Voortgezette getaltheorie (Klassenlichamentheorie) (Stieltjescollege)

H. W. Lenstra (Mathematisch Instituut Leiden, kamer 227,
tel. 071–527 7127, e-mail hwl@wi.leidenuniv.nl).

Voorjaar 1999, vrijdag 10–13 u.

Op 22 januari, 5 februari, 26 februari, 12 maart, 26 maart, 1 april en 7 april zal het college in Amsterdam worden gegeven, in gebouw Euclides, Plantage Muidergracht 24, zaal P017 (1 april: zaal P015A; 7 april: zaal P015B), en op 29 januari, 12 februari, 19 februari, 5 maart, 19 maart, 23 april en 7 mei in Leiden, in het Mathematisch Instituut, Niels Bohrweg 1, zaal WI 401. Op andere dagen wordt het college niet gegeven.

Het college is bestemd voor doctoraalstudenten wiskunde. Voorkennis: *Kernvak getaltheorie* (Stevenhagen) in Amsterdam of *Algebraïsche getaltheorie* (de Smit) in Leiden.

Toetsing: elke week wordt huiswerk opgegeven, dat de week erna bij Richard Groenewegen moet worden ingeleverd. Er is geen tentamen.

Klassenlichamentheorie vormt een onderdeel van de geavanceerde algebraïsche getaltheorie. De voornaamste stelling van de klassenlichamentheorie geeft een classificatie van de abelse uitbreidingen van een gegeven algebraïsch getallenlichaam; onder een abelse uitbreiding moet men hierbij een Galoisuitbreiding met een abelse Galoisgroep verstaan. Bovendien krijgt men een beschrijving van het splitsingsgedrag van priemen in dergelijke uitbreidingen. Een belangrijk onderdeel van de klassenlichamentheorie wordt gevormd door de reciprociteitswet van Artin, die een verregaande veralgemening van de kwadratische reciprociteitswet vormt.

Literatuur over klassenlichamentheorie. De belangrijkste stellingen uit de klassenlichamentheorie werden in de periode 1920–1927 bewezen door de Japanse wiskundige Teiji Takagi (1875–1960; *Collected papers*, Iwanami Shoten, Tokyo, 1973; tweede uitgebreide druk, Springer-Verlag, Tokyo, 1990) en door de Duitse wiskundige Emil Artin (1898–1962; *Collected papers*, Addison-Wesley, 1965; herdrukt bij Springer-Verlag, New York, 1982). Voor de geschiedenis van de klassenlichamentheorie zie men Chapter XI door H. Hasse in het beneden genoemde boek van Cassels en Fröhlich. De bewijzen van Takagi en Artin maakten onder andere van analytische technieken gebruik, in het bijzonder van Dirichlet L-functies; zie H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, I, Ia, II, *Jber. dt. Mat. Verein.* **35** (1926), 1–55; **36** (1927), 233–311; *Erg. Bd.* **6** (1930), 1–204; herdruk: Physica-Verlag, Würzburg, 1965.

Een moderne behandeling van de bewijzen die van L-functies gebruik maken kan men vinden in S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, 1970; second edition: Graduate Texts in Mathematics **110**, Springer-Verlag, New York, 1994.

Na de tweede wereldoorlog werd een bewijs van de stellingen uit de klassenlichamentheorie ontdekt dat niet van analyse maar van *cohomologie van groepen* gebruik maakt. De belangrijkste referentie is: E. Artin, J. Tate, *Class field theory*, Benjamin, New York, 1967 (later herdrukt). Voor een toegankelijker behandeling zie men J. W. S. Cassels, A. Fröhlich (eds), *Algebraic number theory*, Academic Press, London-New York, 1967; herdrukt als paperback in 1986.

De boeken door Lang en Cassels-Fröhlich worden speciaal aanbevolen.

Op college zullen we een benadering volgen waarin zowel de L-functies als de cohomologische technieken vermeden worden. Deze benadering gaat terug op C. Chevalley, *La théorie des corps de classes*, Ann. Math. **41** (1940), 394–417, en is niet in boeken te vinden.

Voor andere behandelingen van de klassenlichamentheorie zie men: A. Weil, *Basic number theory*, Springer-Verlag, Berlin, 1967; J. Neukirch, *Class field theory*, Springer-Verlag, Berlin, 1986; J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 1992.

Extra literatuur. Over valuatietheorie and locale lichamen: J-P. Serre, *Corps locaux*, Hermann, Paris, 1962 (Engelse vertaling: *Local fields*, Springer-Verlag); E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963 (herdruk: Chelsea Publishing Company, New York, 1976); N. Bourbaki, *Commutative algebra*, Chapter VI; S. Lang, *Algebra*, third edition, Chapter XII, Addison-Wesley, Reading, 1993; J. W. S. Cassels, *Local fields*, Cambridge University Press, Cambridge, 1986.

Over oneindige Galoistheorie: J. W. S. Cassels, A. Fröhlich (eds), *Algebraic number theory* (zie boven), Chapter V; S. Lang, *Algebra*, third edition (zie boven), Chapter VI, §14; N. Bourbaki, *Algebra*, Chapter V; J. Neukirch, *Algebraische Zahlentheorie* (zie boven), Kapitel 4, §1.

Opgave 1. Laat p een oneven priemgetal zijn, en schrijf $p^* = \left(\frac{-1}{p}\right)p$. Zij verder R een ring en $\zeta \in R$ een element met $\sum_{i=0}^{p-1} \zeta^i = 0$. Definieer $\tau \in R$ door

$$\tau = \sum_{i=1}^{p-1} \left(\frac{i}{p}\right)\zeta^i.$$

Bewijs dat in R geldt: $\zeta^p = 1$ en $\tau^2 = p^*$. Kunt U ook bewijzen dat in de polynoomring $R[X]$ de identiteit $\prod_{i=0}^{p-1}(X - \zeta^i) = X^p - 1$ geldt?

Opgave 2. (a) Laat de notatie zijn als in Opgave 1, en laat bovendien l een priemgetal zijn zodanig dat in R geldt $l = 0$. Bewijs: $\tau^l = \left(\frac{l}{p}\right)\tau$.

(b) Laten l en p twee verschillende oneven priemgetallen zijn, en zij p^* als in Opgave 1. Bewijs: $\left(\frac{p^*}{l}\right) = \left(\frac{l}{p}\right)$. Leid hieruit de kwadratische reciprociteitswet af.

Opgave 3. Stel dat p een oneven priemgetal is. Bewijs: als 27 een primitieve wortel modulo p is, dan geldt $p \equiv 5 \bmod 12$. Geldt de omkering ook?

Opgave 4. Laten p en q twee oneven priemgetallen zijn. Bewijs dat p en q congruent modulo 24 zijn dan en slechts dan als voor elke $a \in \{-1, 2, 3\}$ geldt $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

Opgave 5. Zij $\bar{\mathbf{Q}}$ een vast gekozen algebraïsche afsluiting van $\mathbf{Q}$. Voor een positief geheel getal n geven we met ζ_n een primitieve n-de machts eenheidswortel in $\bar{\mathbf{Q}}$ aan.

Zij $K \subset \bar{\mathbf{Q}}$ een deellichaam met $[K : \mathbf{Q}] = 2$. Bewijs dat er een positief geheel getal n is met $K \subset \mathbf{Q}(\zeta_n)$, en dat men n gelijk kan nemen aan de absolute waarde van de discriminant $\Delta_{K/\mathbf{Q}}$ van K over $\mathbf{Q}$.

Opgave 6. Laat de notatie zijn als in Opgave 5. Stel dat $K \subset \bar{\mathbf{Q}}$ een deellichaam met $[K : \mathbf{Q}] = 2$ is, en dat n een positief geheel getal is met $K \subset \mathbf{Q}(\zeta_n)$. Bewijs dat n deelbaar is door $\Delta_{K/\mathbf{Q}}$.

Opgave 7. Zij p een priemgetal met $p > 3$. Bewijs dat het getal

$$\frac{p^p - \left(\frac{-1}{p}\right)}{p - \left(\frac{-1}{p}\right)}$$

niet een priemgetal is.

Opgave 8. Zij $f = X^3 - 3X + 1$, laat α een nulpunt van f in een uitbreidingslichaam van $\mathbf{Q}$ zijn, en schrijf $K = \mathbf{Q}(\alpha)$.

(a) Bewijs dat K een Galoisuitbreiding van graad 3 van $\mathbf{Q}$ is, en dat de Galoisgroep $\mathrm{Gal}(K/\mathbf{Q})$ wordt voortgebracht door een automorfisme σ van K waarvoor geldt $\sigma(\alpha) = \alpha^2 - 2$.

(b) Bereken $\Delta_{K/\mathbf{Q}}$, en bewijs dat de ring van gehelen van K gelijk is aan $\mathbf{Z}[\alpha]$.

Opgave 9. Laat de notatie zijn als in Opgave 8. Laat $b = 100$ of $b = 20$, al naar gelang U bij deze som een rekenapparaat gebruikt of niet. Bepaal voor elk priemgetal $p < b$, $p \neq 3$, een element $\varphi_p \in \mathrm{Gal}(K/\mathbf{Q}) = \{1, \sigma, \sigma^2\}$ met de eigenschap

$$\varphi_p(\beta) \equiv \beta^p \bmod p\mathbf{Z}[\alpha] \qquad \text{voor alle } \beta \in \mathbf{Z}[\alpha].$$

Opgave 10. Laat α een element van een lichaam K zijn, en σ een lichaamsautomorfisme van K van eindige orde. Veronderstel dat $\sigma(\alpha) = \alpha^2 - 2$. Bewijs dat elk nulpunt

van $X^2 - \alpha X + 1$ (in een algebraïsche afsluiting van K) een eenheidswortel van oneven orde is.

