APPENDIX B
SUMMARY OF GALOIS THEORY

TESTS FOR INTEGER POLYNOMIALS BEING PRIME OVER Q

- **DEGREE ≤ 3:** No zeros ↔ prime
- **PRIME OVER Z_p** → prime
- **EISENSTEIN** → prime

[p divides a_i except a_n and p^2 divides a_0]

- **TOO MANY PRIME/UNIT VALUES** → prime

[deg 4 or 5, target = 9, deg = n > 5, target = n + 3]

FIELD EXTENSIONS

$F[\alpha_1, \ldots, \alpha_k]$ = smallest field containing F and the α_i

Polynomial Extension:

F[f(x)] = $F[\alpha_1, \ldots, \alpha_k]$ where α_i's are the zeros of f(x).

Radical Extension: $F[x^n = \alpha]$ for $\alpha \in F$.

|K:F| = dim of K as vector space over F.

If $F \leq K \leq H$ then $|H:F| = |H:K|.|K:F|$

GALOIS GROUP

G(K/F) = group of automorphisms of K that fix the elements of F

If $F \leq K \leq H$ and K, H are polynomial extensions of F then $G(H/F)/G(H/K) \cong G(K/F)$.

FUNDAMENTAL THEOREM

If K is a Galois extension of F (eg a polynomial extension of number fields) there is a 1-1, order reversing correspondence (called the Galois correspondence) between the subfields of K which contain F and the subgroups of G(H/K).
Larger subgroups correspond to smaller subfields.
Smaller subfields correspond to larger subgroups.
Extensions [K:H] correspond to quotient groups.
Degree of extension = order of subgroup.
Normal extensions correspond to normal subgroups.

GALOIS GROUP OF A POLYNOMIAL EXTENSION

Let F be a field of characteristic zero and suppose that $f(x) \in F[x]$ splits in some extension, K, of F. Then $f(x)$ is soluble by radicals over F if and only if G(K/F) is a soluble group. For all $n \geq 5$ there is a prime polynomial whose Galois group is isomorphic to S_n and which is therefore not soluble by radicals.

Every finite soluble group is the Galois group of some polynomial extension of $\mathbb{Q}$. Every finite group is the Galois group of some finite extension of $\mathbb{Q}$, but it is not known whether it must be the Galois group of some polynomial extension of $\mathbb{Q}$.

GALOIS GROUPS OF FINITE FIELDS

$G(GF(p^m)/GF(p^n))$ is a cyclic group of order $m - n$ generated by the Frobenius automorphism $x \to x^p$.

Galois Group of $\mathbb{Q}[x^n = 1]$

The minimum polynomial of $\omega = e^{2\pi i/n}$ over $\mathbb{Q}$ is called the ***n*'th cyclotomic polynomial** and has degree $\varphi(n)$.
$G(\mathbb{Q}[x^n = 1]/\mathbb{Q}) \cong \mathbb{Z}_n^{\#}$, the group of units of the ring $\mathbb{Z}_n$.

RULER AND COMPASS CONSTRUCTIBILITY

A complex number α is constructible by ruler and compass if and only if $|\mathbb{Q}[\alpha]:\mathbb{Q}|$ is a power of 2. Hence a 60° angle (and most others) cannot be trisected by ruler and compass. A regular n-sided polygon is constructible if and only if $\varphi(n)$ is a power of 2.
A field extension, [K: F] is a pair of fields with $F \leq K$. They are classified as follows:

TYPES OF FIELD EXTENSIONS $F \leq K$

Type	Definition
algebraic	every element of K is a zero of some non-zero polynomial over F
separable	every element of K is a zero of some prime polynomial over F with no repeated zeros
normal	every prime polynomial over F either has no zeros in K or splits completely in H
finite	K is finite-dimensional over F

simple	$K = F[\alpha]$ for some $\alpha \in K$
polynomial	$K = F[f(x) = 0]$ for some $f(x) \in F[x]$
radical	$K = F[x^n = \alpha]$ for some $n > 0$ and $\alpha \in F$
type 1 radical	$K = F[x^n = 1]$ for some $n > 0$
type 2 radical	$K = F[x^n = \alpha]$ for some $n > 0$ and $\alpha \in F$ where F contains all the n'th roots of unity
quadratic	$K = F[f(x) = 0]$ where f(x) is a quadratic
constructible	there is a sequence of quadratic extensions which reaches K from F
soluble	there is a sequence of radical extensions which reaches K from F
algebraic	a finite-dimensional extension

ALGEBRAIC EXTENSIONS OF A FIELD