FIELD THEORY HOMEWORK SET III

JAMES CUMMINGS

You may collaborate on this homework set, but must write up your solutions by yourself. Please contact me by email if you are puzzled by something, would like a hint or believe that you have found a typo.

(1) Find a basis for $F = \mathbb{Q}(i, \sqrt{2})$ over $\mathbb{Q}$. Compute the group $Aut(F/\mathbb{Q})$. Find all its subgroups, and describe their fixed fields.
(2) Prove that if F is a finite field it has size p^n where p is the characteristic and $n > 0$.
(3) Show that a polynomial $f(x)$ is irreducible in $\mathbb{Z}[x]$ iff $f(x+1)$ is irreducible. Use this to show that $(x^p - 1)/(x - 1)$ is irreducible for every prime p.
(4) Find an algebraic extension of $\mathbb{Q}$ which is not of finite degree.
(5) Let p be an odd prime. Prove that -1 has a square root mod p iff $p \equiv 1$ mod 4.
(6) (Challenging) Prove that if p is an odd prime and $p \equiv 1 \mod 4$ then p is the sum of two perfect squares. Hint: use some old HW about the ring $\mathbb{Z}[i]$, think about what happens to primes of $\mathbb{Z}$ in this bigger ring.