Solution Sheet 7:

1. Observe that μ is a root of x^n-1 if and only if μ is a dth root of unity for some d dividing n. Therefore $\Phi_n(x)$ is given by $\Phi_n(x) = (x^n-1)/\prod_{d|n}\Phi_d(x)$. We reason by induction over n. Clearly for $n=1$ $\Phi_1(x) = x-1 \in \mathbb{Z}[x]$ and it is monic. Now suppose that $\forall m<n$ $\Phi_m(x)\in\mathbb{Z}[x]$ and is monic. Then $\Phi_n(x)\prod_{d|n}\Phi_d(x) = x^n-1$ in $\mathbb{Q}[x]$ and $\prod_{d|n}\Phi_d(x)$ is monic and it is in $\mathbb{Z}[x]$. Then by Gauss' lemma $\Phi_n(x)$ is in $\mathbb{Z}[x]$ monic.

It remains to show that $\Phi_n(x)$ is irreducible in $\mathbb{Q}[x]$. It is enough to show this in $\mathbb{Z}[x]$ by Gauss' lemma. Suppose that $\Phi_n(x) = f\cdot g$ with $f,g\in\mathbb{Z}[x]$ and f irreducible. Let w be a root of f then w is a primitive nth root of unity. Let $p<n$ be a prime number not dividing n. Then w^p is also a primitive nth root of unity $\Rightarrow$ either $f(w^p)=0$ or $g(w^p)=0$. Suppose that $g(w^p)=0$ Then $f(x)\mid g(x^p)$ because w is a root of both $f(x)$ and $g(x^p)$ moreover f is irreducible.

Reduce the coefficients of $\Phi_n(x), f(x)$ and $g(x)$ modulo p and denote the new polynomials by $\bar{\Phi}_n(x), \bar{f}(x), \bar{g}(x)$. Then $\bar{f}(x)\mid\bar{g}(x^p) = \bar{g}(x)^p$. Let $\bar{q}$ be an irreducible factor of $\bar{f}(x)$, then $\bar{q}\mid\bar{g}(x)^p \Rightarrow \bar{q}\mid\bar{g}(x) \Rightarrow \bar{q}\cdot\bar{q}\mid\bar{f}\cdot\bar{g}$
$\Rightarrow \bar{q}^2\mid\bar{f}\cdot\bar{g} = \bar{\Phi}_n(x)$. However $\bar{\Phi}_n(x)\mid x^n-1 \Rightarrow \bar{q}^2\mid x^n-1$.
But x^n-1 is separable in $\mathbb{F}_p[x]$ so we get a contradiction and $f(x^p)=0$.

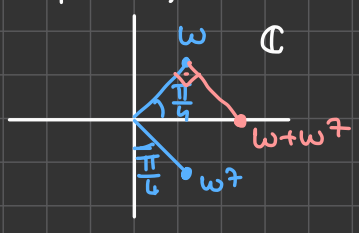
Repeating this argument by using various prime numbers p' we obtain that $f(x^{p'})=0$ This way we obtain that for every primitive nth root of unity ξ_n, $f(\xi_n)=0$
$\Rightarrow f = \Phi_n(x) \Rightarrow \Phi_n(x)$ is irreducible.

2. (i) Notice that $\mathbb{Q}_n = \mathbb{Q}(w)$ where w is a primitive nth root of unity. Indeed, every nth root of unity is given by a power of w.
By the first exercise, $\min_{w,\mathbb{Q}} = \Phi_n(x)$ and $\deg\Phi_n(x) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.
$\Rightarrow [\mathbb{Q}(w):\mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times|$.
Finally, $\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}) \le (\mathbb{Z}/n\mathbb{Z})^\times$ & $|\mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q})| = |(\mathbb{Z}/n\mathbb{Z})^\times|$
$\Rightarrow \mathrm{Gal}(\mathbb{Q}(w)/\mathbb{Q}) = \mathbb{Z}/n\mathbb{Z}^\times$.

(ii) Clearly, $\mathbb{Q}_n \subseteq \mathbb{Q}_{2n}$. As n is odd $\gcd(2,n)=1$ therefore $\phi(2n) = \phi(2)\cdot\phi(n)$
$= 1\cdot\phi(n)$ where ϕ is the Euler totient function.
$\Rightarrow \phi(n) = [\mathbb{Q}_{2n}:\mathbb{Q}_n][\mathbb{Q}_n:\mathbb{Q}] = [\mathbb{Q}_{2n}:\mathbb{Q}_n]\cdot\phi(n) \Rightarrow [\mathbb{Q}_{2n}:\mathbb{Q}_n] = 1$.

