Emil Schönbaum

Ke Kummerovým pracím o Fermatově větě

Časopis pro pěstování mathematiky a fysiky, Vol. 37 (1908), No. 5, 484--506

Persistent URL: http://dml.cz/dmlcz/122626

zvolíme na dané tečně m tři body A_1, B_1, C_1 tak, aby řada bodová $A_1B_1C_1\ldots$ byla projektivní se svazkem paprskovým $abc\ldots$; A_1 jest průsečík přímky m se spojnicí jejího pólu M a pólu A paprsku a, obdobně B_1 a C_1. Nyní pokládáme body A_1, B_1, C_1 za dotyčné body kuželoseček přímky m se dotýkajících a danou kuželosečku k_0 ve vyšším stupni oskulujících a sestrojíme příslušné body oskulace A_3, B_3, C_3 resp. A'_3, B'_3, C'_3. Křivé řady bodové $A_2B_2C_2\ldots$ a $A'_2B'_2C'_2\ldots$ jsou patrně projektivními s křivou řadou bodovou $A_3B_3C_3\ldots$ i $A'_3B'_3C'_3\ldots$ Celkem obdržíme čtyři projektivní vztahy těchto křivých soumístných řad. Sestrojíme-li jich samodružné body, dospíváme k bodům oskulace žádané. Obecně jest úloha tato osmiznačnou.

Ke Kummerovým pracím o Fermatově větě.

Dr. **E. Schoenbaum.**

Známá věta Fermatova o nemožnosti řešení rovnice $u^n + v^n + w^n = 0$ v celých číslech pro $n \geqq 3$ není dosud dokázána. Fermat pronesl svou větu těmito slovy: „Cubum autem in duos cubos, aut quadrato quadratum in duos quadrato-quadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duas ejusdem nominis fas est dividere. Cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.“ *) Fermat tedy tvrdí přímo, že zná důkaz své věty. Byl spor o tom, možno-li Fermatovi věřiti. Faktum jest, že všechny cesty, které byly od r. 1670 k správnému provedení důkazu nastoupeny, týkají se buď jednotlivých případů věty **), anebo vyžadují prostředků, jichž neovládá dnešní mathematika, a jichž neznal pravděpodobně ani Fermat před 250 lety. Tak

*) Fermatova věta poprvé byla uveřejněna roku 1670 ve vydání Bachetova Diophanta, jakožto poznámka »ad quaestion. VIII. Diophanti Alexandrini Arithmeticorum Libri II.« Opis Bachetova Diophanta doprovázel totiž Fermat poznámkami na okraji. Vydání obstaral F-ův syn.

**) Pro $n = 3, 4, 5, 7, 14$ byla F. věta dokázána Eulerem, Fermatem samotným, Legendrem, Lamé-em, Dirichletem.

lze nahraditi Fermatovu větu výrokem:

$$\frac{u}{w} = \sqrt[n]{1 - \left(\frac{v}{w}\right)^n}$$

jest nemožný vztah pro celistvá u, v, w a celé $n \geqq 3$, nebo výraz $\sqrt[n]{1 - x^n}$ jest pro positivní rationální číslo x vždy irrationální. Důkaz vyžaduje tedy nějakého kriteria pro rationální a irrationální čísla, jehož neznáme.

Ze spousty prací, jichž předmětem byla Fermatova věta, a mezi nimiž je mnoho nesprávných*), vynikají nade všechny ostatní práce Kummerovy**) z roku 1850 a 1857. V prvé své práci dokazuje Kummer správnost F.–ovy věty pro všechna *pravidelná* prvočísla, t. j. taková prvočísla l, že v algebraických tělesech sestrojených z l-tého kořene jedničky jest počet tříd ideálů nedělitelný prvočíslem l. Důkaz sám rozpadá se ve dvě části. Kdežto důkaz Fermatova tvrzení nevyžaduje žádných hlubších vlastností zmíněných těles v případě, že žádné z čísel u, v, w není dělitelné prvočíslem l, jest pro provedení důkazu, je-li jedno z těchto čísel dělitelno l, nutno dokázati jistou větu z theorie jednotek, která zasahuje hluboko do vlastností kruhových těles. Po dokázání zmíněné věty lze vésti další důkaz methodou „la descente", kterou udal již Fermat sám. V druhé své práci učinil Kummer pokus dokázati F.—ovu větu též tehdy, je-li počet tříd ideálů tělesa z l-tého kořene dělitelný prvočíslem l a sice jen prvou mocninou l. Úplně se mu to ale nepodařilo. Jest nucen učiniti jistou omezující podmínku, jež se týče dělitelnosti určitého Bernoulliovského čísla prvočíslem l***). Tolik

*) Obšírnější literárně-historické poznámky viz ku př. *H. Smith*: Collected Mathem. Papers 1. sv.: »Report on the theory of numbers.« odstavec 61.

**) Journal für die r. u. ang. Math. Bd. 40 a Abhandlungen der königl. Akademie der Wissenschaften in Berlin 1857. Prvá práce jest otištěna též s malými změnami v Journal de Mathém. T. 16, jakožto § X. velikého »Mémoire sur la théorie des nombres complexes composées de racine de l'unité et de nombres entiers.«

***) Není tedy tvrzení Hilbertovo, že Kummer dokázal F. větu, je-li l v počtu tříd obsaženo v prvé a ne vyšší mocnině, správné. (Die Theorie der algebr. Zahlkörper. Bericht. Str. 523.)

ale plyne z obou prací, že F. věta je správna pro všechny exponenty $n \leqq 100$.

Výsledky Kummerem docílené nebyly dosud předstiženy. Byly sice učiněny po Kummerovi mnohé pokusy dokázati Fermatovu větu, ale ponejvíce navazovaly pokusy ty na starší práce (Legendreovy a jiné), kdežto práce Kummerovy zůstaly v celku neznámy, snad pro zavedení poněkud abstraktního pojmu ideálního čísla. To platí v prvé řadě o druhé práci Kummerově. Velmi cenné pojednání p. Mirimanova*) předpokládá výsledky Kummerem docílené a snaží se pro praktické jich použití nahraditi Kummerovo kriterium jiným. *Omezuje se ale jen na případ, kdy žádné z čísel u, v, w není dělitelné číslem l.* Výsledek práce je hlavně ve větě: Rovnice $x^l + y^l + z^l = 0$ je nemožná v celých číslech nedělitelných číslem l, není-li aspoň jedno z čísel Bernoulliho $B_{\mu-1}$, $B_{\mu-2}$, $B_{\mu-3}$, $B_{\mu-4}$ dělitelno číslem l. Při tom jest l liché prvočíslo a $\mu = \frac{l-1}{2}$. Toto kriterium lze ostatně rozšířiti prostředky již v druhé Kummerově práci obsaženými.

Rovněž práce p. E. Mailleta**) jsou hlavně applikací Kummerových method na obecnější diophantickou rovnici $u^\lambda + v^\lambda = cw^\lambda$.

Jakožto příklad prací připínajících se na starší methody Legendreovy uvádím *E. Wendt*: Arithmetische Studien über den letzten Fermatschen Satz***), kde se dokazuje na př. věta: Je-li n prvočíslo a $p = 2^\nu n^{k+1} + 1$ taktéž prvočíslo, jež není obsaženo v determinantu $D_{2^\nu n^k}$, je-li dále ν nesoudělné s n, pak musí, má-li býti rovnice $u^n + v^n = w^n$ v celých číslech řešitelna ($n > 2$), jedno z čísel u, v, w býti dělitelno prvočíslem n. Při tom jest D_m orthosymmetrický determinant

---

*) Mirimanoff: »L'équation indéterminée $x^l + y^l + z^l = 0$ et le criterium de Kummer.« Journal f. d. reine u. ang. Math. 1905.

