

## Iwasawa Theory – Past and Present

Ralph Greenberg

*Dedicated to the memory of Kenkichi Iwasawa*

Let  $F$  be a finite extension of  $\mathbb{Q}$ . Let  $p$  be a prime number. Suppose that  $F_\infty$  is a Galois extension of  $F$  and that  $\Gamma = \text{Gal}(F_\infty/F)$  is isomorphic to  $\mathbb{Z}_p$ , the additive group of  $p$ -adic integers. The nontrivial closed subgroups of  $\Gamma$  are of the form  $\Gamma_n = \Gamma^{p^n}$  for  $n \geq 0$ . They form a descending sequence and  $\Gamma/\Gamma_n$  is cyclic of order  $p^n$ . If we let  $F_n = F_\infty^{\Gamma_n}$ , then we obtain a tower of number fields

$$F = F_0 \subset F_1 \subset \cdots \subset F_n \subset \cdots$$

such that  $F_n/F$  is a cyclic extension of degree  $p^n$  and  $F_\infty = \bigcup_n F_n$ . In 1956, at the summer meeting of the American Mathematical Society in Seattle, Iwasawa gave an invited address entitled *A theorem on Abelian groups and its application to algebraic number theory*. The application which he discussed is the following now famous theorem.

**Theorem.** *Let  $p^{e_n}$  be the highest power of  $p$  dividing the class number of  $F_n$ . Then there exist integers  $\lambda, \mu$ , and  $\nu$  such that  $e_n = \lambda n + \mu p^n + \nu$  for all sufficiently large  $n$ .*

Iwasawa's proof of this theorem is based on studying the Galois group  $X = \text{Gal}(L_\infty/F_\infty)$ , where  $L_\infty = \bigcup_n L_n$  and  $L_n$  is the  $p$ -Hilbert class field of  $F_n$ . (That is,  $L_n$  is the maximal abelian  $p$ -extension of  $F_n$  which is unramified at all primes of  $F_n$ . By class field theory,  $L_n$  is a finite extension of  $F_n$  and  $[L_n:F_n] = p^{e_n}$ .) The extension  $L_\infty/F$  is Galoisian, and one has an exact sequence

$$0 \rightarrow X \rightarrow \text{Gal}(L_\infty/F) \rightarrow \Gamma \rightarrow 0.$$

Since  $X$  is a projective limit of finite abelian  $p$ -groups, we can regard  $X$  as a compact  $\mathbb{Z}_p$ -module. ( $\mathbb{Z}_p$  denotes the ring of  $p$ -adic integers.) But

---

Received November 16, 1998.

Revised May 13, 1999.