THE UNIVERSITY OF SYDNEY

MATH3962: Rings, Fields and Galois Theory

(http://www.maths.usyd.edu.au/u/UG/SM/MATH3962/)

Semester 1, 2009 Lecturer: Adrian Nelson

Tutorial 12

1. Let $\omega = e^{2\pi i/7}$. It was shown in Tut. 10, Q 3., that $\mathbb{Q}(\omega)$ has an automorphism ϕ such that $\phi(\omega) = \omega^3$, and all automorphisms of $\mathbb{Q}(\omega)$ are powers of ϕ. Now consider the polynomial

$$f(x) = (x-\omega-\omega^2)(x-\omega^3-\omega^6)(x-\omega^2-\omega^4)(x-\omega^6-\omega^5)(x-\omega^4-\omega)(x-\omega^5-\omega^3),$$

and *without calculating them* show that the coefficients of $f(x)$ are fixed by all six automorphisms of $\mathbb{Q}(\omega)$. Deduce, using the Main Theorem of Galois Theory, that the coefficients are all rational.

Solution.

We know that the Galois group $\mathscr{G} = \mathrm{Gal}[\mathbb{Q}(\omega) : \mathbb{Q}] = \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) = \{\, \phi^k \mid k \in \mathbb{Z} \,\}$. For each polynomial $p(x) \in \mathbb{Q}(\omega)[x]$, define $(\phi p)(x) \in \mathbb{Q}(\omega)[x]$ to be the polynomial obtained by applying ϕ to the coefficients of $p(x)$; that is, if $p(x) = \sigma_j a_j x^j$ then $(\phi p)(x) = \sum_j (\phi a_j)x^j$. Then $p(x) \mapsto (\phi p)(x)$ is an automorphism of the polynomial ring $\mathbb{Q}(\omega)[x]$, so that in particular if $p(x) = q(x)s(x)$ then $(\phi p)(x) = (\phi q)(x)(\phi s)(x)$. We deduce that

$$\begin{aligned}(\phi f)(x) &= (x - \phi(\omega + \omega^2)(x - \phi(\omega^3 + \omega^6))(x - \phi(\omega^2 + \omega^4)) \\ &\qquad (x - \phi(\omega^6 + \omega^5))(x - \phi(\omega^4 + \omega))(x - \phi(\omega^5 + \omega^3)) \\ &= (x - \omega^3 - \omega^6)(x - \omega^2 - \omega^4)(x - \omega^6 - \omega^5) \\ &\qquad (x - \omega^4 - \omega)(x - \omega^5 - \omega^3)(x - \omega - \omega^2)\end{aligned}$$

which equals $f(x)$. That is, the automorphism ϕ permutes the factors of $f(x)$ and thus fixes $f(x)$ itself. So ϕ fixes the coefficients of $f(x)$. So all the powers of ϕ fix the coefficients of $f(x)$. But since every element of the Galois group $\mathscr{G}$ is a power of ϕ, this shows that the coefficients of $f(x)$ all lie in $\mathrm{Fix}(\mathscr{G}) = \mathrm{Fix}(\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega))$. But the Main Theorem of Galois Theory says that when E is the splitting field of a polynomial in $F[x]$ then $K \mapsto \mathrm{Aut}_K(E)$ and $\mathscr{H} \mapsto \mathrm{Fix}(\mathscr{H})$ are mutually inverse bijections between the set of subfields of E containing F and the set of subgroups of the Galois group. So $\mathrm{Fix}(\mathrm{Aut}_K(E)) = K$. In particular, applying this to the present situation, $\mathrm{Fix}(\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega)) = \mathbb{Q}$. So all the coefficients of $f(x)$ are in $\mathbb{Q}$. (We have used the following general principle: if an element $t \in E$ is fixed by all elements of the Galois group $\mathrm{Gal}[E : F]$ then $t \in F$.)

2. With the notation as in Question 1, show that $\mathbb{Q}(\omega + \omega^2) = \mathbb{Q}(\omega)$, and deduce that the $f(x)$ is irreducible over $\mathbb{Q}$. (Hint: Show that no element of $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\omega))$ fixes $\omega + \omega^2$, and use the Main Theorem of Galois Theory.)

Solution.

