ALGEBRAIC STRUCTURES
HOMEWORK 3

Due 11 December, 2009 (in Swedish or English)

1. Let $\alpha = \sqrt{2} + \mathrm{i}\sqrt{3}$.
   (i) Show that α is algebraic over $\mathbb{Q}$.
   (ii) Find the irreducible polynomial $\mathrm{Irr}(\alpha : \mathbb{Q})$.
   (iii) Find the conjugates of α over $\mathbb{Q}$.
   (iv) What is the degree $[\mathbb{Q}(\alpha) : \mathbb{Q}]$?
   (v) Show that $\mathbb{Q}(\alpha)$ is the splitting field of $q = \mathrm{Irr}(\alpha : \mathbb{Q})$.
   (vi) Find the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha) : \mathbb{Q})$.

2. Consider the Galois field $GF(9)$.
   (i) Write addition and multiplication tables for $GF(9)$.
   (ii) Find a generator z for the multiplicative group of non-zero elements of $GF(9)$, and list its powers $z, z^2, \dots, z^8$ in order.

3. Let $F = GF(p^n)$, where p is a prime and $n \geq 1$.
   (i) F is an extension of $\mathbb{Z}_p$. Show that it is a Galois extension.
   (ii) Show that every automorphism of F fixes every $a \in \mathbb{Z}_p$; thus the group $\mathrm{Aut}(F)$ of all automorphisms of F equals the Galois group $\mathrm{Gal}(F : \mathbb{Z}_p)$.
   (iii) What is the order of the Galois group $\mathrm{Gal}(F : \mathbb{Z}_p)$?
   (iv) Show that the mapping $\varphi : a \mapsto a^p$ is an automorphism in $\mathrm{Gal}(F : \mathbb{Z}_p)$. ($\varphi$ is called the Frobenius automorphism.)
   (v) Show that φ generates $\mathrm{Gal}(F : \mathbb{Z}_p)$, which thus is a cyclic group. (*Hint:* Find the order of φ in $\mathrm{Gal}(F : \mathbb{Z}_p)$.)

Svante Janson