Let $E = \sigma \tau$ be a field intermediate between $K$ and $K(\alpha)$. Clearly contains $\alpha$ expressions is 10, is fixed by $\alpha$, which fixes $\tau \sigma$, which fixes $\alpha$. The square of each of the automorphisms is the identity; for example, if $\alpha$ sends $2$ to $2^\tau$, then $\alpha^2$ sends $2$ to $2^\tau \alpha = \alpha$. Hence the field $\alpha$ is a Klein 4-group (and not a cyclic group of order 4).

If $\sigma$ is an automorphism of $K$, $\sigma$ is determined by $\sigma(\alpha)$, which is one of the four roots of $t^4 - 6t^2 + 4$. The square of each of the automorphisms is the identity; for example, if $\tau$ sends $\alpha$ to $2/\alpha$, then $\tau^2$ sends $\alpha$ to $2/\tau(\alpha) = \alpha$, so $\tau$ is the identity. It is clear, then, that $G$ is a Klein 4-group (and not a cyclic group of order 4).

1. Suppose that $K$ is a subfield of the complex field $\mathbb{C}$ and that $\alpha \in \mathbb{C}$ is algebraic over $K$. Let $E$ be a field intermediate between $K$ and $K(\alpha)$: $K \subseteq E \subseteq K(\alpha)$. Let

$$p(t) = t^d + a_{d-1}t^{d-1} + \cdots + a_1t + a_0$$

be the minimal polynomial of $\alpha$ over $E$. Show that $E = K(a_0, a_1, \ldots, a_{d-1})$.

This was on the homework some weeks ago. Let $F = K(a_0, a_1, \ldots, a_{d-1})$, so that $F \subseteq E$. The degree of $K(\alpha)$ over $E$ is $d$ because of the definition of $p$. On the other hand, $\alpha$ satisfies $p(t)$ over the field $F$, so that $[K(\alpha) : F] \leq d$. We have, on the other hand, $[K(\alpha) : F] = [K(\alpha) : E][E : F] = d[E : F]$, so we get $[E : F] \leq 1$, which implies that $E = F$.

2. Let $\alpha = \sqrt{3 + \sqrt{5}} \approx 2.2882$, and let $K = \mathbb{Q}(\alpha)$. Let $L$ be the splitting field of the minimal polynomial of $\alpha$. (a) Find the Galois group $G = \text{Gal}(L : \mathbb{Q})$ of the extension $L : \mathbb{Q}$. (b) Find all subgroups of $G$. (c) For each subgroup $H$ of $G$, identify the fixed field of $H$.

We see that $\alpha$ satisfies the polynomial $t^4 - 6t^2 + 4$, whose roots are $\pm \alpha, \pm \frac{2}{\alpha}$. Since these roots can be expressed as polynomials in $\alpha$, $L = K$. If we square the symmetric-looking expressions $\alpha + 2/\alpha$ and $\alpha - 2/\alpha$, we get $10$ and $2$, respectively. Thus, the field $K$, which clearly contains $\sqrt{5}$, contains $\sqrt{2}$ as well. We have seen in previous computations and homework problems that $2$ is not a square in $\mathbb{Q}(\sqrt{5})$. (We’ve seen enough similar things that I won’t require you to prove this fact.) Hence the field $\mathbb{Q}(\sqrt{2}, \sqrt{5})$, which is contained in $K$, has degree $4$. Since $t^4 - 6t^2 + 4$ is of degree $4$, $[K : \mathbb{Q}] \leq 4$, and we get that $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. This field has exactly $4$ automorphisms, including the identity. If $\sigma$ is an automorphism of $K$, $\sigma$ is determined by $\sigma(\alpha)$, which is one of the four roots of $t^4 - 6t^2 + 4$. The square of each of the automorphisms is the identity; for example, if $\tau$ sends $\alpha$ to $2/\alpha$, then $\tau^2$ sends $\alpha$ to $2/\tau(\alpha) = \alpha$, so $\tau$ is the identity. It is clear, then, that $G$ is a Klein $4$-group (and not a cyclic group of order $4$). If $\sigma$ sends $\alpha$ to $-\alpha$ and $\tau$ is as described, then $\alpha^2$ is fixed by $\sigma$, so the fixed field of $\sigma$ is $\mathbb{Q}(\sqrt{5})$. The quantity $\alpha + 2/\alpha$, whose square is $10$, is fixed by $\tau$, so the fixed field of $\tau$ is $\mathbb{Q}(\sqrt{10})$. The final non-identity element of $G$ is $\sigma \tau = \tau \sigma$, which fixes $\alpha - 2/\alpha$. Thus the fixed field of the group generated by $\sigma \tau$ is $\mathbb{Q}(\sqrt{2})$. 

