1_{R_2})$(проверите ако желите).

0.3.2 Потпрстени и хомоморфизми

Дефиниција 0.9. Нека је $(R, +, \cdot)$ прстен са јединицом 1_R. За прстен $(K, +, \cdot)$ кажемо да је *потпрстен* прстена R ако је $(K, +)$ подгрупа адитивне групе $(R, +)$, а $(K, \cdot)$ подмоноид мултипликативног моноида $(R, \cdot)$. То значи да је K непразан подскуп скупа R за који важи:
1) $a, b \in K \ \Rightarrow\ a - b \in K$,
2) $a, b \in K \ \Rightarrow\ a \cdot b \in K$,
3) $1_R \in K$.

Напомена 0.7. Ако је $(R, +, \cdot)$ прстен без јединице, у претходној дефиницији изостављамо услов 3). Надаље, сви прстени које ћемо посматрати ће бити прстени са јединицом.

Пример 0.8. $(\mathbb{Z}_n, +_n, \cdot_n)$ није потпрстен прстена $(\mathbb{Z}, +, \cdot)$, јер није затворен за његове операције.

Пример 0.9. Скуп свих матрица из $M_n(\mathbb{R})$ чије су све компоненте једнаке је комутативан прстен у ком су сви не-нула елементи инверзибилни. Међутим, он није потпрстен прстена $M_n(\mathbb{R})$, јер не садржи јединичну матрицу (његова јединица је матрица чије су све компоненте 1)!

Дефиниција 0.10. Нека су $(R_1, +_1, \cdot_1)$ и $(R_2, +_2, \cdot_2)$ два прстена са јединицом. Пресликавање $f : R_1 \to R_2$ је *хомоморфизам* прстена R_1 у прстен R_2 ако је истовремено хомоморфизам групе $(R_1, +_1)$ у групу $(R_2, +_2)$ и моноида $(R_1, \cdot_1)$ у моноид $(R_2, \cdot_2)$, односно ако задовољава услове:
1) $f(a +_1 b) = f(a) +_2 f(b)$,
2) $f(a \cdot_1 b) = f(a) \cdot_2 f(b)$,
3) $f(1_{R_1}) = 1_{R_2}$.

Хомоморфизам који је инјективан зове се мономорфизам, а онај који је сурјективан, епиморфизам. Бијективан хомоморфизам прстена је изоморфизам прстена. За прстене R_1 и R_2 кажемо да су *изоморфни* ако постоји бар један изоморфизам $f : R_1 \to R_2$ и тада пишемо $R_1 \cong R_2$.

Пример 0.10. Пресликавање $f : \mathbb{Z} \to \mathbb{Z}_n$ дефинисано са $f(m) = rest(m, n) = \rho(m, n)$ - остатак који m даје при еуклидском дељењу са n, је један хомоморфизам прстена (ово пресликавање је сагласно са сабирањем и множењем, тј. остатак збира једнак је збиру остатака и остатак производа једнак је производу остатака - проверите ако нисте раније код конгруенција по модулу n).

Пример 0.11. Нека је $f : R_1 \to R_2$ хомоморфизам прстена. Његова слика, која се дефинише као $Imf = \{f(a) : a \in R_1\}$ је један потпрстен прстена R_2. Ово се лако проверава: $f(a) +_2 f(b) = f(a +_1 b) \in Imf$, $f(a) \cdot_2 f(b) = f(a \cdot_1 b) \in Imf$, и још $1_{R_2} = f(1_{R_1}) \in Imf$.

0.3.3 Идеали прстена

Нека су дати прстени R и K. Надаље ћемо операције ова два прстена означавати исто, $+$ и $\cdot$, а из контекста ће бити јасно у ком прстену се радња дешава. Такође, производ елемената a и b ћемо скоро увек означавати са ab уместо $a \cdot b$. Видели смо да је слика сваког хомоморфизма $f : R \to K$ један потпрстен прстена K. Његово језгро, које се дефинише као

$$Kerf = \{x \in R : f(x) = 0_K\}$$

је затворено за сабирање и множење, али ако би му припадала јединица прстена R, онда би било $f(a) = f(a \cdot 1_R) = f(a) \cdot f(1_R) = f(a) \cdot 0_K = 0_K$ и за све елементе $a \in R$, па $1_R \in Kerf$ само у случају нула-хомоморфизма. Дакле, језгро није потпрстен, али има следећу особину: довољно је да неки елемент припада језгру да би његов производ са било којим елементом прстена био опет у језгру, јер

$$a \in Kerf \;\Rightarrow\; f(ax) = f(a) \cdot f(x) = f(a) \cdot 0_K = 0_K$$

за све $x \in R$. Исто важи и за xa. То нас мотивише да дефинишемо следећу подструктуру прстена:

Дефиниција 0.11. Нека је R прстен и I непразан подскуп од R. I је *идеал* прстена R ако важи:
1) $(I, +)$ је подгрупа адитивне групе прстена $(R, +)$,
2) за све $x \in R$ и $a \in I$ је $ax,\ xa \in I$.

Да је I идеал прстена R означавамо са $I \lhd R$.

Напомена 0.12. Први услов из дефиниције се може заменити условом $a, b \in I \;\Rightarrow\; a+b \in I$.

Зашто? Из другог услова ћемо добити: $0 \in R$ и $a \in I$ повлачи $a \cdot 0 = 0 \in I$, као и $(-a) = (-1) \cdot a \in I$ за све $a \in I$, па је $(I, +)$ заиста подгрупа од $(R, +)$.
Такође, ако је прстен R комутативан, што ће углавном бити случај, други услов постаје само $x \in R$ и $a \in I$ повлачи $ax \in I$.

Пример 0.13. Нека је R комутативан прстен и $a \in R$ произвољан елемент. Лако се провери да је скуп

$$\langle a \rangle = aR = \{ax : x \in R\}$$

један идеал прстена R ($ax + ay = a(x + y) \in \langle a \rangle$, као и $(ax)y = y(ax) = a(xy) \in \langle a \rangle$) и кажемо да је то *главни идеал генерисан елементом a.*

Пример 0.14. У прстену $\mathbb{Z}$ сви идеали су главни.

- $I \lhd \mathbb{Z}$ повлачи $(I, +) \leq (\mathbb{Z}, +)$, а знамо да су подгрупе цикличне групе такође цикличне, па је I облика $n\mathbb{Z}$ за неки цео број n. Сада се лако провери да $n\mathbb{Z}$ задовољава и други услов из дефиниције идеала ($(nx)y = y(nx) = n(xy) \in n\mathbb{Z}$). Дакле, осим $\{0\}$ и целог прстена, идеали прстена целих бројева су $2\mathbb{Z}$, $3\mathbb{Z}$ итд.

Пример 0.15. Ако идеал садржи јединицу или било који инверзибилни елемент прстена, он је једнак целом прстену.

- $1 \in I,\ x \in R \ \Rightarrow\ 1 \cdot x \in I$, па би било $R \subset I$, тј. $I = R$. Слично, ако је неки инверзибилни елемент у I, онда ће производ њега и његовог инверза бити опет у I, а тај производ је 1.

Последица: Нека је $\mathbb{F}$ поље и $I \lhd \mathbb{F}$. Тада је $I = \{0\}$ или $I = \mathbb{F}$. (У пољу нема правих идеала.)

Пример 0.16. Језгро хомоморфизма прстена је идеал.

-Видели смо већ да је за хомоморфизам $f : R \to K$, скуп

$$Kerf = \{x \in R : f(x) = 0_K\}$$

затворен за сабирање и да је довољно да један чинилац припада њему да би производ опет био ту. Као и код векторских простора и група, и овде важи:

$$f \text{ је } "1 - 1" \Leftrightarrow Kerf = \{0_R\}.$$

Пример 0.17. Ако је $\mathbb{F}$ поље, сваки идеал прстена $\mathbb{F}[X]$ је главни.

-Нека је $I \lhd \mathbb{F}[X]$. Ако је $I = \{0\}$, он је главни, генерисан нула-полиномом. Нека је сада $I \neq \{0\}$ и нека је $a(x)$ не-нула полином из I чији је степен минималан. Узмимо било који полином $p(x)$ из I и еуклидски га поделимо полиномом $a(x)$: $p = aq + r$, при чему је степен полинома r строго мањи од степена полинома a. Из $a \in I$ следи да је и $aq \in I$, па даље из $p \in I$ добијамо $r = p - aq \in I$. Због степена сада мора бити $r \equiv 0$, што значи да је $p = aq$, односно да $p \in \langle a \rangle$. Дакле, $I = \langle a \rangle$.

Операције са идеалима

Нека су I и J идеали прстена R. Тада је њихов пресек такође један идеал:

$$a, b \in I \cap J \ \Rightarrow a, b \in I \wedge a, b \in J \Rightarrow a + b \in I \wedge a + b \in J \Rightarrow a + b \in I \cap J,$$

$$a \in I \cap J,\ x \in R \Rightarrow a \in I \wedge a \in J \wedge x \in R \Rightarrow ax, xa \in I \wedge ax, xa \in J \Rightarrow ax, xa \in I \cap J.$$

Ово је очекивано, али исто тако знамо да унија неће бити идеал (није ни подгрупа, знамо од раније). Зато правимо најмањи идеал који садржи два дата, и зовемо га збир идеала I и J:

$$I + J = \{a + b : \ a \in I, \ b \in J\}$$

Лако се провери да смо добили идеал:

$$a + b + a_1 + b_1 = (a + a_1) + (b + b_1) \ \in I + J$$

$$(a + b)x = ax + bx \in I + J$$

за $a \in I, \ b \in J, \ x \in R$.

Пошто у прстену, осим сабирања, постоји и множење, природно је да се питамо шта бисмо подразумевали под производом два идеала. Ако бисмо, по аналогији са сабирањем, IJ дефинисали као $IJ = \{ab : a \in I, \ b \in J\}$, наишли бисмо на проблем код провере да је овај скуп затворен за сабирање: $ab+a_1b_1$ не мора да буде облика нешто из I пута нешто из J. То превазилазимо тако што за елементе производа идеала узимамо суме коначно производа:

$$IJ = \{a_1b_1 + \cdots + a_nb_n : \ a_k \in I, \ b_k \in J\}$$

Сада се лако види да је збир два елемента из IJ опет елемент из IJ, а други услов је свакако испуњен: $x(a_1b_1 + \cdots + a_nb_n) = (xa_1)b_1 + \cdots + (xa_n)b_n$, а xa_k припада I. Исто и за множење здесна, само ће тада b_kx припадати J.

Важи: $IJ \subset I \cap J$.

Зашто? Нека је $a_1b_1 + \cdots + a_nb_n$ произвољан елемент из IJ. Пошто су сви a-ови у I, њихови производи са b-овима ће бити опет у I, а како је I затворен за сабирање, и цела сума $a_1b_1 + \cdots + a_nb_n$ ће припадати I. Исте аргументе користимо да покажемо да је ова сума у J: b_k припада J за свако k, па a_kb_k припада J за свако k, а онда и њихов збир. Дакле, елемент $a_1b_1 + \cdots + a_nb_n$ је и у I, и у J, па и у $I \cap J$. Обрнуто не важи у општем случају, а нешто касније ћемо видети у ком односу треба да буду два идеала да би њихов пресек био садржан у производу.

Пример 0.18. Пошто су у прстену $\mathbb{Z}$ сви идеали главни, збир, пресек и производ два идеала ће опет бити главни идеал. Тако је, на пример,

$$24\mathbb{Z} + 40\mathbb{Z} = 8\mathbb{Z},$$

$$24\mathbb{Z} \cap 40\mathbb{Z} = 120\mathbb{Z},$$

$$24\mathbb{Z} \cdot 40\mathbb{Z} = 960\mathbb{Z}.$$

Проверите да важи:

$$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z},$$

$$m\mathbb{Z} \cap n\mathbb{Z} = s\mathbb{Z},$$

$$m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z},$$

где је $d = NZD(m, n)$, а $s = NZS(m, n)$.

0.3.4 Карактеристика прстена

Нека је R прстен и P било који његов потпрстен. По дефиницији, P садржи 1_R, па пошто је затворен за операције прстена, садржаће и $1_R + 1_R$, затим $1_R + 1_R + 1_R$ итд, као и (-1_R), $(-1_R) + (-1_R) \ldots$ Такође, $0_R \in P$, па P сигурно садржи скуп

$$\{m1_R : \ m \in \mathbb{Z}\}$$

Овај скуп је сам за себе један прстен који се зове *карактеристични потпрстен* прстена R и означава са R_0. То је, дакле, минимални потпрстен прстена R. У односу на његову кардиналност разликујемо две врсте прстена. Прва могућност је да је $R_0 \cong \mathbb{Z}$, при чему је изоморфизам дат са $m \leftrightarrow m1_R$. Из инјективности овог пресликавања следи да је онда

$$k1_R = 0 \ \Leftrightarrow \ k = 0$$

Тада кажемо да је прстен R *карактеристике нула* и пишемо $charR = 0$. Дакле, $charR = 0$ значи да је $R_0 \cong \mathbb{Z}$ и да сабирањем 1_R саме са собом не можемо добити 0_R.
У супротном, односно ако је збир неколико 1_R једнак 0_R, *карактеристика прстена* је најмањи природан број k за који је $k1_R = 0_R$. Приметимо да је онда и за сваки елемент $x \in R$:

$$kx = k(1_R x) = 1_R x + \cdots + 1_R x = (1_R + \cdots + 1_R)x = (k1_R)x = 0_R x = 0_R$$

Такође, јасно је да је

$$charR = k \ \Leftrightarrow \ R_0 \cong \mathbb{Z}_k,$$

јер $m1_R = (kq + r)1_R = kq1_R + r1_R = r1_R$, где је $0 \leq r < k$.

