AC, 21/11/16

M345P11 Galois Theory, Solutions to problem Sheet 2

1.

(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.

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.

2. (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 what we did in class 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 ω 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 ω is positive; the other root is ω^2).

(c) We have $\alpha \in \mathbf{R}$. Furthermore $\overline{\omega}$ is another cube root of 1 so it must be ω^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 ω 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.

3. In the language of rings, the argument goes like this: the kernel is an ideal, and if it is non-zero then it contains an invertible element (as every non-zero element of a field is invertible) and hence contains 1; but 1 maps to 1 and hence cannot be in the kernel.

Without this language, the argument goes something like this. Say $\phi : K \to L$ is a homomorphism of fields. By definition $\phi(1) = 1$. Say $\phi(t) = 0$ for some $t \neq 0$. Then $1\phi(1) = \phi(t)\phi(1/t) = 0.\phi(1/t)$. But in any field we have $0.x = 0$ for all x, as $0 + 0 = 0$ so $0.x + 0.x = (0 + 0).x = 0.x$ and cancelling $0.x$ in the additive group of K we deduce $0.x = 0$. This is a contradiction.

4. I showed in class that F was a field near (the point was that if $\alpha, \beta \in F$ then $E(\alpha, \beta)$ is finite over E by the tower law, so $E(\alpha+\beta)$ is finite over E, and hence $\alpha+\beta$ is algebraic; now repeat for $-$, $\times$ and division). Next we need to check that any non-constant polynomial $p(x) \in F[x]$ has a root in F. Because K is algebraically closed, $p(x)$ certainly has a root in K. This root α generates a finite extension $F(\alpha)$ of F. Now $F(\alpha)$ is algebraic over F (as it's finite), and F is algebraic over E (by definition), and hence $F(\alpha)$ is algebraic over E, by the result right at the end of section 2; hence α is algebraic over E, and hence in F!

Note also that F is normal over E, because any polynomial in $E[x]$ has all its roots in F.

5.

(a) We want to show that K/F is normal so let $a \in K$. By assumption a is algebraic over F so let $f \in F[X]$ be the minimal polynomial of a over F. We want to show that f splits completely in $K[x]$. Now a is algebraic over E too and denote by $g \in E[X]$ the minimal polynomial of a over E. Note that $g(a) = 0$ in K, therefore $f|g$ in $F[X]$. We are assuming that K/E is normal, therefore g splits completely in $K[X]$ but then its factor f also splits completey in $k[X]$.

(b) First note that if $\alpha = 2^{1/3}$ then K is the splitting field of $x^3 - 2$ over $\mathbf{Q}$; indeed the splitting field is by definition $\mathbf{Q}(\alpha, \omega\alpha, \omega^2\alpha)$ (as these are the roots), and this field must be $\mathbf{Q}(\alpha, \omega)$ because each of the generators of one field can be easily checked to be in the other.

We immediately deduce that K/E and K/F are normal because (both are the splitting field of $X^3 - 2$, seen as a polynomial in either $E[X]$ or $F[X]$. We can also use (a) to deduce normality of K/F from normality of K/E). However F/E is not normal, because $x^3 - 2$ is irreducible over E and has one, but not all, roots in F.

(c) Let's first compute some degrees. We know the min poly of $\sqrt{2}$ over $\mathbf{Q}$ has degree 2, so $[F : E] = 2$. Also the min poly of $2^{1/4}$ over $\mathbf{Q}$ must be $x^4 - 2$ (because this poly is irred by Eisenstein), and hence $[K : E] = 4$. By the tower law we deduce $[K : F] = 2$ (and hence that $x^2 - \sqrt{2}$ must be the min poly of $2^{1/4}$ over F, but we don't need this). We could use Q7 to deduce that K/F and F/E are normal, but we could also see it directly: F is the splitting field of $x^2 - 2$ over E and K is the splitting field of $x^2 - \sqrt{2}$ over F, so they're both normal. However $x^4 - 2$ is irreducible over E and has one root in K (in fact two roots in K) but not all its roots (as two are not real, whereas $K \subseteq \mathbf{R}$ so K/E is not normal.

(d) If H is normal in G then $g^{-1}Hg = H$ for all $g \in H$, so trivially $g^{-1}Hg = H$ for all $g \in K$, so H is normal in K.

Examples: $H = \{1\} \subseteq K = \langle (1\,2) \rangle \subseteq S_3$ for the first, and $H = \langle \sigma \rangle \subseteq K = \langle \sigma, \rho^2 \rangle \subseteq G = D_8$ for the second, with $D_8 = \langle \rho, \sigma \rangle$ the dihedral group generated by a rotation ρ of order 4 and a reflection σ of order 2.

6.

(i) $\mathbf{Q}(\sqrt{6})$ is the splitting field of the polynomial $x^2 - 6$ and is hence normal over $\mathbf{Q}$.

(ii) $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2 - 2)(x^2 - 3)$ and is hence normal.

