MAT3011 GALOIS THEORY ANSWERS FOR CHAPTER 2

Exercises 2.1

1. $\mathbb{C}$ has elements which are not algebraic over $\mathbb{Q}$, such as π and e, so $\mathbb{C} : \mathbb{Q}$ is a transcendental extension. By Proposition 2.1 every finite extension is algebraic, so $\mathbb{C} : \mathbb{Q}$ is not finite.

2. (a) $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$. Basis $\{1, \alpha\}$. (b, c): $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Basis $\{1, \alpha, \alpha^2\}$.

   (d, e, f): $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Basis $\{1, \alpha, \alpha^2, \alpha^3\}$.

3. (a) $[\mathbb{Q}(\sqrt{7}) : \mathbb{Q}] = 2$. Basis is $\{1, \sqrt{7}\}$.

   (b) $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$.
   $\{1, 2^{1/3}, 2^{2/3}\}$ is a basis for $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$.
   By the same reasoning as in Examples 2.1.4 (ii), $\{1, 2^{1/3}, 2^{2/3}\}$ is also a basis for $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ over $\mathbb{Q}(\sqrt{2})$, and $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}] = 3 \times 2 = 6$.
   A basis is $\{1, 2^{1/3}, 2^{1/2}, 2^{2/3}, 2^{5/6}, 2^{7/6}\}$. (Can take $2^{1/6}$ instead of $2^{7/6}$.)

   (c) $[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) : \mathbb{Q}] = 8$.
   Basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{6}, \sqrt{10}, \sqrt{15}, \sqrt{30}\}$.

4. $[L : K] = 3 \times 3 = 9$.

   $\{1, \alpha, \alpha^2\}$ is a basis for M over K. $\{1, \beta, \beta^2\}$ is a basis for L over M.

   Hence, as in the proof of the tower law,

   $\{1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2, \alpha^2, \alpha^2\beta, \alpha^2\beta^2\}$ is a basis for L over K.

5. Suppose z is a non-real zero of f with modulus $r \in \mathbb{Q}$. Then $z = re^{i\theta}$ for some $\theta \in \mathbb{R}$, so $\mathbb{Q}(z) = \mathbb{Q}(e^{i\theta})$. By Examples 2.1.4 (iii), $[\mathbb{Q}(z) : \mathbb{Q}]$ is a multiple of 2.

   But f (divided if necessary by its leading coefficient) is the minimal polynomial of z over $\mathbb{Q}$, so $[\mathbb{Q}(z) : \mathbb{Q}] = \partial$f which is odd (given). We have a contradiction so $r \notin \mathbb{Q}$, i.e. $|z|$ is not rational.

6. From Ex. 1.4 Q.3, $t^4 - 2pt^2 + (p^2 - p)$ is the minimal polynomial of α over $\mathbb{Q}$.

   This is a quadratic in t^2. Its other zeros, the conjugates of α, are found to be $-\alpha, \beta, -\beta$ where $\beta = \sqrt{p + \sqrt{p}}$. By Proposition 2.3, $\mathbb{Q}(\alpha) \cong \mathbb{Q}(\beta)$.

   If $\sqrt{p-1} \in \mathbb{Q}$ then $p - 1 = k^2$ for some $k \in \mathbb{Q}$.

   Then $\alpha^2\beta^2 = p^2 - p = p(p-1) = pk^2$, so $\alpha\beta = k\sqrt{p}$.

   Now $\sqrt{p} = p - \alpha^2 \in \mathbb{Q}(\alpha)$, so $\beta = \dfrac{k\sqrt{p}}{\alpha} \in \mathbb{Q}(\alpha)$. Thus $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$.

   As $\mathbb{Q}(\beta) \cong \mathbb{Q}(\alpha)$, it follows that $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$.

7. $(\beta - \mathrm{i})^3 = 2$ so $\beta^3 - 3\mathrm{i}\beta^2 - 3\beta + \mathrm{i} = 2$. Hence $\mathrm{i} = \dfrac{\beta^3 - 3\beta - 2}{3\beta^2 - 1}$.