Пример 0.19. $char\mathbb{Z} = 0$, $char\mathbb{Z}_k = k$

Пример 0.20. Ако је R прстен, онда прстени $R[X]$ и $M_n[R]$ имају исту карактеристику као и сам прстен R.
(Одмах се види, јер $1_{R[X]} = 1_R$, а јединична матрица E_n има на дијагонали 1_R.)

0.3.5 Делитељи нуле и домени

Дефиниција 0.12. Елемент a прстена R је *леви делитељ нуле* у том прстену ако постоји елемент $b \in R \setminus \{0\}$ за који је $ab = 0$. (a је *десни делитељ нуле* ако постоји $b \in R \setminus \{0\}$ за који је $ba = 0$.)

Нула прстена је увек делитељ нуле. Ако је $a \neq 0$ делитељ нуле, кажемо да је a прави делитељ нуле (било леви било десни).
За прстен који нема праве делитеље нуле кажемо да је *домен*, а ако је уз то и комутативан, кажемо да је *област целих*(или комутативни домен, или интегрални домен). Дакле, R је домен ако за било која два елемента важи:

$$ab = 0 \ \Rightarrow \ a = 0 \ \vee \ b = 0.$$

Пример 0.21. Прстен целих бројева је домен, док $\mathbb{Z}_n$, где n није прост број, није. На пример, у $\mathbb{Z}_{20}$ је $4 \cdot 5 = 0$. Такође, знамо да у прстену матрица (нпр. у $M_2[\mathbb{R}]$) постоје прави делитељи нуле, односно да постоје не-нула матрице такве да је њихов производ нула-матрица.

Делитељи нуле су блиско повезани са регуларношћу у прстену:

$$ax = ay \;\Leftrightarrow\; a(x-y) = 0,$$

па ако a није регуларан слева, постојаће различити x и y за које је $ax = ay$, а самим тим и елемент $b = x - y$ различит од нуле за који је $ab = 0$, и обрнуто. Дакле, a је леви делитељ нуле акко није регуларан слева (односно, a је десни дељитељ нуле акко није регуларан здесна.)

Видели смо да у прстенима $\mathbb{Z}_n$, где n није прост број, постоје прави делитељи нуле, док у $\mathbb{Z}_p$, где је p прост број, не постоје:

$$r \cdot_p s = 0 \text{ за неке } r, s \in \mathbb{Z}_p \;\Rightarrow\; p|rs \text{ у } \mathbb{Z} \;\Rightarrow\; p|r \vee p|s \;\Rightarrow\; r = 0 \vee s = 0$$

Важи и следеће:

Тврђење 0.11. *Ако је R домен, онда је његова карактеристика или нула или неки прост број.*

Доказ. Ако је $charR = 0$, онда је у реду. Нека је сада $charR = k > 0$. Покажимо да је k прост. Претпоставимо да је $k = rs$. Пошто је збир k јединица прстена R једнак 0_R, биће

$$0_R = k1_R = rs1_R = (r1_R)(s1_R),$$

па пошто R нема праве делитеље нуле, биће $r1_R = 0_R$ или $s1_R = 0_R$. По дефиницији карактеристике прстена, k је најмањи природан број за који је $k1_R = 0_R$, па из претходног следи да је $k \leq r$ или $k \leq s$. Сада из $k = rs$ имамо $k = r$ или $k = s$. Дакле, k нема прави растав, то јест, прост је. □

0.3.6 Количнички прстен

Као што је то случај са нормалним подгрупама код група, код прстена су идеали у тесној вези са конгруенцијама и хомоморфизмима. Језгро било ког хомоморфизма је идеал, као и класа нуле било које конгруенције. С друге стране, сам идеал индукује и хомоморфизам и конгруенцију.

Теорема 0.12. *Нека је R прстен и I његов идеал. Тада је релација $\sim$ дефинисана са:*

$$a \sim b \;\Leftrightarrow\; a - b \in I$$

једна конгруенција прстена R.

Доказ. Да је $\sim$ еквиваленција следиће из тога што је $(I, +)$ група:

рефлексивност $a \sim a \;\Leftrightarrow\; a - a = 0 \in I$
симетричност $a \sim b \;\Leftrightarrow\; a - b \in I \;\Leftrightarrow\; b - a = -(a - b) \in I \;\Leftrightarrow\; b \sim a$

транзитивност $a \sim b \ \wedge \ b \sim c \ \Leftrightarrow \ a-b \in I \ \wedge \ b-c \in I \ \Rightarrow \ (a-b)+(b-c) \in I \ \Rightarrow$
$a-c \in I \ \Rightarrow \ a \sim c$

Проверимо сада да је $\sim$ сагласна са сабирањем:

$$a \sim a' \wedge b \sim b' \ \Leftrightarrow \ a-a' \in I \wedge b-b' \in I \ \Rightarrow \ (a-a')+(b-b') \in I \ \Rightarrow \ (a+b)-(a'+b') \in I \ \Rightarrow \ a+b \sim a'+b'$$

и са множењем:

$$a \sim a' \ \wedge \ b \sim b' \ \Leftrightarrow \ a-a' \in I \ \wedge \ b-b' \in I \ \Rightarrow \ ab-a'b' = (a-a')b+a'(b-b') \in I \Rightarrow \ ab \sim a'b',$$

где смо искористили друго својство идеала, то јест да $a - a' \in I$ и $b \in R$ повлачи $(a - a')b \in I$ и исто за $a'(b - b') \in I$.

□

Шта су класе ове еквиваленције, односно конгруенције?

$$C_a = a/\sim = \{x \in R : x \sim a\} = \{x \in R : x - a \in I\} = \{x \in R : x \in a + I\} = a + I$$

Од раније знамо да када имамо конгруенцију, количнички скуп (скуп класа) је алгебарска структура истог типа као и полазна. У овом случају то значи да смо добили прстен $R/\sim$, који ћемо надаље означавати R/I и звати *количнички прстен* датог прстена R по његовом идеалу I:

$$R/I = \{a + I : a \in R\}.$$

Његова нула је $I = 0+I$ (класа нуле прстена R), јединица $1+I$ (класа јединице прстена R), а операције у њему су:

$$(a + I) + (b + I) = a + b + I$$

$$(a + I) \cdot (b + I) = ab + I$$

(збир класа је класа збира представника, производ класа је класа производа).

Такође, као и увек код конгруенција, имамо природни епиморфизам (прстена R и R/I) дат са $\pi(a) = a + I$.

Напомена 0.22. Могли смо прво адитивну групу прстена $(R, +)$ да посечемо по њеној подгрупи $(I, +)$ (која је нормална јер је група комутативна) и да добијемо количничку групу (скуп косета): $(R, +)/(I, +) = \{a + I : a \in R\}$, а онда на њој да додефинишемо множење са $(a + I) \cdot (b + I) = ab + I$ и проверимо да важе преостале аксиоме прстена.

Пример 0.23. Нека је дат прстен $R = \mathbb{Z}$ и његов идеал $I = n\mathbb{Z}$. Тада је количнички прстен

$$R/I = \mathbb{Z}/n\mathbb{Z} = \{m + n\mathbb{Z} : m \in \mathbb{Z}\} = \{nq + r + n\mathbb{Z} : 0 \leq r < n\} = \{r + n\mathbb{Z} : 0 \leq r < n\}$$

односно,

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n - 1) + n\mathbb{Z}\}.$$

Операције у њему су

$$(r + n\mathbb{Z}) + (s + n\mathbb{Z}) = (r +_n s) + n\mathbb{Z} \text{ и}$$

$$(r + n\mathbb{Z}) \cdot (s + n\mathbb{Z}) = (r \cdot_n s) + n\mathbb{Z},$$

а нула и јединица, редом, $n\mathbb{Z}$ и $1 + n\mathbb{Z}$.

Очигледно је $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.
Приметимо да је

$$\mathbb{Z}/n\mathbb{Z} \;=\; \mathbb{Z}/=_n,$$

где је $=_n$ конгруенција по модулу природног броја n, јер

$$a-b \in I \;\Leftrightarrow\; a-b \in n\mathbb{Z} \;\Leftrightarrow\; n \mid a-b \;\Leftrightarrow\; a =_n b.$$

Теореме о изоморфизмима

Поновимо да је код прстена улога идеала иста као улога нормалних подгрупа код група. Такође, потпрстени одговарају подгрупама, па су теореме о изоморфизмима у класи прстена формулисане на буквално исти начин као и теореме о изоморфизмима у класи група, само се свуда реч "подгрупа" замењује са "потпрстен", а "нормална подгрупа" са "идеал". Тако прва теорема гласи:

Теорема 0.13. (Прва теорема о изоморфизмима за прстене) *Нека је $f : R \to K$ хомоморфизам прстена. Ако је $\pi : R \to R/Kerf$ природни епиморфизам и $\sigma : Imf \to K$ инклузија, тада постоји тачно једно пресликавање $\Phi : R/Kerf \to Imf$ за које је $f = \sigma \circ \Phi \circ \pi$. При том је Φ и изоморфизам, и важи*

$$R/Kerf \cong Imf$$

.

Пример 0.24. Нека је $f : \mathbb{Z} \to \mathbb{Z}_n$ хомоморфизам прстена дат са $f(m) = \rho(m, n)$, где је $\rho(m, n)$ остатак који m даје при еуклидском дељењу са n. Ово је епиморфизам, па је $Imf = \mathbb{Z}_n$. Шта му је језгро?

$$Kerf = \{m \in \mathbb{Z} : \rho(m, n) = 0\} = n\mathbb{Z}$$

Дакле, на основу претходне теореме је

$$\mathbb{Z}/n\mathbb{Z} \cong \;\mathbb{Z}_n.$$

Видели смо већ да је збир два идеала идеал. Аналогно се дефинише и збир идеала I и потпрстена P, и лако се провери да је тај скуп $I + P$ један потпрстен.

Теорема 0.14. (Друга теорема о изоморфизмима за прстене) *Ако је P потпрстен, а I идеал прстена R, тада је њихов пресек идеал од P и важи:*

$$(I + P)/I \cong P/(I \cap P).$$

На крају, ако је I идеал, а P потпрстен прстена R, P/I ће бити потпрстен прстена R/I.

Теорема 0.15. (Трећа теорема о изоморфизмима за прстене) *За сваки идеал I прстена R постоји бијекција $P \leftrightarrow P/I$ скупа свих потпрстена прстена R који садрже I и скупа свих потпрстена прстена R/I. Такође, постоји бијекција $J \leftrightarrow J/I$ између скупа свих идеала прстена R који садрже I и скупа свих идеала прстена R/I, и за сваки од тих идеала $J \supset I$ важи*

$$(R/I)/(J/I) \cong R/J.$$

Докази ових теорема су скоро исти као одговарајући за групе, наравно уз поистовећивање "подгрупа" $\leftrightarrow$ "потпрстен" и "нормална подгрупа" $\leftrightarrow$ "идеал". (Не треба да их знате, а не морате ни формулације теорема осим прве.)

0.3.7 Кинеска теорема о остацима за прстене

Знамо да се највећи заједнички делилац два природна броја може изразити као њихова "линеарна комбинација" са целобројним коефицијентима, то јест да за све $m, n \in \mathbb{Z}$ постоје $a, b \in \mathbb{Z}$ за које је $ma + nb = d = NZD(m, n)$ (показали смо ово користећи Еуклидов алгоритам, у првом семестру). Посебно, ако су m и n узајамно прости, то јест ако је $NZD(m, n) = 1$, постојаће a и b такви да је $1 = ma + nb$. Приметимо да је онда и за свако $k \in \mathbb{Z}$: $k = mak + nbk$, односно да се сваки елемент прстена $\mathbb{Z}$ може написати као збир једног елемента из идеала $m\mathbb{Z}$ и једног из $n\mathbb{Z}$, па је $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Тада кажемо и да су идеали $m\mathbb{Z}$ и $n\mathbb{Z}$ узајамно прости или копрости. То мотивише следећу дефиницију:

Дефиниција 0.13. За идеале I и J прстена R кажемо да су *копрости* ако је њихов збир цео прстен, односно ако је $I + J = R$.

Теорема 0.16. (Кинеска теорема о остацима) *Ако су идеали I и J комутативног прстена R копрости, њихов производ је једнак њиховом пресеку, $IJ = I \cap J$, и важи*

$$R/IJ \cong R/I \times R/J.$$

Такође, $R/I_1 \dots I_n \cong R/I_1 \times \cdots \times R/I_n$, кад год су свака два од наведених идеала копроста.