Note first that since 1, ω, ω^2, ω^3, ω^4, ω^5, ω^6 are linearly independent over $\mathbb{Q}$ the polynomial $f(x)$ has six distinct roots. Now suppose that $f(x)$ has a nontrivial factorization in $\mathbb{Q}[x]$ as $a(x)b(x)$. Then γ must be a root either of $a(x)$ or $b(x)$, and we may choose the notation so that it is a root of $a(x)$. Since $a(x) \in \mathbb{Q}[x] \subset \mathbb{Q}(\omega)[x]$ and $\gamma \in \mathbb{Q}(\omega)$ we have that $a(x) = (x - \gamma)g(x)$ for some $g(x) \in \mathbb{Q}(\omega)[x]$. Applying the automorphism of $\mathbb{Q}(\omega)[x]$ given by $p(x) \mapsto (\phi^j p)(x)$ we deduce that $(\phi^j a)(x) = (x - \phi^j(\gamma))(\phi^j g)(x)$. But the coefficients of $a(x)$ lie in $\mathbb{Q}$, and ϕ and all its powers fix all the elements of $\mathbb{Q}$. So $(\phi^j a)(x) = a(x)$, and so $a(x) = (x - \phi^j(\gamma))(\phi^j g)(x)$. Thus $\phi^j(\gamma)$ is a root of $a(x)$, for all j. Furthermore, we saw in the solution to Question 1 that

$$\phi\gamma = \omega^3 + \omega^6,\ \phi^2\gamma = \omega^2 + \omega^4,\ \phi^3\gamma = \omega^6 + \omega^5,\ \phi^4\gamma = \omega^4 + \omega,\ \phi^5\gamma = \omega^5 + \omega^3.$$

So all the roots of $f(x)$ are roots of $a(x)$, contrary to the assumption that the factorization $f(x) = a(x)b(x)$ is nontrivial. So $f(x)$ has no such factorization, and hence is irreducible.

Since $f(x)$ is irreducible it is the minimal polynomial of γ over $\mathbb{Q}$, and so $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ is $\deg f(x) = 6$. But $\gamma \in \mathbb{Q}(\omega)$, and so $\mathbb{Q}(\gamma) \subseteq \mathbb{Q}(\omega)$. Since also $[\mathbb{Q}(\omega) : \mathbb{Q}] = 6$ it follows that $\mathbb{Q}(\gamma) = \mathbb{Q}(\omega)$.

An alternative method is use the Main Theorem of Galois Theory to show that γ cannot possibly lie in a proper subfield F of $\mathbb{Q}(\omega)$. Put $\mathscr{H} = \mathrm{Aut}_F(\mathbb{Q}(\omega))$, the subgroup of $\mathrm{Gal}[E : \mathbb{Q}]$ corresponding to the intermediate field F. If $\psi \in \mathscr{H}$ then $\psi\gamma = \gamma$. But every ψ in the Galois group is a power of the automorphism ϕ defined above, and we saw above that none of the ϕ^j fixes γ. Hence $\mathscr{H} = \{\mathrm{id}\}$, the subgroup consisting of the identity alone, and $F = \mathrm{Fix}(\mathscr{H}) = \mathrm{Fix}(\mathrm{id}) = E$. (We have used the following general principle: if an element $t \in E$ is not fixed by any element of the Galois group $\mathrm{Gal}[E : F]$ then $F(t) = E$.)

Of course one could also use an explicit calculation to express ω as a $\mathbb{Q}$-linear combination of powers of γ, and deduce that $\omega \in \mathbb{Q}(\gamma)$. Perhaps it would be nice to do this, just to confirm our theoretical reasoning above. Expressing ω as a linear combination of powers $(\omega + \omega^2)^j$, for j from 0 to 5, does, however, involve solving a system of six linear equations in six unknowns; specifically, the following system:

$$\begin{pmatrix} 1 & 0 & 0 & -1 & -2 & 5 \\ 0 & 1 & 0 & -1 & -5 & 5 \\ 0 & 1 & 1 & -1 & -6 & 0 \\ 0 & 0 & 2 & 0 & -6 & -4 \\ 0 & 0 & 1 & 2 & -5 & -5 \\ 0 & 0 & 0 & 2 & -2 & -4 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \\ e \\ f \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

(For example, the sixth column comes from $(\omega+\omega^2)^5 = 5+5\omega-4\omega^3-5\omega^4-4\omega^5$, obtained by using the Binomial Theorem and the relation $\omega^6 = -\sum_{j=0}^{5}\omega^j$). I got as the solution $\omega = -\frac{3}{2} - 2\gamma - \frac{3}{2}\gamma^2 - \frac{1}{2}\gamma^3 - \frac{1}{2}\gamma^4$, but I am not prepared claim that my calculations are bound to be right.