   Thus i is obtained from β and rationals by field operations, so $\mathrm{i} \in \mathbb{Q}(\beta)$.

   Then also $2^{1/3} = \beta - \mathrm{i} \in \mathbb{Q}(\beta)$.

   It follows that $\mathbb{Q}(2^{1/3}, \mathrm{i}) \subset \mathbb{Q}(\beta)$. Also $\beta \in \mathbb{Q}(2^{1/3}, \mathrm{i})$ so $\mathbb{Q}(\beta) \subset \mathbb{Q}(2^{1/3}, \mathrm{i})$.

   Thus $\mathbb{Q}(2^{1/3}, \mathrm{i}) : \mathbb{Q}$ is the simple extension $\mathbb{Q}(\beta) : \mathbb{Q}$.

8. (a) $K \subset K(\alpha) \subset L$, so by the tower law, $[L : K] = [L : K(\alpha)][K(\alpha) : K]$.

Thus $[K(\alpha) : K]$ divides $[L : K]$.

(b) If $[L : K]$ is a prime p, part (a) gives $[K(\alpha) : K] = 1$ or p.

As $K(\alpha) \neq K$, $[K(\alpha) : K] \neq 1$ so $[K(\alpha) : K] = p$.

Thus $[L : K(\alpha)] = 1$, so $L = K(\alpha)$, i.e. α is a primitive element for $L : K$.

(c) We have $[K(\alpha, \beta) : K] = [K(\alpha, \beta) : K(\alpha)][K(\alpha) : K]$
$= [K(\alpha, \beta) : K(\beta)][K(\beta) : K]$.

Thus both m and n divide $[K(\alpha, \beta) : K]$ so, as $gcd(m, n) = 1$, mn divides $[K(\alpha, \beta) : K]$.

By Proposition 2.4, $[K(\alpha, \beta) : K(\alpha)] \leq n$, so $[K(\alpha, \beta) : K] \leq mn$.

Hence $[K(\alpha, \beta) : K] = mn$,

so $[K(\alpha, \beta) : K(\alpha)] = n$, which equals $[K(\beta) : K]$.

Exercises 2.2

1. (a) An angle of $\frac{\pi}{8}$. Yes: construct a right angle, bisect it and bisect it again.

(b) An acute angle $\frac{\theta}{3}$, where $\cos\theta = \frac{1}{3}$.

$\cos\theta = 4\cos^3\frac{\theta}{3} - 3\cos\frac{\theta}{3}$, so if $u = \cos\frac{\theta}{3}$ we have $\frac{1}{3} = 4u^3 - 3u$, i.e. $12u^3 - 9u - 1 = 0$.

$12u^3 - 9u - 1$ is irreducible over $\mathbb{Q}$ by EIC with $p = 3$ and Proposition 1.13. Thus $[\mathbb{Q}(u) : \mathbb{Q}] = 3 \neq 2^m$, so u is is not constructible, hence nor is $\frac{\theta}{3}$.

(c) A triangle equal in area to a given pentagon. Yes. The pentagon can be reduced to a quadrilateral and then

a triangle of equal area by methods similar to Example 7 on page 30 of the notes.

(d) A circle with circumference equal to the perimeter of a given square. No. If the square has side a then the circle has radius r where $2\pi r = 4a$, so $r = \dfrac{2a}{\pi}$ which is not constructible in general.

(e) A regular heptagon. No. 7 is prime, but it is not of the form $2^m + 1$.

(f) $60 = 2^2 \times 3 \times 5$, a product of a power of 2 and distinct Fermat primes, so by Proposition 2.9 the polygon can be constructed.

2. Start with a line, construct another line at an angle θ to it, then a third line making an angle ϕ with the second one. The first and last lines contain an angle $\theta + \phi$. A similar method gives $\theta - \phi$.