This exam was an 80-minute exam. It began at 3:40PM. There were 4 problems, for which the point counts were 7, 8, 8 and 7. The maximum possible score was 30.

Please put away all books, calculators, electronic games, cell phones, pagers, .mp3 players, PDAs, and other electronic devices. You may refer to a single 2-sided sheet of notes. Please write your name on each sheet of paper that you turn in; don’t trust staples to keep your papers together. Explain your answers in full English sentences as is customary and appropriate. Your paper is your ambassador when it is graded.

Midterm Exam April 8, 2004
Math 114 Professor K. A. Ribet
3. Let $L = \mathbb{Q}(\sqrt[3]{-3}, \sqrt[3]{2})$ be the splitting field of $t^3 - 2$. How many different fields $K$ (other than $\mathbb{Q}$ and $L$) satisfy $\mathbb{Q} \subset K \subset L$? For each field $K$, indicate the degree $[K : \mathbb{Q}]$ and write $K$ in the form $\mathbb{Q}(\alpha)$.

This is a bread and butter sort of problem. The extension $L : \mathbb{Q}$ has degree 6; its Galois group is isomorphic to the symmetric group $S_3$, which is not all that complicated a group. It has 3 subgroups of order 2 and 1 subgroup of order 3. By Galois theory, there are 3 fields $K$ with $[K : \mathbb{Q}] = 3$ and one field $K$ with $[K : \mathbb{Q}] = 2$. The cubic fields are $\mathbb{Q}(\alpha \omega^i)$ where $\alpha$ is the real cube root of 2 and $\omega$ is a non-trivial cube root of 1. The quadratic field is $\mathbb{Q}(\omega)$. You can also label the 6 automorphisms by their effect on $\alpha$ and $\omega$. Let $\sigma$ be the automorphism that sends $\alpha$ to $\alpha \omega$ and that fixes $\omega$. Let $\tau$ be the automorphism that fixes $\alpha$ and sends $\omega$ to $\omega^{-1} = \omega^2$. Then $\sigma$ has order 3 and $\tau$ has order 2. The elements of order 2 are $\tau, \tau \sigma, \tau \sigma^2$. They fix $\alpha, \alpha \omega$ and $\alpha \omega^2$, respectively.

4. Suppose that $p(t)$ is a monic polynomial over $\mathbb{Q}$ and let $p'(t)$ be the derivative of $p(t)$. Suppose that 1 is the highest common factor of $p(t)$ and $p'(t)$ in the ring $\mathbb{Q}[t]$. If $n$ is the degree of $p$, prove that $p(t)$ has $n$ distinct roots in $\mathbb{C}$.

We did this in class—twice. The polynomial $p(t)$ factors over $\mathbb{C}$ into a product of $n$ factors of the form $t - \alpha$ with $\alpha \in \mathbb{C}$. If the roots $\alpha$ are not all distinct, $t - \alpha$ appears as a factor of both $p$ and $p'$ in $\mathbb{C}[t]$. This is impossible for various reasons. For example, by the “hcf” assumption, we may find polynomials $a(t)$ and $b(t)$ with rational coefficients such that $1 = a(t)p(t) + b(t)p'(t)$. If $t - \alpha$ divides both $p$ and $p'$, $t - \alpha$ divides 1, which we know not to be true.