As a result of the arguments we have used, we can enunciate another general principle, as follows: if $F(t)$ is a normal extension of F then $F(t)$ contains all the roots of the minimal polynomial of t. Furthermore, if E is a normal extension of F then $E = F(t)$ whenever $t \in E$ has the property that no nonidentity F-automorphism of E fixes t.

3. (Not examinable.) Let F be a field and $\alpha_1, \alpha_2, \dots, \alpha_n$ a set of n distinct automorphisms of F. Suppose that $u_1, u_2, \dots, u_n \in F$ satisfy

$$u_1(\alpha_1 t) + u_2(\alpha_2 t) + \cdots u_n(\alpha_n t) = 0 \qquad (*)$$

for all $t \in F$. Prove that $u_i = 0$ for all i, by means of the following steps.

(i) The proof is by induction on n. Start it off by doing the case $n = 1$.

(ii) Suppose now that $n > 1$ and that the result holds for sets of fewer than n automorphisms. Put tv in place of t in Eq.$(*)$, and also multiply Eq.$(*)$ by $\alpha_1 v$. Using the difference between these two equations, and the inductive hypothesis, deduce that $\lambda_i(\alpha_i v - \alpha_1 v) = 0$ for all i and all $v \in F$.

(iii) Use the fact that $\alpha_1 \neq \alpha_i$ for all i to complete the proof.

Solution.

In the case $n = 1$, if we put $t = 1$ in Eq.$(*)$ we obtain $u_1(\alpha_1 1) = 0$, and hence $u_1 = 0$ since $\alpha_1 1 = 1$.

Since the α_j are automorphisms we have $\alpha_j(tv) = (\alpha_j t)(\alpha_j v)$, and so putting tv in place of t in Eq.$(*)$ gives

$$u_1(\alpha_1 t)(\alpha_1 v) + u_2(\alpha_2 t)(\alpha_2 v) + \cdots u_n(\alpha_n t)(\alpha_n v) = 0,$$

whereas multiplying Eq.$(*)$ by $\alpha_1 v$ gives

$$u_1(\alpha_1 t)(\alpha_1 v) + u_2(\alpha_2 t)(\alpha_1 v) + \cdots u_n(\alpha_n t)(\alpha_1 v) = 0.$$

Subtracting the second of these equations from the first gives

$$u_2'(\alpha_2 t) + u_3'(\alpha_3 t) + \cdots u_n'(\alpha_n t) = 0,$$

for all t, where $u_j' = u_j(\alpha_j v - \alpha_1 v)$. Since this equation involves fewer than n automorphisms the inductive hypothesis is applicable, and we conclude that $u_j' = 0$ for all j (from 2 to n). Furthermore, v was an arbitrary element of F, and so the above holds for all $v \in F$. Since $\alpha_j \neq \alpha_1$ whenever $2 \leq j \leq n$, we can choose $v \in F$ (dependent on j) such that $\alpha_j v \neq \alpha_1 v$, and then $u_j(\alpha_j v - \alpha_1 v) = u_j' = 0$ forces $u_j = 0$. So $u_j = 0$ for all $j \in \{2, 3, \dots, n\}$, and then the $n = 1$ case gives $u_1 = 0$ as well, as required. (In his book "Galois Theory", I. Stewart attributes this proof to Dedekind, although it is commonly attributed to Artin.)

4. Let $F = \mathbb{Q}(\zeta)$, where $\zeta = e^{2\pi i/5}$ (a complex 5th root of 1). Suppose also that K is a normal extension of F with $|K : F| = 5$, and let $\alpha \in \mathrm{Aut}_F(K)$ have order 5.

(i) Let $t \in K$ such that $t \notin F$, and let $p(x) \in F[x]$ be the minimal polynomial of t. Prove that the degree of $p(x)$ is 5.

(ii) Prove that t, $\alpha(t)$, $\alpha^2(t)$, $\alpha^3(t)$ and $\alpha^4(t)$ are the roots of $p(x)$.