**) Sur les équations indeterminées $x^\lambda + y^\lambda = cz^\lambda$ Annali di Math. 1905.

***) Journ. f. d. r. u. ang. Math. 1894.

$$Dm = \begin{vmatrix} 1 & \binom{m}{1} & \binom{m}{2} & \cdots & \binom{m}{m-1} \\ \binom{m}{m-1} & 1 & \binom{m}{1} & \cdots & \binom{m}{m-2} \\ \cdots & \cdot & \cdot & \cdots & \cdots \\ \cdots & \cdot & \cdot & \cdots & \cdots \\ \cdots & & \cdot & \cdots & \cdots \\ \binom{m}{1} & \binom{m}{2}\binom{m}{3} & & \cdots & 1 \end{vmatrix}$$

Také tato práce nepodává nových výsledků. Předložil jsem si úkol užíti nových resultátů v theorii ideálů ku zjednodušení Kummerových důkazů. V obou svých pracích Kummer vychází z výrazu pro počet tříd ideálů kruhového tělesa, jehož odvození vyžaduje transcendentních prostředků zavedených do nauky o číslech Dirichletem. V druhé práci provedení důkazu vyžaduje celé řady početních operací namnoze velmi složitých. Učinil jsem pokus obejíti se při důkaze Kummerově bez použití onoho analytického výrazu pro počet tříd jen na základě arithmetických pojmů. Jakožto vhodný prostředek k dosažení tohoto cíle objevila se mně theorie *tělesa tříd* založená v nejnovější době Hilbertem, Fueterem a Furtwänglerem.

V této práci dokážu jen pomocí jednoduchých pojmů z theorie algebraických těles větu: *Je-li l pravidelné prvočíslo, jest rovnice $u^l + v^l + w^l = 0$ pro $l \geqq 3$ v celých, od nully různých číslech nemožná.* V druhé, samostatné práci dokážu za pomoci několika vět z theorie tělesa tříd větu: *Je-li počet tříd tělesa sestrojeného z $e^{\frac{2\pi i}{l}}$, kdež l jest prvočíslo > 3, dělitelný jen prvou mocninou l, pak jest rovnice $u^l + v^l + w^l = 0$ v celých, od nully různých číslech nemožná.*

Toto odpoutání Kummerových důkazů od vyšetřování čísel Bernoulliho, k němuž vedou, zdá se mi i pro rozšíření důkazů na dělitelnost vyššími mocninami l důležito. K vůli větší srozumitelnosti omezuji předpoklady z theorie algebraických těles na nejzákladnější pojmy a věty a dokazuji vše ostatní přímo.

I.

1. Souvislost tvrzení, že rovnice

$$u^l + v^l = -w^l \qquad (1)$$

je řešitelna celými od nully různými čísly u, v, w pro prvočíselná $l \geqq 3$, s theorií algebraických těles jest očividná, píšeme-li rovnici (1) ve tvaru

$$(u + v)\,(u + \zeta v)\,(u + \zeta^2 v) \ldots (u + \zeta^{l-1} v) = -w^l,$$

kde $\zeta = e^{\frac{2\pi i}{l}}$ jest l-tý kořen jedničky, a definuje t. zv. kruhové těleso*) $k(\zeta)$, t. j. souhrn všech čísel tvaru

$$\alpha(\zeta) = a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{l-2}\zeta^{l-2},$$

kde $a_0, a_1, \ldots a_{l-2}$ značí obyčejná rationální čísla. Jsou-li koëff. $a_0, \ldots a_{l-2}$ čísla celistvá, pak slove α *celé* číslo tělesa $k(\zeta)$. Jsou tedy činitelé levé strany rovnice (1) celá čísla v $k(\zeta)$, a lze snadno ukázati, že jsou kterákoli dvě z nich nesoudělná, nemají-li přirozená čísla u, v společného dělitele**). Máme zde tedy případ, kdy součin nesoudělných celých čísel jest roven l-té mocnině celého čísla. Kdyby šlo o obyčejná přirozená čísla, mohli bychom hned souditi, že každý z činitelů jest roven l-té mocnině celého čísla. V našem případě učinil podobný závěr *Lamé****). Závěr tento předpokládá ale, že celé číslo $\alpha(\zeta)$ může býti rozloženo jediným způsobem v součin prvočinitelů, a je tedy nesprávný †), pokud se omezujeme na obor čísel tělesa $k(\zeta)$, t. j. pokud pokládáme za prvočinitele *čísla* tělesa $k(\zeta)$ nerozložitelná v další činitele. Neboť lze na jednoduchých příkladech††) ukázati, že tento rozklad v prvočinitele

*) Vzhledem k původním důvodům, jež vedly Dedekinda k zavedení pojmu »Körper«, bylo by vlastně lépe říkati »*algebraické tělo*«. — Věty zde nedokázané lze najíti i s důkazy v úvodních kapitolách *Hilbertova* Berichtu, jehož označování se v celku držím, nebo ve *Webrově* Algebře II. Bd. III. Buch, v *Bachmannově* Zahlentheorie V. Bd. a zvláště též v *Minkowski*: Diophantische Approximationen 1907.

**) Důkaz viz v oddílu III.

***) Comptes Rendus vol. XXIV.

†) To vytkl Lamé-ově pojednání již *Liouville*.

††) Tak jest ku př. v tělese $k(\sqrt{-6})$, jež sestává z čísel tvaru $a + b\sqrt{-6}$, (a, b rationální čísla), -6 rovno jednak $-2 \cdot 3$, jednak $(\sqrt{-6})^2$, a celá čísla -2, 3, $\sqrt{-6}$ nejsou v tělese $k(\sqrt{-6})$ dále rozložitelná.

jen výjimkou je jednoznačný. Závěr svrchu zmíněný, kdyby byl správný, byl by pro důkaz Fermatovy věty důležitý. Podobně jevila se při důkaze vyšších recipročních vět ona mnohoznačnost rozkladu celých čísel v prvočinitele jako závada. Tyto a jiné důvody vedly Kummera ke geniálnímu činu: zavedení *ideálních čísel* a Dedekinda k vytvoření *ideálů*, jakožto nových elementů, které přistupují k algebraickým číslům a umožňují teprve vyvinutí theorie algebraických těles úplně obdobné obyčejné nauce o číslech.

2. Je-li α kořenem irreducibilní rovnice s celými ration. koëfficienty $a_0, a_1, \ldots a_n$ stupně n

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n = 0,$$

a tedy celým číslem definujícím těleso $k(\alpha)$ stupně n-tého, nazýváme dle Dedekinda *ideálem* systém celých čísel tělesa $k(\alpha)$ té vlastnosti, že sečítání a odčítání čísel systému a násobení čísel systému libovolnými čísly tělesa $k(\alpha)$ vede opět k číslům systému. Jinými slovy: Jsou-li $\alpha_1, \alpha_2, \ldots$ čísla systému, musí též každé číslo tvaru

$$\lambda_1 \alpha_1 + \lambda_2 \alpha_2 + \ldots,$$

kdež $\lambda_1, \lambda_2, \ldots$ jsou libovolná čísla tělesa $k(\alpha)$, náležeti témuž systému.

Je-li zvláště ideál složen veskrze z čísel tvaru $\lambda\beta$, kde β je určité číslo tělesa $k(\alpha)$ a λ je libovolné číslo tělesa $k(\alpha)$, pak nazývá se zmíněný ideál *hlavním ideálem* a označuje se

$$\mathfrak{b} = (\beta).$$

V každém jiném případě lze najíti v ideálu $\mathfrak{a}$ n čísel té vlastnosti, že všechna ostatní čísla ideálu se z těchto n čísel dají lineární kombinací vyvoditi; jsou-li tato čísla, jež tvoří *basi* ideálu, $\omega_1, \omega_2, \ldots \omega_n$, označujeme ideál

$$\mathfrak{a} = (\omega_1, \omega_2, \ldots \omega_n),$$

a každé jiné číslo ideálu $\mathfrak{a}$ dá se vyjádřiti ve tvaru

$$\omega = \omega_1 a_1 + \omega_2 a_2 + \ldots + \omega_n a_n,$$

kde $a_1, a_2, \ldots a_n$ jsou celá rationální čísla.

Definujeme-li ještě dělitelnost čísel a ideálů vhodným způsobem*), lze odvoditi pro ideály všechny věty obyčejné theorie čísel. Platí pak zvláště věta o jednoznačném rozkladu každého čísla a ideálu v konečný počet ideálů nedělitelných žádným jiným ideálem čili t. zv. *prvoideálů*, platí všechny věty o dělitelnosti, o shodách, jsou-li moduly prvoideály, věta Fermatova a její rozšíření, jinými slovy: celá multiplikativní theorie čísel má svůj pendant v multiplikativní nauce o ideálech.