(iii) We claim that $\mathbb{Q}_8$ is such a field. By point (v) of this exercise,

$\mathbb{Q}(w+w^7) \subseteq \mathbb{Q}_8$ where $w = e^{\frac{\pi i}{8}}$. We show that $w+w^7 = \sqrt{2}$. This can be seen for instance by considering w and w^7 in the complex plane:



Clearly $w+w^7\in\mathbb{R}$ as $\bar{w} = w^7$.
Now $0, w, w+w^7$ form a perpendicular triangle and two sides of this triangle are $|w|=1$, $|w^7|=1$. By Pythagoras' theorem $|w+w^7| = \sqrt{2}$.

Therefore $\mathbb{Q}(w+w^7) = \mathbb{Q}(\sqrt{2})$. Now $\mathbb{Q}(\sqrt{2})\subseteq\mathbb{R}$ but $\mathbb{Q}(\xi_n)\not\subseteq\mathbb{R}$ where ξ_n is a primitive nth root of unity with $n\ge 3$ therefore $\mathbb{Q}(\sqrt{2})$ is not cyclotomic.

(iv) We follow Exercise 3.2 of Milne's book. Let p be an odd prime. And let ω be a primitive pth root of unity and $E = \mathbb{Q}(\omega)$. Let $G = Gal(E/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$ recall that $G \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Let $H \leq G$ be a subgroup of index 2, it exists as p is odd. let $\alpha = \sum_{i \in H} \omega^i$, $\beta = \sum_{i \in G \setminus H} \omega^i$. Let us show that H fixes α and β. It is clear that $H\alpha = \alpha$. To see that H also fixes β note that $G = H \sqcup \sigma H$ for any $\sigma \in G \setminus H$.

Therefore we may write $\beta = \sum_{\psi \in H} \sigma\psi(\omega)$ and for $\delta \in H$, $\delta(\beta) = \delta(\sum_{\psi \in H} \sigma\psi(\omega))$ $= \sum_{\psi \in H} \delta\sigma\psi(\omega) \overset{(*)}{=} \sum_{\psi \in H} \sigma(\delta\psi)(\omega) = \beta$ where $(*)$ holds as G is abelian.

Now let $\sigma \in G \setminus H$ then $\sigma(\alpha) = \sum_{\psi \in H} \sigma\psi(\omega) = \beta$. Note that as $\sigma \notin H$, we also have that $\sigma^{-1} \notin H$ therefore we can write $\beta = \sum_{\psi \in H} \sigma^{-1}\psi(\omega)$ this shows that clearly $\sigma.\beta = \alpha$.

Notice that $[\mathbb{Q}(\omega)^H : \mathbb{Q}] = 2$ and define $L := \mathbb{Q}(\omega)^H$. Then $Gal(L/\mathbb{Q}) = \{id, \sigma\}$ where $\sigma(\alpha) = \beta$ and $\sigma(\beta) = \alpha$ therefore $\alpha, \beta \in L \setminus \mathbb{Q}$. $\Rightarrow L \supseteq \mathbb{Q}(\alpha)$ but by a degree argument we see that $L = \mathbb{Q}(\alpha)$. Now as $L/\mathbb{Q}$ is Galois σ permutes the roots of $m_{\alpha,\mathbb{Q}}$ therefore $m_{\alpha,\mathbb{Q}} = (X-\alpha)(X-\beta) = X^2 - (\alpha+\beta)X + \alpha\beta$. By definition of α, β we see that $\alpha + \beta = -1$. $\Rightarrow m_{\alpha,\mathbb{Q}} = X^2 + X + \alpha\beta$.

Once the computation of $\alpha\beta$ is carried out, it can be observed that the roots of $X^2 + X + \alpha\beta$ are $\begin{cases} -1 \pm \sqrt{p}/2 & \text{if } p = 1 \bmod 4 \\ -1 \pm \sqrt{-p}/2 & \text{if } p = 3 \bmod 4 \end{cases}$

This shows that the fixed field of H is $\mathbb{Q}(\sqrt{p})$ if $p = 1 \bmod 4$ and it is $\mathbb{Q}(i\sqrt{p})$ if $p = 3 \bmod 4$. The computation of α, β is somewhat complicated we refer to the solution of exercise 3.2 in Milne's notes for it.