(iii) Prove that if u is an arbitrary element of K then u and $\alpha^j(u)$ have the same minimal polynomial for all j.

(iv) Show that $t + \zeta\alpha(t) + \zeta^2\alpha^2(t) + \zeta^3\alpha^3(t) + \zeta^4\alpha^4(t) \neq 0$ for some $t \in K$. (Use Exercise 3.)

(v) Prove that if $u = t + \zeta\alpha(t) + \zeta^2\alpha^2(t) + \zeta^3\alpha^3(t) + \zeta^4\alpha^4(t)$ and $u \neq 0$ then $\alpha^j(u) = \zeta^{-j}u$ for each j, and deduce that the minimal polynomial of u over F has degree 5.

(vi) With u as in Part *(iv)*, let $u^5 = r$. Show that r is fixed by α and deduce that $r \in F$. Deduce further that $x^5 - r$ is the minimal polynomial of u over F.

Solution.

(i) For each i let $t_i = \alpha^i(t)$. Since $t \notin F$ it follows that t_0, t_1, t_2, t_3 and t_4 are distinct. To see this, suppose that $t_i = t_j$. Then $\alpha^{i-j}(t) = t$, and so $\alpha^{k(i-j)} = t$ for all t. If $i - j$ is not divisible by 5 then there is a value of k such that $k(i-j) \cong 1$ (mod $5\mathbb{Z}$) (since every nonzero element of $\mathbb{Z}_5$ has an inverse). Since $\alpha^5 = 1$ this yields that $\alpha(t) = t$, and indeed that $\alpha^l(t) = t$ for all l. As $|\mathrm{Aut}_F(K)| = |K : F| = 5$ we know that the powers of α give all the elements of $\mathrm{Aut}_F(K)$. Now by the Main Theorem of Galois Theory,

$$F = \mathrm{Fix}(\mathrm{Aut}_F(K)) = \{\, u \in K \mid \sigma(u) = u \text{ for all } \sigma \in \mathrm{Aut}_F(K) \,\},$$

and we have just shown that t is in this set, since it is fixed by all the powers of α, contrary to the assumption that $t \notin F$.

As $t_i = \alpha^i(t)$ is a root of $(\alpha^i p)(x) = p(x)$ we deduce that $p(x)$ has at least 5 distinct roots, and hence has degree at least 5. Furthermore, the roots of $p(x)$ lie in a degree 5 extension of F, and so the degree of $p(x)$ is at most 5.

(ii) This has been proved in the process of proving Part *(i)*.

(iii) So has this (at least for $u = t$). If $q(x) \in F[x]$ then $q(u) = 0$ if and only if $q(\alpha^i(u)) = 0$ (since $q(\alpha^i(u)) = (\alpha^i q)(\alpha^i(u)) = \alpha^i(q(u))$); hence $q(x)$ is the minimal polynomial of u over F if and only if $q(x)$ is the minimal polynomial of $\alpha^i(u)$ over F.

(iv) Since $\mathrm{id} = \alpha^0$, α^1, α^2, α^3 and α^4 are distinct automorphisms of E, Dedekind's argument shows that they are linearly independent elements of the vector space over E consisting of all functions $E \to E$over E; so the function $\mathrm{id} + \zeta\alpha + \zeta^2\alpha^2 + \zeta^3\alpha^3 + \zeta^4\alpha^4$ is nonzero. Hence a $t \in E$ can be chosen on which this function takes a nonzero value.

(v) Since $\zeta \in F$ we have that $\alpha(\zeta) = \zeta$, and thus

$$\begin{aligned}\alpha(u) &= \alpha(t + \zeta\alpha(t) + \zeta^2\alpha^2(t) + \zeta^3\alpha^3(t) + \zeta^4\alpha^4(t)\\ &= \alpha(t) + \zeta\alpha^2(t) + \zeta^2\alpha^3(t) + \zeta^3\alpha^4(t) + \zeta^4\alpha^5(t)\\ &= \zeta^{-1}(\zeta\alpha(t) + \zeta^2\alpha^2(t) + \zeta^3\alpha^3(t) + \zeta^4\alpha^4(t) + \zeta^5\alpha^5(t)\\ &= \zeta^{-1}u\end{aligned}$$

since ζ and α both have order 5. Applying α again gives

$$\alpha^2(u) = \alpha(\zeta^{-1}u) = \zeta^{-1}\alpha(u) = \zeta^{-2}u,$$

and clearly repeating this argument gives $\alpha^j(u) = \zeta^{-j}u$ for all j. Now since $u \neq 0$ (by assumption), it follows that the 5 numbers $\alpha^j(u)$ are all distinct, and hence their minimal polynomial has degree 5.

