KMB, October 29, 2013

M3P11 Galois Theory, Problem Sheet 3

1. (a) Say $E \subseteq F$ are fields, and $z_1, z_2, \ldots, z_n \in F$. Prove that

$$(E(z_1, z_2, \ldots, z_m))(z_{m+1}, z_{m+2}, \ldots, z_n) = E(z_1, \ldots, z_n).$$

(b) Prove that if $E \subseteq F$, and $z_1, z_2, \ldots, z_n \in F$ are all algebraic over E, then $[E(z_1, z_2, \ldots, z_n) : E]$ is finite.

2. Prove that if $K \subseteq L \subseteq M$ are fields, and L/K, M/L are both algebraic, then M/K is algebraic.

3. In Chapter 3 of the course, we showed that if $P = (x, y)$ is a constructible (with straightedge and compasses) point in $\mathbb{R}^2$, then $\mathbb{Q}(x, y)$ is a finite extension of $\mathbb{Q}$, of degree a power of 2. We did this by showing that $\mathbb{Q}(x, y) \subseteq K_N$ for some tower of fields $\mathbb{Q} = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_N$, such that $[K_{n+1} : K_n] = 2$ for all n (note that in the notation of the lectures we had $[K_{n+1} : K_n] = 1$ or 2, but we can just throw away the K_{n+1} that give degree 1 extensions).

Prove the converse! If $P = (x, y)$ and there is a tower of extensions as above, i.e. each of degree 2 over the one before, and such that x, y are both in the top field, then P is constructible.

Remark: when we've done some Galois theory we will be able to construct extensions $K/\mathbb{Q}$ of degree 4 which cannot be embedded into a tower like this; in particular Corollary 3.2 is *not* a necessary and sufficient condition for constructibility.

4. This question is a preliminary investigation of the question of constructing a regular n-gon using straightedge and compasses only.

(a) Check that if we can construct any old regular n-gon, then we can construct one with centre at the origin and one vertex on $(1, 0)$.

(b) Deduce that if we can construct a regular n-gon, then $\mathbb{Q}(\cos(2\pi/\mathrm{n}), \sin(2\pi/\mathrm{n}))$ has degree a power of 2 over $\mathbb{Q}$.

(c) Deduce that if we can construct a regular n-gon, then $\mathbb{Q}(\zeta_n)$ has degree a power of 2 over $\mathbb{Q}$, where $\zeta_n = e^{2\pi i/n}$.

(d) A *Fermat prime* is a prime of the form $p = 2^m + 1$ for $m \geq 1$. There are only five known Fermat primes, namely 3, 5, 17, 257, 65537. Maybe there are no more, but maybe there are infinitely many more – no-one knows. It *is* known that any other Fermat primes must be of the form $2^m + 1$ with m a power of 2 and $m \geq 2^{33}$. No-one seems to know whether $2^{2^{33}} + 1$ is prime or not! Why not try figuring it out on your computer?

Prove that if p is a prime which is not a Fermat prime, then it is not possible to construct a regular p-gon with straightedge and compasses only.

5. Here is a full proof of a result that I will claim/have claimed in lectures:

Proposition. If K is a field, and $G \subseteq (K^\times, \times)$ is a finite subgroup, then G is cyclic.

(a) We first do some elementary number theory. If C_n denotes the cyclic group of order n, then let $\phi(n)$ denote the number of elements of C_n that generate C_n. Recall (or prove, if you didn't know it) that the subgroups of C_n are precisely the C_d for $d \mid n$. Deduce that $\sum_{d|n} \phi(d) = n$ (hint: every element of C_n must generate *something*!).

(b) Now some elementary theory of polynomials: prove that if K is a field and $0 \neq p \in K[x]$ is a polynomial of degree $d \geq 0$, then p has at most d roots in K (hint: induct on degree).

(c) Now let G be as in the question. Say the order of G is n. We know that if $g \in G$ then the order of the element divides the order of the group, so the order of g will divide n. For $d \mid n$ let G_d denote the set of elements of G with order precisely d. Prove that if G_d is non-empty then $|G_d| = \phi(d)$ (hint: if $a \in G_d$ then show that $\langle a \rangle$ must be the d roots of $x^d - 1 = 0$).

(d) By summing over d, prove that G_d must be non-empty for all d, and in particular G_n is non-empty. Deduce the result.