**Zeitschrift:** L'Enseignement Mathématique

**Herausgeber:** Commission Internationale de l'Enseignement Mathématique

**Band:** 20 (1974)

**Heft:** 3-4: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** EXTENSIONS CUBIQUES CYCLIQUES DE Q DONT L'ANNEAU DES ENTIERS EST MONOGÈNE

**Autor:** Archinard, Gabriel

**Kapitel:** 1. Les corps modérément ramifiés

**DOI:** https://doi.org/10.5169/seals-46902

**Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

**Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

**Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

**Download PDF:** 15.07.2025

**ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch**

## Chapitre 4. — Exemples numériques

Dans ce chapitre, $m$ est le produit de $r \geqslant 1$ nombres premiers distincts et congrus à 1 modulo 3.

*Note.* En plus des critères obtenus aux chapitres 2 et 3, on utilise, pour étoffer la liste des résultats, un critère donné par Payan dans [6] (proposition 1).

Soit $m = p_1 p_2 \dots p_r$ la décomposition de $m$ en facteurs premiers. On sait que si $K/Q$ est modérément ramifiée de discriminant $m^2$ (resp. sauvagement ramifiée de discriminant $81\, m^2$), $K$ est le corps de rupture de $X^3 - 3\, m\, X - a\, m$, avec $4\, m = a^2 + 27\, b^2$ et $a \equiv 1 \pmod 3$ (resp. avec $4\, m = a^2 + 3\, b^2$, $a \equiv 1 \pmod 3$ et $b \not\equiv 0 \pmod 3$). Le critère s'énonce alors ainsi:

Pour que $O_K$ soit monogène, il faut $a^{\frac{p_i - 1}{3}} \equiv 1 \pmod{p_i}$ pour $i = 2, 3, \dots r$ si $K/Q$ est modérément ramifiée et $(3a)^{\frac{p_i - 1}{3}} \equiv 1 \pmod{p_i}$ pour $i = 1, 2, \dots r$ si $K/Q$ est sauvagement ramifiée.

### 1. Les corps modérément ramifiés

Parmi les 4 entiers canoniques unitaires équivalents engendrant un corps modérément ramifié, on choisit l'entier canonique unitaire positif $\alpha = a_1 j + a_2 j^2$ (donc avec $a_1 \equiv a_2 \equiv -1 \pmod 3$) tel que $|a_1| > |a_2|$. On associe ainsi à chaque corps modérément ramifié un entier canonique unique $\alpha$ et réciproquement.

Si $\alpha = (a+1)\, j - a\, j^2$ (avec $a \equiv 1 \pmod 3$), on a $m = 3\, a^2 + 3\, a + 1$, et l'équation (3.10) admet, pour cette valeur de $m$, la solution $X = 9\, a + 3$ et $Y = 3$, $X$ étant congru à 12 (mod 27). Le nombre $\theta$, construit avec $(\beta, 0)$, où $\beta = (3a+2)\, j + (3a+1)\, j^2$, engendre un corps dont l'anneau des entiers est $Z\,[\theta]$ (théorème 3.4).

Comme $\dfrac{\beta'^2 \beta}{\alpha^2 \alpha'} = (j^2 - j)^3$, $\alpha$ engendre aussi le corps $Q\,(\theta)$. On dit, dans ce cas, que $O_K$ est presque trivialement monogène. Le polynôme irréductible de $\theta$ est $X^3 - mX + \dfrac{m}{3}(2a+1)$.

*Remarque 4.1* Si $O_K$ est trivialement (resp. presque trivialement) monogène (définition 3.1), on a $4m = a^2 + 27$ (resp. $4m = 1+27b^2$) et inversement. Ces cas sont signalés dans [6].

Pour chaque nombre $m < 2000$, on a calculé les entiers canoniques associés aux $2^{r-1}$ corps modérément ramifiés de discriminants $m^2$ (cf. corollaire 1.5).

Si pour un nombre $m$, l'un de ces entiers canoniques ne satisfait pas l'une des conditions permettant de dire que l'anneau des entiers du corps qu'il engendre admet 2 comme diviseur commun des indices (propriété 2.2), ou qu'il est trivialement ou presque trivialement monogène, on a cherché les solutions $(X, Y)$ de l'équation (3.10), avec $X > 0$ et $0 < Y < 300\,000$ pour $m < 853$ et $0 < Y < 30000$ pour $853 < m < 2000$. Pour chaque solution obtenue, on a calculé le polynôme irréductible du nombre $\varphi$ construit avec $(\beta, S)$, où $\beta = \dfrac{X+3}{Y} j + \dfrac{X}{Y} j^2$ et où $S = \pm 1$ et $S \equiv -XY \pmod 3$ si $X \not\equiv 0 \pmod 3$ et où $S = 0$ si $X \equiv 0 \pmod 3$; $\varphi$ est donc un générateur de l'anneau des entiers de $Q(\varphi)$. On a, ensuite, cherché le générateur canonique $\alpha$ du corps $Q(\varphi)$.