We also know that $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}_8$ moreover $i \in \mathbb{Q}_4$. Using all this we obtain the square root of every prime number in some cyclotomic extension. Writing $\alpha = \frac{a}{b}$ for $a, b \in \mathbb{Z}$ and using the prime decompositions of a and b we can find a cyclotomic extension such that $\mathbb{Q}(\sqrt{a}, \sqrt{b}) \subseteq \mathbb{Q}_n$. $\Rightarrow \mathbb{Q}(\sqrt{\alpha}) \subseteq \mathbb{Q}_n$.

(v) $Gal(\mathbb{Q}_8/\mathbb{Q}) = (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
Let ω be a primitive 8th root of unity. Then $\mathbb{Q}_8 = \mathbb{Q}(\omega)$.

The primitive 8th roots of unity are $\omega, \omega^3, \omega^5, \omega^7$ therefore the automorphisms in $Gal(\mathbb{Q}_8/\mathbb{Q})$ are id, $\sigma_3 : \omega \mapsto \omega^3$, $\sigma_5 : \omega \mapsto \omega^5$, $\sigma_7 : \omega \mapsto \omega^7$. Notice that the nontrivial intermediate fields $\mathbb{Q} \subsetneq L \subsetneq \mathbb{Q}_8$ are of the form $\mathbb{Q}_8^{\sigma_3}$, $\mathbb{Q}_8^{\sigma_5}$, $\mathbb{Q}_8^{\sigma_7}$. Notice that

$\omega + \omega^3 \in \mathbb{Q}_8^{\sigma_3}$ and $\omega + \omega^7 \in \mathbb{Q}_8^{\sigma_7}$ moreover $\omega + \omega^3, \omega + \omega^7 \notin \mathbb{Q}$
$\Rightarrow \mathbb{Q}_8^{\sigma_3} = \mathbb{Q}(\omega + \omega^3)$ & $\mathbb{Q}_8^{\sigma_7} = \mathbb{Q}(\omega + \omega^7)$.

For $\mathbb{Q}_8^{\sigma_5}$ note that $\omega + \omega^5 = 0$. Therefore we notice that $\omega.\omega^5 \in \mathbb{Q}_8^{\sigma_5}$. As before $\omega.\omega^5 = \omega^6 \notin \mathbb{Q} \Rightarrow \mathbb{Q}_8^{\sigma_5} = \mathbb{Q}(\omega^6)$.

3. Recall that $\zeta_n := e^{\frac{2\pi i}{n}} = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ therefore

$$\zeta_n + \zeta_n^{-1} = \zeta_n + \overline{\zeta_n} = 2\cos\left(\frac{2\pi}{n}\right)$$ therefore $\mathbb{Q}(\cos(\frac{2\pi}{n}))$ fits into the tower extensions:

$$\mathbb{Q} \subseteq \mathbb{Q}(\cos(\tfrac{2\pi}{n})) \subseteq \mathbb{Q}(\zeta_n)$$

and $Gal(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \leq (\mathbb{Z}/n\mathbb{Z})^\times$ is abelian therefore $\mathbb{Q}(\cos(\frac{2\pi}{n}))/\mathbb{Q}$ is Galois.

4. Define $n := [L:\mathbb{Q}]$. Note that the set, $X = \{m \in \mathbb{N} \mid \phi(m) \leq n\}$ is finite. Indeed, let $p_1^{r_1} \cdots p_s^{r_s}$ be the prime decomposition of $m \in \mathbb{N}$. Then

$$\phi(m) = p_1^{r_1-1}(p_1-1) \cdot p_2^{r_2-1}(p_2-1) \cdots p_s^{r_s-1}(p_s-1)$$

therefore for $m \in \mathbb{N}$ st $\phi(m) \leq n$ there are finitely many possibilities for primes and exponents showing up in the prime decomp. of m.
$\Rightarrow |X| < \infty$.