Zvláště důležité jsou věty o rozkladu prvočísel v prvoideály, z nichž plyne, že rationálné prvočíslo může býti v tělese n-tého stupně součinem nejvýše n prvoideálů**), a jak se tento rozklad dá v daných případech prováděti. Pro náš účel jest kromě právě uvedené věty potřebná jen věta o jednoznačnosti rozkladu v prvoideály, věty o jednotkách a o rozkladu prvočísla l v prvoideály v tělese l-tého kořene jedničky, jež odvodíme přímo, a věta o konečnosti *počtu tříd*.

3. Dva ideály $\mathfrak{a}$ a $\mathfrak{b}$ slují *aequivalentními* v libovolném algebraickém tělese, je-li jich podíl roven *číslu* tělesa.

Z pojmu aequivalence ideálů plyne ihned věta: Dva ideály aequivalentní třetímu jsou aequivalentní navzájem, ve značkách:

Je-li $\mathfrak{a} \sim \mathfrak{b}$, $\mathfrak{c} \sim \mathfrak{b}$, jest $\mathfrak{a} \sim \mathfrak{c}$.

Jest tedy možné děliti všechny ideály tělesa v *třídy* aequivalentních ideálů. Počet tříd ideálů libovolného algebraického tělesa $k(\alpha)$ je konečný a označujeme jej h. Třídu ideálů lze representovati kterýmkoli ideálem v ní obsaženým. Dvě třídy lze komponovati na základě věty: Je-li $\mathfrak{a} \sim \mathfrak{b}$ a $\mathfrak{a}_1 \sim \mathfrak{b}_1$, jest $\mathfrak{a}\mathfrak{a}_1 \sim \mathfrak{b}\mathfrak{b}_1$, při čemž se dva ideály násobí, násobí-li se každé číslo jednoho ideálu každým číslem ideálu druhého. Zvláště platí pro libovolný ideál $\mathfrak{a}$ a hlavní ideál $\mathfrak{h}$

$$\mathfrak{a} \cdot \mathfrak{h} \sim \mathfrak{a}.$$

Z konečnosti počtu tříd plyne ihned, že existuje pro každý ideál $\mathfrak{a}$ nejmenší celé kladné číslo g té vlastnosti, že $\mathfrak{a}^g$ jest hlavním ideálem. Toto číslo g jest dělitelem počtu tříd h, neboť

*) Číslo α je dělitelno ideálem $\mathfrak{a}$, náleží-li α ideálu $\mathfrak{a}$, ideál $\mathfrak{a}$ jest dělitelen ideálem $\mathfrak{b}$, náleží-li všechna čísla ideálu $\mathfrak{a}$, též ideálu $\mathfrak{b}$.

**) To plyne ku př. z Henselových vět Crellův Journ. Bd 113.

jest vždy $\mathfrak{a}^h \sim \mathfrak{h}$. A naopak, je-li pro libovolný ideál $\mathfrak{a}$

$$\mathfrak{a}^g \sim \beta,$$

t. j. $\mathfrak{a}^g$ rovné nějakému celému číslu násobenému jednotkou, pak musí býti g dělitelem počtu tříd h. Při tom jest třeba míti na mysli, že všechny hlavní ideály jsou aequivalentní ideálu (1), jenž sestává ze všech celých čísel tělesa a definuje třídu zvanou *hlavní třídou*, která se při komposici tříd chová jako jednotkový element.

II.

1. V theorii algebraických čísel je velmi ztěžující okolnost, že na rozdíl od nižší nauky o číslech počet jednotek v libovolném tělese algebraickém je všeobecně nekonečně veliký. Při tom nazýváme *jednotkou* celé číslo ε, jehož reciproká hodnota $\frac{1}{\varepsilon}$ jest opět celé číslo. Norma jednotky, t. j. součin $\varepsilon(\alpha)$ $\varepsilon(\alpha') \ldots \varepsilon(\alpha'^{n-1})$, kde α', α'', $\ldots$ $\alpha^{(n-1)}$ jsou ostatní kořeny irreducibilní rovnice, jíž hoví α, a která definuje těleso, jest vždy $= \pm 1$, a naopak. Je proto důležita věta, dokázaná Dirichletem, že se dají všechny jednotky vyvoditi z konečného počtu určitých jednotek pouhým násobením a mocněním. Soustava jednotek takových sluje *fundamentálním systémem*. Důkaz existence tohoto systému vyžaduje věty: *Je-li ϱ celé číslo tělesa $k(\alpha)$ a ϱ', ϱ'', $\ldots$ $\varrho^{(n-1)}$ konjugovaná čísla*) taková, že absolutní hodnoty všech n čísel jsou* 1, *pak jest ϱ kořenem jednotky t. j. $\varrho^k = 1$ pro určité celé positivní k.*

2. Všechny následující úvahy týkají se kruhového tělesa l-tého kořene jednotky. Toto těleso je tedy definováno kořenem rovnice

$$x^l - 1 = 0, \tag{1}$$

kdež l jest všude prvočíslo ≥ 3.

Rovnice (1) není ale irreducibilní v oboru rationálných čísel, neboť $x^l - 1 = (x - 1)(x^{l-1} + \ldots x + 1)$. Hoví tedy

---

*) Je-li $\varrho = \varrho(\alpha)$ číslo tělesa $k(\alpha)$, slují čísla $\varrho(\alpha), \ldots \varrho(\alpha^{(n-1)})$ konjugovanými, při čemž α', α'', $\ldots$ $\alpha^{(n-1)}$ jsou ostatní kořeny irreducibilní rovnice definující α.

l-tý kořen jedničky $\zeta = l^{\frac{2\pi i}{l}}$ rovnici stupně $l - 1$

$$x^{l-1} + x^{l-2} + \ldots x + 1 = 0.$$

Vzhledem k tomu, že též $\zeta^2, \zeta^3, \ldots \zeta^{l-1}$ jsou kořeny této rovnice, platí identicky

$$x^{l-1} + x^{l-2} + \ldots + x + 1 = (x - \zeta)(x - \zeta^2) \ldots (x - \zeta^{l-1}).$$

Klademe-li $x = 1$, obdržíme rozklad prvočísla l

$$l = (1 - \zeta)(1 - \zeta^2) \ldots (1 = \zeta^{l-1}).$$

Činitelé pravé strany se liší od sebe pouze jednotkami; opravdu jest

$$\frac{1 - \zeta^s}{1 - \zeta} = \varepsilon_s, \qquad (s = 1, 2, 3 \ldots l - 1)$$

celé číslo

$$\varepsilon_s = 1 + \zeta + \zeta^2 + \ldots + \zeta^{s-1},$$

ale také

$$\frac{1}{\zeta_s} = \frac{1 - \zeta}{1 - \zeta^s}$$

jest celé číslo, což plyne ihned, určíme-li číslo s' tak, aby $ss' \equiv 1 \pmod{l}$, potom jest $\zeta^{ss'} = \zeta$ a tedy

$$\frac{1}{\varepsilon_s} = 1 + \zeta^s + \zeta^{2s} + \ldots + \zeta^{(s'-1)s}.$$

Jest tedy ε_s jednotka, a pro l máme rozklad

$$l = \varepsilon_2 \varepsilon_3 \ldots \varepsilon_{l-1} (1 - \zeta)^{l-1}.$$

Uvažujeme-li hlavní ideál $\mathfrak{l} = (1 - \zeta) = (\lambda)$, kdež jsme položili $1 - \zeta = \lambda$, bude

$$l = \mathfrak{l}^{l-1}.$$

Z irreducibilnosti rovnice

$$x^{l-1} + x^{l-2} + \ldots + x + 1 = 0,$$

kterou lze ostatně odvoditi přímo z vedeného důkazu *), a z věty, že počet prvoideálných činitelů rationálního prvočísla nesmí pře-

*) Viz Hilbertův Bericht str. 326.

vyšovati stupeň tělesa, plyne ihned, že $\mathfrak{l}$ jest prvoideálem *). Prvoideál $\mathfrak{l}$ jest jediný prvoideál, vzhledem k němuž jakožto modulu budeme celá čísla kruhového tělesa uvažovati. Při tom definujeme celá čísla tělesa $k(\zeta)$ takto: Jsou to čísla tvaru

$$\alpha = a_0 + a_1\zeta + a_2\zeta^2 + \ldots + {}'a_{l-2}\zeta^{l-2},$$

kde $a_0, a_1, \ldots a_{l-2}$ značí celá rationální čísla **). Z toho následuje, že každé celé číslo α lze též vyjádřiti tvarem

$$\alpha = b_0 + b_1\lambda + b_2\lambda^2 + \ldots b_{l-2}\lambda^{l-2},$$

kde $b_0, b_1, \ldots b_{l-2}$ jsou opět celá rationální čísla.