Opgave 11. Laat K zijn als in Opgave 8, en ζ_n als in Opgave 5.

(a) Bewijs dat K kan worden ingebed in een lichaam van de vorm $\mathbf{Q}(\zeta_n)$.

(b) Bewijs dat er voor *ieder* priemgetal $p \neq 3$ een element $\varphi_p \in \{1, \sigma, \sigma^2\}$ met de eigenschap uit Opgave 9 bestaat.

Opgave 12. Stel dat n een geheel getal groter dan 1 is met de eigenschap dat voor elke commutatieve ring R waarin n gelijk is aan 0 de afbeelding $F\colon R \to R$ gedefinieerd door $F(x) = x^n$ een ringhomomorfisme is. Bewijs dat n een priemgetal is.

Opgave 13. Een *topologische groep* is een groep G die tegelijk een topologische ruimte is, met de eigenschap dat de afbeeldingen $m\colon G \times G \to G$ en $i\colon G \to G$ gedefinieerd door $m(g,h) = gh$ en $i(g) = g^{-1}$ continu zijn; hier heeft $G \times G$ de product-topologie.

(a) Zij G een topologische groep, en $g \in G$. Bewijs dat de afbeelding $G \to G$, $x \mapsto gx$, een homeomorfisme is.

(b) Zij G een topologische groep, en g, $h \in G$. Bewijs dat er een homeomorfisme $f\colon G \to G$ is met $f(g) = h$ en $f(h) = g$.

Opgave 14. Zij G een topologische groep, en laat $H \subset G$ een ondergroep zijn.

(a) Bewijs: als H open is dan is H ook gesloten.

(b) Stel dat G compact is. Bewijs: H is open dan en slechts dan als H gesloten is en eindige index in G heeft.

Opgave 15. Zij L een lichaam, en laat $\operatorname{Aut} L$ de automorfismengroep van L zijn. Noem een deelverzameling $U \subset \operatorname{Aut} L$ *open* als er voor elke $\sigma \in U$ een eindige deelverzameling $E \subset L$ is waarvoor de verzameling

$$U_{\sigma,E} = \{\tau \in \operatorname{Aut} L : \tau|E = \sigma|E\}$$

in U bevat is.

Bewijs dat $\operatorname{Aut} L$ met deze definitie een topologische groep is.

Opgave 16. Zij L een lichaam, K een deellichaam van L, en G een ondergroep van $\operatorname{Aut} L$. Bewijs: L is een Galoisuitbreiding van K met groep G dan en slechts dan als G *compact* is in de van $\operatorname{Aut} L$ geïnduceerde topologie (zie Opgave 15) en K gelijk is aan het invariantenlichaam $\{x \in L : \sigma x = x \text{ voor alle } \sigma \in G\}$ van G.

Een *gerichte partieel geordende verzameling* is een verzameling I die voorzien is van een partiële ordening $\geq$ zodanig dat er voor elk tweetal elementen i, $j \in I$ een element $k \in I$ is met $k \geq i$ en $k \geq j$. Een *projectief systeem* van verzamelingen bestaat uit (ten eerste) een gerichte partieel geordende verzameling I, (ten tweede) voor elke $i \in I$ een verzameling V_i, en (ten derde) voor elk tweetal elementen i, $j \in J$ met $i \geq j$ een afbeelding $f^i_j \colon V_i \to V_j$, op een dusdanige manier dat f^i_i de identieke afbeelding op V_i is voor elke $i \in I$, en $f^i_k = f^j_k \circ f^i_j$ voor elk drietal elementen i, j, $k \in I$ met $i \geq j \geq k$. De *projectieve limiet* van een dergelijk systeem is gedefinieerd door

$$\lim_{\leftarrow} V_i = \{(v_i)_{i \in I} \in \prod_{i \in I} V_i : f^i_j(v_i) = v_j \text{ voor alle } i, j \in I \text{ met } i \geq j\}.$$

Als alle V_i groepen (of ringen) zijn, en alle f^i_j zijn groepshomomorfismen (of ringhomomorfismen), dan is de projectieve limiet weer een groep (of een ring).

Opgave 17. (a) Laten X en Y twee verzamelingen zijn, en zij I de verzameling van eindige deelverzamelingen E van X. Laat I geordend zijn door inclusie. Voor $E \in I$ zij V_E de verzameling injectieve afbeeldingen $E \to Y$, en voor $E' \subset E \in I$ zij $f^E_{E'} \colon V_E \to V_{E'}$ de restrictie-afbeelding. Bewijs dat we op deze manier een projectief systeem hebben gekregen, en dat de limiet kan worden geïdentificeerd met de verzameling injectieve afbeeldingen $X \to Y$.

(b) Bewijs dat er een projectief systeem bestaat waarin alle verzamelingen V_i niet-leeg zijn, alle "overgangsafbeeldingen" f^i_j surjectief, maar waarvan de limiet leeg is.

Opgave 18. (a) Stel we hebben een projectief systeem waarin I aftelbaar is, elke V_i niet-leeg is, en elke f^i_j surjectief. Bewijs dat de projectieve limiet niet-leeg is.

(b) Stel we hebben een projectief systeem waarin elke V_i eindig en niet-leeg is. Bewijs dat de projectieve limiet niet-leeg is.

We geven met $\hat{\mathbf{Z}}$ de projectieve limiet van de eindige ringen $\mathbf{Z}/n\mathbf{Z}$ aan, waarbij n loopt over de verzameling positieve gehele getallen, geordend door deelbaarheid; de overgangsafbeeldingen $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ (voor m een deler van n) zijn de unieke ringhomomorfismen. Op college hebben we op $\hat{\mathbf{Z}}$ een topologie gedefinieerd.

Opgave 19. (a) Bewijs dat $\mathbf{Z}$, beschouwd als deelring van $\hat{\mathbf{Z}}$, dicht ligt in $\hat{\mathbf{Z}}$.

(b) Zij n een positief geheel getal. Bewijs dat vermenigvuldiging met n een exacte rij $0 \to \hat{\mathbf{Z}} \to \hat{\mathbf{Z}} \to \mathbf{Z}/n\mathbf{Z} \to 0$ induceert.

Opgave 20. Laat μ de groep van alle eenheidswortels in een gegeven algebraïsch afgesloten lichaam van karakteristiek nul zijn.

(a) Bewijs dat $\hat{\mathbf{Z}}$ als ring isomorf is met de endomorfismenring van de abelse groep μ.

(b) Bewijs dat de eenhedengroep $\hat{\mathbf{Z}}^*$ van $\hat{\mathbf{Z}}$, met de van $\hat{\mathbf{Z}}$ afkomstige topologie, een pro-eindige groep is, en dat $\hat{\mathbf{Z}}^*$ isomorf is met de automorfismengroep $\operatorname{Aut}\mu$ van μ.

Opgave 21. Laten G en H pro-eindige groepen zijn, en $f\colon G \to H$ een continu groepshomomorfisme. Bewijs dat het geïnduceerde groepsisomorfisme $G/\ker f \to fG$ tevens een *homeomorfisme* is, als we $G/\ker f$ de quotiënt-topologie van G geven en fG de relatief-topologie van H.

Opgave 22. Zij K een lichaam van karakteristiek nul, en μ de groep van alle eenheidswortels in een gegeven algebraïsche afsluiting van K. Bewijs dat $K(\mu)$ een Galoisuitbreiding van K is, en dat $\operatorname{Gal}(K(\mu)/K)$ isomorf is met een gesloten ondergroep van $\hat{\mathbf{Z}}^*$. Komt iedere gesloten ondergroep voor, als K loopt over alle lichamen van karakteristiek nul?

Opgave 23. Een topologische groep G heet *topologisch eindig voortgebracht* als er een eindige verzameling $S \subset G$ is zodanig dat G de afsluiting is van de ondergroep $\langle S\rangle$ van G.

Welke van de topologische groepen $\mathbf{C}^*$, $\hat{\mathbf{Z}}$ en $\hat{\mathbf{Z}}^*$ zijn topologisch eindig voortgebracht? Bewijs de correctheid van Uw antwoord.

Opgave 24. Zij G een pro-eindige groep. Bewijs dat er voor elke $g \in G$ precies één continu groepshomomorfisme $\hat{\mathbf{Z}} \to G$ is dat 1 op g afbeeldt.

Opgave 25. (*Factoriële notatie.*) Bewijs dat er voor elk element $a \in \hat{\mathbf{Z}}$ een unieke rij gehele getallen $(c_n)_{n=1}^{\infty}$ met de eigenschappen

$$a = \sum_{n=1}^{\infty} c_n n!, \qquad 0 \le c_n \le n$$

bestaat, en dat omgekeerd voor elke rij gehele getallen $(c_n)_{n=1}^{\infty}$ met $0 \le c_n \le n$ de som $\sum_{n=1}^{\infty} c_n n!$ convergeert in $\hat{\mathbf{Z}}$. Welke c_n moet men nemen om $a = -1$ te krijgen?

