SOLUTIONS TO PROBLEM SET 4

MATTI ÅSTRAND

The Cubic Formula

Denote $L = k(\alpha_1, \alpha_2, \alpha_3)$ and $K = k(a_1, a_2, a_3)$, and define permutations: $\rho = (123)$ and $\nu = (12)$.

Problem 3. The element $\epsilon_1 + \epsilon_2 \in k[S_3]$ is equal to $(1 + \rho + \rho^2)/3$. Thus M is the same as the image of $(1 + \rho + \rho^2)/3$, which I'll denote by φ.

Notice that if $\beta \in L$, then $\rho(\varphi\beta) = (\rho\varphi)\beta = \varphi\beta$. This means that M is contained in the fixed field of ρ, i.e. $M \subseteq L^\rho$. Let's show that in fact $M = L^\rho$. We need to prove the other inclusion, that $L^\rho \subseteq M$. If $\beta \in L^\rho$, then $\rho(\beta) = \beta$, so

$$\varphi(\beta) = (\beta + \rho(\beta) + \rho^2(\beta))/3 = (\beta + \beta + \beta)/3 = \beta.$$

Thus β is the image of itself under the map φ, so $\beta \in M$.

We have shown that $M = L^\rho$, so in particular it is a field. Clearly $M \neq L$, since ρ is a nontrivial automorphism. Also it is easy to see that $M \neq K$: consider

$$\varphi(\alpha_1\alpha_2^2) = \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2.$$

This element is in M, but it is not symmetric: it is not fixed by transpositions. We get that $K \subsetneq M \subsetneq L$, and since $\dim_K L = 6$, we know that $\dim_K M$ and $\dim_M L$ are 2 and 3 in some order.

We can finish the argument by finding an element in $M \setminus K$ whose square is in K. Such an element is for example

$$\sqrt{\sigma} = (1 - \nu)\varphi(\alpha_1\alpha_2^2) = \alpha_1\alpha_2^2 + \alpha_2\alpha_3^2 + \alpha_3\alpha_1^2 - (\alpha_1^2\alpha_2 + \alpha_2^2\alpha_3 + \alpha_3^2\alpha_1).$$

Since $\nu(\sqrt{\sigma}) = -\sqrt{\sigma}$, it follows that $\nu(\sigma) = \sigma$, so $\sigma \in K$.

Remark: You can find an explicit formula for σ in terms of a_1, a_2, a_3:

$$\sigma = a_1^2a_2^2 - 4a_3a_1^3 - 4a_2^3 + 18a_1a_2a_3 - 27a_3^2.$$

Problem 4. This follows directly from the previous problem set: L/M is a degree 3 extension, M contains a cube root of unity, and there is a nontrivial automorphism ρ of L/M. Thus $\mathrm{Aut}(L/M) = \{1, \rho, \rho^2\} = A_3$.

Problem 5. The e_1 in the earlier problem set corresponds to $1 + \mu^2\rho + \mu\rho^2$ in our notation (up to a constant factor), so we get

$$\eta = e_1(\alpha_1) = \alpha_1 + \mu^2\alpha_2 + \mu\alpha_3.$$

It easy to see that $\rho(\eta) = \mu\,\eta$, so $\rho(\eta^3) = \eta^3$. This means that $\eta^3 \in M$, so η is the desired element, and we can choose $\tau = \eta^3$.

Remark: Again, we can find an expression for τ in terms of $a_1, a_2, a_3, \sqrt{\sigma}$:

$$\tau = a_1^3 - \frac{9a_1a_2}{2} + \frac{(6\mu + 3)\sqrt{\sigma}}{2} + \frac{27a_3}{2}.$$

Problem 6. Follows from earlier problems: we know that $\{1, \sqrt{\sigma}\}$ is a basis for M/K and $\{1, \eta, \eta^2\}$ is a basis for L/M.

Problem 7. Denote

$$\eta' = \nu(\eta) = \mu^2\alpha_1 + \alpha_2 + \mu\alpha_3.$$

This satisfies $\rho(\eta') = \mu^2\eta'$, so

$$\rho(\eta\eta') = (\mu\eta)(\mu^2\eta') = \eta\eta'.$$

We get that $\eta\eta' \in M$, so it can be written in terms of $a_1, a_2, a_3, \sqrt{\sigma}$. In fact, we can check that

$$\begin{aligned}\eta\eta' &= \mu^2(\alpha_1^2 + \alpha_2^2 + \alpha_3^2) + (\mu + 1)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1)\\ &= \mu^2(a_1^2 - 2a_2) - \mu^2 a_2 = \mu^2(a_1^2 - 3a_2).\end{aligned}$$

Thus we have an expression for η' in terms of a_i and $\eta = \sqrt[3]{\tau}$. Now we can easily write α_i as linear combinations of the following:

$$\begin{aligned}a_1 &= \alpha_1 + \alpha_2 + \alpha_3\\ \eta &= \alpha_1 + \mu^2\alpha_2 + \mu\alpha_3\\ \eta' &= \mu^2\alpha_1 + \alpha_2 + \mu\alpha_3\end{aligned}$$

Namely:

$$\begin{aligned}\alpha_1 &= \frac{1}{3}(a_1 + \eta + \mu\eta')\\ \alpha_2 &= \frac{1}{3}(a_1 + \mu\eta + \eta')\\ \alpha_3 &= \frac{1}{3}(a_1 + \mu^2\eta + \mu^2\eta')\end{aligned}$$