Stačí jen užíti identity

$$\zeta^k = (1 - (1 - \zeta))^k = (1 - \lambda)^k$$

a srovnati dle potencí čísla λ.

3. Při důkaze Fermatovy věty je důležita věta:

Každá jednotka $\varepsilon(\zeta)$ tělesa $k(\zeta)$ dá se vyjádřiti ve tvaru

$$\varepsilon(\zeta) = \zeta^k\eta(\zeta),$$

kdež k jest celé positivní číslo a η *reálná* jednotka tělesa.

Důkaz je jednoduchý. Je-li $\varepsilon(\zeta)$ jednotka, jest též $\varepsilon(\zeta^{-1})$ jednotka a sice imaginárně konjugovaná hodnota k $\varepsilon(\zeta)$; též $\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})}$ jest jednotka, jejíž absolutní hodnota

$$\left|\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})}\right| = \sqrt{\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})} \cdot \frac{\varepsilon(\zeta^{-1})}{\varepsilon(\zeta)}} = 1.$$

Dle věty dříve uvedené je tedy $\pm\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})}$ kořenem jedničky.

V tělese l-tého kořene jedničky nemohou se ale jiné kořeny jedničky vyskýtati než mocniny ζ. Je tedy

$$\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^{-1})} = \pm\zeta^g.$$

---

*) a sice 1. stupně, což ale pro následující úvahy není nutné znáti; je-li $\mathfrak{p}$ prvoideálným činitelem prvočísla (přirozeného) p, a je-li norma $N(\mathfrak{p}) = p^f$, sluje f stupněm prvoideálu $\mathfrak{p}$.

**) Že tato definice se kryje s obyčejnou definicí celých algebraických čísel, (viz též I. 2.) co kořenů algebr rovnic s celistvými ration. koefficienty, lze ukázati snadno na základě fakta, že $1, \zeta, \zeta^2, \ldots \zeta^{l-2}$ tvoří basi tělesa (viz Hilbert Ber. 327).

Toto g lze považovati za sudé, neboť jinak stačí přičísti l, čímž se nic nezmění, a $g + l$ je pak sudé. Klademe-li tedy $g = 2k$ a $\eta(\xi) = \varepsilon(\xi)\xi^{-k}$, bude

$$\frac{\eta(\xi)}{\eta(\xi^{-1})} = \pm 1.$$

Zde může platiti však jen znamení $+$. Uvážíme-li totiž, že $\eta(\xi) - \eta(1)$ je dělitelno $\xi - 1$ a tedy též prvoideálem $\mathfrak{l}$, bylo by

$$\eta(\xi) \equiv \eta(1) \equiv -\eta(1) \pmod{\mathfrak{l}}$$

a tedy $2\eta(1) \equiv 0 \pmod{\mathfrak{l}}$.

Protože ale 2 jest nesoudělno s $\mathfrak{l}$, musilo by býti $\eta(1)$ dělitelno prvoideálem $\mathfrak{l}$ a tedy též *jednotka* $\eta(\xi)$, což je nemožné. Z toho plyne, že $\eta(\xi) = \eta(\xi^{-1})$, a tedy je $\eta(\xi)$ reálná jednotka. Vskutku je pak

$$\varepsilon(\xi) = \xi^k . \eta(\zeta),$$

jak bylo tvrzeno.

4. Největší obtíže působila Kummerovi věta: *Je-li l pravidelné prvočíslo, t. j. takové, že počet tříd kruhového tělesa $k(\xi)$ není dělitelen l, a je-li v tělese $k(\xi)$ jednotka $\varepsilon(\xi)$ shodna s celým rationálním číslem a dle modulu l, pak jest ε l-tou mocninou jiné jednotky tohoto tělesa.* Kummer dokázal tuto větu tím, že ji převedl na otázku dělitelnosti t. zv. druhého činitele počtu tříd číslem l. Tento druhý činitel je podíl dvou determinantů z logarithmů neodvislých a fundamentálních jednotek. Vyšetřování jeho dělitelnosti vyžaduje zvláštních rozvojů pro logarithmy čísel tělesa $k(\zeta)$ a vede posléze na vyšetřování dělitelnosti t. zv. prvého činitele. Tento je nedělitelný prvočíslem l, není-li žádné z $\frac{l-3}{2}$ prvých Bernoulliho čísel dělitelno v čitateli prvočíslem l. Za této podmínky je pak i druhý faktor a tedy celý počet tříd nedělitelný l, a věta zmíněná je správna.

Prvý činitel je celé rationální číslo P'

$$P' = \frac{\Pi \Sigma\, n e^{\frac{2\pi i n' u}{l-1}}}{(2l)^{\frac{l-3}{2}}},$$

kde u probíhá lichá čísla $1, 3, 5, \ldots l-2$, n čísla $1, 2, \ldots l-1$, n' je index čísla n dle l, t. j. pro primitivní kořen r jest $r^{n'} \equiv n \pmod{l}$.

Jest ale možno za pomoci pojmu *tělesa tříd* dokázati tuto větu mnohem snadněji, neodvisle od výrazu pro počet tříd, jehož odvození samo vyžaduje celé řady pomocných vět. Cestu k provedení důkazu naznačil *Hilbert* *).

5. Budiž tedy $\varepsilon(\xi)$ jednotka v pravidelném tělese $k(\xi)$ taková, že

$$\varepsilon(\xi) \equiv a \pmod{l},$$

kde a je celé rationální číslo.

Tvrdím pak, že $\varepsilon(\xi)$ jest l-tou mocninou jiné jednotky v $k(\xi)$.

Kdyby tomu tak nebylo, pak bychom mohli sestrojiti jednotku $\eta(\xi)$, která rovněž není l-tou mocninou jednotky v $k(\xi)$, té vlastnosti, že

$$\eta(\xi) \equiv 1 \pmod{l^l}.$$

Jest totiž třeba jen položiti $\eta(\xi) = \frac{\varepsilon(\xi)}{\varepsilon(\xi^r)}$, kdež r jest primitivní kořen prvočísla l, takže $1, r, r^2, \ldots r^{l-2}$ vyčerpává úplný systém zbytků dle l.

$\eta(\xi)$ jest potom jednotka, neboť podíl dvou jednotek jest opět jednotka. Podle předpokladu jest

$$\varepsilon(\xi) = a + l\alpha(\xi),$$

kde $\alpha(\xi)$ jest nějaké celé číslo v $k(\xi)$ a tedy celá rationální funkce ξ s celistvými koeff. Tato rovnice se nemění, píšeme-li v ní místo ξ jiný kořen ξ^r. (To plyne z irreducibilnosti rovnice pro ξ.)

Jest tedy též

$$\varepsilon(\xi^r) = a + l\alpha(\xi^r)$$

a odečtením obou rovnic

$$\varepsilon(\xi) = \varepsilon(\xi^r) + l\,(\alpha(\xi) - \alpha(\xi^r)).$$

Protože jest ale $\alpha(\xi) - \alpha(\xi^r)$ dělitelno číslem $\xi - \xi^r$ a tedy též $1 - \xi = \lambda$, jež se od $\xi - \xi^r$ liší pouze jednotkou, jest

*) Hilbert Bericht str. 440.

opravdu

$$\eta(\zeta) = \frac{\varepsilon(\zeta)}{\varepsilon(\zeta^r)} \equiv 1 \pmod{\mathfrak{l}'},$$

uvážíme-li, že $l = \mathfrak{l}^{l-1}$ a $(1 - \zeta) = (\lambda) = \mathfrak{l}$.

