

Publications de Roland GILLARD (2010)

- [1] *Sur le problème du plongement des extensions galoisiennes.* C. R. Acad. Sci., Paris, Ser. A 274, 1436-1438 (1972).
- [2] *Sur le problème de plongement.* Semin. Delange-Pisot-Poitou, 14e année 1972/73, Théorie des Nombres, Fasc. 1, 2, Exposé G11, 5 p. (1973).
- [3] *Exemples de plongements d'extensions galoisiennes.* Bull. Soc. Math. France, Suppl., Mem. No.37, 87-90 (1974).
- [4] *Plongement d'une extension d'ordre p ou p^2 dans une surextension non abélienne d'ordre p^3 .* J. reine angew. Math. 268/269, 418-426 (1974).
- [5] *Remarques sur certaines extensions prodiedrales de corps de nombres.* C. R. Acad. Sci., Paris, Ser. A 282, 13-15 (1976).
- [6] *Sur le groupe des classes des extensions abéliennes réelles.* Semin. Delange-Pisot-Poitou, 18e Année 1976/77, Théor. des Nombres, Fasc. 1, Exposé 10, 6 p. (1977).
- [7] *\mathbb{Z}_l -extensions, fonctions L ℓ -adiques et unités cyclotomiques.* Semin. Théor. Nombres 1976-1977, Univ. Bordeaux, Exposé No.24, 19 p. (1977).
- [8] *Unités cyclotomiques, unités semi-locales et \mathbb{Z}_ℓ -extensions.* Ann. Inst. Fourier 29, No.1, 49-79 (1979).
- [9] *Formulations de la conjecture de Leopoldt et étude d'une condition suffisante.* Abh. Math. Semin. Univ. Hamb. 48, 125-138 (1979).
- [10] *Unités cyclotomiques, unités semilocales et \mathbb{Z}_ℓ -extensions. II.* Ann. Inst. Fourier 29, No.4, 1-15 (1979).
- [11] *Remarques sur les unités cyclotomiques et les unités elliptiques.* J. Number Theory 11, 21-48 (1979).
- [12] *Unités elliptiques et unités cyclotomiques.* Math. Ann. 243, 181-189 (1979).
- [13] *Groupes d'unités elliptiques.* en coll. avec Robert, Gilles, Bull. Soc. Math. Fr. 107, 305-317 (1979).
- [14] *Unités elliptiques et fonctions L p -adiques.* Compos. Math. 42, 57-88 (1980).
- [15] *Unités elliptiques et unités de Minkowski.* J. Math. Soc. Japan 32, 697-701 (1980).
- [16] *Unités elliptiques et fonctions L p -adiques.* Semin. Théor. Nombres, Univ. Grenoble I 1979-1980, Exposé No.1, 18 p. (1980).
- [17] *Unités elliptiques et fonctions L p -adiques.* Théorie des nombres, Semin. Delange-Pisot-Poitou, Paris 1979-80, Prog. Math. 12, 99-122 (1981).
- [18] *Séries d'Eisenstein et critère de Kummer.* Théorie des nombres, Semin. Delange-Pisot-Poitou, Paris 1981/82, Prog. Math. 38, 59-72 (1983).
- [19] *Unités elliptiques et groupes de classes. (Elliptic units and class groups).* En coll. avec Charkani El Hassani, Ann. Inst. Fourier 36, No.3, 29-41 (1986).

- [20] *Transformation de Mellin-Leopoldt des fonctions elliptiques.* J. Number Theory 25, 379-393 (1987).
- [21] *Fonctions L p-adiques des corps quadratiques imaginaires et de leurs extensions abéliennes.* J. Reine Angew. Math. 358, 76-91 (1985).
- [22] *Nombres de classes dans certaines extensions infinies.* Algebraic number Theory, Proc. Symp. RIMS, Kyoto/Jap. 1986, RIMS Kokyuroku 603, 60-71 (1987).
- [23] *Sur la structure galoisienne de certains groupes de classes.* Class numbers and fundamental units of algebraic number fields, Proc. Int. Conf., Katata/Jap. 1986, 99-123 (1986).
- [24] *Croissance du nombre de classes dans des \mathbb{Z}_ℓ -extensions liées aux corps quadratiques imaginaires.* Math. Ann. 279, No.3, 349-372 (1988).
- [25] *Relations monomiales entre périodes p-adiques. (Monomial relations between p-adic periods).* Invent. Math. 93, No.2, 355-381 (1988).
- [26] *Etude d'une famille modulaire de variétés abéliennes.* Number Theory, Proc. 15th Journ. Arith., Ulm/FRG 1987, Lect. Notes Math. 1380, 75-86 (1989).
- [27] *Remarques sur l'invariant mu d'Iwasawa dans le cas CM.* Pub. Sem. Th. Nbs Bordeaux., Ser. II 3, No.1, 13-26 (1991).
- [28] *A la mémoire de Kenkichi Iwasawa.* Gaz. Math., 82, 109-111 (1999).
- [29] *Groupe des obstructions pour les déformations de représentations galoisiennes.* Miyake, Katsuya (ed.), Class field theory - its centenary and prospect. Proceedings of the 7th MSJ International Research Institute of the Mathematical Society of Japan, Tokyo : Mathematical Society of Japan. Adv. Stud. Pure Math. 30, 259-285 (2001).
- [30] *Utilisation des modules de Drinfeld en cryptologie* en collaboration avec F. Leprévost, A. Pantchishkine, J.-F. Roblot, CR. Acad. Sci Paris 336, 2003, 879-882
- [31] *Construction of elliptic S-boxes,* en collaboration avec F. Leprévost, 2007, article soumis
- [32] *Adaptive Loops with kaapi on Multicore and Grid : Applications in Symmetric Cryptography* en collaboration avec V. Danjean, S. Guelton, J.-L. Roch, T. Roche, Parallel Symbolic Computation 07, 27 - 28 July 2007, 10 pages (2 colonnes), ACM
- [33] *Morpho-Cryptography : a new way for securing both information and storage media* en collaboration avec Fournel, T., Becker J.-M., Boutant Y., Sar-ssi 2007, Annecy, 12-15 juin, 4 pages
- [34] *Provable Security against impossible differential cryptanalysis , application to cs-cipher* en collaboration avec T. Roche , J.L. Roch, in Le Thi Hoai , Pascal Bouvry, Pham Dinh Tao editors, MCO, vol 14 in Communications

in Computer and Information Science,pp 597-606, Springer 2008

[35] *Remote Object Authentication : confidence model, cryptosystem and protocol* en collaboration avec Jean Lancrenon et Thierry Fournel ,Data Mining, Intrusion Detection, Information Security and Assurance, and Data Networks Security 2009 conference in Orlando, Spie vol 7344 paper nb 20