KMB, 17/11/15

## M345P11 Galois Theory, Solutions to problem Sheet 3

**1.** (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 (drawing lines from the centre $C$ and using the compass) 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 $\mathbf{Q}(\cos(2\pi/n), \sin(2\pi/n))$ (as it is not real), so $\mathbf{Q}(\cos(2\pi/n), \sin(2\pi/n), i)$ has degree a power of 2 over $\mathbf{Q}$ 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 $\zeta_p$, for $p$ prime? Well certainly $\zeta_p \neq 1$ but $(\zeta_p)^p = 1$, so $\zeta_p$ 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 $[\mathbf{Q}(\zeta_p) : \mathbf{Q}] = p-1$ by 2.3 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.

**2.**

(a) Well $z^5 = 1$ and $z \neq 1$ so $z$ is a root of $x^5 - 1 = (x-1)(1+x+x^2+x^3+x^4)$ and not a root of $(x-1)$ so it must be a root of the other factor.

(b) $x^2 = z^2+2+z^{-2}$ so $x^2+x-1 = z^{-2}+z^{-1}+1+z+z^2 = z^{-2}(1+z+z^2+z^3+z^4) = 0$.

(c) $z = \cos(72^\circ) + i\sin(72^\circ)$ and $z^{-1} = \cos(72^\circ) - i\sin(72^\circ)$, so $x = 2\cos(72^\circ)$. We deduce that if $c = x/2 = \cos(72^\circ)$ then $(2c)^2 + (2c) - 1 = 0$ and hence (completing the square because I'm old-fashioned like that) $(4c+1)^2 = 5$, so $c = \frac{-1\pm\sqrt{5}}{4}$, and clearly $c > 0$ so done.

(d) Construct a circle centre the origin radius 1, and then its diameter has length 2. Draw a right angle at the end of this length 2 line and then use the compass to mark a point one unit up; the hypotenuse of the resulting right-angled triangle is $\sqrt{1^2+2^2} = \sqrt{5}$. Use the compass to mark a point a distance one from an end of the circumference; the distance to the other end is now $\sqrt{5}-1$. Now bisect this length twice and you have made $\cos(72^\circ)$; plot $(\cos(72^\circ), 0)$ and draw a vertical line up to hit the unit circle at $(\cos(72^\circ), \sin(72^\circ))$, and now it's easy.

For bonus points: now do a regular 17-gon. Actually, if I were you I would wait until we've done some Galois theory before you start on this.

**3.**

(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 $d$th 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 $G$.

Well done if you got through this question. The proof can be simplified if you know that any finite abelian group is a direct product of cyclic groups, because then (if you know what you're doing) it's not hard to show that if $G$ is an abelian group which is not cyclic then there exists some $n$ such that there are more than $n$ solutions to $g^n = 1$, and this contradicts (b) immediately. But proving that a finite abelian group is a direct product of cyclic groups is a little tricky, whereas the above argument is completely self-contained.

**4.** (a) Well $z^3 = \omega^3\alpha^3 = 1 \times 2 = 2$ so $z$ is a root of $x^3 - 2 = 0$, which is irreducible over $\mathbf{Q}$ by Eisenstein, so $x^3 - 2$ is the min poly of $z$, and by 2.3 this means $[\mathbf{Q}(z) : \mathbf{Q}] = 3$. Although we don't need it, we can note that in fact $\mathbf{Q}(z)$ is isomorphic to, but not equal to, $\mathbf{Q}(\alpha)$, as an abstract field.

(b) We know $\omega^3 = 1$ but $\omega \neq 1$ so $\omega$ is a root of $(x^3 - 1)/(x - 1) = x^2 + x + 1$. This polynomial is irreducible as it has no rational (because no real) roots, so $[\mathbf{Q}(\omega) : \mathbf{Q}] = 2$. Note also while we're here that solving the quadratic gives $\omega = \frac{-1+i\sqrt{3}}{2}$ (plus sign because the imaginary part of $\omega$ is positive; the other root is $\omega^2$).

(c) We have $\alpha \in \mathbf{R}$. Furthermore $\overline{\omega}$ is another cube root of 1 so it must be $\omega^2$. Hence $\overline{z} = \overline{\omega\alpha} = \omega^2\alpha = \omega z$. In particular if $\overline{z} \in \mathbf{Q}(z)$ then $\omega = \overline{z}/z \in \mathbf{Q}(z)$. This means $\mathbf{Q}(\omega) \subseteq \mathbf{Q}(z)$, and by the first two parts and the tower law we deduce $[\mathbf{Q}(z) : \mathbf{Q}(\omega)] = \frac{3}{2}$, which is nonsense because the dimension of a (finite-dimensional) vector space is a whole number.

(d) If $x \in \mathbf{Q}(z)$ then $\overline{z} = -z + 2x \in \mathbf{Q}(z)$, contradiction. So $x$ is not in. If $i \in \mathbf{Q}(z)$ then $\mathbf{Q}(i) \subseteq \mathbf{Q}(z)$ and this contradicts the tower law like in part(c). Finally because the imaginary part of $\omega$ is $\sqrt{3}/2$ we see $y = \alpha\sqrt{3}/2$, so if $y \in \mathbf{Q}(\omega)$ then $y^3 = 3\alpha^3/8\sqrt{3} = 3/4\sqrt{3} \in \mathbf{Q}(z)$, implying $\sqrt{3} \in \mathbf{Q}(z)$ which again contradicts the tower law.