Math 504, Fall 2013
HW 5

1. Let G be a group and N a normal subgroup. Show that G is solvable if and only if N and G/N are solvable.

($\Leftarrow$) Let G be a group and $H \lhd G$. Suppose that H and G/H are solvable. Then we can build a solvable series for G in the following manner.

Consider a solvable series $1 \lhd \cdots H_i \lhd \cdots \lhd H$ for H, and a solvable series $1 \lhd K_i \lhd \cdots \lhd G/H$ for G/H. Let $\phi\colon G \to G/H$ be the quotient map. Then ϕ defines a bijection

$$\{\text{subgroups of } G \text{ containing } H\} \iff \{\text{subgroups of } G/H\}$$

Moreover, by the Third Isomorphism Theorem we know that $\phi^{-1}(K_{i+1})/\phi^{-1}(K_i) \cong K_{i+1}/K_i$. It follows that the quotients of consecutive groups in the series are unchanged under ϕ^{-1}. Thus

$$1 \lhd \cdots H_i \lhd \cdots \lhd H \lhd \cdots \lhd \phi^{-1}(K_i) \cdots \lhd G$$

is a solvable series for G.

($\Rightarrow$) Suppose G is solvable and $H \lhd G$. If $1 \lhd \cdots G_i \lhd \cdots \lhd G$ is a solvable series for G, then consider the groups $H_i = H \cap G_i$. We claim that $1 \lhd \cdots H_i \cdots \lhd H$ is a solvable series for G. First, we need to verify that $H_i \lhd H_{i+1}$.

Let $q\colon G_{i+1} \to G_{i+1}/G_i$ be the projection. Then $q|_N\colon H_{i+1} \to G_{i+1}/G_i$ has kernel H_i. Thus $H_i \lhd H_{i+1}$. By the subgroup correspondence used in the previous part, it follows that H_{i+1}/H_i is a subgroup of G_{i+1}/G_i, which is abelian. So H_{i+1}/H_i is abelian, and thus the H_i form a solvable series for H.

Now we construct a solvable series for G/H. Use the same map $\phi\colon G \to G/H$ from the last part. We claim that

$$1 \lhd \cdots \phi(G_i) \cdots \lhd \phi(G)$$

is a solvable series for G/H (obviously since ϕ is surjective, $\phi(G) = G/H$). Let $K_i = \phi(G_i)$. By the subgroup correspondence, $K_i \lhd K_{i+1}$.

Moreover, K_{i+1}/K_i is abelian. Indeed, consider the map

$$\rho\colon G_{i+1} \to K_{i+1}/K_i$$

given by applying ϕ followed by applying the quotient map. Then $\rho(G_i) = 1$, so ρ passes to the quotient over G_{i+1}/G_i. Thus there is a surjective map $\tilde{\rho}\colon G_{i+1}/G_i \to K_{i+1}/K_i$. Since G_{i+1}/G_i is abelian, it follows that K_{i+1}/K_i is also abelian. Hence the K_i form a solvable series for G/H.

■

2. Compute the Galois group of $x^6 - 2x^3 - 1$ over $\mathbb{Q}$.

Define $f(x) = x^6 - 2x^3 - 1$.

Let $y = x^3$. It's clear that $f(x) = g(y) = y^2 - 2y - 1$, so:

$$f(x) = 0 \Leftrightarrow g(y) = 0 \Leftrightarrow y = \frac{2 \pm \sqrt{8}}{2} = 1 \pm \sqrt{2}$$

Let $\alpha = \sqrt[3]{1+\sqrt{2}}$, $\beta = \sqrt[3]{1-\sqrt{2}}$, $\omega = \frac{1+\sqrt{-3}}{2}$. Then clearly, $f(x)$ splits as:

$$f(x) = (x-\alpha)(x-\omega\alpha)(x-\omega^2\alpha)(x-\beta)(x-\omega\beta)(x-\omega^2\beta)$$

