SOLUTIONS TO WORKSHEETS #9 & #10

Problem 1. — *Let K be a field containing μ_n for some n prime to* $\mathrm{char}(K)$*. Choose $a, b \in K$ and let $\alpha, \beta \in \bar{K}$ be such that $a = \alpha^n$ and $b = \beta^n$. Assuming that $[K(\alpha) : K] = [K(\beta) : K] = n$, prove that $K(\alpha) = K(\beta)$ if and only if there exist some $r \in (\mathbf{Z}/n\mathbf{Z})^\times$ and some $c \in K^\times$ such that $a = b^r c^n$.*

Solution. By Kummer theory, $K(\alpha) = K(\beta)$ if and only if the cyclic subgroups of $K^\times/K^{\times,n}$

$$A := \{a^i \cdot K^{\times,n} : 0 \leq i \leq n-1\} \text{ and } B := \{b^i \cdot K^{\times,n} : 0 \leq i \leq n-1\}$$

generated by a and b coincide: that is to say, $A = B$ as subgroups of $K^\times/K^{\times,n}$. In particular, $a \cdot K^{\times,n} \in B$ is a generator of B, which implies that there is some $r \in (\mathbf{Z}/n\mathbf{Z})^\times$ such that $a \cdot K^{\times,n} = b^r \cdot K^{\times,n}$. That these cosets of $K^\times/K^{\times,n}$ coincide now means that there is some $c^n \in K^{\times,n}$ such that $a = b^r c^n$. ∎

Problem 2. — *Let $K = \mathbf{C}(x, y, z)$ be the trivariate field of rational functions and let*

$$L := K(\sqrt[4]{xyz}, \sqrt[4]{yz}, \sqrt[4]{xz^2}).$$

Prove that the extension L/K is 4-Kummer of degree 32.

Solution. Since $i := \sqrt{-1}$ is a primitive 4-th root of unity and it is contained in K, that L is a 4-Kummer extension follows directly from the presentation given as adjoining three 4-th roots of elements in K. Kummer theory now applies to show that its degree is but the cardinality of the group

$$G := \langle a, b, c\rangle \subset K^\times/K^{\times,4}$$

where a, b, and c are the images of xyz, yz, and xz^2 in $K^\times/K^{\times,4}$, respectively.

Observe first that the subgroup

$$H := \langle a, b\rangle = \{a^i b^j : 0 \leq i, j \leq 3\}$$

generated by a and b is of cardinality 16; that is, we claim that the displayed elements $a^i b^j$ are pairwise distinct. If $a^i b^j = a^s b^t$ for some quadruple $0 \leq i, j, s, t \leq 3$, then this means that there are nonzero rational functions $f(x, y, z)$ and $g(x, y, z)$ such that

$$x^i y^{i+j} z^{i+j} \cdot f(x, y, z)^4 = x^s y^{s+t} z^{s+t} \cdot g(x, y, z)^4.$$

Upon clearing denominators, we may assume that both $f(x, y, z)$ and $g(x, y, z)$ are polynomials. Expanding these polynomials in terms of monomials and examining the exponent of the variables x, y, and z on both sides then yields the following congruences:

$$i \equiv s \pmod 4 \text{ and } i + j \equiv s + t \pmod 4.$$

Since $0 \leq i, j, s, t \leq 3$, combining the two congruences shows that $(i, j) = (s, t)$, meaning that the $a^i b^j$ are pairwise distinct, as claimed.

Next, observe that $c^2 = x^2 \cdot K^{\times,4} = a^2 b^2$, so this means that H has index at most 2 in G. To see that the index is indeed 2, we must show that $c \notin H$. Suppose that $c = a^i b^j$ for some $0 \leq i, j \leq 3$. Then, as above, this means that

$$xz^2 \cdot f(x, y, z)^4 = x^i y^{i+j} z^{i+j} \cdot g(x, y, z)^4$$

for some polynomials f and g. Comparing the exponents of the variables y and z then gives the congruences $i + j \equiv 0 \pmod 4$ and $i + j \equiv 2 \pmod 4$, which is, of course, impossible. Thus $H \subset G$ has index 2, so that $[L : K] = \#G = 2 \cdot \#H = 32$. ∎

Date: November 20, 2025.

