Definition 8.1. Let K be a field and $\bar{K}$ an algebraic closure of K. As follows from Theorem 6.1 for any other algebraic closure $\bar{K}'$ of K there exists a K-isomorphism $f : \bar{K} \to \bar{K}'$. Therefore the groups $Gal(\bar{K}/K), Gal(\bar{K}'/K)$ are isomorphic and we denote by G_K the Galois group $Gal(\bar{K}/K)$. This group is finite iff the extension $\bar{K}/K$ is finite.

Lemma 8.1. Let $L \supset K$ be a finite extension. Show that

a) there exists a K-monomorphism $f : L \to \bar{K}$,

By the definition the group $Gal(\bar{K}/f(L))$ is a subroup of G_K.

b) the map $g \to g \circ f$ defines a bijection between the quotient $G_K/Gal(\bar{K}/f(L))$ and the set of K-monomorphisms from L to $\bar{K}$,

For any $\sigma \in Gal(\bar{K}/K)$ we denote by $Ad(\sigma) : G_K \to G_K$ be the automorphism given by $Ad(\sigma)(g) = \sigma g \sigma^{-1}$.

c) Let $\sigma \in Gal(\bar{K}/K), f' = \sigma \circ f : L \to \bar{K}$. Then

$Ad(\sigma)(Gal(\bar{K}/f(L)) = Gal(\bar{K}/f'(L))$,

d) an extension $L \supset K$ is normal iff the subgroup $Gal(\bar{K}/f(L) \subset Gal(\bar{K}/K)$ is normal.

I'll leave the proof of Lemma 8.1 as a homework.

Definition 8.2. We say that a finite extension $L \supset K$ is a Galois extension if $|Gal(L/K)| = [L : K]$.

Lemma 8.2. A finite separable extension $L \supset K$ is a Galois extension iff for any two K-homomorphism $f', f'' : L \to \bar{K}$ we have $Im(f') = Im(f'')$.

Proof . Suppose that $L \supset K$ is a Galois extension. We want to show that for any two K-homomorphism $f', f'' : L \to \bar{K}$ we have $Im(f') = Im(f'')$. Fix a K-homomorphism $f : L \to \bar{K}$ and for any $\sigma \in Gal(L/K)$ consider the composition $f \circ \sigma : L \to \bar{K}$. It is clear that $Im(f \circ \sigma) = Im(f), \forall \sigma \in Gal(L/K)$. But the number of distinct K-homomorphisms from L to $\bar{K}$ is equal to $[L : K]_s = [L : K]$. Since the extension $L \supset K$ is a Galois extension we see that all K-homomorphisms from L to $\bar{K}$ have the form $f \circ \sigma$ for some $\sigma \in Gal(L/K)$. Therefore $Im(f') = Im(f'')$ for any two K-homomorphism $f', f'' : L \to \bar{K}$.$\square$

Conversely assume that $Im(f') = Im(f'')$ for all K-homomorphism $f', f'' : L \to \bar{K}$. Let $f_i, 1 \leq i \leq n$ be the set of all K-homomorphisms from L to $\bar{K}$. By the definition $n = [L : K]_s$. Since the extension $L \supset K$ is separable we see that $n = [L : K]$. Since $Im(f_1) = Im(f_i), \forall i, 1 \leq i \leq n$ we can define $\sigma_i \in Gal(L/K), i, 1 \leq i \leq n$ by $\sigma_i(\alpha) := f_i^{-1}(f_1(\alpha)), \forall \alpha \in L$. In this way we obtained $n == [L : K]$ different elements of $Gal(L/K)$. So $|Gal(L/K)| = [L : K]$.$\square$

Let K be a field such that $\mathrm{ch}(K) \neq 2, a \in K$. We choose $\sqrt{a} \in \bar{K}$ and consider the subfield $K(\sqrt{a}) \subset \bar{K}$.