Also, compute that $\alpha\beta = \sqrt[3]{(1+\sqrt{2})(1-\sqrt{2})} = \sqrt[3]{1-2} = \sqrt[3]{-1} = -1$, so $\alpha = -\beta^{-1}$. Thus, $\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha)$, and consequently, $K = \mathbb{Q}(\alpha, \omega)$ is a splitting field for f over $\mathbb{Q}$. Note that K is the smallest such field: obviously $\alpha, \omega \in K$ because α is a root and ω is a quotient of roots. We know $\alpha \notin \mathbb{Q}$, because $\alpha^3 - 1 = \sqrt{2} \notin \mathbb{Q}$, and we know $\omega \notin \mathbb{Q}(\alpha)$ because $\mathbb{Q}(\alpha)$ is a real extension. Consequently, we need exactly those two elements to generate K over $\mathbb{Q}$.

Next, note that $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\alpha)$, so

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})].$$

Note that in $\mathbb{Q}(\sqrt{2})[x]$:

$$f(x) = (x^3 - \sqrt{2} - 1)(x^3 + \sqrt{2} - 1)$$

I claim that those factors are irreducible.

Let $a, b \in \mathbb{Z}$ and suppose that:

$$\begin{aligned}(a + b\sqrt{2})^3 &= a^3 + 3a^2b\sqrt{2} + 6ab^2 + 2\sqrt{2}b^3 \\ &= (a^3 + 6ab^2) + \sqrt{2}(3a^2b + 2b^3) \\ &= 1 \pm \sqrt{2}\end{aligned}$$

Then $a^3 + 6ab^2 = a(a^2 + 6b^2) = 1$. Since $a, b \in \mathbb{Z}$ and a is a unit, $a = \pm 1$. But since $a^2 + 6b^2 = 1 + 6b^2$ is also a unit, $b = 0$, which forces $a = 1$ because $a(a^2 + 6b^2) = a^3 = 1$. But $1^3 \neq 1 \pm \sqrt{2}$; thus, there do not exist $a, b \in \mathbb{Z}$ for which $(a + b\sqrt{2})^3 = 1 \pm \sqrt{2}$, or equivalently, $f(x)$ does not have a root in $\mathbb{Z}[\sqrt{2}]$. Since f is a product of cubics, neither of which has a root, in $\mathbb{Z}[\sqrt{2}]$, those cubics remain irreducible over $\mathbb{Z}[\sqrt{2}]$. Since $\mathbb{Z}[\sqrt{2}]$ is a UFD and $\mathbb{Q}[\sqrt{2}]$ is its field of fractions, the cubic factors of f are still irreducible over $\mathbb{Q}[\sqrt{2}]$. As a result, $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2})] = 3$, and $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$. To get the full splitting field, we need to adjoin ω, which is quadratic over any real field. Thus, $[\mathbb{Q}(\alpha, \omega) : \mathbb{Q}] = 12$, which means we are looking for a group of order 12. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 6$, f is irreducible, so the group will be a transitive subgroup of S_6. There are only two such groups: D_{12} and $\mathbb{Z}_2 \times \mathbb{Z}_6$, and since $\mathbb{Q}(\alpha)/\mathbb{Q}$ is a non normal extension, G cannot be abelian, hence G is isomorphic to the dihedral group D_{12}. ∎

3. Solve the equation $x^6 - x^5 + x^4 - x^3 + x^2 - x + 1 = 0$ by radicals. Hint: Think about $t = x + x^{-1}$.

Start by computing that:

$$(x+1)f(x) = x^7 + 1$$

Thus, the roots of $f(x)$ are primitive 7^{th} roots of -1, i.e. they are equal to $e^{\frac{\pi i}{7}}$, where $i = 1, 3, 5, 9, 11, 13$.