Zbývá jen ukázati, že $\eta(\zeta)$ nemůže býti l-tou mocninou jednotky. Kdyby ale bylo

$\frac{\varepsilon(\zeta)}{\varepsilon(\zeta^r)} = (e(\zeta))^l$, kde $e(\zeta)$ značí opět jednotku v $k(\zeta)$, bylo by též, zaměníme-li ζ kořenem ζ^{r^i},

$$\frac{\varepsilon(\zeta^{r^i})}{\varepsilon(\zeta^{r^{i+1}})} = (e(\zeta^{r^i}))^l \qquad (i = 0,\ 1,\ 2,\ \ldots\ l-2)$$

a tedy též

$$\left(\frac{\varepsilon(\zeta^{r^i})}{\varepsilon(\zeta^{r^{i+1}})}\right)^{i+1} = (e(\zeta^{r^i})^{i+1})^l.$$

Znásobíme-li všechny tyto rovnice počtem $l - 1$, dostaneme na pravé straně opět l-tou mocninu jednotky H^l, kdežto na levo jest v čitateli po zkrácení $\varepsilon(\zeta)\,\varepsilon(\zeta^r)\ldots\varepsilon(\zeta^{r^{l-2}}) = 1$ jakožto norma jednotky. Jest tedy

$$\frac{1}{\varepsilon(\zeta^{r^{l-1}})^{l-1}} = H^l,$$

a vzhledem k $r^{l-1} \equiv 1 \pmod{l}$ konečně

$$\varepsilon(\zeta) = (\varepsilon(\zeta) \cdot H(\zeta))^l = H_1{}^l,$$

proti předpokladu.

Jest tedy vskutku $\eta(\zeta) \equiv 1 \pmod{\mathfrak{l}'}$, aniž by bylo η l-tou mocninou jednotky. Následkem toho bude $\sqrt[l]{\eta(\zeta)} = \mu$ obecně číslo k tělesu $k(\zeta)$ nepatřící, bude hověti rovnici

$$x^l - \eta(\zeta) = 0, \qquad (1),$$

která má své koeff. v tělese $k(\zeta)$, jest v něm irreducibilní a definuje těleso K (Kummerovo) stupně l nad kruhovým tělesem $k(\zeta)$. Ostatní kořeny rovnice (1) jsou $\zeta\mu$, $\zeta^2\mu$, $\ldots$ $\zeta^{l-1}\mu$. Toto těleso jest tudíž relativně cyklické, neboť grupa substitucí jest tu 1, ζ, ζ^2, $\ldots$, ζ^{l-1} cyklická. Jest ale možno velmi snadno ukázati, že jest toto těleso *nerozvětvené**) t. j. že jeho rel. diskri-

*) »unverzweigt«.

minant jest 1. Vskutku jest $\frac{\eta(\xi) - 1}{\lambda^l}$ = celé číslo v $k(\xi)$ a tedy číslo $\frac{1-\mu}{\lambda}$ celé číslo v tělese K, neboť hoví rovnici $\frac{(\lambda x - 1)^l + \eta}{\lambda^l} = 0$, jejíž koeff. jsou celá čísla v $k(\xi)$, protože jest $l = (\lambda^{l-1})$. Dle toho bude rel. diskriminant *) tohoto čísla $\frac{1-\mu}{\lambda}$:

$$1 \frac{\mu^{l(l-1)}}{\lambda^{l(l-1)}} \cdot \left((1-\xi)^2 (1-\xi^2)^2 \ldots (\xi^{l-2} - \xi^{l-1})^2\right) = \eta^{l-1} E(\xi),$$

vzhledem k tomu, že $\xi^r - \xi^r = \varepsilon_{rs}(\xi)\,(1-\xi) = \varepsilon_{rs}(\xi) \cdot \lambda$, kde $\varepsilon_{rs}(\xi)$, $E(\xi)$ jsou jednotky. Je tedy diskriminant čísla $\frac{1-\mu}{\lambda}$ jednotka v $k(\xi)$, a protože rel. diskriminant tělesa K musí býti dělitelem diskriminantů všech čísel, jest roven 1, jak bylo tvrzeno.

Jest tedy vskutku těleso K nerozvětvené a rel. cyklické vzhledem ke $k(\xi)$, a lze použíti pro ně vlastnosti *tělesa tříd*, jež zní **): ***Existují ideály základního tělesa, které jsou v tělese tříd hlavními ideály.*** Z toho následuje okamžitě nemožnost učiněného předpokladu takto: Zvolme ideál $\mathfrak{a}$ v tělese $k(\xi)$, který zde není hlavním ideálem; $\mathfrak{a}$ jest též ideálem v K a sice dle uvedené vlastnosti hlavním, tedy $\mathfrak{a} = (A)$, kde A jest číslo v K závislé na $\mu = \sqrt[l]{\eta}$. Nahradíme-li v $A(\mu)$ μ konjugovanými kořeny $\zeta\mu$, $\zeta^2\mu$, $\ldots$ $\zeta^{l-1}\mu$ a znásobíme, dostaneme relativní normu čísla A vzhledem ku $k(\xi)$

$$n(A) = \alpha, \text{ která jest číslo v } k(\xi).$$

Z toho plyne, že relativní norma ideálu $\mathfrak{a}$ obsaženého v $k(\xi)$ bude

$$n(\mathfrak{a}) = \mathfrak{a}^l = n[(A)] = (\alpha); \text{ t. j. } \mathfrak{a}^l \text{ jest hlavní ideál v } k(\xi).$$

*) Rel. diskriminant čísla $A(\mu)$ tělesa K jest číslo v $k(\zeta)$:

$$(A(\mu) - A(\mu\zeta))^2 (A(\mu) - A(\mu\zeta^2))^2 \ldots (A(\mu\zeta) - A(\mu\zeta^2))^2$$
$$\ldots (A(\mu\zeta^{l-2}) - A(\mu\zeta^{l-1}))^2.$$

**) Viz *Hilbert*: Über die Theorie der relativ Abelschen Zahlkörper *Acta Math.* Bd. 26, *Furtwängler*: Allgemeiner Existenzbeweis für den Klassenkörper eines beliebigen algebr. Körpers *Math. Annalen 1907.*

Musilo by tedy býti l dělitelem počtu tříd, což je proti předpokladu. Jest tedy vskutku $\varepsilon(\zeta)$ l-tou mocninou jednotky.

III.

Můžeme nyní přistoupiti k důkazu *věty Fermatovy* pro pravidelná prvočísla a dokážeme tedy větu: Značí-li l pravidelné prvočíslo a u, v, w celá čísla tělesa $k(\zeta) = k\left(e^{\frac{2\pi i}{l}}\right)$, pak jest rovnice

$$u^l + v^l + w^l = 0$$

nemožná, není-li aspoň jedno z čísel u, v, w rovno nulle.

Jest především patrno, že lze se při důkaze omeziti vůbec na prvočísla, neboť platí-li věta pro libovolná prvočísla, platí pak také pro čísla z nich složená. Dále jest dovoleno předpokládati čísla u, v, w zbavená číselných činitelů. Jest pak ještě možno, že kterákoli dvě a tedy všechna tři mají společný ideálný faktor*)

Při vedení důkazu jest třeba rozeznávati dva případy: Předně, není-li žádné z čísel u, v, w dělitelno prvoideálem $\mathfrak{l} = (1 - \zeta) = (\lambda)$, a za druhé, je-li aspoň jedno z nich dělitelno $\mathfrak{l}$.

1. Rovnici

$$u^l + v^l + w^l = 0, \tag{1}$$

kde žádné z čísel u, v, w není dělitelno $\mathfrak{l}$, pišme ve tvaru

$$(u + v)(u + \zeta v) \ldots (u + \zeta^{l-1} v) = -w^l. \tag{2}$$

Čísla u, v, w můžeme předpokládati vždy shodná s celými rationálnými čísly dle modulu $\mathfrak{l}^2$, t. j. ve tvaru

$$u = a + (1 - \zeta)^2 \alpha(\zeta),\ v = b + (1 - \zeta)^2 \beta(\zeta),\ w = c + (1 - \zeta)^2 \gamma(\zeta),$$

kde a, b, c jsou celá rat. čísla nedělitelná l a α, β, γ celá čísla tělesa $k(\zeta)$. Neboť rovnice bude též splněna, násobíme-li každé z čísel u, v, w mocninami kořene ζ. Je-li pak ku př.

$$u = a + (1 - \zeta) a_1 + (1 - \zeta)^2 a_2 + \ldots,$$

*) Na tuto možnost, která komplikuje poněkud jeho důkaz, Kummer zapomněl. V tomto směru doplnil jeho geniální důkaz *Hilbert*, Bericht, jehož se též s různými změnami přidržím.

kde $a, a_1, a_2, \ldots$ jsou celá čísla rationální, a nedělitelná l, bude

$$\xi^k u = a + (1 - \xi)\{a_1 - ka\} + (1 - \xi)^2 A + \ldots,$$

uvážíme-li totiž, že

$$\xi^k = (1 - (1 - \xi))^k = 1 - k(1 - \xi) + \frac{k(k-1)}{2}(1-\xi)^2 - \ldots$$

Zvolíme-li tedy k tak, aby $a_1 - ka \equiv 0 \pmod{l}$, což je vždy možno, bude $\xi^k u = u' = a + (1 - \xi)^2 \alpha$, a podobně v', w'.