Opgave 26. Zij k een niet-negatief geheel getal, en definieer $(a_n)_{n=0}^{\infty}$ door $a_0 = k$, $a_{n+1} = 2^{a_n}$. Bewijs dat de rij $(a_n)_{n=0}^{\infty}$ een limiet a in $\hat{\mathbf{Z}}$ heeft, en dat deze limiet onafhankelijk van k is. Bereken bovendien de cijfers $c_1, c_2, \ldots, c_b$ van a in de factoriële notatie (zie Opgave 25), waarbij $b = 20$ als U een computer gebruikt en $b = 6$ anders.

Opgave 27. Voor een priemgetal p zij $\mathbf{Z}_p$ de *ring der p-adische (gehele) getallen*, d. w. z. de projectieve limiet van de ringen $\mathbf{Z}/p^n\mathbf{Z}$, waarbij n over de verzameling positieve gehele getallen loopt.

Bewijs dat er isomorfismen

$$\hat{\mathbf{Z}} \cong \prod_p \mathbf{Z}_p, \qquad \hat{\mathbf{Z}}^* \cong \prod_p \mathbf{Z}_p^*$$

van topologische ringen en topologische groepen (respectievelijk) zijn, waarbij p over de verzameling priemgetallen loopt.

Opgave 28. Laat het uitbreidingslichaam L van $\mathbf{Q}$ verkregen worden door aan $\mathbf{Q}$ beide vierkantswortels $\pm\sqrt{a}$ van alle rationale getallen a (in een vaste algebraïsche afsluiting) te adjungeren. Bewijs dat L een Galoisuitbreiding van $\mathbf{Q}$ is, en dat $\mathrm{Gal}(L/\mathbf{Q})$ isomorf is met het directe product van aftelbaar oneindig veel groepen van orde 2.

Opgave 29. Zij K een lichaam, en $\bar{K}$ een algebraïsche afsluiting van K. Men noemt $K_\mathrm{s} = \{\alpha \in \bar{K} : \alpha \text{ is separabel over } K\}$ een *separabele afsluiting* van K.

Bewijs dat K_s een lichaam is, en dat het een Galoisuitbreiding van K is. De groep $G_K = \mathrm{Gal}(K_\mathrm{s}/K)$ heet de *absolute Galoisgroep* van K.

Opgave 30. (a) Zij G een topologische groep, en X een verzameling voorzien van een werking van G op X. De werking heet *continu* als de afbeelding $G \times X \to X$ die de werking definieert continu is; hier heeft X de discrete topologie en $G \times X$ de producttopologie. Bewijs: de werking is continu dan en slechts dan als voor elke $x \in X$ de stabilisator G_x van x in G een *open* ondergroep van G is.

(b) Laten K, K_s en G_K als in Opgave 29 zijn. Geef met $\mathbf{Sep}_K$ de categorie van eindige separabele lichaamsuitbreidingen van K aan (met als morfismen de lichaamshomomorfismen die op K de identiteit zijn), en met $\mathbf{trans}_{G_K}$ de categorie van eindige verzamelingen voorzien van een continue transitieve werking van G_K (met als morfismen de afbeeldingen die de G_K-werking respecteren). Bewijs dat er een anti-equivalentie $F\colon \mathbf{Sep}_K \to \mathbf{trans}_{G_K}$ van categorieën is waarvoor $F(L)$, voor een object L van $\mathbf{Sep}_K$, gelijk is aan de verzameling K-inbeddingen $L \to K_\mathrm{s}$.

Opgave 31. Zij A een commutatieve ring en $\mathfrak{m}$ een maximaal ideaal van A. Bewijs dat de completering $\hat{A}_\mathfrak{m}$ van de localisatie $A_\mathfrak{m}$ van A bij $\mathfrak{m}$ isomorf is met de projectieve limiet van de ringen $A/\mathfrak{m}^n$, waarbij n over de positieve gehele getallen loopt.

Opgave 32. Laat $f\colon A \to B$ een ringhomomorfisme van een locale ring A naar een locale ring B zijn, en geef met $\mathfrak{m}_A$ en $\mathfrak{m}_B$ de maximale idealen van deze ringen aan.

(a) Bewijs: er geldt $f(\mathfrak{m}_A) \subset \mathfrak{m}_B$ dan en slechts dan als $\mathfrak{m}_A = f^{-1}\mathfrak{m}_B$, en dan en slechts dan als $A^* = f^{-1}B^*$. Als deze drie equivalente voorwaarden vervuld zijn heet *f locaal*.

(b) Stel f is locaal. Bewijs dat f een homomorfisme van het restklassenlichaam van A naar het restklassenlichaam van B induceert.

(c) Geef een voorbeeld van twee discrete valuatieringen A, B en een ringhomomorfisme $A \to B$ dat *niet* locaal is.

Opgave 33. Zij k een lichaam. Bewijs dat de ring $k[[X]]$ van formele machtreeksen in één variabele X over k een complete discrete valuatiering is. *Kunt U bewijzen dat de eenhedengroep $k[[X]]^*$ voor geen enkele k topologisch eindig voortgebracht is?

Opgave 34. Zij A een complete discrete valuatiering, en $\mathfrak{m}$ het maximale ideaal. Zij n een geheel getal dat niet deelbaar is door de karakteristiek van $A/\mathfrak{m}$. Bewijs dat de afbeelding $1 + \mathfrak{m} \to 1 + \mathfrak{m}$, $x \mapsto x^n$, een automorfisme van de multiplicatieve groep $1 + \mathfrak{m}$ is.

Opgave 35. Zij p een priemgetal. Bewijs dat de volgende isomorfieën van topologische groepen bestaan:

$$\mathbf{Z}_p^* \cong \mathbf{F}_p^* \times (1 + p\mathbf{Z}_p),$$
$$1 + p\mathbf{Z}_p \cong \mathbf{Z}_p \qquad (\text{voor } p > 2),$$
$$1 + 2\mathbf{Z}_2 \cong \{\pm 1\} \times (1 + 4\mathbf{Z}_2) \cong (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}_2.$$

Welke van deze groepen zijn topologisch eindig voortgebracht?

Opgave 36. Zij A de completering van de localisatie van $\mathbf{Z}[\mathrm{i}]$ bij het priemideaal $(2 - \mathrm{i})\mathbf{Z}[\mathrm{i}]$; hier is $\mathrm{i}^2 = -1$.

(a) Bewijs: $A \cong \mathbf{Z}_5$.

(b) Bewijs dat er een unieke rij $(c_n)_{n=0}^{\infty}$ elementen $c_n \in \{0, 1, \mathrm{i}, -1, -\mathrm{i}\}$ bestaat zodanig dat in $\mathbf{Z}_5$ geldt

$$2 = \sum_{n=0}^{\infty} c_n 5^n.$$

Bepaal bovendien c_0, c_1 en c_2.

Opgave 37. Laat p een oneven priemgetal zijn.

(a) Zij $(c_n)_{n=0}^{\infty}$ een rij gehele getallen met $0 \leq c_n \leq p - 1$. Hoe kan men aan de c_n zien of het element $a = \sum_{n=0}^{\infty} c_n p^n$ van $\mathbf{Z}_p$ tot $\mathbf{Z}$ behoort? of tot $\frac{1}{2} + \mathbf{Z}$?

(b) Dezelfde vragen met de voorwaarde $0 \leq c_n \leq p - 1$ vervangen door $|c_n| \leq (p - 1)/2$.

Opgave 38. Merk op dat het kwadraat van 76 op 76 eindigt, en het kwadraat van 25 op 25:

$$76^2 = 5776, \qquad 25^2 = 625.$$

Laat, in het algemeen, $b \geq 2$ een geheel getal zijn, en $n \geq 1$. In de puzzelwiskunde noemen we een getal *a automorf van orde n in basis b* als geldt dat $a^2 \equiv a \bmod b^n$; dus 76 en 25 zijn automorf van orde 2 in basis 10. Zij $S_{b,n} \subset \mathbf{Z}/b^n\mathbf{Z}$ de verzameling restklassen $(\bmod b^n)$ van automorfe getallen van orde n in basis b.

(a) Bepaal $S_{10,1}$.

(b) Bewijs: als x automorf van orde n in basis b is, dan is $3x^2 - 2x^3$ automorf van orde $2n$ in basis b.

(c) Bewijs dat reductie modulo b^n een bijectie $S_{b,2n} \to S_{b,n}$ definieert.

(d) Bepaal $S(10, 8)$.

Opgave 39. Zij A een valuatiering. Bewijs: A is noethers dan en slechts dan als A een discrete valuatiering of een lichaam is.

Opgave 40. Zij A een valuatiering, n een geheel getal groter dan 1, en $a_1, \ldots, a_n$ elementen van A met $\sum_{i=1}^{n} a_i = 0$. Bewijs: er bestaan i, j met $1 \leq i < j \leq n$ en $Aa_i = Aa_j$.

Opgave 41. (a) Zij A een valuatiering met quotiëntenlichaam K, en zij n een positief geheel getal. Voor $h \in \{1, 2, \ldots, n\}$ geven we met S_h de verzameling vectoren $(x_1, x_2, \ldots, x_n) \in K^n \backslash \{0\}$ aan met de eigenschap

$$h = \min\bigl\{i \in \{1, 2, \ldots, n\} : Ax_i = \sum_{j=1}^{n} Ax_j\bigr\}.$$

Bewijs: elke rij vectoren $v_1, \ldots, v_n \in K^n$ met $v_i \in S_i$ voor elke i vormt een basis voor K^n over K.

