# FIELD THEORY HOMEWORK SET III SOLUTIONS

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 $\mathbb{Q}$.

$\sqrt{2}$ has degree 2 over $\mathbb{Q}$, and since $i$ is not real it has degree two over $\mathbb{Q}(\sqrt{2})$. So we get $\{1, i, \sqrt{2}, i\sqrt{2}\}$.

Compute the group $Aut(F/\mathbb{Q})$. Find all its subgroups, and describe their fixed fields.

There are four elements. If $\rho$ fixes $i$ and maps $\sqrt{2}$ to $-\sqrt{2}$ and $\sigma$ fixes $\sqrt{2}$ and maps $i$ to $-i$, the group is $\{e, \rho, \sigma, \rho\sigma\}$ and is the non-cyclic group of order four.

Subgroups and fixed fields:

(a) $\{e\}$ has fixed field $F$.
(b) $\{\rho\}$ has fixed field $\mathbb{Q}(i)$.
(c) $\{\sigma\}$ has fixed field $\mathbb{Q}(\sqrt{2})$.
(d) $\{\rho\sigma\}$ has fixed field $\mathbb{Q}(i\sqrt{2})$.

(2) Prove that if $F$ is a finite field it has size $p^n$ where $p$ is the characteristic and $n > 0$.

Let $E$ be the characetristic subfield, it has $p$ elements. $[F : E]$ is finite, say it is $n$. So as an $E$-VS $F$ is isomorphic to $E^n$, in particular it has size $|E|^n = p^n$.

(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 $p$.

The map which takes $f$ to $f(x + 1)$ is an AM of the polynomial ring. $((x + 1)^p - 1)/x$ is irreducible by Eisenstein.

(4) Find an algebraic extension of $\mathbb{Q}$ which is not of finite degree.

Consider the subfield of $\mathbb{C}$ generated over $\mathbb{Q}$ by all elements $2^{1/n}$. It is generated by algebraic elements hence is algebraic. Also since $x^n - 2$ is irreducible, $2^{1/n}$ has degree $n$, so this extension must have infinite degree.

(5) Let $p$ be an odd prime. Prove that $-1$ has a square root mod $p$ iff $p \equiv 1$ mod 4.

By elementary number theory the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$ is cyclic with $p-1$ elements. Let $a$ be a generator. Then $a^{p-1} = 1$ so $a^{(p-1)/2} = -1$. Hence $a^{(p-1)/4}$ is a square root of $-1$.

(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.

Let $p$ be such a prime. Suppose for contradiction that $p$ is prime in $\mathbb{Z}[i]$, then since we are in a PID $\mathbb{Z}[i]/p\mathbb{Z}[i]$ is a field. But if $0 \le b < p$ with

$b^2 + 1 \equiv 0 \mod p$ there are too many square roots of $-1$ in that field, namely (the classes of) $i, -i, b, -b$.

So $p$ can't be prime, and as we saw (eesentially) in the old HW it must split as $p = (a+bi)(a-bi)$ where $a+bi$ and $a-bi$ are prime and $a^2+b^2 = p$.