Now note that any kth root of unity is an mth primitive root of unity. Therefore it is sufficient to show that L contains finitely many primitive roots of unity. Let $w \in L$ be a primitive mth root of unity. Then

$$[\mathbb{Q}(w):\mathbb{Q}] = \phi(m) \quad \text{and} \quad [L:\mathbb{Q}] = n \Rightarrow \phi(m) < n.$$

Therefore the number of roots of unity in L is smaller than $|X| < \infty$

5. Clearly $L \subseteq \overline{\mathbb{F}_p}$ as L is algebraic. Now let $\mu \in \overline{\mathbb{F}_p}$ then

$\mathbb{F}_p(\mu) = \mathbb{F}_{p^e}$ for some e therefore μ is a root of $X^{p^e} - X \Rightarrow X$ is a root of $X^{p^e-1} - 1$. Notice that if ζ_m, ζ_n are mth and nth root of unity respectively with $\gcd(m,n)=1$ then $\zeta_m\zeta_n$ is an $m \cdot n$th root of unity As p^e-1 is coprime with p so is every prime q in the prime decomposition of p^e-1. Therefore every p^e-1th root of unity is in L and $L = \overline{\mathbb{F}_p}$.

6. Note that $FK_j = K_j(\mu_m)$ by definition. Therefore we may write FK_{j+1}/FK_j as $K_{j+1}(\mu_m)/K_j(\mu_m)$. Write $K_{j+1} = K_j(\sqrt[m_j]{\alpha})$ for some $\alpha \in K_j$ then

$$K_{j+1}(\mu_m) = K_j(\mu_m)(\sqrt[m_j]{\alpha}).$$ Moreover $K \subseteq F$ is obtained by adjoining an mth root of unity therefore FL/K is radical.

Note that $K_{j+i}(\mu_m)$ contains a primitive m_kth root of unity for all k as $m_k \mid m$. Therefore $K_{j+i}(\mu_m) = K_j(\mu_m)(\sqrt[m_j]{\alpha_j}, \sqrt[m_{j+1}]{\alpha_{j+1}}, \dots, \sqrt[m_{j+i-1}]{\alpha_{j+i-1}})$ is the splitting field of the polynomial

$$f_{j+i} = \prod_{k=0}^{i-1} X^{m_{j+k}} - \alpha_{j+k}$$

and therefore $K_j(\mu_m) \subseteq K_{j+i}(\mu_m)$ is normal. It is also separable as $(\mathrm{char}K, \deg f_m) = 1$ and $K_j(\mu_m) \subseteq K_{j+i}(\mu_m)$ is Galois.

The fact that $K_j(\mu_m) \subseteq K_{j+1}(\mu_m) = K_j(\mu_m)(\sqrt[m_j]{\alpha_j})$ is cyclic is a direct consequence of a theorem in the course.

7. Let $F \subseteq K \subseteq E$ be a chain of field extensions. We show that

$$F \subseteq K \text{ and } K \subseteq E \text{ is solvable} \iff F \subseteq E \text{ is solvable.}$$

$\Rightarrow$: Let M_1 be a radical extension of F containing K and M_2 be a radical extension of K containing E.
We claim that $F \subseteq M_1M_2$ is radical. Note that $M_1 \subseteq M_2M_1$ is radical
Therefore $F \subseteq M_1 \subseteq M_1M_2$ is radical. and $E \subseteq M_1M_2 \Rightarrow F \subseteq E$ is solvable.

$\Leftarrow$: Now suppose that $F \subseteq E$ is solvable and let $F \subseteq M$ be a radical extension containing E. Then clearly $F \subseteq K \subseteq M$ and $F \subseteq K$ is solvable. Moreover $K \subseteq KM$ is radical and clearly $E \subseteq KM$ therefore $K \subseteq E$ is solvable.

Applying this lemma to $K \subseteq M$ and $M \subseteq LM$ we obtain that $K \subseteq LM$ is solvable and thus $K \subseteq L$, $L \subseteq LM$ are both solvable.

8. Let us start by showing that LM/M & $L/L\cap M$ are Galois.
As L/K is normal L is the splitting field of some set of polynomials $S \subseteq K[x]$. Write $L = K(\alpha_1, \_, \alpha_n)$ where α_i are the roots of the polynomials in S. Then $LM = M(\alpha_1, \_, \alpha_n) = SF_M(S) \Rightarrow LM/M$ is normal.
For seperability it suffices to show that $m_{\alpha_i, M}$ is seperable $\forall i$.
As $m_{\alpha_i, M} \mid m_{\alpha_i, K}$ and L/K is seperable we are done.
The same argument shows that $L/L\cap M$ is normal and seperable.