(b) Bewijs dat het platte vlak $\mathbf{R}^2$ geschreven kan worden als vereniging van drie dicht liggende deelverzamelingen met de eigenschap dat geen enkele rechte lijn met elk van deze drie deelverzamelingen een niet-lege doorsnede heeft.

Opgave 42. Zij A een complete discrete valuatiering met quotiëntenlichaam K, zij L een eindige lichaamsuitbreiding van K, en B de gehele afsluiting van A in L. Op college is bewezen dat B een complete discrete valuatiering is. Geef met $f(B/A)$ de restklassengraad aan, en met $N_{L/K}$ de norm $L \to K$.

(a) Laat π_A een priemelement van A zijn, en π_B van B. Bewijs dat er een $u \in A^*$ is met $N_{L/K}(\pi_B) = u \cdot \pi_A^{f(B/A)}$.

(b) Zij $x \in L$. Bewijs: $x \in B \Leftrightarrow N_{L/K}(x) \in A$.

Opgave 43. Laat l een eindig lichaam zijn, en $k \subset l$ een deellichaam. Bewijs: de norm en het spoor zijn allebei surjectieve functies van l naar k.

Opgave 44. Laat A een complete discrete valuatiering met quotiëntenlichaam K zijn, en veronderstel dat het restklassenlichaam van A *eindig* is. Zij L een eindige uitbreiding van K die *onvertakt* is, in de zin dat de vertakkingsindex $e(B/A)$ van de gehele afsluiting B van A in L gelijk is aan 1.

(a) Bewijs dat $N_{L/K}$ een surjectieve afbeelding $B^* \to A^*$ induceert.

(b) Bewijs dat er een exacte rij abelse groepen

$$L^* \xrightarrow{N} K^* \xrightarrow{r} \mathrm{Gal}(L/K) \to 1$$

is, waarbij $N = N_{L/K}$ en waarbij r elk priemelement van A op het Frobeniuselement $\mathrm{Frob} \in \mathrm{Gal}(L/K)$ afbeeldt.

Opgave 45. Laat A een complete discrete valuatiering met quotiëntenlichaam K en met een eindig restklassenlichaam k zijn. Zij M de vereniging (binnen een vaste algebraïsche afsluiting van K) van alle eindige onvertakte lichaamsuitbreidingen L van K. Bewijs dat M een lichaam is, en dat M Galois over K is met $\mathrm{Gal}(M/K) \cong \hat{\mathbf{Z}}$. Bewijs ook dat M verkregen wordt door aan K alle eenheidswortels van orde niet deelbaar door de karakteristiek van k te adjungeren.

Opgave 46. Laat A een locale ring zijn, met restklassenlichaam k. Zij p de karakteristiek van k.

(a) Stel dat α een element van de kern van de natuurlijke afbeelding $A^* \to k^*$ is. Bewijs dat voor elke $n \in \mathbf{Z}\backslash p\mathbf{Z}$ geldt: $(\alpha^n - 1)A = (\alpha - 1)A$.

(b) Zij T de torsie-ondergroep van de kern van $A^* \to k^*$. Bewijs: $T = \{1\}$ als $p = 0$, en T bestaat uit alle elementen van A^* van p-macht orde als $p > 0$.

Opgave 47. Laat A een discrete valuatiering zijn waarvan het restklassenlichaam karakteristiek $p > 0$ heeft. Stel dat $\zeta \in A^*$ orde p^n heeft, voor een positief geheel getal n. Bewijs: $(\zeta - 1)^{\varphi(p^n)}A = pA$.

Opgave 48. Zij p een priemgetal en n een positief geheel getal. Bewijs dat het p^n-de cyclotomische polynoom Φ_{p^n} irreducibel is over het lichaam $\mathbf{Q}_p$ der p-adische getallen, en dat voor een nulpunt ζ van Φ_{p^n} geldt dat $\mathbf{Z}_p[\zeta]$ een complete discrete valuatiering met $e(\mathbf{Z}_p[\zeta]/\mathbf{Z}_p) = \varphi(p^n)$, $f(\mathbf{Z}_p[\zeta]/\mathbf{Z}_p) = 1$ is.

In Opgaven 49–56 zal A steeds een discrete valuatiering met quotiëntenlichaam K zijn, en $v\colon K^* \to \mathbf{Z}$ is het groepshomomorfisme dat elk priemelement van A op 1 afbeeldt (dus $v(u\pi^m) = m$, voor $u \in A^*$, $\pi \in A$ priem, en $m \in \mathbf{Z}$); we nemen $v(0) = \infty$.

Opgave 49. Voor $r \in \mathbf{R}$ en $f = \sum_i a_i X^i \in K[X]$, $f \neq 0$, geven we de grootste en kleinste waarde van i waarvoor geldt $v(a_i) + ir = \min_j\big(v(a_j) + jr\big)$ aan met $g_r(f)$ respectievelijk $k_r(f)$.

(a) Bereken $g_r(f)$ en $k_r(f)$ voor $A = \mathbf{Z}_{(2)}$, $f = 2X^4 - 6X^3 - X^2 + 3X - 8$, en alle waarden van r.

(b) Bewijs dat voor iedere $r \in \mathbf{R}$ de functies g_r en k_r voortgezet kunnen worden tot groepshomomorfismen $K(X)^* \to \mathbf{Z}$.

(c) Zij $f \in K[X]$, $f \neq 0$, en neem aan dat f in $K[X]$ in lineaire factoren splitst. Bewijs dat voor elke $r \in \mathbf{R}$ het aantal nulpunten α van f in K met $v(\alpha) = r$, geteld met multipliciteiten, gelijk is aan $g_r(f) - k_r(f)$.

Opgave 50 (Newton-polygonen). Het *Newton-polygoon* van een polynoom $f = \sum_i a_i X^i \in K[X]$, $f \neq 0$, is gedefinieerd als de 'onderkant' van het convexe omhulsel van de punten $\big(i, v(a_i)\big)$, waarbij i loopt over de niet-negatieve gehele getallen met $a_i \neq 0$; preciezer, als $C \subset \mathbf{R} \times \mathbf{R}$ het convexe omhulsel van de verzameling van die punten is, dan is het Newton-polygoon gelijk aan $\{(x, y) \in C : \text{er is geen } (x, y') \in C \text{ met } y' < y\}$. Het Newton-polygoon is de vereniging van eindig veel lijnsegmenten met verschillende richtingscoëfficiënten. (De *richtingscoëfficiënt* van een lijn gegeven door $y = ax + b$ is gelijk aan a.)

(a) Teken, voor elk priemgetal p, het Newton-polygoon van $3X^3 - \frac{6}{7}X^2 + \frac{3}{2}X + 5 \in \mathbf{Q}[X]$ in het geval $A = \mathbf{Z}_{(p)}$.

(b) Bewijs: als $-r$ gelijk is aan de richtingscoëfficiënt van één van de lijnsegmenten waar het Newton-polygoon van f uit bestaat, dan is het getal $g_r(f) - k_r(f)$ uit Opgave 49 gelijk aan de lengte van de projectie van dat lijnsegment op de x-as, en voor andere r geldt $g_r(f) - k_r(f) = 0$.

Opmerking. Uit (b) en Opgave 49(c) volgt dat men de valuaties van de nulpunten van f (in een algebraïsche uitbreiding van K) kan aflezen aan het Newton-polygoon van f.

Opgave 51. Zij $f \in K[X]$, en neem aan dat $f(0) \neq 0$.

(a) Stel dat A compleet is en dat f irreducibel is in $K[X]$. Bewijs dat het Newton-polygoon van f uit een enkel lijnsegment bestaat.

(b) Stel dat het Newton-polygoon van f de verzameling $\mathbf{Z} \times \mathbf{Z}$ in precies twee punten snijdt. Bewijs dat f irreducibel is in $K[X]$.

(c) Bewijs dat $3X^3 - \frac{6}{7}X^2 + \frac{3}{2}X + 5$ in elk van de ringen $\mathbf{Q}_2[X]$ en $\mathbf{Q}_7[X]$ het product van twee irreducibele factoren is, dat het in $\mathbf{Q}_3[X]$ irreducibel is, en dat het in $\mathbf{Q}_5[X]$ het product van drie lineaire factoren is. Hoe ziet de ontbinding in $\mathbf{Q}[X]$ eruit?

Opgave 52. Een *Eisenstein-polynoom* is een monisch polynoom $f \in A[X]$ van positieve graad waarvan het Newton-polygoon gelijk is aan het lijnsegment dat de punten $(0, 1)$ en $(\deg f, 0)$ verbindt.

(a) Is dit equivalent met de definitie van een Eisenstein-polynoom die U al kent?

(b) Zij $f \in K[X]$. Bewijs: f is Eisenstein dan en slechts dan als er een discrete valuatiering B in een eindige uitbreiding van K bestaat, met $B \cap K = A$, $e(B/A) = \deg f$ en $f(B/A) = 1$, zodanig dat B een priemelement heeft waarvan f het minimumpolynoom over K is.

Opgave 53. Stel A is compleet, en zij B de gehele afsluiting van A in een eindige uitbreiding van K. Neem aan dat $f(B/A) = 1$.