(vi) Let $u^5 = r$. Then $\alpha(r) = \alpha(u)^5 = (\zeta^{-1}u)^5 = u^5$ since ζ is a 5th root of 1. So u^5 is fixed by all 5 elements of $\mathrm{Aut}_F(K)$ (the powers of α), and so $u^5 \in F$. (Let us re-emphasize this important corollary of the Main Theorem of Galois Theory: if an element of a Galois extension of F is fixed by all the elements of the Galois group then it must in fact be in the base field F.) So u is a root of $x^5 - r \in F[x]$, which must be the minimal polynomial of u since its degree is 5.

Note that the reasoning used in the above question applies in the same manner if 5 is replaced by any positive integer. It shows that if the Galois group of a normal extension of F is cyclic of order n then, provided F contains the nth roots of 1, the extension is the splitting field of a polynomial of the form $x^n - r$.)

5. Let $A = \mathrm{Alt}(5)$, the group of all even permutations of $\{1,2,3,4,5\}$. Show that A contains 15 permutations of cycle type $(i,j)(k,l)$, forming a single conjugacy class, 20 permutations of cycle type (i,j,k), forming a single conjugacy class, and 24 permutations of cycle type (i,j,k,l,m) forming two equal sized conjugacy classes. Using Lagrange's Theorem, deduce that A has no normal subgroups apart from A itself and $\{1\}$. By a similar method, find all the normal subgroups of $\mathrm{Sym}(5)$, the group of all permutations of $\{1,2,3,4,5\}$.

Solution.

Let us first decide how many permutations of type $(i,j)(k,l)$ there are altogether in the set of permutations of $\{1,2,3,4,5\}$. The numbers i, j, k and l must be all distinct; so there are $\binom{5}{4} = 5$ possibilities for the set $\{i,j,k,l\}$. Now there are $\binom{4}{2} = 6$ ways to choose $\{i,j\}$ from $\{i,j,k,l\}$, but since $(i,j)(k,l) = (k,l)(i,j)$ each permutation of the required type is obtained from two choices of a two-element subset of $\{i,j,k,l\}$. So there are $5 \times 3 = 15$ such permutations altogether.

Recall that transpositions are odd permutations, and the product of two odd permutations is always even. So all the elements $(i,j)(k,l)$ are even; that is, they lie in the group $A = \mathrm{Alt}(5)$.

We must show that these elements are all conjugate in A. Since conjugacy is an equivalence relation, it is sufficient to show that for any given $(i,j)(k,l)$ there is a $\sigma \in A$ such that $\sigma(1,2)(3,4)\sigma^{-1} = (i,j)(k,l)$. Now there is certainly a $\sigma \in \mathrm{Sym}(5)$ satisfying this; indeed

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5\\ i & j & k & l & m\end{pmatrix}$$

will do (where m is the "other" number – i.e. $\{i,j,k,l,m\} = \{1,2,3,4,5\}$). Now observe that if $\tau = \sigma(1,2)$ then

$$\tau(1,2)(3,4)\tau^{-1} = \sigma(1,2)(1,2)(3,4)(1,2)\sigma^{-1} = \sigma(1,2)(3,4)\sigma^{-1} = (i,j)(k,l),$$

and since $(1,2)$ is an odd permutation it follows that if σ is odd then τ is even, and *vice versa*. So one or other of σ and τ is in A, and hence $(i,j)(k,l)$ is conjugate to $(1,2)(3,4)$ in A, as required.

Every three-cycle (i,j,k) is an even permutations, since it can be expressed as the product of two transpositions: $(i,j,k) = (i,j)(j,k)$. Thye are all conjugate in $\mathrm{Sym}(5)$, since any σ satisfying $\sigma 1 = i$, $\sigma 2 = j$ and $\sigma 3 = k$ has the property that $\sigma(1,2,3)\sigma^{-1} = (i,j,k)$. And if we put $\tau = \sigma(4,5)$ then $\tau(1,2,3)\tau^{-1} = (i,j,k)$ also, since $(4,5)(1,2,3)(4,5) = (1,2,3)$. Since one or other of σ and τ is even, it follows that $(1,2,3)$ and (i,j,k) are conjugate in A.