(iii) $\mathbf{Q}(7^{1/3})$ contains one, but not all, roots of the irreducible polynomial $x^3 - 7$ (because the other roots are not even real), so it is not normal over $\mathbf{Q}$.

(iv) $\mathbf{Q}(7^{1/3}, e^{2\pi i/3})$ is the splitting field of $x^3 - 7$ and is hence normal.

(v) $\mathbf{Q}(\sqrt{1+\sqrt{7}})$ is not normal over $\mathbf{Q}$. Here's why. If $\alpha = \sqrt{1+\sqrt{7}}$ then $\alpha^2 - 1 = \sqrt{7}$, so $(\alpha^2 - 1)^2 = 7$ and α is hence a root of $x^4 - 2x^2 - 6 = 0$. We can spot the four complex roots of this polynomial; they are $\pm\sqrt{1 \pm \sqrt{7}}$ (just substitute in to see that all of these are roots). Two of these numbers are real and two pure imaginary; in particular not all of them are in $\mathbf{Q}(\sqrt{1+\sqrt{7}})$, which is a subfield of the reals. However, $x^4 - 2x^2 - 6 = 0$ is irreducible over $\mathbf{Q}$ by Eisenstein, so this polynomial has some but not all roots in $\mathbf{Q}(\sqrt{1+\sqrt{7}})$ which is hence not normal over $\mathbf{Q}$.

(vi) $\mathbf{Q}(\sqrt{2+\sqrt{2}})$ is normal over $\mathbf{Q}$, despite the formal similarity with part (v). If $\alpha = \sqrt{2+\sqrt{2}}$ then (as in the previous question) we see $(\alpha^2 - 2)^2 = 2$ and hence α is

a root of $x^4 - 4x^2 + 2 = 0$. This polynomial is irreducible by Eisenstein, but in this case $\mathbf{Q}(\sqrt{2+\sqrt{2}})$ is actually its splitting field. For two of its roots are $\pm\alpha$ and the other two are $\pm\sqrt{2-\sqrt{2}}$ and if $\beta = \sqrt{2-\sqrt{2}}$ then we see $\alpha\beta = \sqrt{2} = \alpha^2 - 2$, and hence $\beta = (\alpha^2 - 2)/\alpha \in \mathbf{Q}(\alpha)$! So the extension is a splitting field and hence normal.

7. (a) If $\lambda \in F \backslash E$ then $1, \lambda$ is a basis for F over E (extending the linearly independent set $\{1\}$ to a basis) and hence $\lambda^2 = a\lambda + b$ for some $a, b \in E$. The roots of $x^2 - ax - b = 0$ are hence λ and $a - \lambda$, and neither of these are in E, so $x^2 - ax - b$ is irreducible over E and its splitting field is F, which is hence normal over E.

(b) If H is an index 2 subgroup of G then this means that G is the disjoint union of H and Ht for any $t \notin H$. Taking inverses we see that G is also the disjoint union of H and $t^{-1}H$ for any $t \notin H$, and we conclude that if X is the elements of G that aren't in H then $X = tH = Ht$ for any $t \notin H$ (note that for $t \in G$, $t \in H$ iff $t^{-1} \in H$). Now for $g \in G$ let's consider what $g^{-1}Hg$ can be. If $g \in H$ then $g^{-1}Hg = Hg = H$. If on the other hand $g \notin H$ then $g^{-1}Hg = g^{-1}X = H$. So in either case $g^{-1}Hg = H$ and we conclude that H is normal in G.

8. (a) Say $e_1, \ldots, e_n$ is an K-basis for L. Let $p_i(x)$ denote the min poly of e_i over K and let $p(x) = \prod_i p_i(x)$. Let M be a splitting field for $p(x)$ over L (for the pedantic: you could use the result that says that fields satisfying property $(*)$ exist and then the result that says that these are splitting fields, to deduce that any polynomial has a splitting field). The e_i are all roots of $p(x)$; let β_j denote the others. We now see $M = L(e_i, \beta_j) = K(e_i, \beta_j)$, so M is a splitting field for $p(x)$ over K too, and is hence normal over K. We claim that it is the normal closure of L. For if $L \subseteq N \subseteq M$ and N/K is normal, then each $p_i(x)$ is irreducible over K and has a root in F and hence in N, so splits completely in N; hence p splits completely in N and all the e_i and β_j are in N; thus $N = M$.

(b) Let's stick with the same notation (e_i and p_i) as in the first part, but this time don't let M be a splitting field, let M/L be any normal closure for L/K. Then M/K is normal, and all the p_i are irreducible in $K[x]$ and have a root (namely e_i) in M, so they all split completely in M. Hence p splits completely in M. If N is the subfield of M generated over K by the roots of p then N is a normal extension of K and $L \subseteq N \subseteq M$, so by normal-closure-ness we deduce $N = M$ and in particular M is a splitting field for $p(x)$ over K, and hence a splitting field for $p(x)$ over L. But splitting fields are unique up to isomorphhism, and hence normal closures are too.