Les résultats sont les suivants:

| $m$ | $X$ | $Y$ | Irr $(\varphi)$ | $\alpha$ |
|---|---|---|---|---|
| 241 | 286 | 7 | $X^3+X^2-562X+4945$ | $-16j-j^2$ |
| 373 | 1598 | 19 | $X^3-X^2-2362X+44981$ | $17j-4j^2$ |
| 379 | 911 | 13 | $X^3-X^2-1642X+26165$ | $-22j-7j^2$ |
| 463 | 397 | 7 | $X^3+X^2-1080X+13307$ | $-22j-j^2$ |
| 751 | 1283 | 13 | $X^3-X^2-3254X+72541$ | $-31j-10j^2$ |
| 1159 | 629 | 7 | $X^3-X^2-2704X+55031$ | $35j+2j^2$ |
| 1213 | 7837 | 37 | $X^3+X^2-14960X+699317$ | $-28j+11j^2$ |
| 1321 | 506370 | 579 | $X^3-254953X+49549389$ | $-40j-31j^2$ |
| 1381 | 12745 | 49 | $X^3+X^2-22556X+1296401$ | $35j-4j^2$ |
| 1603 | 740 | 7 | $X^3-X^2-3740X+89293$ | $41j+2j^2$ |

Si $m$ est un nombre premier, il n'y a qu'un corps de discriminant $m^2$ et $\alpha$ est défini par $m$. C'est le cas pour tous les nombres $m$ de ce tableau sauf pour $1159 = 19 \cdot 61$ et $1603 = 7 \cdot 229$.

Les 2 corps de discriminants $1159^2$ sont engendrés respectivement par $-37j - 7j^2$ et $35j + 2j^2$. Le corps engendré par $-37j - 7j^2$ ayant 2 comme diviseur commun des indices, c'est le corps engendré par $35j + 2j^2$ dont l'anneau des entiers est monogène, de générateur $\varphi$.

Les 2 corps de discriminants $1603^2$ sont engendrés respectivement par $\alpha = 41j + 2j^2$ et $-46j - 19j^2$. Or $\varphi$ est construit avec $\beta = \frac{743}{7}j + \frac{740}{7}j^2$ et on a $\frac{\beta^2\beta'}{\alpha^2\alpha'} = (-2j-3j^2)^3$; c'est donc le corps engendré par $\alpha$ dont l'anneau des entiers est monogène de générateur $\varphi$ (théorème 1.2).

On donne dans le tableau suivant, pour chaque corps de discriminant $< 1000^2$, la racine carrée du discriminant, les valeurs $a_1$ et $a_2$ ($a_1 j + a_2 j^2$ étant l'entier canonique qui engendre le corps) et, si possible, la nature de son anneau des entiers: triv. mon. signifie que l'anneau est trivialement monogène, p. tr. mon. qu'il est presque trivialement monogène, 2 d. c. i. que 2 est diviseur commun des indices (l'anneau n'est donc pas monogène) et, si pour d'autres corps, le critère de Payan (cf. note en début de chapitre) permet d'affirmer que l'anneau n'est pas monogène, on donne la valeur de $a$ correspondante ($4m = a^2+27b^2$). La correspondance entre $\alpha = a_1 j + a_2 j^2$ et $a$ se fait en comparant le polynôme du nombre construit avec $(3\alpha, 0)$ (formule 1.4) et le polynôme $X^3 - 3mX - am$.

Pour 34 des 128 corps de ce tableau, les méthodes utilisées n'ont pas permis de déterminer la nature de l'anneau, si ce n'est que cet anneau n'est ni trivialement ni presque trivialement monogène et que 2 n'est pas d. c. i.

| $m$ | $a_1, a_2$ | Anneau | $m$ | $a_1, a_2$ | Anneau |
|---|---|---|---|---|---|
| 7 | 2, −1 | triv. mon. | 157 | −13, −1 | 2 d. c. i. |
| 13 | −4, −1 | triv. mon. | 163 | 14, 11 | triv. mon. |
| 19 | 5, 2 | triv. mon. | 181 | 11, −4 | ? |
| 31 | 5, −1 | 2 d. c. i. | 193 | −16, −7 | ? |
| 37 | −7, −4 | triv. mon. | 199 | −13, 2 | ? |
| 43 | −7, −1 | 2 d. c. i. | 211 | 14, −1 | ? |
| 61 | 5, −4 | p. tr. mon. | 217=7·31 | −16, −13 | triv. mon. |
| 67 | −7, 2 | ? | 217 | 17, 8 | $a=25$ |
| 73 | 8, −1 | ? | 223 | 17, 11 | 2 d. c. i. |
| 79 | −10, −7 | triv. mon. | 229 | 17, 5 | 2 d. c. i. |
| 91=7·13 | 11, 5 | 2 d. c. i. | 241 | −16, −1 | monogène |
| 91 | −10, −1 | $a=-11$ | 247=13·19 | 17, 14 | triv. mon. |
| 97 | 11, 8 | triv. mon. | 247 | 11, −7 | 2 d. c. i. |
| 103 | 11, 2 | ? | 259=7·37 | −13, 5 | 2 d. c. i. |
| 109 | −7, 5 | 2 d. c. i. | 259 | 17, 2 | $a=19$ |
| 127 | −13, −7 | 2 d. c. i. | 271 | −19, −10 | ? |
| 133=7·19 | 11, −1 | 2 d. c. i. | 277 | −19, −7 | 2 d. c. i. |
| 133 | −13, −4 | $a=-17$ | 283 | −19, −13 | 2 d. c. i. |
| 139 | −13, −10 | triv. mon. | 301=7·43 | 20, 11 | $a=31$ |
| 151 | 14, 5 | ? | 301 | −19, −4 | $a=-23$ |