Доказ. Чињеницу да је $I+J = R$ претварамо у оперативни израз: $x+y = 1$ за неке $x \in I$ и $y \in J$ (сваки елемент из R, па и јединица, се може представити као збир једног из I и једног из J). Одавде следи да је и свако $a \in R$ облика $a = ax + ay$ за те x и y. Знамо да је $IJ \subset I \cap J$. Нека је сада $a \in I \cap J$. Елемент a је облика $a = ax + ay$ за ове $x \in I$ и $y \in J$, па је $ax + ay \in IJ$ (јер $x \in I,\ a \in J$, као и $a \in I,\ y \in J$, и R комутативан). Дакле, $I \cap J \subset IJ$, а тиме и $I \cap J = IJ$. Дефинишимо сада пресликавање $f : R \to R/I \times R/J$ са

$$f(a) = (a + I, a + J)$$

Тврдимо да је ово један хомоморфизам прстена. Пре свега, $R/I \times R/J$ је прстен као Декартов производ два прстена (количничка) (имали смо код примера прстена). Треба показати да је f сагласно са сабирањима и множењима:

$$f(a+b) = (a+b+I, a+b+J) = ((a+I)+(b+I), (a+J)+(b+J)) = (a+I, a+J)+(b+I, b+J) = f(a)+f(b),$$

$$f(ab) = (ab+I, ab+J) = ((a+I)(b+I), (a+J)(b+J)) = (a+I, a+J)\cdot(b+I, b+J) = f(a)\cdot f(b).$$

Овде смо користили дефиниције операција у количничком прстену и у Декартовом производу. Важи и $f(1) = (1 + I, 1 + J) = \mathbf{1}_{R/I\times R/J}$, па је f заиста хомоморфизам. Шта му је језгро?

$$Ker f = \{a \in R : f(a) = \mathbf{0}_{R/I\times R/J}\} = \{a \in R : f(a) = (I, J)\} = \{a \in R : (a + I, a + J) = (I, J)\}$$

$$= \{a \in R : a + I = I \wedge a + J = J\} = \{a \in R : a \in I \wedge a \in J\} = I \cap J.$$

За разлику од досадашњих примера, овде је теже одредити слику него језгро (обично се одмах види да ли је пресликавање "на" или шта му је слика). Тврдимо да је $Imf = R/I \times R/J$, то јест да је f епиморфизам. Нека је $(b+I, c+J)$ произвољан елемент из $R/I \times R/J$. Треба показати да постоји $a \in R$ тако да је $f(a) = (a+I, a+J) = (b+I, c+J)$. Вратимо се на елементе $x \in I$ и $y \in J$ за које је $x + y = 1$. Посматрајмо елемент $a = by + cx$. Он је даље једнак $a = b(1-x) + cx = b + (c-b)x$, односно, $a - b = (c-b)x$, па пошто $x \in I$, биће $a - b \in I$. Ово је еквивалентно са $a + I = b + I$. Аналогно је $a = by + c(1-y) = c + (b-c)y$, односно, $a - c = (b-c)y$, што уз $y \in J$ даје $a - c \in J$. То је опет еквивалентно са $a + J = b + J$. Дакле, за дате b и c нашли смо a тако да је $f(a) = (b+I, c+J)$, па је $Imf = R/I \times R/J$. Применимо сада прву теорему о изоморфизмима за прстене, $R/Kerf \cong Imf$, и то нам даје жељени изоморфизам:

$$R/I \cap J \cong R/I \times R/J,$$

односно,

$$R/IJ \cong R/I \times R/J.$$

Остаје нам случај кад имамо n идеала $I_1, \ldots, I_n$, узајамно простих у паровима. Тврдимо да су онда копрости и идеали $I = I_1$ и $J = I_2 \cdots I_n$. Зашто? I_1 је узајамно прост са сваким I_k за $2 \leq k \leq n$. То значи да за свако $2 \leq k \leq n$ постоје $a_k \in I = I_1$ и $b_k \in I_k$ за које је $a_k + b_k = 1$. Помножимо све те једнакости:

$$(a_2 + b_2)(a_3 + b_3) \ldots (a_n + b_n) = 1 \;\Rightarrow\; A + b_2 b_3 \ldots b_n = 1,$$

где смо са A означили збир свих производа који имају бар један чинилац a_k, то јест који припадају I. Онда је и A као њихов збир поново у I. С друге стране, $B = b_2 b_3 \ldots b_n$ припада $I_2 I_3 \cdots I_n = J$, па из $A + B = 1$ следи $I + J = R$. Према управо доказаном првом делу теореме, важи $R/IJ \cong R/I \times R/J$, односно

$$R/I_1 I_2 \cdots I_n \cong R/I_1 \times R/I_2 \cdots I_n.$$

Сада применимо индуктивну хипотезу и на исти начин раставимо други фактор у овом производу. □

Пример 0.25. Нека је $R = \mathbb{Z}$, $I = m\mathbb{Z}$ и $J = n\mathbb{Z}$. Откоментарисали смо већ да је $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ акко је $NZD(m,n) = 1$, а имали смо и пример да је производ ових идеала $m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z}$, па претходна теорема у овом случају гласи:

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

или

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

Ово је баш *Кинеска теорема о остацима у прстену* $\mathbb{Z}$ коју смо већ имали, јер каже да ако су m и n узајамно прости, једном пару елемената $r \in \mathbb{Z}_m$ и $s \in \mathbb{Z}_n$ одговара тачно један елемент из $\mathbb{Z}_{mn}$, или, еквивалентно, да систем конгруенција

$$x = r \ (mod\ m)$$

$$x = s \ (mod\ n)$$

има бар једно заједничко решење, које је и јединствено по модулу mn.

0.3.8 Прости и максимални идеали

Нагласили смо већ аналогију између нормалних подгрупа код група и идеала код прстена. Као што сечењем групе G по њеној нормалној подгрупи H добијамо нову групу G/H, која може имати неке особине које почетна група нема (што постижемо избором одговарајуће подгрупе H, на пример, код увођења извода смо тражили да количник буде комутативан), тако сечењем прстена R по његовом идеалу I добијамо нови прстен, који може бити "финији" од полазног ако наметнемо додатне услове које треба да испуњава I. За почетак ћемо тражити да количнички прстен нема делиоце нуле.

Дефиниција 0.14. За идеал P прстена R кажемо да је *прост* ако је $P \neq R$ и ако важи:

$$ab \in P \;\Rightarrow\; a \in P \;\vee\; b \in P.$$

Теорема 0.17. *Идеал $P \neq R$ прстена R је прост акко количнички прстен R/P нема праве делитеље нуле.*

Доказ. Нека је $P \neq R$ прост. Посматрајмо два елемента у количнику чији је производ нула (односно сам P).

$$(a+P)(b+P) = P, \text{ то јест}$$
$$ab + P = P,$$

одакле следи $ab \in P$. Како је P прост, следи да $a \in P$ или $b \in P$. Ово опет значи да је $a + P = P$ или $b + P = P$. Дакле, ако је у R/P производ два елемента нула, бар један од њих је нула, па R/P нема праве делитеље нуле. Обрнуто, нека R/P нема праве делитеље нуле. То значи да за све $a, b \in R$ важи:

$$(a+P)(b+P) = P \;\Rightarrow\; a + P = P \;\vee\; b + P = P.$$

Ово је еквивалентно томе да

$$ab + P = P \;\Rightarrow\; a + P = P \;\vee\; b + P = P,$$

односно

$$ab \in P \;\Rightarrow\; a \in P \;\vee\; b \in P,$$

па је P прост. □

Пример 0.26. Нека је $R = \mathbb{Z}$ и $P = p\mathbb{Z}$. За које $p \in \mathbb{Z}$ је P прост идеал? (Приметимо да $a \in n\mathbb{Z}$ значи да $n \mid a$.) Услов

$$ab \in p\mathbb{Z} \;\Rightarrow\; a \in p\mathbb{Z} \;\vee\; b \in p\mathbb{Z}$$

је еквивалентан са

$$p \mid ab \;\Rightarrow\; p \mid a \;\vee\; p \mid b,$$

а ово значи да је p прост број. Дакле, прости идеали у прстену целих бројева су тачно они генерисани простим бројевима.

Пример 0.27. Нека је $R = \mathbb{F}[X]$, где је $\mathbb{F}$ поље. Показали смо већ да су и у њему сви идеали главни. Покажите да је главни идеал $P = \langle p(X) \rangle$ прост акко је $p(X)$ нерастављив полином.

Направили смо домен сечењем. Можемо ли да "профинимо" количнички прстен још мало, рецимо да тражимо да он буде поље? Испоставиће се да за испуњење овог захтева треба да почетни прстен посечемо по довољно великим идеалима, односно *максималним*.

Дефиниција 0.15. Идеал M прстена R је *максималан* ако је прави и ако не постоји прави идеал различит од њега који га садржи, то јест, прави идеал M је максималан ако важи

$$M \subset I \subset R \;\Rightarrow\; M = I \;\vee\; I = R.$$

Теорема 0.18. *Нека је M прави идеал комутативног прстена R. Тада је M максималан акко је R/M поље.*

Доказ. Нека је M максималан идеал комутативног прстена R. Треба показати да је R/M поље, то јест да у њему сваки елемент различит од нуле има инверз. Шта значи да је $a + M \in R/M$ различит од нуле? Нула у R/M је M, па је $a + M \neq M$ акко a не припада M. То даље значи да је идеал M строго садржан у збиру идеала генерисаног са a и идеала M: $M \subset \langle a \rangle + M$. Дакле, постоји идеал који садржи M, па из дефиниције максималности, следи да је тај идеал једнак целом прстену: $\langle a \rangle + M = R$. Ово значи да се сваки елемент из R може представити као збир једног из $\langle a \rangle$ и једног из M, а то посебно важи и за јединицу овог прстена: $1 = ab + m$ за неке $b \in R$, $x \in M$. Приметимо да је ово еквивалентно томе да се елемент ab разликује од јединице прстена до на елемент из M, па је: $(a + M)(b + M) = ab + M = (1 - m) + M = 1 + (-m + M) = 1 + M$. Ово је потврда да је $b + M$ инверз од $a + M$ у R/M.

Обрнуто, нека је M идеал такав да је R/M поље, и нека је $M \subset I \subset R$. Треба показати да је $M = I$ или $I = R$. Нека не важи прва једнакост, то јест $M \neq I$. То значи да постоји $x \in I \setminus M$, што даље повлачи да је $x + M \neq M$. У количничком прстену ово значи да $x + M$ није нула, па пошто је по претпоставци тај количник поље, $x + M$ ће имати инверз. Дакле, постоји $y \in R$ тако да је $(x + M)(y + M) = 1 + M$, односно, $xy + M = 1 + M$. То сад значи да $xy - 1 \in M$, односно $xy - 1 = m$ за неко $m \in M$. Сада јединицу можемо да представимо као збир неког елемента из M и xy: $1 = xy + (-m)$. Овде је $x \in I$, па са њим и $xy \in I$, а $(-m) \in M \subset I$, па и $(-m)$ припада I. На крају, како је I затворен за сабирање, биће $1 = xy + (-m) \in I$, што повлачи да је идеал I једнак целом прстену R. Дакле, ако не важи једнакост код прве инклузије, мораће да важи код друге, што показује да је M максималан идеал. □

Приметимо да је сваки максималан идеал уједно и прост (ако је R/M поље, онда је свакако и област целих). Обрнути не важи: узмемо било који идеал P такав да је R/P без делитеља нуле, а да није поље, на пример у $R = \mathbb{Z}[X]$ узмемо $P = \langle X \rangle$. Шта је овде R/P? У P су сви полиноми облика $X \cdot (...)$, то јест сви полиноми чији је слободан члан нула. Онда у количничком прстену има онолико елемената колико има могућности за слободан члан:

$$p(X) + \langle X \rangle = a_0 + a_1 X + \ldots + a_m X^m + \langle X \rangle = a_0 + \langle X \rangle,\ a_0 \in \mathbb{Z}$$

Дакле, $\mathbb{Z}[X]/\langle X \rangle \cong \mathbb{Z}$. Како је $\mathbb{Z}$ област целих, идеал $\langle X \rangle$ је прост, али није максималан, јер $\mathbb{Z}$ није поље.

Пример 0.28. У прстену целих бројева прости и максимални идеали се поклапају.

-Видели смо већ да су прости идеали у $\mathbb{Z}$ облика $p\mathbb{Z}$ за p прост број. Зашто су они и максимални? Нека је $M = p\mathbb{Z} \subset I = n\mathbb{Z}$ (сви идеали у $\mathbb{Z}$ су главни.) То значи да и

$p \in n\mathbb{Z}$, то јест да $n \mid p$, па је $n = p$ или $n = 1$, односно $I = p\mathbb{Z} = M$ или $I = \mathbb{Z}$. По дефиницији, M је максималан.

Пример 0.29. Прости и максимални идеали се поклапају и у прстену полинома $\mathbb{F}[X]$, где је $\mathbb{F}$ поље. Они су генерисани нерастављивим полиномима.

Пример 0.30. Нека је $R = \mathbb{R}[X]$ и $M = \langle X^2 + 1 \rangle$. Полином $X^2 + 1$ је нерастављив над $\mathbb{R}$, па као количник очекујемо поље. Тврдимо да је

$$\mathbb{R}[X]/\langle X^2 + 1 \rangle \cong \mathbb{C}.$$

Уочимо хомоморфизам прстена $f : \mathbb{R}[X] \to \mathbb{C}$ дат са $f(p) = p(i)$ (ово јесте хомоморфизам јер се израчунавање вредности полинома у тачки слаже са сабирањем и множењем полинома). Ово је и епиморфизам, јер за свако $a + bi \in \mathbb{C}$ се бар $a + bX$ слика у њега. Дакле, $Imf = \mathbb{C}$. Шта му је језгро? Нека $p(X) \in Kerf$. То значи да је $p(i) = 0$. Поделимо p еуклидски са $X^2 + 1$: $p(X) = (X^2 + 1)q(X) + a + bX$, где $a, b \in \mathbb{R}$, и заменимо $X = i$. Добијамо $0 = p(i) = 0 + a + bi$, то јест $a + bi = 0$, а одавде $a = b = 0$. Следи да је $p(X) = (X^2 + 1)q(X)$, односно $p \in \langle X^2 + 1 \rangle$. Обрнуто свакако важи, јер је $f(X^2 + 1) = 0$, па је $Kerf = \langle X^2 + 1 \rangle$. Сада применимо прву теорему о изоморфизмима:

$$\mathbb{R}[X]/\langle X^2 + 1 \rangle \cong \mathbb{C}.$$

0.3.9 Дељивост у прстенима

Надаље ће нам R увек бити област целих или комутативан домен, то јест, комутативан прстен без правих делитеља нуле. Приметимо да је скуп свих инверзибилних елемената овог домена, R^*, комутативна група у односу на множење. За два елемента $a, b \in R$ ћемо рећи да су *придружени* ако се разликују до на инверзибилни елемент, и писаћемо $a \sim b$. Дакле,

$$a \sim b \;\Leftrightarrow\; a = \alpha b, \text{ за неко } \alpha \in R^*.$$

Придружене елементе поистовећујемо када говоримо о дељивости, што ће бити јасно у наставку.

