International Colloquium of
Algebra, Number Theory, Cryptography and Information Security (ANCI),
Taza, $11^{\mathbf{th}}$ – $12^{\mathbf{th}}$ November, 2016,
Faculté Polydisciplinaire de Taza (FPT),
Université Sidi Mohamed Ben Abdellah Fès (USMBA).

Abstract of the lecture to be presented by **Daniel C. Mayer** (Graz, Austria) with title

Recent Progress in Determining p-Class Field Towers

For an assigned algebraic number field $K|\mathbb{Q}$ and a prime number $p \geq 2$, the Hilbert p-class field tower $\mathrm{F}_p^\infty(K)$ is the maximal unramified pro-p extension of K. The automorphism group $G := \mathrm{Gal}(\mathrm{F}_p^\infty(K)|K)$ is briefly referred to as the p-tower group of K. Either G is an infinite topological pro-p group or a finite p-group. The derived length of G is called the length $\ell_p(K) := \mathrm{dl}(G)$ of the p-class tower of K. Several kinds of constraints restrict the possibilities for the group G.

- Firstly, a sufficiently large p-class rank $\varrho := r_p(K)$ of K forces G into being infinite, according to Golod and Shafarevich [5].
- Secondly, a theorem by Shafarevich [17] gives upper and lower bounds for the relation rank $d_2(G) := \dim_{\mathbb{F}_p} \mathrm{H}^2(G, \mathbb{F}_p)$ of G in terms of the generator rank $d_1(G) := \dim_{\mathbb{F}_p} \mathrm{H}^1(G, \mathbb{F}_p) = \varrho$ and of the torsion-free Dirichlet unit rank $r := r_1 + r_2 - 1$ of a number field K with signature (r_1, r_2).
- Finally, the capitulation kernels $\ker(j_{L|K} : \mathrm{Cl}_p(K) \to \mathrm{Cl}_p(L))$ and p-class groups $\mathrm{Cl}_p(L)$ of finite unramified p-extensions $L|K$ determine the Artin pattern $\mathrm{AP}(G) := (\tau(G), \varkappa(G))$ of G which consists of the targets $\tau(G) = (H/H')_{(G:H)<\infty}$ and kernels $\varkappa(G) = (\ker T_{G,H})_{(G:H)<\infty}$ of the Artin transfer homomorphisms $T_{G,H} : G \to H/H'$ from G to its subgroups H of finite index $(G : H)$ [15].

For a complex quadratic field $K = \mathbb{Q}(\sqrt{d})$, $d < 0$, and an odd prime $p \geq 3$, the Shafarevich theorem requires a Schur σ-group G with balanced presentation $d_2(G) = d_1(G)$. This fact enables short proofs for p-class towers of length $\ell_p(K) = 2$, recalling well-known results by Scholz and Taussky for $p = 3$ [16], and establishing new examples for $p \in \{5, 7\}$ [6, 7].

However, for 3-class towers of quadratic fields K with length $\ell_3(K) \geq 3$, the Shafarevich condition must be combined with the strategy of pattern recognition via Artin transfers, which is based on a partial order relation $\mathrm{AP}(\pi(G)) < \mathrm{AP}(G)$ for Artin patterns of parent-descendant pairs $(\pi(G), G)$ on descendant trees of finite p-groups [8].

With the aid of this technique, we were in the position to provide the first rigorous proofs of length $\ell_3(K) = 3$ for various infinite series of quadratic fields K [9, 10, 11, 12, 13, 14], partially in collaboration with M.R. Bush [4].

In contrast to quadratic base fields, the Shafarevich theorem in its published form gave rise to contradictions against recent results on bicyclic biquadratic fields $K = \mathbb{Q}(\sqrt{c}, \sqrt{d})$ containing either the third or fourth roots of unity, according to whether $c = -3$ or $c = -1$. These quartic fields were first investigated in joint work by A. Azizi, his team of collaborators, and ourselves [3, 1, 2, 11]. Fortunately, we were able to discover that the paper by Shafarevich [17] contains a fatal misprint, and we published the proof of a correction [14], which is now in perfect accordance with the joint theorems on biquadratic fields.