   OR: $\cos(\theta + \phi) = \cos\theta\cos\phi - \sin\theta\sin\phi$ and $\cos(\theta - \phi) = \cos\theta\cos\phi + \sin\theta\sin\phi$

   As $\cos\theta$ is constructible, so is $\sin\theta = \sqrt{1 - \cos^2\theta}$. The product, sum and difference of constructible numbers are constructible, so $\cos(\theta+\phi)$ and $\cos(\theta-\phi)$ are constructible, hence so are are $\theta + \phi$ and $\theta - \phi$.

3. Take $5\theta = \phi$, so $\theta = \dfrac{\phi}{5}$ and $\cos 5\theta = \dfrac{5}{6}$. Then $\dfrac{5}{6} = 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta$,

   so $96\cos^5\theta - 120\cos^3\theta + 30\cos\theta - 5 = 0$.

   Thus $\cos\theta$ is a zero of $96t^5 - 120t^3 + 30t - 5$. This is irreducible over $\mathbb{Q}$ by EIC with $p = 5$, so $[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 5$.

   As 5 is not a power of 2, $\cos\theta$ is not a constructible real number. Hence θ is not a constructible angle, so ϕ cannot

be divided into five equal parts by construction.

4. An angle of n degrees, where $n \in \mathbb{N}$, is constructible if and only if n is an integer multiple of 3. For a proof of this see, for example,

   `http://planetmath.org/constructibleangleswithintegervaluesindegrees`

   (a) $= 39°$ so is constructible. (b) $= 40°$ so is not constructible.

   (c) is not an integer number of degrees, so we cannot tell.

5. $\sum_{i=0}^{2n}(-r)^i$ has first term 1, common ratio $-r$ and $2n+1$ terms, so it equals $\dfrac{1-(-r)^{2n+1}}{1-(-r)}$. As $2n+1$ is odd, $(-1)^{2n+1} = -1$ so the sum equals $\dfrac{1+r^{2n+1}}{1+r}$.

   Clearly this sum is an integer, so $1+r$ divides $1+r^{2n+1}$. Taking $r = 2^{2^k}$ and $2n+1 = a$ (odd), $m = a(2^k)$, it follows that $1+2^{2^k}$ divides $1+2^m$, as required.

   Thus if $a > 1$, $1+2^{a(2^k)}$ has a factor $1+2^{2^k}$ so it is composite. Hence if $1+2^{2^k}$ (which is certainly odd) is prime, we must have $a = 1$ so $m = 2^k$ for some $k \geq 0$.

Exercises 2.3

1. The splitting fields can be described (not necessarily uniquely) as

   Q.3: (a) $\mathbb{Q}(\alpha, \omega)$, (b) $\mathbb{Q}(\omega)$, (c) $\mathbb{Q}$, (d) $\mathbb{Q}(\alpha, \omega)$, (e) $\mathbb{Q}(\sqrt{3}(e^{\pi i/18} + e^{-\pi i/18}))$.

   Q.9: (a) $\mathbb{Q}(i\sqrt{6}, \sqrt{2})$, (b) $\mathbb{Q}(i\sqrt{5}, \sqrt{3})$.

2. (a) $t^4+5t^2+6 = (t^2+2)(t^2+3) = (t+\mathrm{i}\sqrt{2})(t-\mathrm{i}\sqrt{2})(t+\mathrm{i}\sqrt{3})(t-\mathrm{i}\sqrt{3})$ over its splitting field $\mathbb{Q}(\mathrm{i}\sqrt{2},\mathrm{i}\sqrt{3})$.

   (b) Solving as a quadratic in t^2 we find that t^4+3t^2-1 has zeros $\pm\alpha, \pm\beta$ where $\alpha = \frac{1}{2}\sqrt{2\sqrt{13}-6}$ and $\beta = \frac{1}{2}\mathrm{i}\sqrt{2\sqrt{13}+6}$,

   so $t^4+3t^2-1 = (t-\alpha)(t+\alpha)(t-\beta)(t+\beta)$.

   $\alpha\beta = \mathrm{i}$ so $\beta \notin \mathbb{Q}(\alpha)$, so the splitting field is $\mathbb{Q}(\alpha,\beta)$, or equivalently $\mathbb{Q}(\alpha,\mathrm{i})$ or $\mathbb{Q}(\beta,\mathrm{i})$.