Пример 0.31. У прстену целих бројева инверзибилни елементи су $\{-1, 1\}$, па су два елемента придружена ако се разликују до на знак. У прстену $\mathbb{F}[X]$, где је $\mathbb{F}$ поље, инверзибилни елементи су инверзибилни скалари, тј. $\mathbb{F}[X]^* = \mathbb{F} \setminus \{0\}$. Приметимо да када говоримо о дељивости, највећем заједничком делиоцу, растављању и сличним појмовима, бројеви 20 и -20 имају исте особине, као и полиноми $X^2 + 5X + 4$ и $3X^2 + 15X + 12$, само што обично бирамо позитиван број, и моничан полином, за представнике својих класа.

Сада ћемо дефинисати појмове везане за дељивост у произвољном домену, аналогне онима у $\mathbb{Z}$.

Дефиниција 0.16. Нека је R комутативан домен. За елемент $b \neq 0$ кажемо да *дели* елемент a ако је $a = bq$ за бар једно $q \in R$. Пишемо $b \mid a$.

Ако је $a = bq$, кажемо да је a дељиво са b у прстену R, а b је делилац елемента a. Шта можемо да закључимо из претходне дефиниције? Прво да је количник q јединствен: R нема делиоце нуле, па су у њему сви не-нула елементи регуларни, што значи да из $a = bq = bq'$ следи $q = q'$. Даље, $a = bq$ значи да је a у главном идеалу генерисаном са b, па је онда и читав идеал генерисан са a садржан у идеалу генерисаном са b:

$$a = bq \;\Rightarrow\; a \in \langle b\rangle \;\Rightarrow\; \langle a\rangle \subset \langle b\rangle.$$

Дакле, на језику главних идеала,

$$b \mid a \;\Leftrightarrow\; \langle a\rangle \subset \langle b\rangle.$$

Такође, за не-нула елементе a и b

$$a \mid b \;\wedge\; b \mid a \;\Leftrightarrow\; \langle a\rangle = \langle b\rangle,$$

али одавде не следи $a = b$ већ $a \sim b$: $a \mid b \;\wedge\; b \mid a \;\Leftrightarrow\; b = ap \;\wedge\; a = bq$ за неке $p, q \in R$, па је $a = apq$ и пошто је a регуларан, биће $pq = 1$, односно $p, q \in R^*$, а тиме и $a \sim b$. (Тако је и у прстену $\mathbb{Z}$ и код полинома, приметите да $10 \mid (-10)$, као и $(-10) \mid 10$, али није $10 = -10$ него $10 \sim (-10)$).

Означимо са $D(a)$ скуп свих делилаца датог елемента a. Јасно је да $D(a)$ садржи све инверзибилне елементе прстена R, као и све елементе придружене елементу a ($a = \alpha\alpha^{-1}a$ за све $\alpha \in R^*$). За остале делиоце елемента a кажемо да су *прави*. За елементе који немају праве делиоце користимо исти назив као и у $\mathbb{Z}$.

Дефиниција 0.17. За елемент p комутативног домена R кажемо да је *нерастављив* или *атом* у том домену ако није инверзибилан или нула и ако нема праве делиоце у R. Другим речима, p је атом ако важи

$$p = ab \;\Rightarrow\; a \in R^* \;\vee\; b \in R^*$$

или, еквивалентно,

$$p = ab \;\Rightarrow\; p \sim a \;\vee\; p \sim b.$$

То опет на језику главних идеала значи да не постоји прави идеал који строго садржи $\langle p\rangle$, па је p нерастављив акко је идеал $\langle p\rangle$ максималан у скупу свих главних идеала домена R.

Дефиниција 0.18. За елемент p комутативног домена R кажемо да је *прост* у том домену ако није инверзибилан или нула и ако важи:

$$p \mid ab \;\Rightarrow\; p \mid a \;\vee\; p \mid b.$$

Одавде одмах следи да је елемент p прост акко је идеал $\langle p\rangle$ прост ($p \mid ab \;\Leftrightarrow\; ab \in \langle p\rangle$, а $p \mid a \;\vee\; p \mid b \;\Leftrightarrow\; a \in \langle p\rangle \;\vee\; b \in \langle p\rangle$.

Важи: Сваки прост елемент је и нерастављив.

-Нека је p прост.

$$p = ab \;\Rightarrow\; p \mid ab \;\Rightarrow\; p \mid a \;\vee\; p \mid b.$$

Нека, на пример, $p \mid a$. Онда је $a = pq$ за неко $q \in R$, па из $p = ab$ имамо даље $p = pqb$, односно $qb = 1$, па је b инверзибилан. Аналогно, ако би $p \mid b$, добили бисмо да $a \in R^*$.

Обрнуто не важи!

Пример 0.32. Пример прстена у ком атоми нису прости Нека је R скуп свих полинома из $\mathbb{Z}[X]$ којима су коефицијенти уз X парни,

$$R = \{p = a_0 + a_1X + a_2X^2 + \ldots + a_mX^m : m \in \mathbb{N}_0, a_i \in \mathbb{Z}, a_1 - \text{паран}\}.$$

Лако се провери да је R потпрстен прстена $\mathbb{Z}[X]$ (коефицијент уз X у збиру два полинома је збир њихових коефицијената уз X, а коефицијент уз X у производу два полинома је збир производа слободних чланова и коефицијената уз X; јединица и нула имају коефицијент нула уз X, па су у R). Уочимо елемент $X^2 \in R$. Он је нерастављив у R (иако је растављив у $\mathbb{Z}[X]$, али X не припада R!) Међутим, X^2 није прост у прстену R, јер на пример, $X^2 \mid 10X \cdot 20X$, али X^2 не дели ни $10X$ ни $20X$.

Пример 0.33. Још један пример прстена у ком атоми нису прости Нека је

$$R = \mathbb{Z}[\sqrt{-5}] = \{p(\sqrt{-5}) : p \in \mathbb{Z}[X]\} = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\}.$$

У њему важи

$$(1 + \sqrt{-5})(1 - \sqrt{-5}) = 9 = 3 \cdot 3,$$

па 3 дели производ на левој страни, а не дели ниједан од фактора. Дакле, 3 је у овом прстену нерастављив, али није прост.
(За доказ да је 3 нерастављив уочи се функција $N(a + b\sqrt{-5}) = a^2 + 5b^2$-норма, која слика R у $\mathbb{N}$ (то је заправо квадрат модула овог комплексног броја) за коју важи да је $N(xy) = N(x)N(y)$. Ако би било $3 = pq$, важило би и $N(3) = N(p)N(q)$, односно $9 = N(p)N(q)$. Ово је сада растав у $\mathbb{N}$, па су могућности $1 \cdot 9$ и $3 \cdot 3$. Откоментаришимо само случај $N(p) = 1$, $N(q) = 9$. Ако је $p = a + b\sqrt{-5}$, шта значи $N(p) = 1$? То значи да је $a^2 + 5b^2 = 1$ за неке $a, b \in \mathbb{Z}$. Одавде следи $a = 1$ или $a = -1$, а $b = 0$, па је $p = 1$ или $p = -1$, односно p је инверзибилан, па ово није прави растав елемента 3. Слично за остале могућности.)

0.3.10 Факторизација

Дефиниција 0.19. За комутативан домен R кажемо да је *атомичан* ако је у њему сваки елемент који није инверзибилан или нула производ коначно много атома, то јест ако свако $a \in R \setminus (R^* \cup \{0\})$ има бар једну факторизацију

$$a = p_1p_2 \cdots p_n$$

у којој је сваки p_i неки атом у R. Међу овим атомима може бити и једнаких, а n је дужина те атомичне факторизације од a. Сматраћемо да инверзибилни елеманти имају атомичну факторизацију дужине нула.

Пример 0.34. У прстену $\mathbb{Z}$ су $28 = 2 \cdot 2 \cdot 7$ и $28 = (-2) \cdot 7 \cdot (-2)$ две атомичне факторизације елемента 28. Приметимо да су оне једнаке до на редослед и придруженост атома који у њима учествују.
Такође, у прстену $\mathbb{Q}[X]$, елемент $X^2 + 5X + 4$ има атомичне факторизације $X^2 + 5X + 4 = (X + 1)(X + 4) = (7X + 7)(\frac{1}{7}X + \frac{4}{7})$ које се опет разликују до на придруженост атома.

Пример 0.35. Нека је R скуп свих полинома из $\mathbb{Z}[X]$ којима су коефицијенти уз X парни (имали смо га у прошлој лекцији). У њему су $8X^2 = 2 \cdot 2X \cdot 2X$ и $8X^2 = 2 \cdot 2 \cdot 2 \cdot X^2$ две атомичне факторизације елемента $8X^2$ које нису исте дужине, нити су сви атоми прве придружени атомима друге.
Такође, у прстену $\mathbb{Z}[\sqrt{-5}]$, елемент 9 има две атомичне факторизације:
$9 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ и $9 = 3 \cdot 3$, и њихови атоми поново нису придружени.

Из претходних примера можемо закључити да се неправилности (са којима се нисмо сусретали до сада, у бројевним скуповима и код полинома) јављају у оним доменима код којих се прости и нерастављиви елементи не поклапају. Наравно, желимо да издвојимо класу домена у којима таквих неправилности нема.

Дефиниција 0.20. Комутативни домен R је *домен са једнозначном факторизацијом* ако је атомичан и ако су атомичне факторизације његових елемената једнозначне до на редослед и придруженост атома. То значи да, ако је

$$a = p_1 p_2 \cdots p_m \text{ и } a = q_1 q_2 \cdots q_n$$

где су p_i и q_j атоми, онда је $m = n$ и постоји пермутација $\sigma \in S_n$ таква да је за свако i, $p_i \sim q_{\sigma(i)}$.

Напомена 0.36. У литератури често домене са једнозначном факторизацијом зовемо UFD домени, од "*unique factorization domain*".

Теорема 0.19. *Атомичан домен R је домен са једнозначном факторизацијом акко су у њему сви атоми и прости.*

Доказ. $\Rightarrow$) Нека је R домен са једнозначном факторизацијом и нека је у њему елемент p атом. Покажимо да је p прост. Нека $p \mid ab$ и нека су $a = p_1 p_2 \cdots p_m$ и $b = q_1 q_2 \cdots q_n$ атомичне факторизације од a и b. Онда је $ab = p_1 p_2 \cdots p_m q_1 q_2 \cdots q_n$ једна атомична факторизација елемента ab. Како $p \mid ab$, биће $ab = pc$, за неко c које опет има своју атомичну факторизацију. Дакле, ab има атомичну факторизацију у којој фигурише атом p, па због једнозначности факторизације, p мора бити придружен неком p_i или q_j. То даље значи да $p \mid a$ или $p \mid b$, па је по дефиницији p прост.
$\Leftarrow$) Нека су сада сви атоми у R прости. Треба показати да су атомичне факторизације (које постоје због атомичности) свих елемената из R једнозначне. Нека је $a = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$. По претпоставци, сви атоми p_i и q_j су прости, па имамо да просто p_1 дели $q_1 q_2 \cdots q_n$, што имплицира да $p_1 \mid q_j$ за неко j. Без умањења општости, претпоставимо да $p_1 \mid q_1$. Међутим, q_1 је атом, па је $q_1 = \alpha p_1$ за неки инверзибилни елемент α. Онда следи $\alpha q_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$, а одавде $\alpha p_2 \cdots p_m = q_2 \cdots q_n$ и сада исти поступак можемо применити на ове две атомичне факторизације дужина $m - 1$ и $n - 1$ итд. Јасно је да ћемо добити да је $m = n$ и да су атоми придружени, до на редослед. □

Осим класе домена са једнозначном факторизацијом увешћемо још једну значајну класу домена.

Дефиниција 0.21. Комутативни домени у којима су сви идеали главни зову се *главни* или *главноидеалски домени*.

Напомена 0.37. У литератури често главноидеалске домене зовемо PID домени, од "*principal ideal domain*".

Пример 0.38. Показали смо већ да су у прстену $\mathbb{Z}$ сви идеали главни, па је $\mathbb{Z}$ главноидеалски домен.
Исто важи и за прстене $\mathbb{F}[X]$, где је $\mathbb{F}$ поље.

Нешто касније ћемо показати да је сваки главноидеалски домен уједно и домен са јединственом факторизацијом, то јест да важи $PID \subset UFD$. Пре тога ћемо увести још две важне класе домена. Знамо да у прстену целих бројева највећи заједнички делилац два броја рачунамо на два начина: или раставимо те бројеве на просте факторе и онда узмемо заједничке ("UFD" својство прстена $\mathbb{Z}$) или га тражимо коришћењем Еуклидовог алгоритма, па онда изразимо као линеарну комбинацију датих бројева ("Безуова релација" која следи из "PID" својства прстена $\mathbb{Z}$).

Увели смо већ ознаку $D(a)$ за скуп свих делилаца елемента a. Означимо сада са $D(a,b)$ скуп свих заједничких делилаца датих елемената a и b. Пошто је $D(a,b) = D(a) \cap D(b)$, овај скуп садржи бар све инверзибилне елементе прстена R. Ако су то и њихови једини заједнички делиоци, за a и b кажемо да су узајамно прости или копрости у прстену R и уместо $D(a,b) = R^*$ пишемо $D(a,b) = D(1)$ (инверзибилни елементи и јесу делиоци јединице).