Lemma 8.3. a) the subfield $K(\sqrt{a}) \subset \bar{K}$ does not depend on a choice of $\sqrt{a} \in \bar{K}$,

b) $K(\sqrt{a}) = K$ iff a is a square in K [that is there exists $b \in K$ such that $a = b^2$],

c) if $K(\sqrt{a}) \neq K$ then $[K(\sqrt{a})/K] = 2$ and $Gal(K(\sqrt{a})/K) = \mathbb{Z}/2\mathbb{Z}$,

Let K be as above $a, b \in K, L := K(\sqrt{a}, \sqrt{b}) \subset \bar{K}$

d) the subfield $K(\sqrt{a}, \sqrt{b}) \subset \bar{K}$ does not depend on a choice of $\sqrt{a}, \sqrt{b} \in \bar{K}$,

e) $[L : K] \leq 4$ and $[L : K] = 4$ if neither a nor b nor ab is a square in K,

f) L/K is a Galois extension and in the case when $[L : K] = 4$ we have $Gal(L/K) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. The parts a)-e) I'll leave as a homework and will prove the part f). I'll consider only the most difficult case when $[L : K] = 4$. In this case I'll give two proofs- a direct one and one which uses Lemma 8.1.

A direct proof. Let $F' = K(\sqrt{a}) \subset L, F'' = K(\sqrt{b}) \subset L$. Since $L = F'(\sqrt{b})$ there exists $\tau' \in Gal(L/F') \subset Gal(L/K)$ such that $\tau'(\sqrt{b}) = -\sqrt{b}$. Analogously there exists $\tau'' \in Gal(L/F'') \subset Gal(L/K)$ such that $\tau'(\sqrt{a}) = -\sqrt{a}$. It is clear now that

$$\tau'\tau''(\sqrt{a}) = -\sqrt{a}, \tau'\tau''(\sqrt{b}) = -\sqrt{b}$$

and

$$\tau''\tau'(\sqrt{a}) = -\sqrt{a}, \tau''\tau'(\sqrt{b}) = -\sqrt{b}.$$

So elements $\tau', \tau'' \in Gal(L/K)$ commute. Since $(\tau')^2 = (\tau'')^2 = e$ we see that the elements $\tau', \tau'' \in Gal(L/K)$ generate a subgroup of $Gal(L/K)$ isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Since we know that

$|Gal(L/K)| \leq [L : K]$ we conclude that $Gal(L/K) = \mathbb{Z}/4\mathbb{Z}$.

The second proof. Let $G_1 := Gal(\bar{K}/F'), G_2 := Gal(\bar{K}/F'') \subset G_K :== Gal(\bar{K}/K)$. The extensions $F'/K, F''/K$ are Galois extensions and $Gal(F'/K) = Gal(F''/K) = \mathbb{Z}/2\mathbb{Z}$. It follos from Lemma 8.1 that $G_1, G_2 \subset G_K$ are normal subgroups such that $G_K/G_1 = G_K/G_2 = \mathbb{Z}/2\mathbb{Z}$ and that : $L = F'F''/K$ is a normal extension and $Gal(L/K) = G_K/G_1 \cap G_2$. Now Lemma 8.3 follows immediately from the following result in the group theory.

Lemma 8.3'. Let G be a group, $G_1, G_2 \subset G$ distinct normal subgroups such that $G/G_1 = G/G_2 = \mathbb{Z}/2\mathbb{Z}, G' := G_1 \cap G_2$ and

$f_i : G/G' \to G/G_i$ be group homomorphisms induced by imbeddings $G' \to G/G_i$. Then the group homomorphism $G/G' \to G/G_1 \times G/G_2, g \to (f_1(g), f_2(g))$ is an isomorphism.

I'll leave the proof of Lemma 8.3' as a homework.

Let K be as above $a \in K$ such that $[K(\sqrt{a})/K] = 2, \alpha := \sqrt{a} \in \bar{K}$ and $b = u + \alpha u, v \in K \in K(\alpha)$ be such that $[L : K] = 2$ where $L := K(\alpha)(\sqrt{b})$.

