KMB, November 11, 2013

M3P11 Galois Theory, Solutions to problem Sheet 3

1. (a) Set $K = E(z_1, z_2, \ldots, z_m)$. Our task is to prove that $K(z_{m+1}, \ldots, z_n) = E(z_1, \ldots, z_m)$. Now $K(z_{m+1}, \ldots, z_n)$ is the intersection of all subfields of F containing K and $z_{m+1}, \ldots, z_n$, and $E(z_1, \ldots, z_m)$ is the intersection of all subfields of F containing E and $z_1, \ldots, z_m$. So it will suffice to prove that if L is an arbitrary subfield of F, then L contains K and $z_{m+1}, \ldots, z_n$ iff L contains E and $z_1, \ldots z_n$. Because K contains E and $z_1, \ldots, z_m$, one implication is clear. For the other, all we have to do is to show that if L contains E and $z_1, \ldots, z_n$ then L contains K; but this is clear from the definition of K as the intersection of all the subfields of F containing E and $z_1, \ldots, z_m$.

(b) We from Proposition 2.4 that if z is algebraic over E then $[E(z) : E]$ is finite. The general result follows by induction on n, part (a), and the (obvious) fact that if z is algebraic over E then it's algebraic over K for any field K containing E.

2. This is slightly tricky I guess. Say $m \in M$. We need to prove that m is a root of a polynomial with coefficients in K. We know M/L is algebraic, so m is the root of a polynomial $p(x)$ with coefficients in L. Write $p(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_d x^d$. The λ_i are all in L, so they're all algebraic over K. Clearly m is algebraic over $N := K(\lambda_0, \lambda_1, \ldots, \lambda_d)$. By Q1(b) we know $[N : K]$ is finite. By Proposition 2.4 we know $[N(m) : K]$ is finite. By Proposition 2.6 m is algebraic over K, and we're home.

3. Say $r \in \mathbb{R}$ is *constructible* if we can construct the point $(r, 0)$ with straightedge and compasses only. If we can construct $(x, 0)$ and $(y, 0)$ then we can easily construct $(0, y)$ and then (x, y). So we just need to check that x and y are constructible. Firstly I claim that every rational is constructible. For clearly every integer is constructible (draw a long straight line through $(0, 0)$ and $(1, 0)$ and then use your compasses to mark off the integer points), and then by a trick with triangles every rational is constructible (to divide a given line into d equal pieces, make a triangle with one side equal to that line and another side of length d, and then slice the triangle up with parallel lines).

So it suffices to check that if $E \subseteq F \subseteq R$ are fields, every element of E is constructible, and $[F : E] = 2$, then every element of F is constructible. Because $[F : E] \neq 1$ we have $E \neq F$ so we can choose $f \in F$ such that $f \notin E$. Note that $\{1, f\}$ are E-linearly independent. However $\{1, f, f^2\}$ is a sequence of three elements in a 2-dimensional space so these elements must be E-linearly dependent; we deduce that $f^2 + af + b = 0$ for some $a, b \in E$. Completing the square and replacing f by $f + a/2$ we can reduce to the case $f^2 \in E$. Hence f is constructible (because f^2 is and you can take square roots using compasses). Now it is easy to check that if $\lambda, \mu \in E$ then $\lambda f + \mu$ is constructible; but the general element of F is of this form, so every element of F is constructible and we're done.

4. (a) If we can construct a regular n-gon somewhere in the plane then (bisect the interior angles) we can construct its centre, and hence an isosceles triangle with side length 1, two equal angles A and B, and the third angle C equal to $2\pi/n$. Setting the compasses to be the distance AB we can then use this to go around the unit circle centre the origin and construct our n-gon.

(b) $(\cos(2\pi/n), \sin(2\pi/n)$ is the coordinate of another point of this n-gon.

(c) i has degree 2 over $\mathbb{Q}(\cos(2\pi/n), \sin(2\pi/n))$ (as it is not real), so $\mathbb{Q}(\cos(2\pi/n), \sin(2\pi/n), i)$ has degree a power of 2 over $\mathbb{Q}$ by the tower law. It also contains $\zeta_n = \cos(2\pi/n) + i\sin(2\pi/n)$ and the result follows again by the tower law.

(d) What is the min poly of ζ_p, for p prime? Well certainly $\zeta_p \neq 1$ but $(\zeta_p)^p = 1$, so ζ_p is a zero of the function $(x^p - 1)/(x - 1)$ which is actually the polynomial $1 + x + \cdots + x^{p-1}$. We showed in lectures (as an application of Eisenstein) that this polynomial was irreducible! Hence $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$ and in particular if $p - 1$ isn't a power of 2 then we cannot construct a regular p-gon. In particular, although we might be able to (and can) construct a regular pentagon, we can't construct a regular heptagon.

5.

(a) If we regard C_n as the set $\{0, 1, 2, \ldots, n-1\}$ under addition, then the reason any subgroup is cyclic is that it is generated by the smallest non-zero element in the subgroup, and the reason that there's only one cyclic subgroup of order d in C_n if $d \mid n$ is that there are only d elements of order dividing d in C_n (namely the multiples of n/d).

The reason $\sum_{d|n} \phi(d) = n$ is that every element of C_n generates a cyclic subgroup of some order $d \mid n$ so is counted once (when computing $\phi(d)$).

(b) If p has no roots then done; if p has a root a then $p(x) = (x-a)q(x) + r(x)$ by Euclid, and r is a constant polynomial. Evaluating at $x = a$ gives $r = 0$. Comparing degree gives that the degree of $q(x)$ is one less than the degree of $p(x)$. Finally if $b \neq a$ is a root of $p(x)$ then $(b-a)q(b) = 0$ and hence $q(b) = 0$, so now we're done by induction.

(c) If G_d is non-empty then choose $a \in G_d$. Then $\{1, a, a^2, \ldots, a^{d-1}\}$ is a subset of G of size d, and all of these elements are dth roots of 1, so by (a) we must have that there are precisely d roots of $x^d - 1 = 0$ in K, and that these are precisely $\{1, a, a^2, \ldots, a^{d-1}\}$. In particular we must have $G_d \subseteq \{1, a, a^2, \ldots, a^{d-1}\}$ and now G_d is the elements of order precisely d in this group, and there are by definition $\phi(d)$ of these.

(d) The G_d partition G, so we have $n = \sum_{d|n} |G_d| \leq \sum_{d|n} \phi(d) = n$. So equality must hold in that middle $\leq$, so $|G_d| = \phi(d) > 0$ for all d and in particular G_n is non-empty. But if $a \in G_n$ has order exactly n, then $\langle a \rangle$ is a subgroup of G of size n and hence must equal G.