Předpokládejme u, v, w v této formě.

Kterékoli dva z faktorů levé strany rovnice (2) mohou míti pouze téhož společného dělitele jako u, v. Společný dělitel čísel $u + \xi^r v$ a $u + \xi^s v$ ku př. musil by býti též společným dělitelem čísel $\xi^r(u + \xi^s v) - \xi^s(u + \xi^r v) = (\xi^r - \xi^s)u$ a

$$(u + \xi^r v) - (u + \xi^s v) = (\xi^r - \xi^s)v.$$

Tato dvě čísla mají ale pouze dělitele $1 - \xi$, který by tedy musil býti obsažen též ve w, což je proti supposici, anebo největšího dělitele společného číslům u, v, jejž chceme zváti $\mathfrak{a}$. Z jednoznačnosti rozkladu v prvoideály následuje ihned, že každý z činitelů $u + \xi^i v$ musí vedle ideálu $\mathfrak{a}$ společného u, v a tedy všem činitelům obsahovati l-tou potenci ideálu. Bude tedy obecně

$$u + \xi^i v = \mathfrak{n}_i^l \cdot \mathfrak{a}, \quad (i = 0, 1, 2, \ldots l - 1).$$

kde $\mathfrak{n}_i$ jsou určité ideály v $k(\xi)$.

Dělme nyní všechny rovnice první rovnicí (pro $i = 0$) a položme k vůli krátkosti

$$\frac{u}{u+v} = \varrho, \quad \frac{v}{u+v} = \sigma,$$

pak obdržíme systém rovnic

$$\left.\begin{aligned} &\varrho + \sigma = 1 \\ &\varrho + \xi\sigma = \left(\frac{\mathfrak{n}_1}{\mathfrak{n}}\right)^l \\ &\ldots\ldots\ldots \\ &\varrho + \xi^{l-1}\sigma = \left(\frac{\mathfrak{n}_{l-1}}{\mathfrak{n}}\right)^l \end{aligned}\right\} \quad (3)$$

O číslech ϱ, σ platí pak, že jsou to čísla tělesa $k(\zeta)$, jichž čítatelé i jmenovatel jsou shodny s celými rationálními čísly (mod. l^2). Neboť u a v jsou v této formě zvolena, kdežto pro $u + v$ to plyne z té okolnosti, že $u + v$ nemůže býti dělitelno l (jinak by bylo též w dělitelno l). Z rovnic (3) plyne důsledek pro celý důkaz nejdůležitější. Vzhledem k tomu, že levé strany jsou *čísla* tělesa $k(\zeta)$, jsou podle definice aequivalence l-té potence ideálů $\mathfrak{n}$, $\mathfrak{n}_1$, . . . $\mathfrak{n}_{l-1}$ aequivalentní

$$\mathfrak{n}^l \sim \mathfrak{n}_1^l \sim \ldots \sim \mathfrak{n}_{l-1}^l,$$

ale protože jest, označíme-li počet tříd ideálů h,

$$\mathfrak{n}^h \sim \mathfrak{n}_l^h \sim \ldots \sim \mathfrak{n}_{l-1}^h,$$

neboť h-té mocniny všech ideálů přísluší hlavní třídě, musí býti též pro největšího spol. dělitele čísel h a l, t. j. 1,

$$\mathfrak{u} \sim \mathfrak{n}_1 \sim \ldots \mathfrak{n}_{l-1},$$

t. j. podíly $\frac{\mathfrak{n}_1}{\mathfrak{n}}$, $\frac{\mathfrak{n}_2}{\mathfrak{n}}$, . . . $\frac{\mathfrak{n}_{l-1}}{\mathfrak{n}}$ jsou *čísla* v $k(\zeta)$ násobená jednotkami, jež lze dle II. 3. vyjádřiti ve tvaru $\eta(\zeta)\zeta^k$, kde $\eta(\zeta)$ jest reálná jednotka v $k(\zeta)$. Bude tedy platný tento systém rovnic

$$\varrho + \sigma = 1$$
$$\varrho + \zeta^i\sigma = \zeta^{ki}\eta_i\beta_i^l, \quad (i = 1, 2, \ldots l-1)$$

při čemž jsou k_i celá positivní čísla, η_i reálné jednotky, β_i čísla v $k(\zeta)$ tvaru $\frac{1}{c}\gamma_i(\zeta)$, kde $\gamma_i(\zeta)$ je celé číslo v $k(\zeta)$ nedělitelné l, kdežto c je celé rationální číslo rovněž nedělitelné l a tedy i l. To plyne z nedělitelnosti čítatele a jmenovatele levé strany. Určíme-li tedy c' shodou $cc' \equiv 1 \pmod{l}$, bude

$$\beta_i = \frac{1}{c}\gamma_i(\zeta) = \frac{1}{c}(C_i + C'_i\lambda + \ldots) \equiv c'C_i \pmod{l}$$

a tedy vzhledem k $l = l^{l-1}$

$$\beta_i^l = c'^l C_i^l + \lambda^l \Gamma_i \text{ čili } \beta_i^l \equiv a_i \pmod{l^l},$$

kde a_i jest celé rationální číslo. Máme tedy systém shod

$$(4)\quad \varrho + \zeta^i\sigma = \zeta^{ki}\eta_i a_i \pmod{l^l},\ i = 1, 2, \ldots l-1).$$

Ukážeme, že vede tato soustava k odporu.

Zaměňme ve shodách (4) ζ^{-1} za ζ, což jest dovoleno, protože můžeme shody vždy zaměniti rovnicemi a v těch je dovoleno klásti za ζ jakýkoli jiný kořen irreducibilní rovnice pro ζ. Z čísel ϱ, σ vzniknou touto substitucí ϱ', σ'. Podle definice jest $\varrho = \frac{u}{u+v}$, kde $u \equiv a \pmod{l^2}$, $u + v \equiv a + b \equiv A \pmod{l^2}$; určíme-li tedy celé číslo rationální m shodou $mA \equiv a \pmod{l}$, bude $\varrho \equiv m \pmod{l^2}$ a podobně $\sigma \equiv n \pmod{l^2}$ a tedy též

$$\varrho' \equiv m \pmod{l^2}, \quad \sigma' \equiv n \pmod{l^2}.$$

Vyloučíme-li ze shod

$$\varrho + \zeta^i\sigma \equiv \xi^{ki}\eta_i a_i, \quad \varrho' + \zeta^{-i}\sigma' \equiv \zeta^{-ki}\eta_i a_i \pmod{l^l}$$

čísla η_i, a_i, dostaneme

$$(5)\quad \varrho + \zeta^i\sigma \equiv \zeta^{2ki}\varrho' + \zeta^{2ki-i}\sigma' \pmod{l^l} \ldots (i = 1, 2, \ldots l-1)$$

a tedy též, užijeme-li relace

$$(\zeta^k = (1-(1-\zeta))^k \equiv 1 - \lambda k \pmod{l^2},$$
$$2k_i(m+n) \equiv 2ni \pmod{l}.$$