Let $t = x + x^{-1}$, and consider $x^{-3}f(x) = x^3 - x^2 + x - 1 + x^{-1} - x^{-2} + x^{-3}$. Since:

$$t^2 = x^2 + 2 + x^{-2}$$
$$t^3 = x^3 + 3x + 3x^{-1} + x^{-3}$$

we have that:

$$x^{-3}f(x) = t^3 - t^2 - 2t + 1 := \tilde{f}(t)$$

Next, compute that:

$$\tilde{f}\left(t + \frac{1}{3}\right) = t^3 - \frac{7}{3}x + \frac{7}{27} := g(t)$$

I will solve $g(t)$ and use that to solve $f(x)$.

To solve a depressed cubic, we begin by solving:

$$\begin{cases} 3st & = -\frac{7}{3} \\ s^3 - t^3 & = -\frac{7}{27} \end{cases}$$

Then, plugging $s - t$ into the cubic will produce 0, because:

$$(s-t)^3 + 3st(s-t) - (s^3 - t^3) = s^3 - 3s^2t + 3st^3 - t^3 + 3s^2t - 3st^3 - s^3 + t^3 = 0$$

Also, if $\omega = e^{2\pi i/3}$, then:

$$\begin{aligned} g(\omega s - \omega^2 t) &= (\omega s - \omega^2 t)^3 + 3(\omega s)(\omega^2 t)(\omega s - \omega^2 t) - ((\omega s)^3 - (\omega^2 t)^3) \\ &= -3(\omega^2 s^2)(\omega^2 t) + 3(\omega s)(\omega^4 t^2) + 3s^2 t\omega - 3\omega^2 s t^3 \\ &= 0 \end{aligned}$$

$$\begin{aligned} g(\omega^2 s - \omega t) &= (\omega^2 s - \omega t)^3 + 3(\omega^2 s)(\omega t)(\omega^2 s - \omega t) - ((\omega^2 s)^3 - (\omega t)^3) \\ &= -3(\omega^4 s^2)(\omega t) + 3(\omega^2 s)(\omega^2 t^2) + 3s^2 t\omega^2 - 3\omega s t^3 \\ &= 0 \end{aligned}$$

Thus, once we have s, t, we have all 3 roots.

Now:

$$3st = -\frac{7}{3} \Longrightarrow s = \frac{-7}{9t} \Longrightarrow -\frac{7}{27} = \left(\frac{-7}{9t}\right) - t^3 = \frac{-7^3}{3^6 t^3} - t^3$$

Rearranging:

$$t^3 - \frac{7}{3^3} + \frac{7^3}{3^6 t^3} = 0 = t^6 - \frac{7}{3^3}t^3 + \frac{7^3}{3^6}$$

Solving the quadratic:

$$t^3 = \frac{\frac{7}{3^3} \pm \sqrt{\frac{7^2}{3^6} - \frac{2^2 7^3}{3^6}}}{2} = \frac{7 \pm 7\sqrt{1-28}}{2 \cdot 3^3} = \frac{7 \pm 21i\sqrt{3}}{54}$$

From that, we can directly obtain s^3:

$$s^3 = t^3 - \frac{-7}{27} = \frac{7 \pm 21i\sqrt{3}}{54} - \frac{7}{27} = \frac{-7 \pm 21i\sqrt{3}}{54}$$

Replace the $\pm$ by a $+$ in both s^3, t^3 from now on.