Скуп заједничких делилаца датих елемената a и b не може увек да се изрази као скуп делилаца једног елемента. Ипак, ако је то случај, то јест ако за дате a и b постоји $d \in R$ за који је $D(a,b) = D(d)$, тај елемент d зовемо *највећи заједнички делилац* елемената a и b и пишемо $d = NZD(a,b)$. Из ове дефиниције следи да је d највећи заједнички делилац елемената a и b ако за свако $c \in R$ важи:

$$c \mid a \ \wedge \ c \mid b \ \Leftrightarrow c \mid d.$$

Највећи заједнички делилац два елемената је одређен једнозначно до на придруженост, јер ако је $NZD(a,b) = d = d'$, из $d' \mid d \ \wedge \ d \mid d'$ следи да је $d \sim d'$. $NZD(a,0)$ дефинишемо као и у $\mathbb{Z}$, $NZD(a,0) = a$.

Дефиниција 0.22. Комутативни домени у којима свака два елемента имају највећи заједнички делилац зову се *Гаусови домени*.

Јасно је да је сваки домен са јединственом факторизацијом и Гаусов. Покажимо да је и сваки главноидеалски домен Гаусов.

Теорема 0.20. *У главноидеалском домену свака два елемента имају највећи заједнички делилац.*

Доказ. Нека је R главноидеалски домен и $a, b \in R$. Посматрајмо идеал $\langle a, b\rangle$ генерисан елементима a и b. Пошто је у R сваки идеал главни, постојаће $d \in R$ такво да је $\langle a, b\rangle = \langle d\rangle$. Докажимо да је то d један највећи заједнички делилац од a и b. Прво, из $a, b \in \langle d\rangle$ следи да постоје $a_1, b_1 \in R$ за које је $a = da_1$ и $b = db_1$. Ово опет не значи ништа друго него да $d \mid a \ \wedge \ d \mid b$, па $d \in D(a,b)$. Нека сада $d' \mid a \ \wedge \ d' \mid b$. Онда постоје $a', b' \in R$ за које је $a = d'a'$ и $b = d'b'$. Искористили смо то да $a, b \in \langle d\rangle$, али важи и обрнуто, $d \in \langle a, b\rangle$. Одавде је $d = ar + bs$ за неке $r, s \in R$. Даље имамо

$$d = d'a'r + d'b's = d'(a'r + b's),$$

па $d' \mid d$. По дефиницији је $d = NZD(a,b)$. □

Дакле, доказали смо не само да свака два елемента a и b у главноидеалском домену имају највећи заједнички делилац, већ и да постоје елементи $r, s \in R$ за које је тај највећи заједнички делилац d облика $d = ar+bs$. Ову релацију зовемо Безуова релација, а домене у којима она важи *Безуови*.

Дефиниција 0.23. Комутативни домени у којима је сума свака два главна идеала такође главни идеал зову се *Безуови домени*.

У доказу претходне теореме смо видели да у Безуовим доменима свака два елемента a и b имају највећи заједнички делилац, и он је управо то d за које је $\langle a\rangle + \langle b\rangle = \langle d\rangle$. Дакле, класа Безуових домена је потклаcа класе Гаусових домена.

Теорема 0.21. *Сваки главноидеалски домен је и домен са јединственом факторизацијом.*

Доказ. Применићемо теорему 0.19 па ћемо прво доказати да је у главноидеалском домену сваки атом прост.

Нека је R главноидеалски домен и p нерастављив елемент у њему. Нека $p \mid ab$ и нека p не дели a. Показаћемо да тада p мора да дели b. Пре свега, из услова да атом не дели неки елемент следи да је њихов највећи заједнички делилац 1: нека је $d = NZD(a, p)$. Одавде је $p = p'd$ за неко $p' \in R$. Али p је атом, па $p' \in R^*$ или $d \in R^*$. Ако би било $p' \in R^*$, било би $p \sim d$, па пошто $d \mid a$, следило би $p \mid a$, супротно претпоставци да p не дели a. Остаје $d \in R^*$, односно $NZD(a, p) \in R^*$, што пишемо $NZD(a, p) = 1$. Покажимо сада да из $p \mid ab$ и $NZD(a, p) = 1$ следи да $p \mid b$. Налазимо се у главноидеалском домену, па је највећи заједнички делилац од a и p облика $ar + ps$ за неке $r, s \in R$, то јест $1 = ar + ps$. Помножимо ову једнакост са b: $b = bar + bps$. Сада из $p \mid ab$ следи да p дели оба сабирка на десној страни, па $p \mid b$.

Да бисмо применили теорему 0.19 остаје да покажемо да је R атомичан. Прво ћемо доказати да сваки непразан скуп идеала у R има максималан елемент. Претпоставимо супротно. Нека је J непразан скуп идеала који не садржи максималан елемент. Нека је $I_1 \in J$ произвољан идеал. Пошто није максималан постојаће идеал $I_2 \in J$ тако да је I_1 садржан у I_2. Из истих разлога постоји I_3 за који је $I_2 \subset I_3$ итд. Добијамо стриктно растући ланац идеала

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

у J. Знамо да унија идеала у општем случају није идеал, али то не важи за растуће уније (исто као код подгрупа и потпростора). Унија $J = \bigcup_{n\in\mathbb{N}} I_n$ је идеал: нека $a, b \in J$, то значи да $a \in I_m$, $b \in I_n$ за неке $m, n \in \mathbb{N}$ и можемо претпоставити да је $m \leq n$, што значи да су онда и a и b у I_n, па је и њихов збир у I_n, а тиме опет у J. Такође, за $a \in I_m$ и $x \in R$, $ax \in I_m \subset J$. Уверили смо се да је J идеал, али R је главноидеалски домен, па постоји a које генерише J, $J = \langle a\rangle$. Сада из $a \in J$ следи да a припада неком I_k. Како је I_k идеал, заједно са a садржи и $\langle a\rangle$. Добијамо $J = \langle a\rangle \subset I_k$, односно $I_n = I_k$ за свако $n \geq k$, па бесконачан строго растући ланац идеала у R и не постоји!

Претпоставимо сада да у R постоје елементи који немају факторизацију на атоме. Уочимо скуп идеала $\mathcal{J}$ задат са:

$$\mathcal{J} = \{\langle a\rangle : a \in R \setminus (R^* \cup \{0\}) \text{ и } a \text{ нема факторизацију на атоме}\}.$$

Управо смо доказали да у $\mathcal{J}$ постоји максималан елемент, нека је то $\langle c\rangle$. Како c нема факторизацију на атоме, c ни сам није атом, па је $c = ab$ где $a, b \neq 0$ и a и b нису инверзибилни. Одавде је $\langle c\rangle \subset \langle a\rangle$ и $\langle c\rangle \subset \langle b\rangle$, па a и b имају факторизације на атоме, јер је $\langle c\rangle$ максималан у $\mathcal{J}$. Нека су њихове атомичне факторизације $a = p_1 p_2 \cdots p_m$ и $b =$

$q_1q_2\cdots q_n$. Онда је $c = ab = p_1p_2\cdots p_mq_1q_2\cdots q_n$ једна атомична факторизација елемента c, што је у супротности са чињеницом да $c \in \mathcal{J}$.
Дакле, сви елементи у R имају атомичне факторизације, па је по теореми 0.19 R домен са једнозначном факторизацијом. □

Дакле, $PID \subset UFD$. Обрнуто не важи. Може се показати да ако је R домен са једнозначном факторизацијом, онда је и $R[X]$ домен са једнозначном факторизацијом (ми нећемо). Одавде следи да је $\mathbb{Z}[X]$ домен са једнозначном факторизацијом. Међутим, он није главноидеалски, на пример идеал генерисан са 7 и са X није главни, то јест не постоји полином $p(X)$ са целобројним коефицијентима такав да је $\langle 7, X\rangle = \langle p(X)\rangle$.

На крају ћемо, ради комплетности, само дефинисати још једну класу домена, који су "најфинији", то јест најближи пољима.

Дефиниција 0.24. Нека је R комутативни домен. За R кажемо да је *еуклидски домен* ако на њему постоји бар један *еуклидски алгоритам*, односно пресликавање $f : R \to \mathbb{N}_0$ које задовољава услове:
1) За свако $a, b \in R$, $b \neq 0$, постоје $q, r \in R$ за које је $a = bq + r$ и $f(r) < f(b)$.
2) За све $a, b \in R \setminus \{0\}$ важи $f(a) \leq f(ab)$.

Први услов је нама добро познато еуклидско дељење с остатком, и на њему се и у овим доменима заснива начин за одређивање највећег заједничког делиоца два елемента - Еуклидов алгоритам. Штавише, еуклидски домени нису само Безуови, они су поткласа класе главноидеалских домена, али то нећемо овде доказати.

Пример 0.39. Прстен $\mathbb{Z}$ је еуклидски, његова еуклидска функција је $f(m) = |m|$. Такође, прстен $\mathbb{F}[X]$, где је $\mathbb{F}$ поље, је еуклидски, $f(p)$ је степен полинома p.

Класе комутативних домена које смо дефинисали задовољавају следећи ланац строгих инклузија:

комутативни домени $\supset$ Гаусови домени $\supset$ домени са једнозначном факторизацијом $\supset$ главноидеалски домени $\supset$ еуклидски домени $\supset$ поља, као и

комутативни домени $\supset$ Гаусови домени $\supset$ Безуови домени $\supset$ главноидеалски домени $\supset$ еуклидски домени $\supset$ поља.

При том су класе Безуових домена и домена са једнозначном факторизацијом неупоредиве, и њихов пресек је тачно класа главноидеалских домена.

0.4 Поља

0.4.1 Раширења поља

Дефиниција 0.25. Поље је комутативан прстен у ком једино нула нема инверз. Другим речима, поље је алгебарска структура $(\mathbb{F}, +, \cdot)$ са две бинарне операције таква да је $(\mathbb{F}, +)$ Абелова група, $(\mathbb{F} \setminus \{0\}, \cdot)$ такође Абелова група и операција $\cdot$ је дистрибутивна у односу на операцију $+$.

Пример 0.40. Најмање поље карактеристике нула је поље рационалних бројева $\mathbb{Q}$. Скупови реалних $\mathbb{R}$ и комплексних бројева $\mathbb{C}$ су такође поља. $\mathbb{Q}$ је *поље разломака* над комутативним доменом $\mathbb{Z}$ (елементима домена додамо и њихове инверзе -то је конструкција која се може извести над сваком облашћу целих R - елементи тог поља су облика $ab^{-1} = b^{-1}a = \frac{a}{b},\ a, b \in R, b \neq 0$). Дефиницију реалних бројева користећи рационалне и непрекидност сте дали у Анализи, а комплексним ћете се бавити у Комплексној анализи. (За потребе нашег курса је довољно оно што сте научили о бројевним скуповима и операцијама у њима у току досадашњег школовања, уз подсећање на особине полинома над поменутим пољима - факторизацију, нуле, кандидате за нуле, нерастављивост - Никола!)

Пример 0.41. Знамо да су $\mathbb{Z}_p$ поља ако је p прост број (инверзибилни елементи у $\mathbb{Z}_n$ су они који су узајамно прости са n, па су сви осим нуле инверзибилни акко је n прост). Дакле, најмање поље има 2 елемента и то је $\mathbb{Z}_2$.
$\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$ итд. су такође поља.

Дефиниција 0.26. За поље $\mathbb{K}$ кажемо да је *раширење* поља $\mathbb{F}$ и пишемо $\mathbb{F} \leq \mathbb{K}$ (или $\mathbb{K} \geq \mathbb{F}$) ако $\mathbb{K}$ има бар једно потпоље $\tilde{\mathbb{F}}$ изоморфно са $\mathbb{F}$.

Обично поља $\mathbb{F}$ и $\tilde{\mathbb{F}}$ идентификујемо, и сматрамо да је $\mathbb{F}$ потпоље од $\mathbb{K}$ (потпоље се дефинише аналогно као потпрстен, садржи нулу и јединицу поља и затворено је за све операције).

Сетимо се сада примера векторских простора из Линеарне алгебре: свако поље је векторски простор над било којим својим потпољем. Шта су операције у том векторском простору? Ако је $\mathbb{F}$ потпоље поља $\mathbb{K}$, сабирање "вектора" у векторском простору $\mathbb{K}$ ће бити обично сабирање у пољу $\mathbb{K}$, а множење "вектора" из $\mathbb{K}$ "скаларом" из $\mathbb{F}$ је опет само множење у пољу $\mathbb{K}$ ($\alpha \in \mathbb{F},\ v \in \mathbb{K} \ \Rightarrow\ \alpha v \in \mathbb{K}$). Овај векторски простор означавамо са $\mathbb{K}_{\mathbb{F}}$ (још једном, то је дакле само поље $\mathbb{K}$, али посматрано као векторски простор над $\mathbb{F}$, што нам омогућава да користимо термине и тврђења из теорије векторских простора).

Пример 0.42. Свако коначно поље има p^n елемената, где је p прост број.

-Нека је $\mathbb{F}$ коначно поље. Онда је његова карактеристика неки прост број p (карактеристика поља је или нула или прост број, имали смо то тврђење за домене). Посматрајмо

карактеристични потпрстен од $\mathbb{F}$, $\mathbb{F}_0 = \{0_\mathbb{F}, 1_\mathbb{F}, \dots (p-1)1_\mathbb{F}\}$. Приметимо да је он изоморфан са $\mathbb{Z}_p$, па је и сам једно поље. Пошто смо поновили да је свако поље векторски простор над било којим својим потпољем, $\mathbb{F}$ ће бити векторски простор над $\mathbb{F}_0$. Како је $\mathbb{F}$ коначно, и његова димензија је коначна, рецимо n. Знамо да је сваки векторски простор V димензије n над пољем $\mathbb{K}$ изоморфан са $\mathbb{K}^n$, па је $\mathbb{F} \cong \mathbb{F}_0^n \cong \mathbb{Z}_p^n$, одакле непосредно следи $\mid \mathbb{F} \mid = p^n$.