9. (i) If $p(x)$ is irreducible over E and has a root in $M \cap N$, then it has a root in M and a root in N, and hence splits completely in both M and N. So all the roots of $p(x)$ in F are in both M and N, and hence in $M \cap N$. Hence $M \cap N$ is normal.

(ii) If M is the splitting field of $f(x)$ and N is the splitting field of $g(x)$ then MN is the splitting field of $f(x)g(x)$ (not hard to check). Hence MN is normal.

10. Say $\alpha \in F$. Let $p(x)$ denote its min poly over E. Then $p(x)$ is irreducible over E and has a root in F, so it has all its roots in F. Similarly $i(\alpha)$ is a root of $i(p(x))$ (the polynomial obtained from $p(x)$ by hitting all the coefficients with i); but $p(x) \in E[x]$ so $i(p(x)) = p(x)$. Moreover $i(F)$ is normal over E (because it is isomorphic to F) and hence p splits completely in $i(F)$ too. In particular this means that $i(F)$ must contain the root α of $p(x)$. Hence $i(F)$ contains F. Now by a dimension count we have $i(F) = F$.

If F/E is not normal then this might fail. For example if $E = \mathbf{Q}$, if $F = \mathbf{Q}(2^{1/3})$ and if $K = \mathbf{C}$ (or any subfield of $\mathbf{C}$ containing a splitting field for $x^3 - 2$ and $z \in \mathbf{C}$ is a non-real root of $x^3 - 2$ then there's an isomorphism $i : F \to \mathbf{Q}(z)$ which is the identity on $\mathbf{Q}$, but $i(F)$ cannot be equal to F because it contains a non-real number.

11.

(a) Sorry I can't be bothered to do this: please please do it on your own.

(b) Again, what could go wrong? First of all, if we are to take a semidirect product $N \rtimes H$ we need to equip ourselves with a group homomorphism $\rho\colon H \to \operatorname{Aut} N$. We choose:

$$\forall\, n \in N\ \rho_h(n) = hnh^{-1} \in N$$

(this is always an element of N because N is a normal subgroup). Please check (u) that for all $h \in H$, $\rho_h \colon N \to N$ is a group automorphism of N, and (ii) that the so defined $\rho \colon H \to \operatorname{Aut} N$ is a group homomorphism.

Next define $\phi \colon N \rtimes H \to G$ by

$$\phi(n, h) = nh$$

and show that it is a group homomorphism and that it is injective and surjective. What could go wrong? Indeed for example

$$\phi(n_1, h_1)\phi(n_2, h_2) = n_1 h_1 n_2 h_2 = n_1(h_1 n_2 h_1^{-1})h_1 h_2 = (n_1 \rho_{h_1}(n_2))(h_1 h_2) = \phi((n_1, h_1)(n_2, h_2))$$

(c)

(i) In the standard presentation,

$$D_{2n} = \langle a, b \mid a^n = b^2 = e, bab = a^{-1} \rangle$$

Here, b generates a group H of order 2 and the expression $\rho_b(a) = a^{-1}$ defines a group homomorphism $\rho \colon H \to \operatorname{Aut} N$, where $N = C_n$ is the cyclic group of order n generated by a. Almost tautologically, this identifies D_{2n} with the semidirect product $N \rtimes H$.

(ii) Fixing an origin $0 \in \mathbf{R}^n$ allows us to speak of the group $O_n(\mathbf{R})$ of linear orthogonal transformations of $\mathbf{R}^n$. ALL you need to do is to persuade yourself that the group $\mathbf{R}^n \subset E_n$ of translations is a normal subgroup. In the following displayed line, for all $v \in \mathbf{R}^n$ T_v denotes translation by v, and R denotes an arbitrary element of $O_n(\mathbf{R})$:

$$RT_v R^{-1}(x) = R(v + R^{-1}x) = Rv + RR^{-1}x = T_{Rv}(x)$$

(iii) Well, the first questions is who are the groups of order 12? From scratch, this is quite a bit of work and this is not supposed to be a course on finite groups. So I tell you there are FIVE groups of order 12.

Two of these are the abelian groups C_{12} and $C_2 \times C_2 \times C_3$.

Next we have the alternating group A_4: the group of even permutations on 4 letters. Of these,

$$\emptyset, (1,2)(3,4), \quad (1,3)(2,4), \quad (1,4)(2,3)$$

form a subgroup N of order 4 isomorphic to $C_2 \times C_2$. It is easy to check that this is normal; for example:

$$(1,2,3)(1,2)(3,4)(1,3,2) = (1,4)(2,3)$$

etc. showing that, actually, $A_4 = (C_2 \times C_2) \rtimes C_3$.

The fourth group is the dyhedral group D_{12} and we already remarked that this group is a semidirect product $C_6 \rtimes C_2$.

The fifth group of order 12 is a nontrivial semidirect product $C_3 \rtimes C_4$. Note that $\operatorname{Aut}(C_3) = C_2$ so there is only one group homomorphism $\rho \colon C_4 \to C_2$.

If you really like, show that these five groups are all the groups of order 12.