By the work I've already done, we know the roots of g, and from those, we get that the roots of $\tilde{f}$ are:

$$\rho_1 = \frac{1}{3}\left(\sqrt[3]{\frac{-7+21i\sqrt{3}}{2}} - \sqrt[3]{\frac{7+21i\sqrt{3}}{2}} - 1\right)$$

$$\rho_2 = \frac{1}{3}\left(\omega\sqrt[3]{\frac{-7+21i\sqrt{3}}{2}} - \omega^2\sqrt[3]{\frac{7+21i\sqrt{3}}{2}} - 1\right)$$

$$\rho_3 = \frac{1}{3}\left(\omega^2\sqrt[3]{\frac{-7+21i\sqrt{3}}{2}} - \omega\sqrt[3]{\frac{7+21i\sqrt{3}}{2}} - 1\right)$$

Let ρ denote any one of the ρ_i. To obtain the roots of f, we need to solve $x + x^{-1} = \rho$ for each of the three ρ's; this will give us the 6 roots of f. Therefore an expression for them by radicals is

$$\frac{\rho_i \pm \sqrt{\rho_i^2 - 4}}{2} \text{ for } i = 1, 2, 3$$

■

4. Let k be a subfield of $\mathbb{C}$ and let $K = k(\alpha, \beta)$ where $\alpha^2 = a \in k$ and $\beta^2 = b \in k$ and none of a, b, or ab, is a square in k. Prove that Gal $(K/k) \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Let k be a subfield of $\mathbb{C}$ and let $K = k(\alpha, \beta)$ where $\alpha^2 = a \in k$ and $\beta^2 = b \in k$ and none of a, b, or ab is a square in k. Since K is the splitting field of the polynomials $x^2 - a$ and $x^2 - b$, it is a normal extension. Since each of α and β are separable, K is a separable extension. Thus, K/k is Galois.

Firstly, $k(\alpha)/k$ is a Galois extension of degree 2 as the splitting field of the irreducible polynomial $x^2 - a$ over k. Suppose that $\beta \in k(\alpha)$, so that $\beta = q + r\alpha$ for some $q, r \in$

k. Squaring both sides, we get that $\beta^2 = q^2 + 2qr\alpha + r^2\alpha^2$ and equivalently, $b = q^2 + 2qr\alpha + r^2 a$. We must have that either q or r is zero; otherwise, this lets us express α as a combination of the elements a, b, q, r in k. Since $\beta \notin k$, we must have $q = 0$ and that $b = r^2 a$. Then $ab = r^2 a^2$, but this contradicts our assumption that ab is not a square in k. Hence, $\beta \notin k(\alpha)$.

Now we see that K is a degree 2 extension of $k(\alpha)$ as the splitting field of $x^2 - b$, so $[K : k] = [K : k(\alpha)][k(\alpha) : k] =$. Then $|\text{Gal}\,(K/k)| = 4$, so our options for the Galois group are $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. We have two distinct intermediate subfields $k(\alpha)$ and $k(\beta)$ lying between k and K (we've already shown that $\beta \notin k(\alpha)$, and the same argument works in the reverse direction). This means that there is a distinct non-trivial subgroup of the Galois group that fixes each of these fields, i.e., there are (at least) two distinct subgroups in the Galois group. The only option is then that Gal (K/k) is $\mathbb{Z}_2 \times \mathbb{Z}_2$, as $\mathbb{Z}_4$ has only one non-trivial subgroup. ∎

5. Let $f \in k[x]$ be an irreducible polynomial where k is a subfield of $\mathbb{C}$. Suppose f has at least one root that is expressible in radicals. Show that all roots of f can be written in terms of radicals.

Let K be a splitting field for f over k, and let $\alpha \in K$ be a root of f that is expressible in radicals. This means $k(\alpha)$ is a radical extension of k.

But, because f is irreducible, the Galois group $G := \text{Gal}\,(K/k)$ acts transitively on the roots of f. Thus, for any root β of f, there exists an automorphism $\tau \in G$ such that $\tau(\alpha) = \beta$. But then, as τ is k-linear ring automorphism, we also have

$$\tau\left(\sum_{i=1}^{n} c_i \alpha^i\right) = \sum_{i=1}^{n} c_i (\tau(\alpha))^i = \sum_{i=1}^{n} c_i (\beta)^i \in k(\beta)$$