Now define $\Phi: Gal(LM/M) \longrightarrow Gal(L/K)$ as $\Phi(\sigma) = \sigma|_L$.
First note that $\Phi(\sigma)$ is an automorphism of L as L/K is normal.
Moreover $\sigma|_L$ fixes K as σ fixes L. Observe that if $\sigma|_L = id_L$ then $\sigma = id_{LM}$. Indeed $\sigma|_M = id_M$ as $\sigma \in Gal(LM/M)$ therefore $\sigma|_L = id_L$, $\sigma|_M = id_M$ and $LM^\sigma \supseteq L, M \Rightarrow LM^\sigma = LM$ and $\sigma = id_{LM}$. This shows that Φ is injective.

Finally, we show that $L^{im\Phi} = L\cap M$. Let $\sigma \in Gal(LM/M)$ as σ fixes M $\sigma|_L$ fixes $L\cap M$ and it is clear that $L\cap M \subseteq L^{im\Phi}$. Let $a \in L^{im\Phi}$ then $\sigma|_L(a) = a \Rightarrow \sigma(a) = a \quad \forall \sigma \in Gal(LM/M) \Rightarrow a \in M$ and $a \in L \Rightarrow a \in L\cap M$.
$\Rightarrow L^{im\Phi} = L\cap M$. By the Galois correspondence this shows that $im\Phi \cong Gal(L/L\cap M) \Rightarrow \Phi: Gal(LM/M) \xrightarrow{\cong} Gal(L/L\cap M)$.

9. (i) Firstly, it is clear that $\alpha_H \in L^H$ therefore $K(\alpha_H) \subseteq L^H$, to finish the proof, it suffices to prove that $Gal(L/K(\alpha_H)) \subseteq Gal(L/H) = H$

Let us start show that $\sigma(\alpha_H) = \alpha_H \Leftrightarrow \sigma \in H$. Suppose that $\sigma \notin H$ then $\sigma(\alpha) \notin H.\alpha$ but

$$\sigma(\alpha_H) - \alpha_H = \sigma(\alpha) + \Big(\sum_{h \in H \setminus \{id\}} \sigma(h(\alpha))\Big) - \sum_{h \in H} h(\alpha) = 0 \text{ is a linear relation}$$

where the coefficient of $\sigma(\alpha)$ is 1. This is a contradiction as $\{\sigma(\alpha) \mid \sigma \in G\}$ is a basis.

(ii) Recall that in this case $K(\alpha_H)/K$ is Galois with the Galois group G/H.
Clearly $\forall \tilde{\sigma} \in G/H$, $\tilde{\sigma}(\alpha_H) \in K(\alpha_H)$, moreover $[K(\alpha_H) : K] = |G|/|H| = |G/H|$ therefore it is sufficient to show that the set $\{\tilde{\sigma}(\alpha_H) : \tilde{\sigma} \in G/H\}$ is linearly independent. This follows directly from the following computation:

$$\sum_{\tilde{\sigma} \in G/H} c_{\tilde{\sigma}} \tilde{\sigma}\Big(\sum_{h \in H} h(\alpha)\Big) = \sum_{\tilde{\sigma} \in G/H} \sum_{h \in H} c_{\tilde{\sigma}}.\, \tilde{\sigma}h(\alpha) = \sum_{g \in G} c_g\, g(\alpha)$$

with $c_{\tilde{\sigma}} \in K$ and $c_g = c_{\tilde{\sigma}}$ where $g = \tilde{\sigma}.h$ for some $h \in H$. We can conclude as $\{g(\alpha) : g \in G\}$ is linearly independent.

10. Let $K = \mathbb{F}_{p^e}$ and $K \subseteq L := \mathbb{F}_{p^l}$ be an extension of K. Note that

$L = SF_K(x^{p^l-1} - 1)$ moreover $\gcd(p, p^l - 1) = 1$ therefore by the course we know that $L = K(\mu)$ where μ is any primitive $(p^l - 1)$th of unity. Therefore it is soluable.