(a) Zij e_0 de grootste deler van $e(B/A)$ die niet deelbaar is door de karakteristiek van het restklassenlichaam van A. Bewijs dat er een priemelement van A is dat een e_0-de machts wortel in B heeft. (*Aanwijzing*: gebruik Opgave 34.)

(b) Stel dat B tam vertakt is over A. Bewijs: er is een priemelement π van A zodanig dat B als ring isomorf is met $A[X]/(X^{e(B/A)} - \pi)A[X]$.

Opgave 54. Neem aan dat A compleet is. Het doel van deze opgave is te bewijzen dat A de enige discrete valuatiering met quotiëntenlichaam K is.

Zij B een discrete valuatiering met quotiëntenlichaam K.

(a) Zij $S = \{x \in K^* : \text{er zijn oneindig veel } n \in \mathbf{Z} \text{ waarvoor } x \text{ een } n\text{-de macht in } K \text{ is}\}$. Bewijs: $1 + \mathfrak{m} \subset S \subset B^*$ en $\mathfrak{m} \subset B$.

(b) Bewijs: $A = B$. (*Aanwijzing*: als $w\colon K^* \to \mathbf{Z}$ bij B hoort, wat weet U dan van de ondergroep $\{\big(v(x), w(x)\big) : x \in K^*\}$ van $\mathbf{Z} \times \mathbf{Z}$?)

Opgave 55. Neem aan dat A compleet is met maximaal ideaal $\mathfrak{m}$, dat de karakteristiek p van het restklassenlichaam $A/\mathfrak{m}$ van A ongelijk is aan 0, en dat K karakteristiek 0 heeft. Schrijf $e = v(p)$. Voor $i \in \mathbf{Z}$, $i > 0$, geven we de open ondergroep $1 + \mathfrak{m}^i$ van K^* aan met U_i.

(a) Zij $u \in U_1$. Beschrijf het Newton-polygoon van $(X + 1)^p - u$ in termen van $v(u - 1)$.

(b) Stel dat i een geheel getal is met $i > e/(p - 1)$. Bewijs dat er een groepsisomorfisme $U_i \to U_{i+e}$ is dat x op x^p afbeeldt.

Opgave 56. Laten de aannamen en de notatie als in de vorige opgave zijn.

(a) Zij n een positief geheel getal. Bewijs: de ondergroep K^{*n} van K^* bestaande uit de n-de machten is een open ondergroep van K^*, en omvat $U_{e'+ke}$, waarbij e' het kleinste gehele getal $> e/(p-1)$ aangeeft en k het aantal factoren p in n is.

(b) Zij $H \subset K^*$ een ondergroep. Bewijs: als H eindige index heeft, dan is H open. Geldt de omkering ook?

(c) Stel dat het restklassenlichaam van A eindig is. Zij L een eindige uitbreiding van K. Bewijs: $N_{L/K}(L^*)$ is een open ondergroep van eindige index van K^*.

Opgave 57. (a) Laten p en p' priemgetallen zijn, en K en K' eindige uitbreidingen van $\mathbf{Q}_p$ respectievelijk $\mathbf{Q}_{p'}$. Laat $\varphi\colon K \to K'$ een lichaamshomomorfisme zijn. Bewijs: $p = p'$, en φ beperkt tot $\mathbf{Q}_p$ is de identiteit.

(b) Zij $\mathfrak{p}$ een priem van $\mathbf{Q}$, en $\mathbf{Q}_\mathfrak{p}$ de bijbehorende completering. Bewijs dat $\mathbf{Q}_\mathfrak{p}$ geen lichaamsautomorfisme behalve de identiteit heeft.

Opgave 58. Zij K het lichaam der reële getallen of het lichaam der complexe getallen, en zij $H \subset K^*$ een ondergroep. Bewijs: H is open dan en slechts dan als H eindige index in K^* heeft, en dan en slechts dan als er een eindige uitbreiding L van K is met $H = N_{L/K}(L^*)$.

Opgave 59. (a) Bewijs: elk element van $1 + 8\mathbf{Z}_2$ is een kwadraat in $\mathbf{Q}_2$.

(b) Bereken voor elk priemgetal p de orde van de groep $\mathbf{Q}_p^*/\mathbf{Q}_p^{*2}$.

(c) Geef voor elk priemgetal p een element $a \in \mathbf{Q}_p$ aan waarvoor $\mathbf{Q}_p(\sqrt{a})$ een onvertakte kwadratische uitbreiding van $\mathbf{Q}_p$ is. Hoeveel vertakte kwadratische uitbreidingen heeft $\mathbf{Q}_p$, op isomorfie na?

Opgave 60. Laat K een eindige uitbreiding van $\mathbf{Q}$ zijn, en zij voor elke priem $\mathfrak{p}$ van K de functie $\| \cdot \|_\mathfrak{p}\colon K \to \mathbf{R}$ als op college gedefinieerd. Bewijs de *productformule*: $\prod_\mathfrak{p} \|x\|_\mathfrak{p} = 1$ voor elke $x \in K^*$, waarbij $\mathfrak{p}$ over alle priemen van K loopt.

Opgave 61. Laat p een priemgetal zijn, en $\bar{\mathbf{Q}}_p$ een algebraïsche afsluiting van het lichaam $\mathbf{Q}_p$ der p-adische getallen. Zij $K = \mathbf{Q}(\alpha)$ een eindige uitbreiding van $\mathbf{Q}$, en $f \in \mathbf{Q}[X]$ het minimumpolynoom van α over $\mathbf{Q}$. Op college definieerden we een oneindige priem van K als een priemideaal van $K \otimes_\mathbf{Q} \mathbf{R}$. Laat nu een *$p$-adische priem* van K een priemideaal van de ring $K \otimes_\mathbf{Q} \mathbf{Q}_p$ zijn.

Toon aan dat er tussen de volgende vier verzamelingen bijecties bestaan: de verzameling p-adische priemen van K; de verzameling monische irreducibele factoren van f in $\mathbf{Q}_p[X]$; de verzameling conjugatieklassen van lichaamsinbeddingen $\varphi\colon K \to \bar{\mathbf{Q}}_p$, waarbij φ en φ' geconjugeerd heten als er een $\sigma \in \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ is met $\sigma\varphi = \varphi'$; en de verzameling eindige priemen $\mathfrak{p}$ van K met $p \in \mathfrak{p}$.

Opgave 62. Laat p een priemgetal zijn en r een positief rationaal getal. In $\mathbf{Q}_p$ heeft r een unieke p-adische expansie $r = \sum_{i\in\mathbf{Z}} c_i p^i$ met $c_i \in \{0, 1, \ldots, p-1\}$, $c_i = 0$ voor $i \ll 0$. Beneden staat een methode om deze expansie te vinden. Pas deze methode toe in het geval $p = 2$, $r = 3\frac{1}{7}$, en bewijs dat de methode in het algemeen correct is. Hoe moet de methode aangepast worden voor negatieve r?

Schrijf eerst r als reëel getal op de gebruikelijke wijze in basis p, dus als $r = \sum_{i\in\mathbf{Z}} a_i p^i$, met $a_i \in \{0, 1, \ldots, p-1\}$, $a_i = 0$ voor $i \gg 0$. Zoals bekend is de rij cijfers $(a_i)_{i=-1}^{-\infty}$ uiteindelijk periodiek; zij m de lengte van de periode. Definieer nu $b_i \in \{0, 1, \ldots, p-1\}$, voor $i \in \mathbf{Z}$, door $b_i = a_{i-km}$, met $k \in \mathbf{Z}$ voldoende groot. Dan is de tweezijdig oneindige rij $(b_i)_{i\in\mathbf{Z}}$ zuiver periodiek met periode m. De p-adische expansie $\sum_{i\in\mathbf{Z}} c_i p^i$ van r verkrijgt men nu door de uitdrukking $\sum_{i\in\mathbf{Z}} b_i p^i$ van $\sum_{i\in\mathbf{Z}} a_i p^i$ af te trekken door middel van de gebruikelijke methode waarmee men getallen in basis p aftrekt.

Voorbeeld. Neem $p = 5$ en $r = 42\frac{8}{15}$. Als reëel getal wordt r in basis 5 gegeven door

$$132.2313131313\ldots .$$

De zuiver periodieke uitdrukking $\sum_{i\in\mathbf{Z}} b_i p^i$ kan men schrijven als

$$\ldots 1313131313.1313131313\ldots .$$

Trekt men deze uitdrukking in basis 5 van de vorige af, gaande van rechts naar links, dan vindt men

$$\ldots 3131313314.1.$$

Dit is de 5-adische expansie van $42\frac{8}{15}$; dus $c_i = 0$ voor $i < -1$, $c_{-1} = 1$, $c_0 = 4$, $c_1 = 1$, $c_2 = 3$, en $c_{2i-1} = 3$, $c_{2i} = 1$ voor $i \geq 2$.

Opgave 63. Laat p een priemgetal zijn en ζ_p een primitieve p-de machts eenheidswortel in een uitbreiding van $\mathbf{Q}_p$. Bewijs: $\mathbf{Q}_p(\zeta_p) = \mathbf{Q}_p\big((-p)^{1/(p-1)}\big)$.