This is well-defined since α, β have the same minimal polynomial f, as f is irreducible. Therefore, τ maps $k(\alpha)$ into $k(\beta)$. Let $\sigma = \tau\,|_{k(\alpha)}$: $k(\alpha) \to k(\beta)$ be the restriction. And, since σ is nonzero an automorphism of a field, $\ker(\sigma) = \{0\}$, and it is injective. Furthermore, by the above, σ is clearly surjective, since all linear combinations of powers of β are hit by σ. Thus, σ is a field isomorphism, and we conclude that

$$k(\alpha) \cong k(\beta).$$

Now, as $k(\alpha)$ is a radical extension, we can write

$$k = k_0 \subset k_1 \subset \cdots \subset k_r = k(\alpha)$$

for subfields k_i, where k_{i+1}/k_i is a cyclic extension, or $k_{i+1} = k_i(\sqrt[n_i]{a_i})$ for some $a_i \in k_i$, $n_i \in \mathbb{N}$. Then, mapping everything by the isomorphism σ, we get a radical tower

$$k = k_0' \subset k_1' \subset \cdots \subset k_r' = k(\beta)$$

for subfields $k_i' = \sigma(k_i)$, where again k_{i+1}'/k_i' is a cyclic extension, or $k_{i+1}' = k_i'(\sqrt[n_i]{a_i})$ for some $a_i \in k_i'$, $n_i \in \mathbb{N}$. Thus, $k(\beta)$ is a radical extension as well. It follows that β is expressible in terms of radicals as well. Hence, all roots of f can be written in terms of radicals.

∎

6. Give an example of an extension K/k such that $[K : k] = n$ and a positive integer d dividing n such that there is no intermediate field $k \subset L \subset K$ with $[L : k] = d$.

Let $K = \mathbb{C}[x_1, x_2, x_3, x_4]$ and let $k = K^{A_4}$ be the ring of invariants under the alternating group. By Artin's theorem, $[K : k] = |A_4| = 12$ and the extension is Galois with Galois group A_4. The integer 3 divides 12, but if there were an intermediate field L with $[L : k] = 3$, then the subgroup of automorphisms in Gal (K/k) fixing L would be a subgroup of A_4 of order 6, of which there are none. ∎

7. Let K/k be a Galois extension of degree n with Galois group G. Define the norm and trace maps $N_{K/k} : K \to k$ and $T_{K/k} : K \to k$ by

$$N(a) = \prod_{\sigma \in G} \sigma(a) \quad \text{and} \quad T(a) = \sum_{\sigma \in G} \sigma(a).$$

Suppose that the minimal polynomial of $a \in K$ is $\sum_{i=0}^{r} c_i x^i \in k[x]$. Show that

1. the norm and trace do take values in k, and
2. $N(a) = (-1)^n c_0^{n/r}$ and $T(a) = -\frac{n}{r} c_{r-1}$, and
3. $N(a) = \det(T)$ and $T(a) = \text{Trace} T$ where $T : K \to K$ is the k-linear map $T(b) := ab$.

1. Let $\tau \in G$. Then $\tau(N(a)) = \prod_{\sigma \in G} \tau\sigma(a) = N(a)$, since as σ runs through all of G, $\tau\sigma$ does. Thus $N(a)$ is in the fixed field of G, which is exactly k. Similarly $\tau(T(a)) = \sum_{\sigma \in G} \tau\sigma(a) = T(a)$ so that $T(a)$ is in the fixed field of G, i.e., in k.

2. Let the roots of f be $\alpha_1, \ldots, \alpha_r$ (one of which is equal to a). Since the minimal polynomial of f has degree r, if we let $H = \text{Gal}(K/k(a))$, then H has index r in G.