Дефиниција 0.27. За раширење $\mathbb{K}$ поља $\mathbb{F}$ кажемо да је *коначно* ако је векторски простор $\mathbb{K}_\mathbb{F}$ коначне димензије. Тада се димензија тог простора означава са

$$dim\ \mathbb{K}_\mathbb{F} = [\mathbb{K} : \mathbb{F}]$$

и зове *степен раширења* $\mathbb{K}$ поља $\mathbb{F}$.

Ако је $[\mathbb{K} : \mathbb{F}] = n$, све $\mathbb{F}$-базе векторског простора $\mathbb{K}_\mathbb{F}$ су кардиналности n. Значи, постоји бар један систем од n елемената поља $\mathbb{K}$, на пример $[e_1, e_2, \dots, e_n]$, такав да сваки елемент из $\mathbb{K}$ може на јединствен начин да се представи као линеарна комбинација e-ова, са коефицијентима из $\mathbb{F}$.

Пример 0.43. Поље комплексних бројева је коначно раширење поља реалних бројева и важи $[\mathbb{C} : \mathbb{R}] = 2$, јер је $[1, i]$ једна база векторског простора $\mathbb{C}_\mathbb{R}$ (сваки комплексан број је облика $z = a \cdot 1 + b \cdot i$ за $a, b \in \mathbb{R}$).

Пример 0.44. Поље реалних бројева није коначно раширење поља рационалних бројева, јер не постоји коначно реалних бројева таквих да се сви остали изражавају као њихове линеарне комбинације са рационалним коефицијентима.

Теорема 0.22. *Ако су $\mathbb{K} \geq \mathbb{F}$ и $\mathbb{L} \geq \mathbb{K}$ коначна раширења поља, тада је поље $\mathbb{L}$ коначно раширење поља $\mathbb{F}$ и важи:*

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

Доказ. Нека је $[\mathbb{L} : \mathbb{K}] = m$ и $[\mathbb{K} : \mathbb{F}] = n$. Ово значи да $\mathbb{L}_\mathbb{K}$ има базу од m елемената, нека је то $e = [e_1, e_2, \dots, e_m]$, и да $\mathbb{K}_\mathbb{F}$ има базу од n елемената, нека је то $f = [f_1, f_2, \dots, f_n]$. Доказаћемо да је систем

$$h = \{e_i f_j : 1 \leq i \leq m,\ 1 \leq j \leq n\}$$

једна база векторског простора $\mathbb{L}_\mathbb{F}$, то јест да је генератриса и линеарно независан.

-генератриса: нека је l произвољан елемент из L. Пошто је e база за $\mathbb{L}$ над $\mathbb{K}$, постоје $\alpha_i \in \mathbb{K}$ за које је $l = \alpha_1 e_1 + \alpha_2 e_2 + \cdots \alpha_m e_m$. Даље, како је f база за $\mathbb{K}$ над $\mathbb{F}$, за свако α_i постоје $\beta_{ij} \in \mathbb{F}$ за које је $\alpha_i = \beta_{i1} f_1 + \beta_{i2} f_2 + \cdots + \beta_{in} f_n$. Дакле, свако $l \in L$ је облика

$$l = \sum_{i=1}^{m} (\sum_{j=1}^{n} \beta_{ij} f_j) e_i = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} e_i f_j$$

при чему су $\beta_{ij} \in \mathbb{F}$, а производи $e_i f_j$ су свакако из L. То значи да је систем h једна генератриса $\mathbb{F}$-векторског простора L.

-линеарна независност: Нека је

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \alpha_{ij} e_i f_j = 0$$

за неке $\alpha_{ij} \in \mathbb{F}$. Ово је еквивалентно са

$$\sum_{i=1}^{m}(\sum_{j=1}^{n}\alpha_{ij}f_j)e_i = 0,$$

па пошто су $e_1, e_2, \ldots, e_m$ линеарно независни у векторском простору $\mathbb{L}_{\mathbb{K}}$, биће $\gamma_i = (\sum_{j=1}^{n}\alpha_{ij}f_j) = 0$ за свако i. Међутим, сваки γ_i је линеарна комбинација f_j-ова, који су линеарно независни у векторском простору $\mathbb{K}_{\mathbb{F}}$, па је $\alpha_{ij} = 0$ за све $1 \leq i \leq m,\ 1 \leq j \leq n$. Закључујемо да систем h и линеарно независан.

Дакле, h је једна база векторског простора $\mathbb{L}_{\mathbb{F}}$, па како она броји mn вектора, димензија овог простора је управо толико, а по дефиницији то је степен раширења $[\mathbb{L} : \mathbb{F}] = mn$. □

Последица. Јасно је да се претходно тврђење о транзитивности степена раширења индукцијом може продужити на коначно поља: ако су $\mathbb{F}_1 \leq \mathbb{F}_2 \leq \cdots \leq \mathbb{F}_n$ поља таква да су сва раширења $\mathbb{F}_i \geq \mathbb{F}_{i-1}$ коначна, онда је и $\mathbb{F}_n$ коначно раширење поља $\mathbb{F}_1$ и важи:

$$[\mathbb{F}_n : \mathbb{F}_1] = [\mathbb{F}_n : \mathbb{F}_{n-1}][\mathbb{F}_{n-1} : \mathbb{F}_{n-2}] \cdots [\mathbb{F}_2 : \mathbb{F}_1].$$

0.4.2 Проста раширења поља

Нека је $\mathbb{K}$ било које раширење поља $\mathbb{F}$ и α фиксиран елемент из $\mathbb{K}$. Шта је најмање потпоље од $\mathbb{K}$ које садржи $\mathbb{F}$ и α? Пошто је поље $\mathbb{F}$ затворено за све операције, остаје да се побринемо за α. То раширење за почетак мора да садржи све степене $1, \alpha, \alpha^2, \ldots$, затим њихове производе са елементима поља $\mathbb{F}$ и све коначне збирове тако добијених елемената. Добићемо скуп

$$\{c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_m\alpha^m : m \in \mathbb{N}_0,\ c_i \in \mathbb{F}\},$$

односно све полиноме по α са коефицијентима из $\mathbb{F}$, и тај скуп означавамо

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

Наравно, овај скуп је затворен за сабирање и множење, па је потпрстен од $\mathbb{K}$, али не садржи инверзе свих својих елемената. Зато додајемо и њих и добијамо

$$\mathbb{F}(\alpha) = \{\frac{p(\alpha)}{q(\alpha)} : p, q \in \mathbb{F}[X], q(\alpha) \neq 0\}.$$

Ово је тражено минимално потпоље од $\mathbb{K}$ које садржи и $\mathbb{F}$ и α. Овакво раширење зове се *просто* раширење поља $\mathbb{F}$ са *примитивним* елементом α.

Општије, за раширење $\mathbb{K}$ поља $\mathbb{F}$ кажемо да је *просто* ако постоји бар једно $\alpha \in \mathbb{K}$ за које је $\mathbb{K} = \mathbb{F}(\alpha)$. Елемент α који одређује овакво раширење зове се *примитивни* елемент тог раширења.

Даље, са сваким елементом α из датог раширења $\mathbb{K}$ поља $\mathbb{F}$ можемо посматрати и одговарајуће просто раширење $\mathbb{F}(\alpha)$ поља $\mathbb{F}$. У њему су свакако елементи $1, \alpha, \alpha^2, \ldots$.

Разликујемо две важне класе елемената из раширења $\mathbb{K}$ у односу на то да ли је наведени низ елемената, тј. вектора из векторског простора $\mathbb{K}_{\mathbb{F}}$, линеарно зависан или независан над $\mathbb{F}$. Ако су вектори $1, \alpha, \alpha^2, \ldots$ линеарно зависни, онда постоје $c_i \in \mathbb{F}$ од којих је бар један различит од нуле, такви да је $c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_k\alpha^k = 0$. То је еквивалентно томе да је α нула бар једног не-нула полинома из $\mathbb{F}[X]$. Тада кажемо да је елемент α *алгебарски* над пољем $\mathbb{F}$. На пример, бројеви $\sqrt{5}$, $\sqrt[3]{7}$, $\sqrt{2}+\sqrt{7}$ су алгебарски над пољем $\mathbb{Q}$.

У супротном, то јест ако је низ вектора $1, \alpha, \alpha^2, \ldots$ линеарно независан, односно ако α поништава једино нула полином из $\mathbb{F}[X]$, за њега кажемо да је *трансцендентан* над пољем $\mathbb{F}$ (тада се α понаша исто као неодређена код полинома, "не меша" се са елементима из $\mathbb{F}$, и важи $\mathbb{F}(\alpha) \cong \mathbb{F}(X)$; на пример, бројеви π и e су трансцендентни над пољем $\mathbb{Q}$).

За алгебарске елементе важи да је прстен $\mathbb{F}[\alpha]$ једнак пољу $\mathbb{F}(\alpha)$ и да је степен раширења $[\mathbb{F}(\alpha) : \mathbb{F}]$ коначан и лако се рачуна.

Теорема 0.23. *Нека је $\mathbb{K}$ раширење поља $\mathbb{F}$ и $\alpha \in \mathbb{K}$. Елемент α је алгебарски над $\mathbb{F}$ акко је $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$. У том случају постоји јединствен моничан полином μ такав да за сваки полином $p \in \mathbb{F}[X]$ важи*

$$p(\alpha) = 0 \quad \Leftrightarrow \quad \mu \mid p.$$

Полином μ је нерастављив у прстену $\mathbb{F}[X]$ и његов степен је управо степен раширења $[\mathbb{F}[\alpha] : \mathbb{F}]$.

Доказ. Ако је $\mathbb{F}(\alpha) = \mathbb{F}[\alpha]$, то значи да се сваки разломак у чијем је имениоцу полином по α може изразити као неки други полином по α (очигледно је да је $\mathbb{F}[\alpha] \subset \mathbb{F}(\alpha)$, а наша претпоставка је да важи и обрнута инклузија). На пример, $\frac{1}{2\alpha-5} = p(\alpha)$ за неки полином $p \in \mathbb{F}[X]$, одакле је $1 = (2\alpha - 5)p(\alpha)$, тј. $2\alpha p(\alpha) - 5p(\alpha) - 1 = 0$, па α поништава полином $q(X) = 2Xp(X) - 5p(X) - 1$ са коефицијентима из поља $\mathbb{F}$, што значи да је α алгебарски над $\mathbb{F}$.

Докажимо сада главни смер тврђења: нека је α алгебарски над $\mathbb{F}$. То значи да α поништава бар један не-нула полином из $\mathbb{F}[X]$, одакле следи да постоји и полином најмањег степена за који то важи. Узмимо моничан такав - нека је μ моничан полином најмањег степена из $\mathbb{F}[X]$ ког α поништава. Ако је p било који полином из $\mathbb{F}[X]$, поделићемо га еуклидски са μ: $p = \mu q + r$, при чему је степен полинома r мањи од степена полинома μ. Заменимо $X = \alpha$: $p(\alpha) = \mu(\alpha)q(\alpha) + r(\alpha)$, па како је $\mu(\alpha) = 0$, добијамо $p(\alpha) = r(\alpha)$. Ако је p полином за који је $p(\alpha) = 0$, претходна једнакост даје $r(\alpha) = 0$. Међутим, степен полинома r је строго мањи од степена полинома μ, па је ово могуће једино ако је $r \equiv 0$ (иначе би r био минималан, што је у супротности са претпоставком да је то μ). Дакле, $p = \mu q$, односно $\mu \mid p$. Приметимо да смо овим добили и следеће: за сваки полином p из $\mathbb{F}[X]$, $p(\alpha) = r(\alpha)$, при чему је r остатак при еуклидском дељењу полинома p са μ. Ово значи да се $p(\alpha)$ може изразити као линеарна комбинација степена елемента α који су мањи од степена полинома μ. Ако је степен полинома μ једнак m, добијамо $p(\alpha) = r(\alpha) \in \mathcal{L}[1, \alpha, \alpha^2, \ldots, \alpha^{m-1}]$, па је овај систем генератриса векторског простора $\mathbb{F}[\alpha]$ над $\mathbb{F}$. Такође, ако направимо $\mathbb{F}$-линеарну комбинацију ових степена која је једнака нули, $c_0 + c_1\alpha + \cdots + c_{m-1}\alpha^{m-1} = 0$, добићемо да су сви $c_i = 0$, јер би у супротном постојао не-нула полином степена строго мањег од m код α поништава. Дакле, систем $[1, \alpha, \alpha^2, \ldots, \alpha^{m-1}]$ је једна база векторског простора $\mathbb{F}[\alpha]$, па је $dim\ \mathbb{F}[\alpha] = m$.

Зашто је полином са наведеним особинама јединствен? Претпоставимо да постоји још један моничан полином $\tilde{\mu}$ који задовољава ове услове. Из управо доказаног својства да тај полином дели сваки други који у α има вредност нула, следи с једне стране да $\mu \mid \tilde{\mu}$, а с друге да $\tilde{\mu} \mid \mu$. То значи да се разликују до на скалар, $\tilde{\mu} = a\mu$, $a \in \mathbb{F}$, али како су оба монична, тај скалар је 1, тј. $\tilde{\mu} = \mu$. Зашто је μ нерастављив? Претпоставимо да за неке полиноме p и q важи $\mu = pq$. Заменимо α: $\mu(\alpha) = p(\alpha)q(\alpha)$, односно $p(\alpha)q(\alpha) = 0$. Налазимо се у пољу L у ком нема правих делитеља нуле, па је $p(\alpha) = 0$ или $q(\alpha) = 0$. Ово повлачи да $\mu \mid p$ или $\mu \mid q$, па је један од њих скалар, а други придружен μ, што значи да μ нема праву факторизацију.