Lemma 8.4. The extension L/K is normal iff either $u^2 - av^2$ is a square in K or $a(u^2 - av^2)$ is a square in K.

Proof. As follows from Lemma 8.2 the extension L/K is normal iff for any two K-homomorphism $f', f'' : L \to \bar{K}$ we have $Im(f') = Im(f'')$. It is clear [and follows from Lemma 8.3 a)] that in the case when $f'(\alpha) = f''(\alpha)$ we have $Im(f') = Im(f'')$. So consider the case when $f' = Id, f''(\alpha) = -\alpha$. Let $\beta := \sqrt{b}, \gamma := f''(\beta)$. Then $\beta^2 = u + \alpha v, \gamma^2 = u - \alpha v$. So we see that the extension L/K is normal iff the equation $t^2 = u - \alpha v$ has a solution ϵ in the field L. But ϵ is a solution of the equation $t^2 = u - \alpha v$ iff $\delta := \epsilon(u + \alpha v)$ is a solution of the equation $z^2 = (u - \alpha v)(u + \alpha v) = u^2 - av^2$ So we see that the extension L/K is normal iff the equation $z^2 = u^2 - av^2$ has a solution in L.

Claim. If the equation $z^2 = u^2 - av^2$ has a solution δ in L then $\delta \in K(\alpha)$.

Proof of the Claim. We show that the assumption that the equation $z^2 = u^2 - av^2$ has a solution in L but not in $K(\alpha)$ leads to a contradiction.

Let $c := u^2 - av^2$. Since the equation $z^2 = c$ has a solution in L we have an imbedding of the field $K(\sqrt{a}, \sqrt{c})$ in L. If δ does not belong to $K(\alpha)$ then $[L : K(\alpha)] = 2$ and therefore $[L : K] = 4$. Since $K \subset L$ we see that $L = K(\sqrt{a}, \sqrt{c})$. Any element ϵ of the field $K(\sqrt{a}, \sqrt{c})$ can be written in the form

$$\epsilon = k + l\alpha + m\delta + n\alpha\delta, k, l, m, n \in K$$

In particular we can write $\beta = k + l\alpha + m\delta + n\alpha\delta, k, l, m, n \in K$. Let $\tau \in Gal(L/K(\alpha)$ be an automorphism such that $\tau(\beta) = -\beta$. Since $L = K(\sqrt{a}, \sqrt{c}), \tau$ is a non-trivial element of the group $Gal(K(\sqrt{a}, \sqrt{c})/K(\sqrt{a}))$. So $\tau(\delta) = -\delta$ and therefore

$$\tau(\beta) = k + \alpha l - \delta m - \alpha\delta$$

Since $\tau(\beta) = -\beta$ we see that $k = l = 0$ and $\beta = \delta(m + \alpha n)$.

We have $\beta^2 = u + \alpha v$. Therefore $\delta^2(m + \alpha n)^2 = u + \alpha v$. In other words $c(m+\alpha n)^2 = u+\alpha v$. Let $\sigma \in Gal(K(\alpha)/K$ be such that $\sigma(\alpha) = -\alpha$. Then $\sigma(c(m+\alpha n)^2) = \sigma(u+\alpha v)$. That is $c(m-\alpha n)^2 = (u-\alpha v)$. By taking the product we see that $c^2(m^2 - an^2)^2 = c$ and therefore $c = (m - \alpha n)^{-2}$. So we see that and equation $z^2 = c$ has a solution in $K(\alpha)$. This contradiction proves the Claim.□

Now we know that the extension L/K is normal iff the equation $z^2 = u^2 - av^2$ has a solution in $K(\alpha)$.