Opgave 64. Doe het volgende voor $p = \infty$, 2, 3, 5, 7 en 31. Bepaal de graad $[L : \mathbf{Q}_p]$ van een ontbindingslichaam L van $X^3 - 2$ over $\mathbf{Q}_p$, evenals de restklassengraad $f(L/\mathbf{Q}_p)$, de vertakkingsindex $e(L/\mathbf{Q}_p)$, de Galoisgroep en de traagheidsgroep van L over $\mathbf{Q}_p$.

Opgave 65. Zij p een priemgetal, en laat L het lichaam zijn dat uit $\mathbf{Q}_p$ verkregen wordt door aan $\mathbf{Q}_p$ de vierkantswortels van alle elementen van $\mathbf{Q}_p$ te adjungeren. Bewijs dat L een eindige abelse uitbreiding van $\mathbf{Q}_p$ is, en bepaal de Galoisgroep en de traagheidsgroep. Bepaal bovendien de ondergroep $N_{L/\mathbf{Q}_p}(L^*)$ van $\mathbf{Q}_p^*$. (Bij het laatste onderdeel mag U locale klassenlichamentheorie gebruiken.)

Rooster voor april en mei: het college zal in Amsterdam worden gegeven op donderdag 1 april (zaal P015A) en op woensdag 7 april (zaal P015B), en in Leiden op vrijdag 23 april en vrijdag 7 mei, in zaal WI 401. De tijden zijn steeds 10–13 u.

Opgave 66. Laat K een algebraïsch getallenlichaam zijn, en $\mathfrak{f} = \mathfrak{f}_\infty\mathfrak{f}_0$ een cykel van K. Bewijs dat elk element $\alpha \in K^*$ met $\alpha \equiv 1 \bmod^* \mathfrak{f}$ geschreven kan worden als quotiënt van twee elementen uit $1 + \mathfrak{f}_0$ die niet nul zijn en bij elke priem die $\mathfrak{f}_\infty$ deelt positief zijn.

Opgave 67. Laat K een algebraïsch getallenlichaam zijn, A zijn ring van gehelen, en $\mathfrak{f} = \mathfrak{f}_\infty\mathfrak{f}_0$ een cykel van K. Bewijs dat de groep gedefinieerd door de volgende voortbrengers en relaties isomorf is met de straalklassengroep $\mathrm{Cl}_\mathfrak{f}$: één voortbrenger $[\mathfrak{p}]$ voor elke eindige priem $\mathfrak{p}$ die $\mathfrak{f}_0$ niet deelt, en één relatie $[\mathfrak{p}_1]\cdot[\mathfrak{p}_2]\cdot\ldots\cdot[\mathfrak{p}_t] = 1$ voor elke eindige rij $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ van dergelijke priemen waarvoor er een $x \in A$ met $x \equiv 1 \bmod \mathfrak{f}_0$ bestaat die bij elke priem die $\mathfrak{f}_\infty$ deelt positief is en voldoet aan $\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_t = Ax$.

Opgave 68. Laat $K = k(t)$, waar k een eindig lichaam is en t transcendent over k is. Geef met C_K de idèle-klassengroep van K aan.

(a) Bewijs: $C_K \cong \mathbf{Z} \times \left(1 + t^{-1}k[[t^{-1}]]\right) \times k[t]\hat{}^*$; hier geeft $1 + t^{-1}k[[t^{-1}]]$ de kern van het natuurlijke groepshomomorfisme $k[[t^{-1}]]^* \to k^*$ aan, en $k[t]\hat{}$ is de projectieve limiet van de ringen $k[t]/fk[t]$, waarbij f over de verzameling monische polynomen in $k[t]$ loopt.

(b) Laten $\mathfrak{p}$ en $\mathfrak{q}$ priemen van K met restklassenlichaam k zijn, met $\mathfrak{p} \neq \mathfrak{q}$. Geef met k^+ de additieve groep van k aan. Bewijs dat de straalklassengroepen Cl_1, $\mathrm{Cl}_\mathfrak{p}$, $\mathrm{Cl}_{\mathfrak{p}^2}$ en $\mathrm{Cl}_{\mathfrak{pq}}$ respectievelijk isomorf zijn met $\mathbf{Z}$, $\mathbf{Z}$, $\mathbf{Z} \times k^+$ en $\mathbf{Z} \times k^*$.

Opgave 69. Laat K een algebraïsch getallenlichaam zijn, met idèlegroep J_K en idèle-klassengroep C_K. Op college is voor elke cykel $\mathfrak{f}$ van K een open ondergroep $W_\mathfrak{f} \subset J_K$ gedefinieerd, en als $\bar{W}_\mathfrak{f}$ het beeld van $W_\mathfrak{f}$ in C_K aangeeft is er een isomorfisme $C_K/\bar{W}_\mathfrak{f} \to \mathrm{Cl}_\mathfrak{f}$ geconstrueerd. Stel nu dat $\mathfrak{f}$ en $\mathfrak{g}$ cykels van K zijn met $\mathfrak{f}|\mathfrak{g}$. Bewijs: $\bar{W}_\mathfrak{g} \subset \bar{W}_\mathfrak{f}$, en het diagram

$$\begin{array}{ccc} C_K/\bar{W}_\mathfrak{g} & \longrightarrow & C_K/\bar{W}_\mathfrak{f} \\ \downarrow & & \downarrow \\ \mathrm{Cl}_\mathfrak{g} & \longrightarrow & \mathrm{Cl}_\mathfrak{f} \end{array}$$

is commutatief; hier zijn de verticale pijlen de geconstrueerde isomorfismen, de bovenste horizontale pijl is de natuurlijke afbeelding, en de onderste horizontale pijl is geïnduceerd door de inclusie $I_\mathfrak{g} \subset I_\mathfrak{f}$. Concludeer dat de afbeelding $\mathrm{Cl}_\mathfrak{g} \to \mathrm{Cl}_\mathfrak{f}$ surjectief is.

Opgave 70. Laat K een algebraïsch getallenlichaam zijn, met ring van gehelen A en klassengroep Cl. Laat $\mathfrak{f} = \mathfrak{f}_\infty \mathfrak{f}_0$ een cykel van K zijn. We schrijven $(A/\mathfrak{f})^* = \{\pm 1\}^r \times (A/\mathfrak{f}_0)^*$, waarbij r het aantal priemen is dat $\mathfrak{f}_\infty$ deelt. Laat zien dat er een exacte rij

$$0 \to \{\alpha \in A^* : \alpha \equiv 1 \bmod^* \mathfrak{f}\} \to A^* \to (A/\mathfrak{f})^* \to \mathrm{Cl}_\mathfrak{f} \to \mathrm{Cl} \to 0$$

van abelse groepen is, en dat $\mathrm{Cl}_\mathfrak{f}$ eindig is.

Opgave 71. Bereken in elk van de volgende gevallen de straalklassengroep $\mathrm{Cl}_\mathfrak{f}$:

$$K = \mathbf{Q}(\mathrm{i}), \quad \mathfrak{f} \in \{(2+2\mathrm{i}), (3), (4), (5)\};$$
$$K = \mathbf{Q}(\sqrt{3}), \qquad \mathfrak{f} \in \{\infty_1, \infty_1\infty_2, \infty_1\infty_2(3\sqrt{3}), (5)\},$$

waarbij ∞_1 en ∞_2 de beide oneindige priemen van $\mathbf{Q}(\sqrt{3})$ aangeven.

Opgave 72. Zij K een algebraïsch getallenlichaam. Construeer een commutatief diagram

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & A^* & \longrightarrow & K^* & \longrightarrow & P & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & W_1 & \longrightarrow & J_K & \longrightarrow & I & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \to & \bar{W}_1 & \longrightarrow & C_K & \longrightarrow & \mathrm{Cl} & \to & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

met exacte rijen en kolommen. Hier geeft A de ring van gehelen van K aan, I de groep gebroken A-idealen, $P \subset I$ de groep gebroken hoofdidealen, Cl de klassengroep, J_K en C_K de idèlegroep en de idèle-klassengroep van K, en $W_\mathfrak{f}$ (voor $\mathfrak{f} = 1$) de op college gedefinieerde ondergroep van J_K, met beeld $\bar{W}_\mathfrak{f}$ in C_K.

Opgave 73. Zij K een algebraïsch getallenlichaam. Op college definieerden we een *ideaalgroep* van K als een equivalentieklasse van paren $(\mathfrak{f}, H)$, waarbij $\mathfrak{f}$ een cykel van K is en H een ondergroep van $\mathrm{Cl}_\mathfrak{f}$, en waarbij twee zulke paren $(\mathfrak{f}_1, H_1)$ en $(\mathfrak{f}_2, H_2)$ equivalent heten als er een derde dergelijk paar $(\mathfrak{f}, H)$ is waarbij $\mathfrak{f}$ zowel door $\mathfrak{f}_1$ als door $\mathfrak{f}_2$ deelbaar is, en waarbij H het inverse beeld van H_i onder de natuurlijke afbeelding

$\mathrm{Cl}_{\mathfrak{f}} \to \mathrm{Cl}_{\mathfrak{f}_i}$ is, voor $i = 1, 2$. Als $\mathcal{H}$ een ideaalgroep is en $\mathfrak{f}$ is een cykel, dan zeggen we dat $\mathcal{H}$ *gedefinieerd kan worden modulo* $\mathfrak{f}$ als er een ondergroep $H \subset \mathrm{Cl}_{\mathfrak{f}}$ is met $(\mathfrak{f}, H) \in \mathcal{H}$.