11. Let us show that if $\alpha_2 \in L$ then L/K is normal.

Let $N = K(\alpha_1, \alpha_2, \_, \alpha_p)$ note that N/K is Galois as $\alpha_1, \_, \alpha_p$ are the roots of $m_{\alpha,K}$ and $m_{\alpha,K}$ is separable. Moreover as N/K is normal the α_i are K-conjugate in N. Now $Gal(N/K)$ acts transitively on $\alpha_1, \_, \alpha_p$ therefore $Gal(N/K) \leq S_p$ the symmetric group on p elements. Moreover $p \mid Gal(N/K)$ as $[L:K] \mid [N:K] = |Gal(N/K)|$ therefore there exists an element σ of order p in $Gal(N/K)$ by Cauchy's theorem. Note that this σ is a p-cycle in S_p and after replacing σ by a suitable power of σ we may assume that $\sigma(\alpha_1) = \alpha_2$. Therefore σ restricts to an element in $Gal(L/K)$ and so does all the powers of σ. And we know that for all i there exists some j such that $\sigma^j(\alpha_1) = \alpha_i$ therefore $\alpha_i \in L$ $\forall i$ and L/K is Galois.

The fact that $Gal(L/K)$ is cyclic is a consequence of $|Gal(L/K)| = p$ for some prime p.

12. Suppose that $\alpha = a^2 + b^2$ with $a, b \in K$. As $\alpha \in K$ is not a square both a and b are non-zero therefore $\pm\sqrt{\alpha \pm a\sqrt{\alpha}}$ are four distinct elements. Out of these 4 distinct elements we can construct the polynomial

$f(X) = X^4 - 2\alpha X^2 + b^2\alpha = (X^2 - \alpha)^2 - a^2\alpha$. whose roots are $\pm\sqrt{\alpha \pm a\sqrt{\alpha}}$. Note that if $f(X)$ is reducible it is given by a product of two degree two polynomials as none of the roots are in $\mathbb{Q}$. A direct computation shows that writing f as a product of two degree two polynomials in $K[X]$ contradicts that D is not a square therefore f is irreducible.

Now let $\gamma = \sqrt{\alpha + a\sqrt{\alpha}}$. Then one can see that $K(\gamma)$ contains all the roots of $f(x)$ and therefore $K(\gamma) = SF_K(f(x))$. Therefore $K(\gamma)/K$ is Galois of degree 4. Let $\sigma \in Gal(K(\gamma)/K)$ such that $\sigma(\sqrt{\alpha + a\sqrt{\alpha}}) = \sqrt{\alpha - a\sqrt{\alpha}}$. then it can be seen that $\sigma(\sqrt{\alpha}) = -\sqrt{\alpha}$ and $\sigma^2 \neq id$ therefore $Gal(K(\gamma)/K) \cong \mathbb{Z}/4\mathbb{Z}$ and $K(\gamma)$ contains L.

Conversely suppose that there exist a cyclic extension $K \subseteq N$ of order 4 containing L. As $[N:L] = 2$ we can write $N = L(\sqrt{\beta})$ for some $\beta \in L$.
Write $\beta = a + b\sqrt{\alpha}$. As L/K is Galois, $Gal(L/K)$ is a quotient of $Gal(N/K)$. let $\sigma \in Gal(N/K)$ be such that its image in $Gal(L/K)$ is non trivial.
Then

$(\sigma(\sqrt{\beta}))^2 = \sigma(\beta) = \sigma(a + b\sqrt{\alpha}) = a - b\sqrt{\alpha}$. Let $v = \sqrt{\beta}.\sigma(\sqrt{\beta})$ then

(*) $v^2 = (a + b\sqrt{\alpha})(a - b\sqrt{\alpha}) = a^2 - b^2\alpha \in K$. Therefore $K \subseteq K(v) \subseteq N$. Now as $Gal(N/K)$ has a unique subgroup of order 2 then $K(v) = L$. Write $v = t + s\sqrt{\alpha}$ $Gal(K(v)/K) \cong \mathbb{Z}/2\mathbb{Z}$ and let ψ be the element of order 2 then $\psi(v) = -v$ as $K \subseteq K(v)$ is Galois and the minimal polynomial of v over K is $X^2 - v^2$ with roots $\pm v$. Therefore $\psi(v) = \psi(t + s\sqrt{\alpha}) = \psi(t) + s.\psi(\sqrt{\alpha}) = t + s\psi(\sqrt{\alpha})$

$= -v = -t - s\psi(\sqrt{\alpha})$. This shows that $t=0$ and $v = s\sqrt{\alpha}$.
By (*): $v^2 = s^2 \cdot \alpha = a^2 - b^2\alpha \Rightarrow \alpha(s^2+b^2) = a^2 \Rightarrow \alpha = \left(\frac{a}{s}\right)^2 + \left(\frac{a}{b}\right)^2$ and we are done.