GALOIS THEORY
Solutions to Worksheet 3

A 1. (a) We have

$$u \mapsto \alpha_2 + \omega\alpha_3 + \omega^2\alpha_1 = \omega^2 u$$

and, similarly, $v \mapsto \omega v$.

(b) Using that $\omega + \omega^2 = -1$ and $\alpha_1 + \alpha_2 + \alpha_3 = 0$, we get, for example:

$$\frac{u+v}{3} = \frac{\alpha_1 + \alpha_1 - \alpha_2 - \alpha_3}{3} = \alpha_1$$

and, similarly, $\alpha_2 = \frac{\omega^2 u + \omega v}{3}$, $\alpha_3 = \frac{\omega u + \omega^2 v}{3}$.

(c) It is pretty obvious that $\tau(u) = v$ and $\tau(v) = u$. The rest of this question requires considerable work and we may return to this point later in the lectures, when we study the Galois group of splitting fields of cubic polynomials in general.

We must use the following facts from elementary algebra:

$$\alpha_1 + \alpha_2 + \alpha_3 = 0, \quad (\alpha_2\alpha_3 + \alpha_1\alpha_3 + \alpha_1\alpha_2) = 3p, \quad \alpha_1\alpha_2\alpha_3 = -2q$$

We will also need to use the (elementary) algebraic identity:

$$(z_1 + z_2 + z_3)(z_2z_3 + z_1z_3 + z_1z_2) = (z_1^2z_2 + z_1^2z_3 + z_1z_2^2 + z_2^2z_3 + z_1z_3^2 + z_2z_3^2) + 3z_1z_2z_3$$

We compute by brute force uv and $u^3 + v^3$: from these quantities it is easy to construct the sought-for quadratic equation. A direct calculation (using $\omega + \omega^2 = -1$!) shows that:

$$uv = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 - \alpha_1\alpha_2 - \alpha_1\alpha_3 - \alpha_2\alpha_3 = (\alpha_1 + \alpha_2 + \alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) = -9p$$

and:

$$\begin{aligned} u^3 + v^3 &= 2(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) - 3(\alpha_1^2\alpha_2 + \alpha_1^2\alpha_3 + \alpha_1\alpha_2^2 + \alpha_2^2\alpha_3 + \alpha_1\alpha_3^2 + \alpha_2\alpha_3^2) + 12\alpha_1\alpha_2\alpha_3 = \\ &= 2(\alpha_1 + \alpha_2 + \alpha_3)^2 - 9(\alpha_1^2\alpha_2 + \alpha_1^2\alpha_3 + \alpha_1\alpha_2^2 + \alpha_2^2\alpha_3 + \alpha_1\alpha_3^2 + \alpha_2\alpha_3^2) = \\ &= 27\alpha_1\alpha_2\alpha_3 = -27 \times 2q \end{aligned}$$

Now write down the quadratic equation and deduce the cubic formula!

A 2. (i) γ clearly satisfies $(\gamma^3 - 1)^2 = 3$, so it's a root of the polynomial $(X^3 - 1)^2 - 3$ which is $X^6 - 2X^3 - 2$. By the Eisenstein criterion this polynomial is irreducible, so it must be the min poly of γ, and the degree of γ over $\mathbb{Q}$ is 6.

Note that $\sqrt{3} = \gamma^3 - 1 \in \mathbb{Q}(\gamma)$ so if $F = \mathbb{Q}(\gamma)$ and $K = \mathbb{Q}(\sqrt{3})$ we must have $\mathbb{Q} \subseteq K \subseteq F$ and the tower law gives $2[F : K] = [K : \mathbb{Q}][F : K] = [F : \mathbb{Q}] = 6$, and we deduce $[F : K] = 3$. Because F contains $\sqrt{3}$ it must contain K and it's not hard to deduce that $F = K(\gamma)$. By the tower law again, the degree of γ over K must then be 3.

Note that if one could show that $X^3 - (1 + \sqrt{3})$ were irreducible in $K[X]$ then this would be another way to do the question, but I did not explain any techniques for tackling this.

(ii) Even more evil trick question. Turns out $\delta = 1 + \sqrt{3}$ (cube it out to check) so the degree is 2 over $\mathbb{Q}$ and also over $\mathbb{Q}(\sqrt{2})$, the latter because $\delta \notin \mathbb{Q}(\sqrt{2})$ (it would imply $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$).

