Math 432 homework Due Friday, August 31, 2001

1. If a field E is a finite extension of a field F, and G is a finite extension of E, prove that G is a finite extension of F and that

$$[G : F] = [G : E][E : F] \ .$$

Remark: The following interesting theorem will be proved in class:

Theorem: Any finite subgroup of the multiplicative group of a field is cyclic.

Note that this implies that the the multiplicative group F^* of a finite field is a cyclic group; generators are sometimes called primitive roots.

2. Explicitly construct a field with $q = 16$ elements and find a primitive root, with proof.

3. Same problem for $q = 27$.

4. Use the aforementioned Theorem to prove that if p is a prime congruent to 2 mod 3 then every element of $\mathbf{F}_p$ is a cube. Prove that if p is 1 mod 3 then exactly one-third of the elements OF $\mathbf{F}_p^*$ are cubes.

5. Let $F = \mathbf{F}_5[x]/(x^5 - x + 1)$. Find the inverse of $\alpha^2 + \alpha + 1$ in F, where α denotes the class of x in F.