Остаје још да докажемо да је $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$. Као што је већ речено, $\mathbb{F}[\alpha] \subset \mathbb{F}(\alpha)$. Треба показати да важи и обрнуто, то јест да се инверзи свих не-нула елемената из $\mathbb{F}[\alpha]$ могу изразити као полиноми по α. Нека је $p(\alpha) \neq 0$ произвољан елемент из $\mathbb{F}[\alpha]$ (p је наравно полином из $\mathbb{F}[X]$). Опет из карактеризације полинома μ имамо: $p(\alpha) \neq 0$ повлачи да μ не дели p. Међутим, μ је атом, па је чињеница да не дели неки други полином еквивалентна томе да су узајамно прости: $NZD(\mu, p) = 1$. Знамо да то даље значи да постоје неки полиноми $a(X)$ и $b(X)$ за које је $\mu a + pb = 1$. Уврстимо α у претходну једнакост: $\mu(\alpha)a(\alpha) + p(\alpha)b(\alpha) = 1$. Овде је $\mu(\alpha) = 0$, па је $p(\alpha)b(\alpha) = 1$. Ово тачно значи да је $b(\alpha)$ инверз елемента $p(\alpha)$: $\frac{1}{p(\alpha)} = b(\alpha) \in \mathbb{F}[\alpha]$. Дакле, сваки не-нула елемент из $\mathbb{F}[\alpha]$ има инверз у $\mathbb{F}[\alpha]$, па је $\mathbb{F}[\alpha]$ поље, то јест $\mathbb{F}[\alpha] = \mathbb{F}(\alpha)$. □

Полином μ који је дефинисан и описан у управо доказаном тврђењу зовемо *минимални полином* елемента α. Његов степен је *степен* елемента α. Показали смо да је тај степен једнак степену раширења $[\mathbb{F}[\alpha] : \mathbb{F}]$.

Пример 0.45. Елемент $\sqrt{7}$ је алгебарски над пољем $\mathbb{Q}$. Он поништава полином $X^2 - 7$, који је нерастављив над $\mathbb{Q}$ по Ајзенштајновом критеријуму (Никола!), па је то и минимални полином овог елемента. Дакле, степен раширења $[\mathbb{Q}[\sqrt{7}] : \mathbb{Q}] = deg(X^2 - 7) = 2$.
На исти начин, $\sqrt[3]{7}$ поништава полином $X^3 - 7$, који је нерастављив над $\mathbb{Q}$ опет по Ајзенштајновом критеријуму, па је то и минимални полином овог елемента. Одатле је степен раширења $[\mathbb{Q}[\sqrt[3]{7}] : \mathbb{Q}] = deg(X^3 - 7) = 3$.

0.4.3 Алгебарска раширења поља

Нека је $\mathbb{K}$ раширење поља $\mathbb{F}$ и $\alpha_1 \in \mathbb{K}$ алгебарски над $\mathbb{F}$. Тада је $[\mathbb{F}_1 : \mathbb{F}] = deg\ \mu_{\alpha_1}$, где је $\mathbb{F}_1 = \mathbb{F}[\alpha_1] = \mathbb{F}(\alpha_1)$. Нека је, даље, $\alpha_2 \in \mathbb{K}$ алгебарски над $\mathbb{F}_1$ и $\mathbb{F}_2 = \mathbb{F}_1[\alpha_2]$. Сваки елемент из $\mathbb{F}_2$ је облика $\sum_j (\sum_i a_{ij}\alpha_1^i)\alpha_2^j$, где $a_{ij} \in \mathbb{F}$ (полином по α_2 са коефицијентима из $\mathbb{F}_1 = \mathbb{F}[\alpha_1]$), односно $\sum a_{ij}\alpha_1^i\alpha_2^j$, па је $\mathbb{F}_2 = \mathbb{F}[\alpha_1][\alpha_2] = \mathbb{F}[\alpha_1, \alpha_2]$. С друге стране, $\mathbb{F}_2 = \mathbb{F}_1[\alpha_2] = \mathbb{F}_1(\alpha_2)$, јер је α_2 алгебарски над $\mathbb{F}_1$, а то је даље $\mathbb{F}(\alpha_1)(\alpha_2)$, што је по дефиницији поље (облим заградама означавамо поље) и то најмање поље које садржи $\mathbb{F}$ и елементе α_1 и α_2. Дакле,

$$\mathbb{F}[\alpha_1, \alpha_2] = \mathbb{F}(\alpha_1, \alpha_2).$$

Сада можемо наставити са неким α_3 алгебарским над $\mathbb{F}_2$ и тако даље.

Теорема 0.24. *Ако су $\alpha_1, \alpha_2, \ldots, \alpha_n$ елементи из раширења $\mathbb{K}$ поља $\mathbb{F}$ такви да је α_1 алгебарски над $\mathbb{F}$ и за свако $i \in \{2, \ldots, n\}$ елемент α_i алгебарски над $\mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_{i-1})$, тада је*

$$\mathbb{F}[\alpha_1, \alpha_2, \ldots, \alpha_n] = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$$

најмање потпоље од $\mathbb{K}$ које садржи све $\alpha_1, \alpha_2, \ldots, \alpha_n$. Такође, у њему су сви елементи алгебарски и над пољем $\mathbb{F}$.

Доказ. Индукцијом по n. За $n = 1$ то је теорема 0.23, а за $n = 2$ коментар који претходи тврђењу које управо доказујемо. Нека је $\mathbb{F}_i = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_i)$ и нека тврђење важи за $n-1$, односно $\mathbb{F}_{n-1} = \mathbb{F}[\alpha_1, \alpha_2, \ldots, \alpha_{n-1}]$. Пошто је α_n алгебарски над $\mathbb{F}_{n-1}$, биће $\mathbb{F}_n = \mathbb{F}_{n-1}[\alpha_n]$, а одатле $\mathbb{F}_n = \mathbb{F}[\alpha_1, \alpha_2, \ldots, \alpha_n]$. Како је $\mathbb{F}_n = \mathbb{F}(\alpha_1, \alpha_2, \ldots, \alpha_n)$, следи први део тврђења.
Докажимо сада да је сваки елемент из $\mathbb{F}_n$ алгебарски и над $\mathbb{F}$. Према теореми 0.23 свако поље $\mathbb{F}_i$ је коначно раширење поља $\mathbb{F}_{i-1}$ (јер је $\mathbb{F}_i = \mathbb{F}_{i-1}[\alpha_i]$, па је степен раширења $[\mathbb{F}_i : \mathbb{F}_{i-1}]$ једнак степену минималномг полинома елемента α_i над пољем $\mathbb{F}_{i-1}$). На основу теореме 0.22 и њене Последице, добијамо да је поље $\mathbb{F}_n$ коначно раширење самог поља $\mathbb{F}$. Узмимо сада произвољан елемент $\alpha \in \mathbb{F}_n$. Посматрајмо елементе (односно векторе из $\mathbb{F}$-векторског простора $\mathbb{F}_n$) $1, \alpha, \alpha^2, \ldots$. Пошто је $\mathbb{F}_n$ коначне димензије као $\mathbb{F}$-векторски простор, ови вектори су линеарно зависни. Дакле, постоји њихова линеарна комбинација са коефицијентима из поља $\mathbb{F}$ који нису сви нула, а чија је вредност нула. То нам даје не-нула полином из $\mathbb{F}[X]$ ког α поништава, што значи да је α алгебарски елемент над $\mathbb{F}$. □

Нека је сада $\mathbb{K}$ раширење поља $\mathbb{F}$ и α и $\beta \neq 0$ елементи из $\mathbb{K}$ који су алгебарски над $\mathbb{F}$ (тим пре је β алгебарски над $\mathbb{F}[\alpha]$, па је $\mathbb{F}[\alpha, \beta] = \mathbb{F}(\alpha, \beta)$ по претходној теореми). То поље $\mathbb{F}[\alpha, \beta]$ садржи све елементе које можемо добити помоћу α и β и сви они су, опет по претходној теореми, и алгебарски над $\mathbb{F}$. Посебно, збир, производ, супротни елементи, као и инверзи алгебарских елемената су поново алгебарски, што значи да је скуп свих елемената из $\mathbb{K}$ који су алгебарски над $\mathbb{F}$ затворен за све операције поља. Дакле, скуп свих елемената из $\mathbb{K}$ који су алгебарски над $\mathbb{F}$ је једно потпоље поља $\mathbb{K}$ које означавамо са $\mathbb{F}[\mathbb{K}]$ и зовемо *алгебарско затворење* поља $\mathbb{F}$ у његовом раширењу $\mathbb{K}$. Такође, за раширење $\mathbb{K}$ поља $\mathbb{F}$ кажемо да је *алгебарско* ако је $\mathbb{K} = \mathbb{F}[\mathbb{K}]$, односно ако су сви елементи из $\mathbb{K}$ алгебарски над $\mathbb{F}$. Приметимо да смо у доказу претходне теореме показали да је свако коначно раширење и алгебарско (последњи део доказа, од $\mathbb{F}_n$ је коначно раширење од $\mathbb{F}$).

Посебно, за $\mathbb{F} = \mathbb{Q}$, а $\mathbb{K} = \mathbb{C}$, комплексни бројеви који су алгебарски над пољем рационалних бројева зову се *алгебарски бројеви*. Они чине једно потпоље поља $\mathbb{C}$ које означавамо са $\mathbb{Q}[\mathbb{C}]$.

Пример 0.46. Одредити степен раширења $[\mathbb{Q}[\sqrt{2}, \sqrt{7}] : \mathbb{Q}]$. Да ли је ово просто раширење поља $\mathbb{Q}$?

-Пре свега, према теореми из овог одељка је $\mathbb{Q}[\sqrt{2}, \sqrt{7}] = \mathbb{Q}(\sqrt{2}, \sqrt{7})$ најмање натпоље поља $\mathbb{Q}$ које садржи елементе $\sqrt{2}$ и $\sqrt{7}$. Према теореми 0.22 важи

$$[\mathbb{Q}[\sqrt{2}, \sqrt{7}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt{2}, \sqrt{7}] : \mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}].$$

Даље је $[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$, јер је степен минималног полинома елемента $\sqrt{2}$ над $\mathbb{Q}$ једнак 2 (полином $X^2 - 2$ је нерастављив према Ајзенштајну). Такође, $[\mathbb{Q}[\sqrt{2}, \sqrt{7}] : \mathbb{Q}[\sqrt{2}]] = 2$,

јер је минимални полином за $\sqrt{7}$ над $\mathbb{Q}[\sqrt{2}]$ једнак X^2-7 (јасно је да је ово минимални полином за $\sqrt{7}$ над $\mathbb{Q}$; минимални полином над ширим пољем би евентуално делио овај, међутим у овом случају то би значило да је првог степена, односно да $\sqrt{7} \in \mathbb{Q}[\sqrt{2}]$; докажите да није $\sqrt{7} = a + b\sqrt{2}$ за неке $a, b \in \mathbb{Q}$!). Дакле, $[\mathbb{Q}[\sqrt{2}, \sqrt{7}] : \mathbb{Q}] = 2 \cdot 2 = 4$.

Ово јесте просто раширење поља $\mathbb{Q}$, са примитивним елементом рецимо $\sqrt{2}+\sqrt{7}$. Да је $\mathbb{Q}[\sqrt{2}+\sqrt{7}] \subset \mathbb{Q}[\sqrt{2}, \sqrt{7}]$ је очигледно, јер елемент $\sqrt{2}+\sqrt{7}$ припада $\mathbb{Q}[\sqrt{2}, \sqrt{7}]$. Обрнуту инклузију показујемо тако што сваки од елемената $\sqrt{2}$ и $\sqrt{7}$ изразимо преко $\sqrt{2}+\sqrt{7}$ и његовог инверза (Никола!). Дакле, $\mathbb{Q}[\sqrt{2}, \sqrt{7}] = \mathbb{Q}[\sqrt{2}+\sqrt{7}]$.

0.4.4 Коренско поље полинома

У претходном делу смо елементима из неког раширења поља $\mathbb{F}$ придружили полиноме из $\mathbb{F}[X]$, помоћу којих смо рачунали степене раширења одређених тим елементима. Нека је сада ситуација таква да је дат полином f из $\mathbb{F}[X]$, степена n. Питамо се шта је најмање раширење поља $\mathbb{F}$ у ком се f може раставити на линеарне факторе. Другим речима, тражимо раширење облика $\mathbb{F}[\alpha_1, \alpha_2, \ldots, \alpha_n]$ у ком су $\alpha_1, \alpha_2, \ldots, \alpha_n$ тачно све нуле полинома f. За почетак ћемо показати да постоји просто раширење $\mathbb{F}(\alpha)$ поља $\mathbb{F}$ такво да је α баш нула полинома f, заправо конструисаћемо један модел таквог раширења.

Теорема 0.25. *За сваки моничан и нерастављив полином f из $\mathbb{F}[X]$ постоји просто раширење $\mathbb{F}[\alpha]$ поља $\mathbb{F}$ у коме је $f(\alpha) = 0$. То поље је одређено једнозначно до на изоморфизам.*

Доказ. Ако такво поље $\mathbb{F}[\alpha]$ постоји, знамо две ствари о њему:

- оно је слика прстена $\mathbb{F}[X]$ у односу на пресликавање $p \mapsto p(\alpha)$;

- пошто је полином f нерастављив, он ће бити и минимални полином елемента α.

