PACIFIC JOURNAL OF MATHEMATICS
Vol. 157, No. 2, 1993

EXPLICIT CONSTRUCTION OF CERTAIN SPLIT EXTENSIONS OF NUMBER FIELDS AND CONSTRUCTING CYCLIC CLASSFIELDS

S. GURAK

The problem of explicitly constructing classfields (Hilbert's Twelfth problem) is largely unresolved, except when a classfield is absolutely abelian or abelian over an imaginary quadratic number field. Here an explicit construction of certain split extensions of number fields is given, which maintains control over the primes which ramify. This naturally leads to the construction of cyclic classifields over a given number field. An algorithm is provided to obtain the minimal polynomials for the generating elements of the extension constructed. The methods employed here rely heavily on classfield theory and the properties of Lagrange resolvents and group determinants.

1. Introduction. The principal goal of this research is to obtain an explicit construction of certain split algebraic extension fields over a given number field F. The characterization of such fields is given for dihedral extensions of degree 6, 8 and 12 over Q in a previous work [**6**]. Those constructions rely on the arithmetic of quadratic fields and explicit formulas such as Cardano's. The constructions given here rely on classfield theory and the properties of Lagrange resolvents. There is a natural extension of the construction for similar extensions over function fields which will be treated in a subsequent paper.

To be more precise about the extensions we seek to construct, let Z_n denote the ring of residues modulo n, for some integer $n > 1$, with unit group Z_n^*. Consider a polynomial $p(x) = x^n + a_1 x^{n-1} + \cdots + a_0$, irreducible over F, with Galois group G of the form $V \cdot T$, where T is cyclic of order n with $T \trianglelefteq G$ and V is isomorphic to a subgroup of Z_n^* (that is, G is a semi-direct product of T by V). Let K be the splitting field of $p(x)$ so $G(K/F) = G$, and let k and R be the subfields fixed by T and V respectively. We wish to give an explicit general construction for the extension K/F (or K/k) in terms of the arithmetic of $k(\zeta)$, where $\zeta = \exp(2\pi i/n)$. Since $K = k \cdot R$, the problem of determining K primarily is one of finding explicit generators for the field R (or a conjugate field). Of course, R is generated by some root of $p(x)$, but actually finding roots of $p(x)$