Tato shoda platí též dle modulu l, neboť obě strany jsou obyčejná celá čísla, a uvážíme-li, že jest $\varrho + \sigma = 1$ a tudíž také $m + n \equiv 1 \pmod{l}$, bude

$$k_i \equiv ni \pmod{l}, \quad (i = 1, 2, \ldots l-1)$$

a shody (5) poskytují pak pro $i = 1, l-1$, připojíme-li k nim shody vznikající z rovnic

$$\varrho + \sigma = 1, \quad \varrho' + \sigma' = 1,$$

tuto soustavu shod:

$$\left.\begin{array}{c} \varrho + \sigma \equiv \varrho' + \sigma' \\ \zeta^{-n}(\varrho + \zeta\sigma) \equiv \zeta^n(\varrho' + \zeta^{-1}\sigma') \\ \zeta^n(\varrho + \zeta^{-1}\sigma) \equiv \zeta^{-n}(\varrho' + \zeta\sigma') \end{array}\right\} \pmod{l^l}.$$

Znásobením posledních shod a s použitím shod

$$\varrho + \sigma \equiv \varrho' + \sigma' \equiv 1 \pmod{l^l}$$

dostaneme

$$\varrho\sigma \equiv \varrho'\sigma' \pmod{l^{l-2}}$$

a tedy též

$$\varrho - \sigma \equiv \varrho' - \sigma' \pmod{\mathfrak{l}^{l-2}}$$

čili

$$\varrho \equiv \varrho', \quad \sigma \equiv \sigma' \pmod{\mathfrak{l}^{l-2}}.$$

Dosadíme-li za ϱ', σ' shodné jim hodnoty ϱ, σ do shod (5) pro $i = 1, 2$, obdržíme

$$\left.\begin{aligned}(\xi^n - \zeta^{-n})\,\varrho + (\zeta^{n-1} - \zeta^{-n+1})\,\sigma &\equiv 0\\ (\zeta^{2n} - \zeta^{-2n})\,\varrho + (\zeta^{2(n-1)} - \zeta^{-2(n-1)})\,\sigma &\equiv 0\end{aligned}\right\} \pmod{\mathfrak{l}^{l-2}}.$$

Vyloučením ϱ, σ dostaneme jako nutný důsledek shodu

$$(1 - \zeta)(1 - \zeta^{2n-1})(1 - \zeta^{2(n-1)}) \equiv 0 \pmod{\mathfrak{l}^{l-2}}.$$

Vyjímaje případy $l = 3$ a $l = 5$ jest však tato shoda nemožná. Pro $l \geqq 7$ obsahuje totiž levá strana činitele $\lambda = 1 - \zeta$ pouze třikráte, kdežto shoda vyžaduje, aby byl na levo obsažen aspoň $l-2$krát. Mohla by tedy shoda platiti jen, je-li některý z faktorů roven nulle. To je ale nemožné. Bylo by totiž pak buď $n \equiv 1$ nebo $2n \equiv 1 \pmod{l}$. V prvém případě bylo by vzhledem k $m + n \equiv 1 \pmod{\mathfrak{l}}$ též $m \equiv 0 \pmod{\mathfrak{l}}$ a tedy $u \equiv 0 \pmod{\mathfrak{l}}$ proti supposici. V druhém případě bylo by $2\sigma \equiv 2n \equiv 1 \pmod{\mathfrak{l}}$ a tedy též $2v \equiv u + v$, čili $u \equiv v$. Vzhledem k symmetrii rovnice (1) můžeme však též souditi, že by bylo $u \equiv w$ a tedy $u^l + v^l + w^l \equiv 3u^l \equiv 0 \pmod{\mathfrak{l}}$. Ale to vyžaduje opět, vyloučíme-li případ $l = 3$, aby $u \equiv 0 \pmod{\mathfrak{l}}$.

Kromě $l = 3$ a $l = 5$ jest tudíž rovnice (1) neřešitelná v celých od nully různých číslech tělesa $k(\zeta)$ nedělitelných prvoideálem $\mathfrak{l}$.

Že ale pro $l = 3$ jest rovnice (1) nemožná, plyne z této úvahy: Každé celé číslo tělesa $k\left(e^{\frac{2\pi i}{8}}\right)$ nedělitelné $\mathfrak{l}$ dá se vyjádřiti tvarem $u = \pm 1 \pm (1-\zeta) \pm (1-\zeta)^2$ a tedy $u \equiv \pm 1 \pmod{\mathfrak{l}}$ $u^3 \equiv \pm 1 \pmod{\mathfrak{l}^3}$ $u^3 + v^3 + w^3 \equiv \pm 1$ nebo $\pm 3 \pmod{\mathfrak{l}^3}$. Protože ale $3 = \mathfrak{l}^2$, jest rovnice $u^3 + v^3 + w^3 = 0$, jež by vyžadovala shodu $u^3 + v^3 + w^3 \equiv 0 (\mathfrak{l}^3)$, nemožná. Podobně jest pro $l = 5$ $u, v, w \equiv \pm 1, \pm 2 \pmod{\mathfrak{l}}$ a tedy $u^5 + v^5 + w^5 \equiv \pm 1, \pm 3, \pm 30, \pm 32, \pm 34, \pm 63, \pm 65, \pm 96 \pmod{\mathfrak{l}^5}$. Zde jest jedině 30 a 65 dělitelno 5, ale jen čtvrtou mocninou $\mathfrak{l}$. Je tedy shoda $u^5 + v^5 + w^5 \equiv 0 \pmod{\mathfrak{l}^5}$ a tedy i rovnice $u^5 + v^5 + w^5 = 0$ nemožná.

2. Budiž za druhé některé z čísel u, v, w dělitelné $\mathfrak{l}$, a sice buď w dělitelno $\mathfrak{l}^m$, takže chceme dokázati neřešitelnost v celých číslech tělesa $k(\zeta)$ rovnice

$$u^l + v^l + (1 - \zeta)^{ml} w^l = 0,$$

anebo obecněji rovnice

$$u^l + v^l = E(\zeta)(1 - \zeta)^{ml} w^l, \qquad (1)$$

kde $E(\zeta)$ je jednotka tělesa $k(\zeta)$, čísla u, v, w nemají společného *číselného* dělitele, a jsou s prvočíslem l nesoudělná. Mimo to chceme je jako dříve předpokládati násobená vhodnými jednotkami ζ^r tak, aby byla shodná s celými rationálními čísly (mod. $\mathfrak{l}^2$) *), tedy ve tvaru

$$u \equiv a, \quad v \equiv b, \quad w \equiv c \pmod{\mathfrak{l}^2}.$$

Rozložíme-li opět levou stranu rovnice (1) v součin činitelů

$$(u + v)(u + \zeta v)(u + \zeta^2 v) \ldots (u + \zeta^{l-1} v) = E(\zeta) \lambda^{ml} w^l,$$

a užijeme opět shody $\zeta^i \equiv 1 - i\lambda \pmod{\mathfrak{l}^2}$, bude

$$u + \zeta^i v \equiv a + b - ib\lambda \pmod{\mathfrak{l}^2}, \quad (i = 0, 1, 2, \ldots l - 1).$$

Protože ale pravá strana rovnice (1) je dělitelna λ, musí též na levo aspoň jeden faktor $u + \zeta^i v \equiv 0 \pmod{\mathfrak{l}}$. To vyžaduje $a + b \equiv 0 \pmod{\mathfrak{l}^2}$. Potom jsou ale všichni činitelé $u + \zeta^i v$ dělitelni $\mathfrak{l}$ a sice pro $i = 1, 2, \ldots l - 1$ pouze jedenkráte. Pro $i = 0$ musí tedy $u + v$ býti dělitelno mocninou $\mathfrak{l}^{ml-l+1}$, a tak máme soustavu rovnic:

$$(2) \begin{cases} u + v = \lambda^{(m-1)l+1} \mathfrak{m}\mathfrak{a} \\ u + \zeta^i v = \lambda \mathfrak{m}_i \mathfrak{a}, \qquad (i = 1, 2, \ldots l - 1), \end{cases}$$

kde $\mathfrak{m}$, $\mathfrak{m}_1, \ldots \mathfrak{m}_{l-1}$, jsou vespolek nesoudělná a nedělitelná též prvoideálem $\mathfrak{l}$. Dosadíme-li do rovnice (1), máme

$$\mathfrak{a}^l \mathfrak{m}\mathfrak{m}_1 \ldots \mathfrak{m}_{l-1} = E(\zeta) \cdot w^l,$$

z čehož plyne ihned, že $\mathfrak{m}$, $\mathfrak{m}_1, \ldots \mathfrak{m}_{l-1}$ musí býti pro sebe l-tými mocninami ideálů $\mathfrak{n}$, $\mathfrak{n}_1, \ldots \mathfrak{n}_{l-1}$.