Посматрајмо пресликавање $\pi : p \mapsto p(\alpha)$. Јасно је да је π хомоморфизам (вредност збира два полинома у неком елементу је збир њихових вредности; исто важи и за производ). Такође је јасно да је "на" (тако је и дефинисан $\mathbb{F}[\alpha]$), $Im\pi = \mathbb{F}[\alpha]$. Хајде да нађемо језгро овог хомоморфизма:

$$Ker\pi = \{p \in \mathbb{F}[X] : \pi(p) = 0\} = \{p \in \mathbb{F}[X] : p(\alpha) = 0\} = \{p \in \mathbb{F}[X] : \mu_\alpha \mid p\} = \{p \in \mathbb{F}[X] : f \mid p\}$$

$$= \{p \in \mathbb{F}[X] : p = fq,\ q \in \mathbb{F}[X]\} = \langle f \rangle.$$

Применимо сада прву теорему о изоморфизмима за прстене:

$$\mathbb{F}[X]/\langle f \rangle \cong \mathbb{F}[\alpha].$$

Означимо са $\mathbb{K}$ овај количнички прстен. Приметимо одмах да је $\mathbb{K}$ поље пошто је f атом у $\mathbb{F}[X]$ (имали смо да су идеали генерисани атомима максимални у скупу главних идеала, али у прстену $\mathbb{F}[X]$ сви идеали су главни, па је $\langle f \rangle$ максималан, и одговарајући количник је поље!). То поље је потпуно одређено полиномом f, узели смо $\mathbb{F}[X]$ и само га посекли по идеалу генерисаном са f. Тврдимо да је то тражено раширење.

Прво, да ли је $\mathbb{K} = \mathbb{F}[X]/\langle f\rangle$ уопште раширење поља $\mathbb{F}$? Треба нам утапање (мономорфизам) поља $\mathbb{F}$ у поље $\mathbb{K}$, а за то ће бити довољно да узмемо рестрикцију одговарајућег количничког пресликавања из $\mathbb{F}[X]$ на $\mathbb{F}[X]/\langle f\rangle$:

$$c \mapsto c + \langle f\rangle$$

је хомоморфизам из $\mathbb{F}$ у $\mathbb{F}[X]/\langle f\rangle$ који јесте "1-1" ($c+\langle f\rangle = c'+\langle f\rangle \Leftrightarrow c-c' \in \langle f\rangle \Leftrightarrow c = c'$). Даље, да ли у том проширењу постоји елемент који је нула полинома f? Означимо са $\mathfrak{a}$ елемент из количника који је одређен полиномом X: $\mathfrak{a} = X + \langle f\rangle$ и израчунајмо вредност полинома f у $\mathfrak{a}$ (радња се, дакле, дешава у $\mathbb{K} = \mathbb{F}[X]/\langle f\rangle$, резултат ће бити неки елемент из количника, односно нека класа идеала $\langle f\rangle$). Нека је $f = c_0 + c_1X + c_2X^2 + \cdots + c_mX^m$. Рачунамо:

$$f(\mathfrak{a}) = f(X + \langle f\rangle) = c_0(1 + \langle f\rangle) + c_1(X + \langle f\rangle) + c_2(X + \langle f\rangle)^2 + \cdots + c_m(X + \langle f\rangle)^m$$

$$= c_0(1+\langle f\rangle)+c_1(X+\langle f\rangle)+c_2(X^2+\langle f\rangle)+\cdots+c_m(X^m+\langle f\rangle) = c_0+c_1X+c_2X^2+\cdots+c_mX^m+\langle f\rangle$$

$$= f(X) + \langle f\rangle = f + \langle f\rangle = \langle f\rangle = \mathbf{0}_{\mathbb{K}}$$

Дакле, $\mathfrak{a}$ је нула полинома f у пољу $\mathbb{K}$!

За сада смо конструисали раширење $\mathbb{K}$ поља $\mathbb{F}$ у ком f има нулу. Показаћемо да је то раширење и просто. Израчунајмо степен $[\mathbb{K} : \mathbb{F}]$. По дефиницији то је димензија векторског простора $\mathbb{K}_{\mathbb{F}}$. Код нас је $\mathbb{K}$ количник $\mathbb{F}[X]/\langle f\rangle$. Шта је база овог векторског простора над $\mathbb{F}$? Елементи у количнику су облика $p + \langle f\rangle$, где $p \in \mathbb{F}[X]$. Поделићемо p еуклидски са f и онда је $p + \langle f\rangle = fq + r + \langle f\rangle$, односно $p + \langle f\rangle = r + \langle f\rangle = b_0 + b_1X + b_2X^2 + \cdots + b_{m-1}X^{m-1} + \langle f\rangle$, где је $m = degf$. Одавде следи да једну $\mathbb{F}$-базу количника чине елементи $[1 + \langle f\rangle, X + \langle f\rangle, X^2 + \langle f\rangle, \ldots, X^{m-1} + \langle f\rangle]$, па је $[\mathbb{K} : \mathbb{F}] = m = degf$.
С друге стране је степен проширења $[\mathbb{F}[\mathfrak{a}] : \mathbb{F}]$ по теореми 0.23 једнак степену минималног полинома елемента $\mathfrak{a}$, а то је f (коментар с почетка доказа, $\mathfrak{a}$ је нула од f, и f је нерастављив над $\mathbb{F}$): $[\mathbb{F}[\mathfrak{a}] : \mathbb{F}] = degf$. Како је $\mathbb{F}[\mathfrak{a}]$ потпоље поља $\mathbb{K}$, а исте су димензије као векторски простори над $\mathbb{F}$, биће $\mathbb{K} = \mathbb{F}[\mathfrak{a}]$.

Дакле, конструисали смо просто раширење $\mathbb{K}$ поља $\mathbb{F}$ у ком полином f има нулу $\mathfrak{a}$. То смо урадили само помоћу полинома f и датог поља $\mathbb{F}$ ($\mathbb{K} = \mathbb{F}[\mathfrak{a}] = \mathbb{F}[X]/\langle f\rangle$, при чему је $\mathfrak{a} = X + \langle f\rangle$). Опет према коментару на почетку доказа, свако раширење са траженим особинама ће бити изоморфно овом, $\mathbb{F}[\alpha] \cong \mathbb{F}[X]/\langle f\rangle$, па је оно и јединствено до на изоморфизам. □

Пример 0.47. Полином $X^2 + 1$ је нерастављив над пољем реалних бројева, па је према претходној теореми $\mathbb{R}[X]/\langle X^2 + 1\rangle$ раширење поља $\mathbb{R}$ у ком овај полином има нулу. Ако ту нулу означимо са i, теорема каже да је $\mathbb{R}[i] \cong \mathbb{R}[X]/\langle X^2 + 1\rangle$. Како је $X^2 + 1$ степена два, раширење $\mathbb{R}[i]$ је облика $\mathbb{R}[i] = \{a + bi : a, b \in \mathbb{R}\}$, а то је управо поље комплексних бројева (имали смо већ код максималних идеала да је $\mathbb{R}[X]/\langle X^2 + 1\rangle \cong \mathbb{C}$). Приметимо да ово раширење садржи и другу нулу датог полинома.

Пример 0.48. Полином $X^2 - 2$ је нерастављив над пољем рационалних бројева, па је према претходној теореми $\mathbb{Q}[X]/\langle X^2 - 2\rangle$ раширење поља $\mathbb{Q}$ у ком овај полином има нулу. Ако ту нулу означимо са $\sqrt{2}$, из доказа теореме следи да је $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[X]/\langle X^2-2\rangle$. Раширење $\mathbb{Q}[\sqrt{2}]$ је облика $\mathbb{Q}[\sqrt{2}] = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ и такође садржи другу нулу датог полинома.

Пример 0.49. Полином X^3-2 је нерастављив над пољем рационалних бројева, па је према претходној теореми $\mathbb{Q}[X]/\langle X^3-2\rangle$ раширење поља $\mathbb{Q}$ у ком овај полином има нулу. Ако је означимо са $\sqrt[3]{2}$, биће $\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[X]/\langle X^3-2\rangle$. Пошто је полином X^3-2 степена три, раширење $\mathbb{Q}[\sqrt[3]{2}]$ је облика $\mathbb{Q}[\sqrt[3]{2}] = \{a+b\sqrt[3]{2}+c(\sqrt[3]{2})^2 : a,b,c \in \mathbb{Q}\}$. Међутим, оно не садржи преостале две нуле овог полинома (оне су комплексне, а $\mathbb{Q}[\sqrt[3]{2}] \subset \mathbb{R}$).

Дефиниција 0.28. Раширење $\mathbb{K}$ поља $\mathbb{F}$ је *коренско поље* полинома $p \in \mathbb{F}[X]$ ако у $\mathbb{K}$ постоје елементи $\alpha_1, \alpha_2, \ldots, \alpha_n$ за које је $\mathbb{K} = \mathbb{F}[\alpha_1, \alpha_2, \ldots, \alpha_n]$ и

$$p = a(X-\alpha_1)(X-\alpha_2)\cdots(X-\alpha_n),$$

где је a водећи коефицијент полинома p.

Дакле, $\mathbb{K}$ је минимално раширење поља $\mathbb{F}$ над којим p има линеарну факторизацију.

Теорема 0.26. *Нека је $\mathbb{F}$ произвољно поље. Сваки полином $p \in \mathbb{F}[X]$ степена n има бар једно коренско поље $\mathbb{K} = \mathbb{F}[\alpha_1, \alpha_2, \ldots, \alpha_n]$.*

Доказ. Индукцијом по $n = deg\ p$. Ако је $n = 1$, p је облика $p = a(X-\alpha)$ за неке $a, \alpha \in \mathbb{F}$, па је његово коренско поље управо $\mathbb{K} = \mathbb{F}$.
Претпоставимо сада да сваки полином степена $n-1$ има коренско поље и узмимо произвољан полином p степена n. Да бисмо искористили индуктивну хипотезу, треба нам "једна нула мање". Зато ћемо прво узети било који атом (нерастављив полином) који дели p (ако је сам p атом, узећемо њега). По претходном тврђењу, постоји раширење $\mathbb{F}_1 = \mathbb{F}[\alpha_1]$ поља $\mathbb{F}$ у ком је α_1 нула тог атома p_1 (самим тим и полинома p). Онда је

$$p = (X-\alpha_1)q,$$

где је q неки полином из $\mathbb{F}_1[X]$. Пошто је $deg\ q = n-1$, на основу индуктивне претпоставке q има коренско поље облика $\mathbb{F}_1[\alpha_2, \ldots, \alpha_n]$, што је даље $\mathbb{F}[\alpha_1][\alpha_2, \ldots, \alpha_n]$, односно $\mathbb{F}[\alpha_1, \alpha_2, \ldots, \alpha_n]$ и то је истовремено тражено коренско поље полинома p. □

У односу на то да ли заиста треба проширити поље да би са сваким полиномом над њим садржало и све његове нуле, истичемо следећу класу поља.

Дефиниција 0.29. За поље $\mathbb{F}$ кажемо да је *алгебарски затворено* ако се подудара са коренским пољем сваког полинома из $\mathbb{F}[X]$, то јест ако сваки полином из $\mathbb{F}[X]$ има линеарну факторизацију у $\mathbb{F}[X]$.

Дефиниција 0.30. *Алгебарско затворење* поља $\mathbb{F}$ је минимално алгебарски затворено поље које садржи $\mathbb{F}$. То је, дакле, раширење поља $\mathbb{F}$ које је и алгебарско и алгебарски затворено.

Пример 0.50. Поље комплексних бројева је алгебарски затворено, док поља реалних и рационалних бројева нису.
Поље комплексних бројева је алгебарско затворење поља реалних бројева. Алгебарско затворење поља $\mathbb{Q}$ је поље свих комплексних алгебарских бројева, $\mathbb{Q}[\mathbb{C}]$ (имали смо дефиницију и ознаку у прошлој лекцији).

Пример 0.51. Одредити коренско поље $\mathbb{K}$ полинома p и степен раширења $[\mathbb{K} : \mathbb{Q}]$.

1) $p = X^4 - 4$

Растављамо p на линеарне факторе тамо где можемо, а у овом случају је то поље комплексних бројева:

$$p = (X^2 - 2)(X^2 + 2) = (X - \sqrt{2})(X + \sqrt{2})(X - i\sqrt{2})(X + i\sqrt{2}).$$

Следи да је коренско поље

$$\mathbb{K} = \mathbb{Q}[\sqrt{2}, -\sqrt{2}, i\sqrt{2}, -i\sqrt{2}] = \mathbb{Q}[\sqrt{2}, i\sqrt{2}] = \mathbb{Q}[\sqrt{2}, i]$$

(последња једнакост се веома лако показује). Треба наћи степен раширења:

$$[\mathbb{K} : \mathbb{Q}] = [\mathbb{K} : \mathbb{Q}[\sqrt{2}]] \cdot [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2 \cdot 2 = 4$$

($[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$ смо већ имали, а $[\mathbb{K} : \mathbb{Q}[\sqrt{2}]] = [\mathbb{Q}[\sqrt{2}, i] : \mathbb{Q}[\sqrt{2}]] = 2$ јер је минимални полином за i и над $\mathbb{Q}[\sqrt{2}]$ такође $X^2 + 1$ - то је његов минимални полином над $\mathbb{Q}$, а над $\mathbb{Q}[\sqrt{2}]$ остаје другог степена јер ако би био првог, следило би да $i \in \mathbb{Q}[\sqrt{2}] \subset \mathbb{R}$, што није тачно).

2) $p = X^4 + 4$

$$p = (X^2 + 2)^2 - 4X^2 = (X^2 + 2X + 2)(X^2 - 2X + 2) = ((X + 1)^2 + 1)((X - 1)^2 + 1) =$$

$$= (X + 1 + i)(X + 1 - i)(X - 1 + i)(X - 1 - i)$$

Одавде је коренско поље

$$\mathbb{K} = \mathbb{Q}[1 + i, 1 - i] = \mathbb{Q}[i]$$

и лако налазимо степен раширења

$$[\mathbb{K} : \mathbb{Q}] = [\mathbb{Q}[i] : \mathbb{Q}] = 2,$$

јер је минимални полином за i над $\mathbb{Q}$ опет $X^2 + 1$.