There are 20 three-cycles altogether: there are $\binom{5}{3} = 10$ ways to choose three numbers to put in a three-cycle, and each choice gives two possible three-cycles. (For example, using the numbers 1, 2 and 3 you can form $(1,2,3)$ and $(1,3,2)$.)

The identity permutation is even, and obviously constitutes a conjugacy class by itself. The three conjugacy classes we have so far gives us $15 + 20 + 1 = 36$ of the 60 elements of A.

The remaining elements are the 5-cycles. There are exactly 24 ways to arrange 1, 2, 3, 4, and 5 into a cycle, as the following argument shows. We may as well think of 1 as the "first" term in the cycle; then the second term can be anything except 1 (4 choices), the third term can be anything different from the first two terms (3 choices), the fourth can be anything different from the first three (two choices), and then the fifth term is the number left over. So $4 \times 3 \times 2 = 24$ possibilities.

These 24 5-cycles are all conjugate in $\mathrm{Sym}(5)$. Indeed, given a 5-cycle (i,j,k,l,m) we can define

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5\\ i & j & k & l & m\end{pmatrix},$$

and it is easily checked that $\sigma(1,2,3,4,5)\sigma^{-1} = (i,j,k,l,m)$. Note that since the given $5 - cycle$ can also be written as (j,k,l,m,i) or (k,l,m,i,j) or (l,m,i,j,k) or (m,i,j,k,l), there are another four permutations that we could use instead of σ. Indeed, these others are the permutations $\sigma(1,2,3,4,5)^n$, for $n = 1$, 2, 3 and 4. But all five possibilities have the same parity, since σ is even.

What we are really saying here is that for each 5-cycle (i,j,k,l,m) the elements $\tau \in \mathrm{Sym}(5)$ satisfying

$$\tau(1,2,3,4,5)\tau^{-1} = (i,j,k,l,m)$$

constitute a coset σH, where H is the cyclic subgroup generated by $(1,2,3,4,5)$. Since exactly 12 of the cosets of H lie inside the group A, exactly 12 of the 5-cycles are conjugate to $(1,2,3,4,5)$ in A.

One of the 5-cycles not conjugate to $(1,2,3,4,5)$ is $(2,1,3,4,5)$. The same argument shows that it also has 12 conjugates in A. So we conclude that A has two conjugacy classes of 5-cycles, 12 elements in each.

Any normal subgroup of A would have to be a union of conjugacy classes, including the identity. But there is no subsequence of 1, 20, 15, 12, 12 that includes 1 and has the property that the terms add up to a divisor of 60, apart from the whole sequence and the sequence consisting of 1 only. So A has no normal subgroups apart from A and $\{1\}$.

In the case of $\mathrm{Sym}(5)$ it is easier to find the conjugacy classes: two permutations are conjugate if and only if they have the same cycle type. So using the calculations we have done for the alternating group, we already know the following conjugacy classes: the 1-cycles (1 element only), the 3-cycles (20 elements), the 5-cycles (24 elements) and the products of two disjoint 2-cycles (15 elements). In addition we have the 2-cycles ($\binom{5}{2} = 10$ elements), the products of a 3-cycle and 2-cycle disjoint from it (20 elements, the same as the number of 3-cycles), and the 4-cycles (30 elements – everything left). So the class sizes are 1, 10, 20, 30, 24, 15, 20. The only ways to get a divisor of 120, given that the 1 must be used, are as follows:

1,
1+20+24+15,
1+24+15,
1+24+15+20,
1+10+20+30+24+15+20.

However, the $1+24+15$ does not give a subgroup: the set consisting of the identity, the 5-cycles and the permutations $(i,j)(k,l)$ is not closed under multiplication. For example, $((1,2)(3,4))((1,2)(4,5)) = (3,4,5)$. This also shows that any normal subgroup that contains the 24 and 15 conjugacy classes must contain the 3-cycles also. So only one of the $1+20+24+15$'s above actually corresponds to a subgroup. So we conclude that there are only three normal subgroups of $\mathrm{Sym}(5)$, namely $\{1\}$, A and $\mathrm{Sym}(5)$.