   (c) t^7-1 has zeros equal to the seventh roots of 1, i.e. $\mathrm{e}^{2k\pi\mathrm{i}/7}, k = 0,\ldots,6$. The splitting field is $\mathbb{Q}(\mathrm{e}^{2\pi\mathrm{i}/7})$.

   Let $\varepsilon = \mathrm{e}^{2\pi\mathrm{i}/7}$; then $t^7-1 = (t-1)(t-\varepsilon)(t-\varepsilon^2)(t-\varepsilon^3)(t-\varepsilon^4)(t-\varepsilon^5)(t-\varepsilon^6)$.

3. $(\sqrt{3}+\sqrt{7})^2 = 10+2\sqrt{21}$.

   Let $y = x^2$, so $\mathrm{f}(x) = y^2-20y+16$ with roots $y = 10\pm 2\sqrt{21}$.

   Thus the zeros of f are $\pm(\sqrt{3}+\sqrt{7}), \pm(\sqrt{3}-\sqrt{7})$. $L = \mathbb{Q}(\sqrt{3},\sqrt{7})$.

   $\mathrm{f} = (t^2-2\sqrt{3}t-4)(t^2+2\sqrt{3}t-4)$ over $\mathbb{Q}(\sqrt{3})$,

   or $\mathrm{f} = (t^2-2\sqrt{7}t+4)(t^2+2\sqrt{7}t+4)$ over $\mathbb{Q}(\sqrt{7})$.

4. (a) $\mathbb{Q}(2^{1/2}) : \mathbb{Q}$ is normal, as $\mathbb{Q}(2^{1/2})$ is the splitting field of $t^2-2 \in \mathbb{Q}[t]$.

   (b) $\mathbb{Q}(2^{1/6}) : \mathbb{Q}$ is not normal, as $t^6-2 \in \mathbb{Q}[t]$ has one zero in $\mathbb{Q}(2^{1/6})$ but its other zeros in $\mathbb{C}$ are not real, so are not in $\mathbb{Q}(2^{1/6})$.

   (c) $\mathbb{Q}(2^{1/6}) : \mathbb{Q}(2^{1/3})$ is normal, as $\mathbb{Q}(2^{1/6})$ is the splitting field of $t^2-2^{1/3} \in \mathbb{Q}(2^{1/3})[t]$.

(d) $\mathbb{Q}(2^{1/6}) : \mathbb{Q}(2^{1/2})$ is not normal, as $t^3 - 2^{1/2} \in \mathbb{Q}(2^{1/2})[t]$ has one zero in $\mathbb{Q}(2^{1/6})$ but its other zeros in $\mathbb{C}$ are not real, so are not in $\mathbb{Q}(2^{1/6})$.

(e) We have seen that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. The minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$ is $\mu = t^4 - 10t^2 + 1$ which has zeros $\pm(\sqrt{2} \pm \sqrt{3})$. These are all in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, which is thus the splitting field of μ over $\mathbb{Q}$. Hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ is a normal extension.

(f) $\mathbb{Q}(5^{1/7})$. Consider the polynomial $\mathrm{f} = t^7 - 5$. One zero of f is $5^{1/7}$, but the other zeros in $\mathbb{C}$ are not real, so are not in $\mathbb{Q}(5^{1/7})$. Thus $\mathbb{Q}(5^{1/7}) : \mathbb{Q}$ is not a normal extension.

(g) $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/5}) : \mathbb{Q}$ is normal, as $\mathbb{Q}(\mathrm{e}^{2\pi \mathrm{i}/5})$ is the splitting field over $\mathbb{Q}$ of Φ_5 (or of $t^5 - 1$).