It is clear that if either $u^2 - av^2$ is a square in K or $a(u^2 - av^2)$ is a square in K then the equation $z^2 = u^2 - av^2$ has a solution ϵ in $K(\alpha)$. Assume conversely that the equation $z^2 = u^2 - av^2$ has a solution $\epsilon \in K(\alpha)$. We can write $\epsilon = x + \alpha y, x, y \in K$. Let $\sigma \in Gal(K(\alpha)/K)$ be an automorphism such that $\sigma(\alpha) = -\alpha$. Then

$$(\sigma(\epsilon))^2 = \sigma(\epsilon^2) = \sigma(u^2 - av^2) = u^2 - av^2$$

Therefore either $\sigma(\epsilon) = \epsilon$ or $\sigma(\epsilon) = -\epsilon$. In the first case the equation $z^2 = u^2 - av^2$ has a solution $x \in K$ and in the second case the equation $z^2 = a(u^2 - av^2)$ has a solution $ay \in K$.□

Let's continue the analysis. Consider first the case when the extension L/K is not normal. Let $M = L(\sqrt{u - \alpha v})$ and D_4 be a group generated by a pair of elements σ, τ and the relations

$\sigma^4 = \tau^2 = e, \tau\sigma\tau^{-1} = \sigma^3$

Lemma 8.5. If the extension L/K is is not normal then the extension M/K is normal and the group $Gal(M/K)$ is isomorphic to the group D_4.

Proof. To prove that M/K is normal we have to show that $|Gal(M/K)| = [M : K] = 8$. Of course it is sufficient to show that $|Gal(M/K)| \geq 8$.

Since $M = K(\alpha)(\sqrt{u + \alpha v}, \sqrt{u - \alpha v})$ we know from Lemma 8.3 the extension $M/K(\alpha)$ is normal and $Gal(M/K(\alpha)) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Let $p \in Gal(M/K(\alpha)(\sqrt{u + \alpha v}), q \in Gal(M/K(\alpha)(\sqrt{u - \alpha v})$ be nontrivial automorphism. Then $p^2 = q^2 = e, pq = qp$ and the group $Gal(M/K(\alpha))$ is generated by p, q.

Fix $\beta, \gamma \in M$ such that $\beta^2 = u + \alpha v, \gamma^2 = u - \alpha v$. It is clear that there exists $g \in Gal(M/K)$ such that $g(\alpha) = -\alpha, g(\beta) = \gamma$. We see that $Gal(M/K) \not\supseteq Gal(M/K(\alpha)$ and therefore

$$|Gal(M/K)| = |Gal(M/K(\alpha)||Gal(M/K)/Gal(M/K(\alpha)| \geq 2|Gal(M/K(\alpha)| = 8$$

So we see that the extension M/K is normal.

It is clear from the construction that $geg^{-1} = f, gfg^{-1} = e$. Consider $g^2 \in Gal(M/K(\alpha))$. Since g^2 commutes with g we see that either $g^2 = ef$ or $g^2 = e$. It is easy to see that in the first case there exists a group isomorphism $\phi : D_4 \to Gal(M/K)$ such that $\phi(\sigma) = g, \phi(\tau) = e$ and in the second case there exists a groups isomorphism $\phi : D_4 \to Gal(M/K)$ such that $\phi(\sigma) = gef, \phi(\tau) = e$.$\Box$

Consider now the case when the extension L/K is normal. Then the group $Gal(L/K)$ is a group of order four. Therefore either $Gal(L/K) = \mathbb{Z}/4\mathbb{Z}$ or $Gal(L/K) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. It is clear that $Gal(L/K) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ iff for some $g \in Gal(L/K) - Gal(L/K(\alpha))$ we have $g^2 = e$.

I claim that $Gal(L/K) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if $u^2 - av^2 \in K^2$ and $Gal(L/K) = \mathbb{Z}/4\mathbb{Z}$ if $a(u^2 - av^2) \in K^2$. I'll analyze the first case and leave for you to analyze the second.

If $u^2 - av^2 = d^2, d \in K$ the we can consider an automorphism $g \in Gal(L/K)$ such that $g(\alpha) = -\alpha, g(\beta) = d/\beta$. So it is clear that $g^2 = e$.$\Box$