A 3. (i) Spot root $X = 2$; so $X^3 - 8 = (X - 2)(X^2 + 2X + 4)$ and roots of the quadratic are non-real and hence non-rational, so the quadratic must be irreducible (as any factors would be linear).

(ii) Irreducible by Eisenstein ($p = 2$ or $p = 3$).

(iii) The polynomial $X^2 - 2X + 2$ is a factor; dividing out we see $X^4 + 4 = (X^2 - 2X + 2)(X^2 + 2X + 2)$. Easy check now that both quadratics have non-real and hence non-rational roots, so must be irreducible.

(iv) Either this is irreducible over $\mathbb{Q}$, or there is a root in $\mathbb{Q}$ (because any factorization must involve a linear term). So let's substitute in $X = p/q$ in lowest terms (i.e. $\gcd(p, q) = 1$) and see what happens. Clearing denominators we get

$$2p^3 + 5p^2q + 5pq^2 + 3q^3 = 0.$$

Now p divides the first three terms of the left hand side, so must divide the fourth which is $3q^3$. But p and q are coprime! So p must divide 3. A similar argument shows that q must divide 2. So $p = \pm 1$ or ± 3 and $q = \pm 1$ or ± 2. Clearly no positive rational is a root (as all the coefficients are positive) so we are left with the possibilities $X = -1, -1/2, -3, -3/2$ and we just try all of them. Miraculously $X = -3/2$ does work! Pulling off the corresponding linear factor gives

$$2X^3 + 5X^2 + 5X + 3 = (2X + 3)(X^2 + X + 1)$$

and the quadratic term has no real roots and hence no rational ones, so this is the factorization into irreducibles.

(v) This one is irreducible by Eisenstein with $p = 3$.

(vi) There's an obvious factor of $X - 1$ and the other factor $X^{72} + X^{71} + \cdots + X + 1$ is irreducible. To see this first substitute $Y = X - 1$, then apply Eisenstein with $p = 73$ prime.

(vii) This polynomial is obtainable from the polynomial in part (vi): start with the part (vi) polynomial, change X to $-X$ and then change the sign of the polynomial. These sorts of things do not affect things like irreducibility and factorization, so the factorization will be $(X + 1)(X^{72} - X^{71} + \ldots - X + 1)$ and the degree 72 polynomial will be irreducible.

(viii) Spot roots $X = 1$ and $X = -1$. Over the complexes we have more roots too, like $\pm i$ and so on – how do these control factorization over the rationals? Well $(X - i)$ and $(X + i)$ are factors over the complexes, so their product $X^2 + 1$ is a factor over the complexes and hence also over the rationals. Similarly the two complex cube roots of 1 are complex conjugates and are the two roots of $X^2 + X + 1$, and the two 6th roots of 1 that we haven't mentioned

yet ($e^{\frac{2\pi\,\mathrm{i}}{6}}$ and its complex conjugate) are roots of $X^2 - X + 1$. So we've just spotted factors whose degrees add up to 8. Let's see what we have so far then: the factors we have spotted are

$$\begin{aligned}&(X+1)(X-1)(X^2+1)(X^2+X+1)(X^2-X+1)\\ &= (X^2-1)(X^2+1)(X^2+X+1)(X^2-X+1)\\ &= (X^4-1)(X^4+X^2+1)\end{aligned}$$

and so what is left is

$$\begin{aligned}&(X^{12}-1)/(X^4-1)(X^4+X^2+1)\\ &= (X^8+X^4+1)/(X^4+X^2+1)\\ &= X^4 - X^2 + 1\end{aligned}$$

The hardest part of this question is figuring out whether that last polynomial $X^4 - X^2 + 1$ factors.

A 4. The min poly of α must be $X^{10} - 2$ because this is irreducible over $\mathbb{Q}$ (by Eisenstein) and has α as a root. In particular there is no non-zero polynomial of degree at most 9 with rational coefficients and α as a root, so $\{1, \alpha, \alpha^2, \ldots, \alpha^9\}$ are linearly independent elements in a vector space of dimension 10, and hence are a basis.