5. (a) $\mathrm{f}(t-1) = (t-1)^6 - (t-1)^3 + 1$
$= t^6 - 6t^5 + 15t^4 - 20t^3 + 15t^2 - 6t + 1 - (t^3 - 3t^2 + 3t - 1) + 1$
$= t^6 - 6t^5 + 15t^4 - 21t^3 + 18t^2 - 9t + 3$ which is irreducible over $\mathbb{Q}$ by EIC with $p = 3$.

(b) If $\alpha^6 - \alpha^3 + 1 = 0$ then $\alpha^3 = \dfrac{1}{2}(1 \pm \sqrt{-3}) = \dfrac{1}{2} \pm \dfrac{\mathrm{i}\sqrt{3}}{2}$
$= \mathrm{e}^{\pi \mathrm{i}/3}$ or $\mathrm{e}^{5\pi \mathrm{i}/3}$.

(c) We have $\varepsilon^6 = \mathrm{e}^{2\pi \mathrm{i}/3} = \omega$.

The values of α^3 found in (b) are ε^3 and ε^{15} so $\alpha = \varepsilon, \varepsilon\omega, \varepsilon\omega^2, \varepsilon^5, \varepsilon^5\omega, \varepsilon^5\omega^2$.

Hence the zeros of f are $\varepsilon, \varepsilon^5, \varepsilon^7, \varepsilon^{11}, \varepsilon^{13}, \varepsilon^{17}$.

(d) The splitting field L must contain ε as this is a zero of f, so $L \subset \mathbb{Q}(\varepsilon)$.

All powers of ε are in $\mathbb{Q}(\varepsilon)$, so $\mathbb{Q}(\varepsilon)$ contains all the zeros of f. No smaller field contains ε, so $\mathbb{Q}(\varepsilon)$ is the splitting field of f.

The minimal polynomial of ε over $\mathbb{Q}$ is $\mathrm{f} = t^6 - t^3 + 1$, as this is monic, irreducible over $\mathbb{Q}$ and has ε as a zero.

(e) $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] = \partial \mathrm{f} = 6$. A basis is $\{1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4, \varepsilon^5\}$. The extension is normal, as $\mathbb{Q}(\varepsilon)$ is a splitting field over $\mathbb{Q}$.

(f) $\mathrm{g}(1)$ and $\mathrm{g}(-1)$ are not zero, so by the RRT g has no linear factor in $\mathbb{Q}[t]$. As g is cubic, this is enough to show that it is irreducible over $\mathbb{Q}$.

(g) The Vieta substitution $x = z + \dfrac{1}{z}$ gives

$\mathrm{g} = z^3 + \dfrac{1}{z^3} - 1 = \dfrac{z^6 - z^3 + 1}{z^3}$. The values of z which make this zero are the values of α found in (c).

Thus the zeros of g are $\varepsilon + \dfrac{1}{\varepsilon}, \varepsilon^5 + \dfrac{1}{\varepsilon^5}, \varepsilon^7 + \dfrac{1}{\varepsilon^7}$.

Using $\varepsilon^{18} = 1$, these are $\varepsilon + \varepsilon^{17}, \varepsilon^5 + \varepsilon^{13}, \varepsilon^7 + \varepsilon^{11}$. All three zeros are real as they are sums of conjugate pairs, or because $\Delta(\mathrm{g}) = 108 - 27 = 81 > 0$.

(h) $\Delta(\mathrm{g})$ has a rational square root, so by Proposition 2.11 the splitting field of g is $\mathbb{Q}(\varepsilon + \varepsilon^{17})$.

6. The polynomial $(t - \alpha_1)(t - \alpha_2) \cdots (t - \alpha_m)$ is not necessarily in $K[t]$, i.e. when it is expanded the coefficients may not be in K.

7. From Proposition 1.6 the zeros of ρ are obtained from the zeros of f by field operations, so they are in the splitting field of f. Hence the splitting field of ρ is contained in that of f.