---

*) Čísla takto upravená nazývá Hilbert semiprimarními na rozdíl od primarních, která hoví ještě podmínce $\alpha(\zeta)\,\alpha(\zeta^{-1}) \equiv b \pmod{\mathfrak{l}^{l-1}}$, kde b je opět celé rat. číslo.

Položíme-li podobně jako dříve,

$$\frac{\lambda^{(m-1)l+1}u}{u+v}=\varrho,\qquad \frac{\lambda^{(m-1)l+1}v}{u+v}=\sigma,$$

budeme míti rovnice

$$\varrho+\sigma=\lambda^{(m-1)l+1}$$

$$\varrho+\zeta^i v=\lambda\left(\frac{\mathfrak{n}_i}{\mathfrak{n}}\right)^l \quad (i=1,2,\ldots l-1).$$

Z nich soudíme jako dříve, že $\left(\frac{\mathfrak{n}_i}{\mathfrak{n}}\right)^l$ musí býti ideály hlavní třídy, a tedy $i\frac{\mathfrak{n}_i}{\mathfrak{n}}$, vzhledem k tomu, že l jest pravidelné prvočíslo. Z rovnic takto vznikajících potřebujeme pouze dvě, a následkem toho jest celý následující důkaz platný též pro $l=3$. Rovnice ty znějí:

$$\varrho+\sigma=\lambda^{(m-1)l+1}$$

$$\varrho+\zeta^i\sigma=\lambda e_i\frac{t_i^l}{w_1^l},$$

$$\varrho+\zeta^k\sigma=\lambda e_k\frac{t_k}{w_1^l};$$

zde jest i od k různé a v případě $l=3$ jest $i=1$, $k=2$; t_i, t_k, w_1 jsou celá *čísla* v $k(\zeta)$ nedělitelná patrně l, e_i, e_k jsou jednotky. Vyloučením ϱ obdržíme nejprve

$$(1-\zeta^i)\,\sigma=\frac{\lambda^{(m-1)l+1}w_1^l-\lambda e_i t_i^l}{w_1^l},$$

$$(1-\zeta^k)\,\sigma=\frac{\lambda^{(m-1)l+1}w_1^l-\lambda e_k t_k^l}{w_1^l}.$$

Násobíme-li prvou rovnici $1-\zeta^k$ a druhou $1-\zeta^i$ a odečteme, dostaneme po krátké redukci

$$t_i^l-\frac{1-\zeta^i}{1-\zeta^k}\frac{e_k}{e_i}t_k^l=\lambda^{(m-1)l}w_1^l\cdot\frac{\zeta^i-\zeta^k}{1-\zeta^k},$$

a klademe-li k vůli zkrácení

$$\frac{1-\zeta^i}{1-\zeta^k}\frac{e_k}{e_i}=-e(\zeta),\qquad \frac{\zeta^i-\zeta^k}{1-\zeta^k}=E_1(\zeta),$$

kde $e(\zeta)$ a $E_1(\zeta)$ znamenají opět jednotky v $k(\zeta)$, bude posléze

$$t_i^l+e(\zeta)\,t_k^l=E_1(\zeta)\,\lambda^{(m-1)l}w_1^l.$$

Uvažme nyní, že t_i^l, t_k^l, jakožto l-té mocniny celých čísel $vk(\zeta)$, jsou (mod. l) shodny s celými rationálními čísly

$$t_i^l \equiv m \text{ (mod. } l) \quad t_k^l \equiv n \text{ (mod. } l).$$

To následuje pro každé číslo $\alpha = a_0 + a_1\zeta + \ldots a_{l-2}\zeta^{l-2}$ z té okolnosti, že až na l-té potence jsou koefficienty všech členů mocniny dělitelny prvočíslem l a tedy

$$\alpha(\zeta)^l \equiv a_0^l + a_1^l + \ldots + a_{l-2}^l \equiv a_0 + a_1 + \ldots a_{l-2} \text{ (mod. } l).$$

Jest tudíž

$$m + e(\zeta)\, n \equiv 0 \text{ (mod. } l),$$

neboť pro $m > 1$ jest $\lambda^{(m-1)\,l}$ dělitelno $l = \mathfrak{l}^{l-1}$.

Stanovme ještě celé rationálné číslo c shodou

$$nc \equiv -m \text{ (mod. } l),$$

což je vzhledem k nedělitelnosti čísel n, m prvočíslem l vždy možno; pak jest

$$e(\zeta) = c \text{ (mod. } l)$$

a tedy dle věty uvedené v II. 4. $e(\zeta)$ rovno l-té mocnině jednotky $e(\zeta) = \varepsilon(\zeta)^l$. Klademe-li konečně $\varepsilon(\zeta)\, t_k = v_1$, $t_i = u_1$, máme

$$u_1^l + v_1^l = E_1(\zeta)\, w_1^l\, \lambda^{(m-1)\,l}. \tag{4}$$

Kdyby tedy byla rovnice (1) možná v celých od nully různých číslech tělesa $k(\zeta)$, byla by možná též rovnice (4) téhož tvaru, v níž však m jest o 1 zmenšeno. Z této rovnice bychom mohli odvoditi novou, v níž na pravo stojí $\lambda^{(m-2)\,l}$, atd.; konečně bychom dospěli k rovnici

$$u_{m-1}^l + v_{m-1}^l = E_{m-1}(\zeta)\, w_{m-1}^l\, \lambda^l.$$

Tato jest ale nemožna, neboť na pravo vyskytuje se činitel λ pouze l-kráte, kdežto na levo obsahuje jej každý faktor $(i = 1, \ldots l-1)$ $u_{m-1} + \zeta^i v_{m-1}$ jednou, faktor $u_{m-1} + v_{m-1}$ ale nejméně dvakráte, levá strana tedy nejméně $(l+1)$ kráte.

Tím je dokázána Fermatova věta pro pravidelná prvočísla l. Zbývá ještě otázka, kdy jest prvočíslo l pravidelné. Pro praktické potřeby jest nutno užíti zde výrazu pro počet tříd. Kummer nalezl pro prvé sto čísel pouze prvočísla $l = 37, 59, 67$, pro něž je počet tříd dělitelný l. Pro ně tedy předcházející důkaz

neplatí. Že ale přes to i pro tato prvočísla Fermatova věta je správna, ukázal Kummer ve své druhé práci, které chci věnovati samostatné pojednání. Jdeme-li nad $l \geqq 101$, hromadí se prvočísla, pro něž je počet tříd dělitelný l, a sice jsou to ku př. prvočísla $l = 101, 103, 131, 149, 157$; z nich je dokonce počet tříd pro $l = 157$ dělitelný 157^2, neboť jest prvý činitel počtu tříd pro $l = 157$

$$P' = 5 \cdot 13 \cdot 3148601 \cdot 13 \cdot 157 \cdot 157 \cdot 857487631729.$$

Je-li pro tato prvočísla Fermatova věta správna, není dosud rozhodnuto*). Výpočty jsou tu velmi obtížné a vyžadují zvláštních obratů počtářských.

Skládání konečných současných rotací pevného tělesa.

Podává Dr. **Ladislav Stjepanek**, prof. reálného gymnasia a soukr. docent na universitě v Záhřebě.

(Dokončení.)

2. Rotace téhož druhu.

Budeme nyní hledati podmínku, pro niž differenciální rovnice (16) dají pohyb šroubový kol pevné osy. V tom případě musí rovnice (17) býti rovnicí roviny, jež v prostoru rovnoběžně k sobě postupuje, t. j. levá strana této rovnice musí býti dělitelna jistou funkcí t — řekněme $\varphi'_0(t)$ — tak že po dělení touto funkcí koefficienty u $\frac{dx}{dt}$, $\frac{dy}{dt}$ a $\frac{dz}{dt}$ zůstávají nezávislé na t.

Této podmínce se vyhoví, když

$$\varphi_r(t) = k_r \varphi_0(t)$$

pro $r = 1, 2, \ldots h$, kde $k_1, k_2, \ldots k_h$ jsou konstanty na čase nezávislé.

Rovnice (17) zní nyní:

---

*) *Kummer*, Monatsberichte der königl. pr. Akad. 1-74.