References

[1] A. Azizi, A. Zekhnini, M. Taous and D.C. Mayer, *Principalization of 2-class groups of type* $(2,2,2)$ *of biquadratic fields* $\mathbb{Q}\left(\sqrt{p_1p_2q},\sqrt{-1}\right)$, Int. J. Number Theory **11** (2015), no.4, 1177 – 1216, DOI 10.1142/S1793042115500645.

[2] A. Azizi, A. Zekhnini and M. Taous, *Coclass of* $\mathrm{Gal}(k_2^{(2)}|k)$ *for some fields* $k=\mathbb{Q}\left(\sqrt{p_1p_2q},\sqrt{-1}\right)$ *with 2-class groups of type* $(2,2,2)$, J. Algebra Appl. **15** (2015), no.2, DOI 10.1142/S0219498816500274.

[3] A. Azizi, M. Talbi, M. Talbi, A. Derhem and D.C. Mayer, *The group* $\mathrm{Gal}(k_3^{(2)}|k)$ *for* $k=\mathbb{Q}\left(\sqrt{-3},\sqrt{d}\right)$ *of type* $(3,3)$, Int. J. Number Theory (2016), DOI 10.1142/S1793042116501207.

[4] M.R. Bush and D.C. Mayer, 3*-class field towers of exact length* 3, J. Number Theory **147** (2015), 766–777, DOI 10.1016/j.jnt.2014.08.010.

[5] E.S. Golod and I.R. Shafarevich, *On the class field tower* (Russian), Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), 261–272. (English transl. in Amer. Math. Soc. Transl. (2) **48** (1965), 91–102.)

[6] D.C. Mayer, *The distribution of second p-class groups on coclass graphs*, 27ièmes Journées Arithmétiques, Faculty of Math. and Informatics, Univ. of Vilnius, Lithuania, presentation delivered on July 01, 2011.

[7] D.C. Mayer, *The distribution of second p-class groups on coclass graphs*, J. Théor. Nombres Bordeaux **25** (2013), no.2, 401–456, DOI 10.5802/jtnb.842.

[8] D.C. Mayer, *Periodic bifurcations in descendant trees of finite p-groups*, Adv. Pure Math. **5** (2015), no.4, 162–195, DOI 10.4236/apm.2015.54020, Special Issue on Group Theory, March 2015.

[9] D.C. Mayer, *Index-p abelianization data of p-class tower groups*, Adv. Pure Math. **5** (2015) no.5, 286–313, DOI 10.4236/apm.2015.55029, Special Issue on Number Theory and Cryptography, April 2015.

[10] D.C. Mayer, *Index-p abelianization data of p-class tower groups*, 29ièmes Journées Arithmétiques, Univ. of Debrecen, Hungary, presentation delivered on July 09, 2015.

[11] D.C. Mayer, *Periodic sequences of p-class tower groups*, J. Appl. Math. Phys. **3** (2015), no.7, 746–756, DOI 10.4236/jamp.2015.37090.

[12] D.C. Mayer, *Periodic sequences of p-class tower groups*, 1st International Conference on Groups and Algebras 2015, Shanghai, China, presentation delivered on July 21, 2015.

[13] D.C. Mayer, *New number fields with known p-class tower*, 22nd Czech and Slovak International Conference on Number Theory 2015, Liptovský Ján, Slovakia, presentation delivered on August 31, 2015.

[14] D.C. Mayer, *New number fields with known p-class tower*, Tatra Mountains Math. Publ. **64** (2015), 21–57, DOI 10.1515/tmmp-2015-0040, Special Issue on Number Theory and Cryptology ‘15.

[15] D.C. Mayer, *Artin transfer patterns on descendant trees of finite p-groups*, Adv. Pure Math. **6** (2016), no.2, 66–104, DOI 10.4236/apm.2016.62008, Special Issue on Group Theory Research, January 2016.

[16] A. Scholz und O. Taussky, *Die Hauptideale der kubischen Klassenkörper imaginär quadratischer Zahlkörper: ihre rechnerische Bestimmung und ihr Einfluß auf den Klassenkörperturm*, J. Reine Angew. Math. **171** (1934), 19–41.

[17] I.R. Shafarevich, *Extensions with prescribed ramification points* (Russian), Publ. Math., Inst. Hautes Études Sci. **18** (1964), 71–95. (English transl. by J.W.S. Cassels in Amer. Math. Soc. Transl., II. Ser., **59** (1966), 128–149.)