   Suppose f is irreducible over $\mathbb{Q}$ and let α_1 be a zero of f, so $[\mathbb{Q}(\alpha_1) : \mathbb{Q}] = \partial \mathrm{f} = 4$. If α_1 is constructible, there is an intermediate field K_1, between $\mathbb{Q}$ and $\mathbb{Q}(\alpha_1)$, such that $[\mathbb{Q}(\alpha_1) : K_1] = [K_1 : \mathbb{Q}] = 2$. Then $K_1 = \mathbb{Q}(\sqrt{\varepsilon})$ for some $\varepsilon \in \mathbb{Q}$.

Thus the minimal polynomial of α_1 over K_1 is quadratic, say $\mu = t^2+pt+q$ where $p, q \in K_1$. f is also a polynomial in $K_1[t]$ having α_1 as a zero, so $\mu \mid$ f. Hence both zeros of μ are zeros of f.

Let α_2 be the other zero of μ. Then $\alpha_1+\alpha_2 = -p = a+b\sqrt{\varepsilon}$ for some $a, b, \varepsilon \in \mathbb{Q}$, so $\alpha_1 + \alpha_2$ is constructible.

Letting α_3, α_4 be the other zeros of f, we have $\alpha_3 + \alpha_4 = -(\alpha_1 + \alpha_2)$, which is also constructible, hence so is $u = (\alpha_1+\alpha_2)(\alpha_3+\alpha_4)$ which is a zero of ρ. Thus $[\mathbb{Q}(u) : \mathbb{Q}] \neq 3$, so ρ is reducible over $\mathbb{Q}$.

Let $\mathrm{f} = t^4 + t - 5$. Then $\mathrm{f}(1) = -3$, $\mathrm{f}(2) = 13$, so f has a real zero $\alpha \in (1, 2)$.

Trying $\pm 1, \pm 5$, we see that f has no rational zeros by the Rational root theorem. We can also check that it has no quadratic factors. Hence f is irreducible over $\mathbb{Q}$, so it is the minimal polynomial of α over $\mathbb{Q}$. Thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, which is a power of 2.

$\rho = t^3+20t+1$, which is irreducible over $\mathbb{Q}$ by the Rational root theorem as $\partial\rho \leq 3, \rho(-1) \neq 0, \rho(1) \neq 0$. Hence by the above, α is not constructible.

8. As $\chi(K) = 0$, K has infinitely many elements so $\{\alpha + k\beta \ : \ k \in K\}$ is an infinite set.

   However, the fields $K(\alpha + k\beta)$ cannot all be distinct since they contain K, and are contained in $K(\alpha, \beta)$, and we are told that there are only finitely many such fields.

   Thus we can find (infinitely many) pairs $k_1, k_2 \in K$ such that $K(\alpha + k_1\beta) = K(\alpha + k_2\beta)$.

   For such k_1, k_2 we have that both $\alpha + k_1\beta$ and $\alpha + k_2\beta$ are in the field $K(\alpha + k_1\beta)$, hence so is their difference

$(k_1 - k_2)\beta$.

As $k_1 - k_2 \in K \subset K(\alpha + k_1\beta)$, it follows that $\beta \in K(\alpha + k_1\beta)$.

But then also $\alpha = (\alpha + k_1\beta) - k_1\beta \in K(\alpha + k_1\beta)$, so $K(\alpha, \beta) \subset K(\alpha + k_1\beta)$.

Clearly $K(\alpha + k_1\beta) \subset K(\alpha, \beta)$, so we have $K(\alpha, \beta) = K(\alpha + k_1\beta)$, i.e. $\alpha + k_1\beta$ is a primitive element for the extension $K(\alpha, \beta) : K$.

Now let $K(\alpha_1, \ldots, \alpha_n)$ where the number of intermediate fields is finite. We have seen that this is a simple extension of K when $n = 2$. (It is trivially so when $n = 1$.)

Assume it is true for some n, so there exists γ such that $K(\alpha_1, \ldots, \alpha_n) = K(\gamma)$.

Then $K(\alpha_1, \ldots, \alpha_{n+1}) = K(\gamma, \alpha_{n+1}) = K(\gamma + k\alpha_{n+1})$ for some $k \in K$, as shown above.

Hence the result holds for $n + 1$, so by induction it is true for all $n \in \mathbb{N}$.