Stel dat $\mathcal{H}$ een ideaalgroep is. Bewijs dat er een cykel $\mathfrak{f}_{\mathcal{H}}$ van K is zodat voor iedere cykel $\mathfrak{f}$ van K het volgende geldt: $\mathcal{H}$ kan gedefinieerd worden modulo $\mathfrak{f}$ dan en slechts dan als $\mathfrak{f}_{\mathcal{H}}$ een deler is van $\mathfrak{f}$. (Deze $\mathfrak{f}_{\mathcal{H}}$ heet de *conductor* van $\mathcal{H}$.)

Opgave 74. (a) Welke cykels van $\mathbf{Q}$ komen voor als conductor van een ideaalgroep, als gedefineerd in Opgave 73?

(b) Dezelfde vraag voor $\mathbf{Q}(\mathrm{i})$.

In Opgaven 75–81 is K een algebraïsch getallenlichaam, E is een eindige uitbreiding van K, en L is een eindige Galoisuitbreiding van K die E bevat. We schrijven $G = \mathrm{Gal}(L/K)$ en $H = \mathrm{Gal}(L/E)$, en met X geven we de transitieve G-verzameling G/H aan die bij E hoort; men kan X identificeren met de verzameling lichaamshomomorfismen $E \to L$ die de identiteit op K zijn, of met de verzameling nulpunten van f in L, wanneer $E \cong_K K[t]/fK[t]$. Verder geven we met $\mathfrak{q}$ een priem van L aan, met $\mathfrak{p}$ en $\mathfrak{r}$ de beperking van $\mathfrak{q}$ tot K en E, respectievelijk, met $G_{\mathfrak{q}} \subset G$ de decompositiegroep van $\mathfrak{q}$, met $I_{\mathfrak{q}} \subset G_{\mathfrak{q}}$ de traagheidsgroep, en met $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \in G_{\mathfrak{q}}/I_{\mathfrak{q}}$ het Frobeniuselement.

Opgave 75. (a) Bewijs dat $G_{\mathfrak{q}} \cap H$ en $I_{\mathfrak{q}} \cap H$ de decompositiegroep en de traagheidsgroep van $\mathfrak{q}$ over $\mathfrak{r}$ zijn.

(b) Stel dat H normaal in G is. Bewijs dat de decompositiegroep en de traagheidsgroep van $\mathfrak{r}$ over $\mathfrak{p}$ gelijk zijn aan het beeld van $G_{\mathfrak{q}}$ en $I_{\mathfrak{q}}$ in de groep G/H ($\cong \mathrm{Gal}(E/K)$).

Opgave 76. Stel dat $\mathfrak{q}$ onvertakt is over $\mathfrak{p}$.

(a) Bewijs: $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{r}} = \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}^{f(\mathfrak{r}/\mathfrak{p})}$.

(b) Stel dat H normaal is in G. Bewijs: $\mathrm{Frob}_{\mathfrak{r}/\mathfrak{p}}$ is de beperking van $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ tot E.

Opgave 77. Stel dat $\mathfrak{q}$ onvertakt is over $\mathfrak{p}$. Bewijs dat er een bijectie is van de verzameling cykels van X onder $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ naar de verzameling priemen $\mathfrak{s}$ van E boven $\mathfrak{p}$, zodanig dat de lengte van een cykel gelijk is aan de restklassengraad $f(\mathfrak{s}/\mathfrak{p})$ van de bijbehorende priem.

Opgave 78. Bewijs dat $G_{\mathfrak{q}}/I_{\mathfrak{q}} = \langle \mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}} \rangle$ op de verzameling $I_{\mathfrak{q}}\backslash X$ van banen van X onder $I_{\mathfrak{q}}$ werkt, en dat er een bijectie is van de verzameling cykels van $I_{\mathfrak{q}}\backslash X$ onder $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ naar de verzameling priemen $\mathfrak{s}$ van E boven $\mathfrak{p}$, zodanig dat de lengte van een cykel gelijk is aan de restklassengraad $f(\mathfrak{s}/\mathfrak{p})$ van de bijbehorende priem, en zodanig

dat de cardinaliteit van elk element van die cykel (opgevat als deelverzameling van X) gelijk is aan de vertakkingsindex $e(\mathfrak{s}/\mathfrak{p})$ van de bijbehorende priem.

Opgave 79. Stel dat G isomorf is met de symmetrische groep S_5 van orde 120, dat $G_\mathfrak{q}$ orde 6 heeft, en $I_\mathfrak{q}$ orde 2.

(a) Bewijs: voor een geschikte identificatie van G met S_5 geldt dat $G_\mathfrak{q}$ is voortgebracht door de permutatie $(1\,2\,3)(4\,5)$ en $I_\mathfrak{q}$ door $(4\,5)$.

(b) Stel dat $[E : K] = 5$. Hoeveel priemen van E liggen boven $\mathfrak{p}$, en wat zijn de vertakkingsindices en restklassengraden?

(c) Stel dat $[E : K] = 15$. Hoeveel priemen van E liggen boven $\mathfrak{p}$, en wat zijn de vertakkingsindices en restklassengraden?

Opgave 80. Stel dat G isomorf is met de symmetrische groep S_4 van orde 24, en dat $\mathfrak{q}$ de *enige* priem van L boven $\mathfrak{p}$ is.

(a) Bewijs dat $\mathfrak{p}$ een 2-adische priem is (in de zin dat $2 \in \mathfrak{p}$), en bepaal $G_\mathfrak{q}$ en $I_\mathfrak{q}$ als ondergroepen van S_4. (U mag gebruiken dat een traagheidsgroep I altijd een normale p-Sylow-ondergroep S met een cyclisch quotiënt I/S heeft, waarbij p de karakteristiek van het restklassenlichaam is, een op college genoemde maar niet bewezen stelling.)

(b) Stel dat H cyclisch is van orde 4. Bepaal $e(\mathfrak{q}/\mathfrak{r})$, $f(\mathfrak{q}/\mathfrak{r})$, $e(\mathfrak{r}/\mathfrak{p})$ en $f(\mathfrak{r}/\mathfrak{p})$.

Opgave 81. Stel $\mathfrak{p}$ is eindig, en laat $\mathfrak{N}\mathfrak{p}$ het aantal elementen van het restklassenlichaam van $\mathfrak{p}$ zijn. Geef met B de ring van gehelen van L aan. Bewijs dat de volgende twee beweringen equivalent zijn: (i) er bestaat $\varphi \in G$ zodanig dat voor alle $\beta \in B$ geldt $\varphi(\beta) \equiv \beta^{\mathfrak{N}\mathfrak{p}} \bmod \mathfrak{p}B$; (ii) de priem $\mathfrak{p}$ is onvertakt in L en $\mathrm{Frob}_{\mathfrak{q}/\mathfrak{p}}$ behoort tot het centrum van G.

Opgave 82. Zij $K = \mathbf{Q}(\sqrt{-5})$ en $L = \mathbf{Q}(\sqrt{5}, \mathrm{i})$.

(a) Bewijs dat L een totaal onvertakte abelse uitbreiding van K is. (Totaal onvertakt betekent dat alle priemen onvertakt zijn.)

(b) Zij $\mathfrak{p}$ een eindige priem van K. Bewijs dat de volgende beweringen equivalent zijn: (i) $\mathfrak{p}$ is een hoofdideaal; (ii) de norm van $\mathfrak{p}$ is 1 mod 4; (iii) de norm van $\mathfrak{p}$ is 0, 1 of 4 mod 5; (iv) $\mathfrak{p}$ splitst volledig in L; (v) het Artin-symbool van $\mathfrak{p}$ in $\mathrm{Gal}(L/K)$ is triviaal.

(c) Bewijs dat het Artin-symbool een isomorfisme van de klassengroep van K naar $\mathrm{Gal}(L/K)$ definieert. (Gebruik geen klassenlichamentheorie.)

Opgave 83. Zij $K = \mathbf{Q}(\sqrt{3})$ en $L = \mathbf{Q}(\sqrt{-3}, \mathrm{i})$. Laten ∞_1 en ∞_2 de beide oneindige priemen van K zijn. Bewijs zonder klassenlichamentheorie te gebruiken dat het Artin-symbool een isomorfisme van de straalklassengroep $\mathrm{Cl}_{\infty_1\infty_2}$ naar $\mathrm{Gal}(L/K)$ induceert.

Opgave 84. Zij K een algebraïsch getallenlichaam met ring van gehelen A, en zij $\bar{W}_1$ als in Opgave 72.

(a) Bewijs dat er een exacte rij van abelse groepen

$$0 \to \hat{A}^* \to \bar{W}_1 \to (K \otimes_{\mathbf{Q}} \mathbf{R})^*/A^* \to 0$$

is. Hier geeft $\hat{A}$ de projectieve limiet van de ringen $A/\mathfrak{a}$ aan, met $\mathfrak{a}$ lopende over alle idealen $\neq 0$ van A.

(b) Bewijs dat $\bar{W}_1$ en C_K isomorf zijn met het product van een compacte groep en de additieve groep $\mathbf{R}$. (*Aanwijzing*: gebruik de eenhedenstelling van Dirichlet.)

In Opgaven 85–88 geeft $G = \langle\sigma\rangle$ een eindige cyclische groep aan, en n is de orde van G.