| $m$ | $a_1, a_2$ | Anneau | $m$ | $a_1, a_2$ | Anneau |
|---|---|---|---|---|---|
| 307 | 17, −1 | 2 d. c. i. | 661 | 29, 20 | ? |
| 313 | −19, −16 | triv. mon. | 673 | 29, 8 | ? |
| 331 | 11, −10 | p. tr. mon. | 679 = 7·97 | 17, −13 | 2 d. c. i. |
| 337 | −13, 8 | ? | 679 | −25, 2 | $a = -23$ |
| 349 | 20, 17 | triv. mon. | 691 | −19, 11 | 2 d. c. i. |
| 367 | −22, −13 | ? | 703 = 19·37 | 29, 23 | 2 d. c. i. |
| 373 | 17, −4 | monogène | 703 | 26, −1 | $a = 25$ |
| 379 | −22, −7 | monogène | 709 | −28, −25 | triv. mon. |
| 397 | 23, 11 | 2 d. c. i. | 721 = 7·103 | 29, 5 | 2 d. c. i. |
| 403 = 13·31 | 23, 14 | $a = 37$ | 721 | −31, −16 | $a = -47$ |
| 403 | −19, 2 | $a = -17$ | 727 | −31, −13 | 2 d. c. i. |
| 409 | 23, 8 | ? | 733 | −31, −19 | 2 d. c. i. |
| 421 | 20, −1 | ? | 739 | 23, −7 | 2 d. c. i. |
| 427 = 7·61 | −22, −19 | triv. mon. | 751 | −31, −10 | monogène |
| 427 | 23, 17 | 2 d. c. i. | 757 | −28, −1 | ? |
| 433 | −13, 11 | 2 d. c. i. | 763 = 7·109 | 29, 26 | triv. mon. |
| 439 | 23, 5 | 2 d. c. i. | 763 | −31, −22 | $a = -53$ |
| 457 | 17, −7 | 2 d. c. i. | 769 | 32, 17 | ? |
| 463 | −22, −1 | monogène | 787 | 29, 2 | ? |
| 469 = 7·67 | 23, 20 | triv. mon. | 793 = 13·61 | −31, −7 | 2 d. c. i. |
| 469 | −25, −13 | 2 d. c. i. | 793 | 32, 11 | $a = 43$ |
| 481 = 13·37 | −25, −16 | $a = -41$ | 811 | −31, −25 | 2 d. c. i. |
| 481 = 13·37 | −19, 5 | 2 d. c. i. | 817 = 19·43 | 17, −16 | p. tr. mon. |
| 487 | 23, 2 | ? | 817 | 32, 23 | $a = 55$ |
| 499 | −25, −7 | 2 d. c. i. | 823 | −19, 14 | ? |
| 511 = 7·73 | 26, 11 | $a = 37$ | 829 | 20, −13 | ? |
| 511 | −25, −19 | 2 d. c. i. | 853 | −31, −4 | ? |
| 523 | 26, 17 | ? | 859 | 23, −10 | ? |
| 541 | −25, −4 | ? | 871 = 13·67 | 29, −1 | 2 d. c. i. |
| 547 | 14, −13 | p. tr. mon. | 871 | −34, −19 | ? |
| 553 = 7·79 | 23, −1 | 2 d. c. i. | 877 | −31, −28 | triv. mon. |
| 553 | −16, 11 | $a = -5$ | 883 | −34, −13 | ? |
| 559 = 13·43 | −25, −22 | triv. mon. | 889 = 7·127 | 32, 5 | $a = 37$ |
| 559 | 17, −10 | $a = 7$ | 889 | −25, 8 | $a = -17$ |
| 571 | 26, 5 | ? | 907 | 26, −7 | ? |
| 577 | −19, 8 | ? | 919 | 35, 17 | 2 d. c. i. |
| 589 = 19·31 | 20, −7 | $a = 13$ | 937 | 32, 29 | triv. mon. |
| 589 | −28, −13 | $a = -41$ | 949 = 13·73 | −28, 5 | $a = -23$ |
| 601 | −25, −1 | 2 d. c. i. | 949 | 35, 23 | 2 d. c. i. |
| 607 | 26, 23 | triv. mon. | 967 | −34, −7 | ? |
| 613 | −28, −19 | ? | 973 = 7·139 | 29, −4 | $a = 25$ |
| 619 | −22, 5 | ? | 973 | −19, 17 | 2 d. c. i. |
| 631 | 29, 14 | ? | 991 | 35, 26 | ? |
| 643 | 29, 11 | 2 d. c. i. | 997 | 23, −13 | 2 d. c. i. |