   Let $\tau_1 H, \ldots, \tau_r H$ be the left cosets of G/H, and fix $\tau_1, \ldots, \tau_r$ as representative elements, and call $T = \{\tau_1 \ldots, \tau_r\}$. First we notice, because $\tau \in G$, that $f(\tau(a)) = \tau(f(a)) = 0$ so that $\tau(a) = \alpha_i$ for some i. Since G acts transitively on the roots of f, for any i there is some $\tau \in G$ so that $\tau(a) = \alpha_i$. Finally, if $\tau(a) \neq \tau_i(a)$ then $\tau \notin \tau_i H$, because H fixes a so every element in the coset must take a to the same point. This means that we can reorder the roots so that $\tau_i(a) = \alpha_i$ (since each α_i must be reached by some τ, and therefore by the representative of the coset that τ is in).

   Notice that $f = (x - \alpha_1) \ldots (x - \alpha_r)$ so that $\prod_{i=1}^{r} (\alpha_i) = (-1)^r c_0$. Therefore, because a lies in the fixed field of H:

$$N(a) = \prod_{\sigma \in G} \sigma(a) = \prod_{\tau \in T} \prod_{\sigma \in H} \tau\sigma(a) = \left(\prod_{\tau \in T} \tau(a) \right)^{n/r} = \left(\prod_{i=1}^{r} \alpha_i \right)^{n/r} = (-1)^n c_0^{n/r}.$$

   Next notice that $\sum_{i=1}^{r} \alpha_i = -c_{r-1}$, so that,

$$T(a) = \sum_{\sigma \in G} \sigma(a) = \sum_{\tau \in T} \sum_{\sigma \in H} \tau\sigma(a) = \frac{n}{r} \sum_{\tau \in T} \tau(a) = \frac{n}{r} \sum_{i=1}^{r} \alpha_i = -\frac{n}{r} c_r.$$

3. To illustrate the idea behind the proof, we first assume that $r = n$. Then $1, a, \ldots, a^{n-1}$ is a basis for K/k (order it and call it $b_1, \ldots, b_n$). Since $f(a) = 0$ then we solve and get that $a^n = -c_0 - \ldots - c_{n-1}a^{n-1}$. So computing the matrix for T as if $r = n$ then if $i \neq n$ then $T(b_i) = T(a^{i-1}) = a^i = b^{i+1}$. And $T(b_n) = T(a^{n-1}) = a^n = -c_0 - \ldots - c_{n-1}a^{n-1} = -c_0 b_1 - \ldots - c_{n-1}b_n$. So we have the following matrix.

$$R = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & 0 & \ddots & 1 \\ -c_0 & -c_1 & -c_2 & \cdots & -c_{n-1} \end{pmatrix}.$$

It is clear that Trace$R = -c_{n-1}$ and cofactor expanding along the first column we see that $\det R = (-1)^r c_0^r$.

Now we assume that $r < n$. We see now that $1, \ldots, a^{r-1}$ is a basis for $k(a)/k$. Let $\beta_1, \ldots, \beta_{r/n}$ be a basis for $K/k(a)$. Then $\{\beta_i a_j | 1 \leq i \leq r/n, 0 \leq j \leq r-1\}$ is a basis for K/k. If we order this as $\beta_1, \beta_1 a \ldots, \beta_1 a^{r-1}, \beta_2, \ldots, \beta_{r/n}a^{r-1}$, we can compute the matrix for T by seeing what T does to the basis elements. But this is easy, because $T(\beta_i a^j) = \beta_i a^{j+1}$ where $j \neq n-1$ and $T(\beta_i a^{n-1}) = -\beta_i c_0 - \beta_i a c_1 - \ldots - \beta_i a^{n-1} c_{n-1}$. So the matrix for T is exactly,

$$T = \begin{pmatrix} R & 0 & \cdots & 0 \\ 0 & R & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & R \end{pmatrix}.$$

Then clearly $\operatorname{Det} T = \operatorname{Det} R^{n/r} = (-1)^r c_0^{n/r} = N(a)$, and Trace$T = \frac{n}{r}$Trace$R = \frac{n}{r}(-c_{n-1}) = T(a)$.

■