Opgave 85. Zij A een G-moduul.

(a) Bewijs: de orde van elk element van $H^0(G, A)$ en van elk element van $H^1(G, A)$ is eindig en deelt n.

(b) Stel dat de afbeelding $A \to A$, $x \mapsto nx$, bijectief is. Bewijs: $H^0(G, A) = H^1(G, A) = 0$.

Opgave 86. (a) Zij p een priemgetal, k een positief getal, en neem aan dat p^k een deler van n is. Laat ζ een primitieve p^k-de eenheidswortel in een lichaamsuitbreiding van $\mathbf{Q}$ zijn. Maak de additieve groep van $\mathbf{Z}[\zeta]$ tot een G-moduul door $\sigma a = \zeta \cdot a$. Bereken het Herbrand-quotiënt $Q(G, \mathbf{Z}[\zeta])$.

(b) Bepaal welke rationale getallen voorkomen als Herbrand-quotiënt $Q(G, A)$, als A over alle G-modulen loopt waarvoor $Q(G, A)$ gedefinieerd is.

Opgave 87. Zij $G_1 \subset G$ een ondergroep, A een G-moduul, en A_1 een deel-G_1-moduul van A. Neem aan dat de natuurlijke afbeelding $\bigoplus_{\tau \in G/G_1} \tau A_1 \to A$ een isomorfisme is. Bewijs: $A^G \cong A_1^{G_1}$, $H^0(G, A) \cong H^0(G_1, A_1)$ en $H^1(G, A) \cong H^1(G_1, A_1)$.

Opgave 88. Voor een G-moduul A schrijven we $A^G = A_\Delta$ en $A_G = A/A^\Delta$, met $\Delta = \sigma - 1$ als op college.

(a) Preciseer en bewijs de bewering dat A_G het grootste quotiëntmoduul van A is waarop G triviaal werkt. Laat ook zien dat A_G onafhankelijk is van de keuze van σ.

(b) Stel dat $0 \to A \to B \to C \to 0$ een exacte rij G-modulen is. Construeer groepshomomorfismen $C^G \to A_G$ en $H^0(G, C) \to A_G$ zodanig dat de rijen $0 \to A^G \to B^G \to C^G \to A_G \to B_G \to C_G \to 0$ en $H^0(G, A) \to H^0(G, B) \to H^0(G, C) \to A_G \to B_G \to C_G \to 0$ exact zijn. Hoe hangen Uw afbeeldingen van de keuze van σ af?

Opgave 89. Zij $K \subset L$ een eindige cyclische uitbreiding van algebraïsche getallenlichamen, met Galoisgroep G. Zij J_L de idèlegroep van L. Bewijs: $H^1(G, J_L) = 0$.

In Opgaven 90–94 mag U de hoofdstelling van de klassenlichamentheorie gebruiken. Met K geven we een algebraïsch getallenlichaam aan. Met h_E geven we het klassengetal van een algebraïsch getallenlichaam E aan.

Opgave 90. (a) Bewijs dat het Hilbert-klassenlichaam van $\mathbf{Q}(\sqrt{-15})$ gelijk is aan $\mathbf{Q}(\sqrt{-3}, \sqrt{5})$.

(b) Bewijs dat het Hilbert-klassenlichaam van $\mathbf{Q}(\sqrt{-23})$ gelijk is aan het ontbindingslichaam van $X^3 - X - 1$ over $\mathbf{Q}$.

Opgave 91. Bewijs: als E en F twee deellichamen van K zijn met $h_E = h_F = 1$, dan geldt $h_{E \cap F} = 1$.

Opgave 92. De *Hilbert-klassenlichamen-toren* van K is de reeks lichamen

$$K = H^{(0)}(K) \subset H^{(1)}(K) \subset H^{(2)}(K) \subset \ldots \subset H^{(i)}(K) \subset \ldots,$$

waar elke $H^{(i)}(K)$ het Hilbert-klassenlichaam van $H^{(i-1)}(K)$ is. De toren heet *eindig* als er een i is met $H^{(i+1)}(K) = H^{(i)}(K)$. Bewijs: de Hilbert-klassenlichamen-toren van K is eindig dan en slechts dan als er een eindige uitbreiding E van K is met $h_E = 1$.

Opmerking. Men kan bewijzen dat er algebraïsche getallenlichamen bestaan waarvan de Hilbert-klassenlichamen-toren niet eindig is.

Opgave 93. Zij L een eindige lichaamsuitbreiding van K.

(a) Bewijs: h_K deelt $h_L \cdot [L : K]$.

(b) Bewijs: de normafbeelding $\mathrm{Cl}_L \to \mathrm{Cl}_K$ tussen klassengroepen is de triviale afbeelding dan en slechts dan als L het Hilbert-klassenlichaam van K omvat.

Opgave 94. Zij p een priemgetal, en laat L een abelse lichaamsuitbreiding van K van graad p zijn.

(a) Zij G een p-groep, d. w. z. een eindige groep waarvan de orde een macht van p is. Laat H een ondergroep van G zijn met $H \neq G$. Bewijs dat G een normale ondergroep N heeft met $H \subset N$ en $N \neq G$.

(b) Stel dat ten hoogste één priem van K vertakt is in L. Bewijs: als h_L deelbaar is door p, dan is h_K ook deelbaar door p.

(c) Stel dat ten minste één priem van K vertakt is in L. Bewijs: als h_K deelbaar is door p, dan is h_L ook deelbaar door p.

Opgave 95. Zij k een lichaam en m een positief geheel getal zodanig dat de ondergroep $\mu = \{\zeta \in k : \zeta^m = 1\}$ van k^* orde m heeft. Geef μ de discrete topologie, en geef met G_k de absolute Galoisgroep van k aan. Bewijs dat de groep continue groepshomomorfismen $G_k \to \mu$ isomorf is met k^*/k^{*m}.

In Opgaven 96–100 mag U de hoofdstelling van de klassenlichamentheorie gebruiken.

Opgave 96. Zij K een eindige abelse uitbreiding van $\mathbf{Q}$ waarvan de discriminant van de vorm $\pm 2^n$ is, met n geheel.

(a) Bewijs: K is één van de lichamen $\mathbf{Q}$, $\mathbf{Q}(\zeta_4)$, $\mathbf{Q}(\zeta_{2^m})$, $\mathbf{Q}(\zeta_{2^m} + \zeta_{2^m}^{-1})$, $\mathbf{Q}(\zeta_{2^m} - \zeta_{2^m}^{-1})$, met $m \geq 3$ geheel; hier geeft ζ_k een primitieve k-de eenheidswortel aan.

(b) Bewijs dat het klassengetal van K oneven is.

Opgave 97. In deze opgave en de volgende nemen we $K = \mathbf{Q}(\sqrt{-3})$ en $L = K(2^{1/3})$. Zij μ_3 de ondergroep van K^* voortgebracht door $(-1 + \sqrt{-3})/2$. De unieke eindige priemen van K die over 2 en 3 liggen geven we aan met respectievelijk 2 en $\mathfrak{t}$.

(a) Bewijs: $K \subset L$ is cyclisch van graad 3, en de afbeelding $\epsilon\colon \mathrm{Gal}(L/K) \to \mu_3$ die σ op $\sigma(2^{1/3})/2^{1/3}$ afbeeldt is een groepsisomorfisme.

(b) Bewijs dat de conductor $\mathfrak{f}_{L/K}$ een deler van $2\mathfrak{t}^4$ is.

(c) Zij $\mathfrak{p}$ een eindige priem van K die $2\mathfrak{t}$ niet deelt, $\mathfrak{N}\mathfrak{p}$ zijn norm, en $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(L/K)$ zijn Frobeniussymbool. Bewijs: $\epsilon(\mathrm{Frob}_\mathfrak{p})$ is het unieke element van μ_3 dat modulo $\mathfrak{p}$ congruent is met $2^{(\mathfrak{N}\mathfrak{p}-1)/3}$.

Opgave 98. (a) Bewijs dat L het straalklassenlichaam van K modulo 6 $(= 2 \cdot \mathfrak{t}^2)$ is.

(b) Zij p een priemgetal, and zij m het aantal verschillende derdemachtswortels van $(2 \bmod p)$ in $\mathbf{F}_p$. Bewijs:

$m = 0$ dan en slechts dan als $p \equiv 1 \bmod 3$ en voor alle a, $b \in \mathbf{Z}$ geldt $p \neq a^2 + 27b^2$;

$m = 1$ dan en slechts dan als $p \not\equiv 1 \bmod 3$;

$m \neq 2$;

$m = 3$ dan en slechts dan als $p = a^2 + 27b^2$ voor zekere a, $b \in \mathbf{Z}$.

Opgave 99. Zij K een algebraïsch getallenlichaam, en x een geheel getal met $x > [K : \mathbf{Q}]$. Bewijs dat het aantal eenheidswortels in K gelijk is aan de grootste gemene deler van alle getallen van de vorm $\mathfrak{N}\mathfrak{p} - 1$, waarbij $\mathfrak{p}$ loopt over de eindige priemen van K die boven een rationale priem groter dan x liggen.

Opgave 100. Zij d een kwadraatvrij geheel getal met $d \equiv 3 \bmod 8$, $d > 3$. Bewijs dat er een lichaam van graad 3 over $\mathbf{Q}$ is met discriminant gelijk aan $-d$ of $-4d$.