Problem 3. — *Let $p_1, \dots, p_n$ be distinct primes. Prove that $[\mathbf{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}), \mathbf{Q}] = 2^n$.*

Solution. This is quite simple from Kummer theory: the degree of this extension is but the cardinality of the group

$$G := \langle p_1, \dots, p_n \rangle \subset \mathbf{Q}^\times / \mathbf{Q}^{\times,2}$$

generated by the residue classes of the primes $p_1, \dots, p_n$. Since a prime is never a square, each residue class p_i is nonzero. Furthermore, the residue classes are pairwise distinct. Suppose for sake of contradiction that there were $i \neq j$ such that the cosets

$$p_i \cdot \mathbf{Q}^{\times,2} = p_j \cdot \mathbf{Q}^{\times,2}$$

were to coincide. This means that $p_i \cdot r^2 = p_j \cdot q^2$ for some $r, q \in \mathbf{Q}^\times$. Clearing denominators, we may assume that $r, q \in \mathbf{Z}$ are nonzero integers. Furthermore, by dividing out common factors, we may assume that r and q are relatively prime. Now, since p_i and p_j are distinct primes, this equation implies, for instance, that $p_i \mid q$. But this implies p_i^2 divides $p_j \cdot q^2 = p_i \cdot r^2$, whence p_i must also divide r. But this means that both r and q are divisible by p_i, contradicting the assumption that they were chosen relatively prime. This shows that the residue classes of the p_i are pairwise distinct, so

$$G := \langle p_1, \dots, p_n \rangle \cong (\mathbf{Z}/2\mathbf{Z})^n$$

and so $[\mathbf{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbf{Q}] = \#G = 2^n$. ∎

Problem 4. — *Show that any nontrivial torsion element of* $\mathrm{Aut}(\bar{\mathbf{Q}})$ *has order two.*

Solution. Let $\sigma : \bar{\mathbf{Q}} \to \bar{\mathbf{Q}}$ be a nontrivial $\mathbf{Q}$-automorphism which is of finite order, and consider its fixed field $K := \bar{\mathbf{Q}}^\sigma$. The proof of Artin's lemma shows that this is a finite Galois extension whose Galois group is isomorphic to the subgroup of $\mathrm{Aut}_{\mathbf{Q}}(\bar{\mathbf{Q}})$ generated by σ. Since $\bar{\mathbf{Q}}$ is algebraically closed, the Artin–Schreier theorem implies that $[\bar{\mathbf{Q}} : K] = \#\langle\sigma\rangle = 2$, so that σ is of order 2. ∎

Problem 5. — *Show that if G is a group of order n, then $n\mathrm{H}^2(G, M) = \{0\}$ for any G-module M.*

Proof. We must show that every 2-cocycle is a 2-coboundary. By definition, a 2-cocycle is a function $f : G \times G \to M$ that satisfies

$$f(\sigma, \tau) = \sigma \cdot f(\tau, g) - f(\sigma\tau, g) + f(\sigma, \tau g) \text{ for all } \sigma, \tau, g \in G.$$

Summing over the n elements $g \in G$ on both sides then shows that

$$\begin{aligned} nf(\sigma, \tau) &= \sum\nolimits_{g \in G} \big(\sigma \cdot f(\tau, g) - f(\sigma\tau, g) + f(\sigma, \tau g)\big) \\ &= \sum\nolimits_{g \in G} \big(\sigma \cdot f(\tau, g) - f(\sigma\tau, g) + f(\sigma, g)\big). \end{aligned}$$

We now claim that this is a 2-coboundary, that is, there is a function $h : G \to M$ such that

$$nf(\sigma, \tau) = \delta^1(h)(\sigma, \tau) = \sigma \cdot h(\tau) - h(\sigma\tau) + h(\sigma) \text{ for all } \sigma, \tau \in G.$$

Comparing the two expressions shows that the function

$$h(\theta) := \sum\nolimits_{g \in G} f(\theta, g)$$

satisfies $nf = \delta^1(h)$, showing that nf is indeed a 2-coboundary, as required. ∎

Problem 6. — *Let $G = \langle\sigma\rangle$ be a cyclic group of order n and M a G-module. Define*

$$M^G := \{m \in M : \sigma \cdot m = m\}$$

and the corresponding trace map $\mathrm{Tr} : M \to M^G$ *given by* $m \mapsto \sum_{g \in G} g \cdot m = \sum_{i=0}^{n-1} \sigma^i \cdot m$.

(i) *Given $m \in M^G$, let $f_m : G \times G \to M$ be the cochain given by*

$$f_m(\sigma^i, \sigma^j) := \begin{cases} 0 & \text{if } i+j < n \\ m & \text{if } i+j \geq n. \end{cases}$$

Prove that f_m is a 2-cocycle.

(ii) *Prove that the map $m \mapsto f_m$ induces an isomorphism $M^G/\operatorname{im}(\mathrm{Tr}) \cong \mathrm{H}^2(G, M)$.*

Solution. That f_m is a 2-cocycle means that, given any $0 \leq i, j, k \leq n-1$,

$$0 = \delta^2(f_m)(\sigma^i, \sigma^j, \sigma^k) = \sigma^i \cdot f_m(\sigma^j, \sigma^k) - f_m(\sigma^{i+j}, \sigma^k) + f_m(\sigma^i, \sigma^{j+k}) - f_m(\sigma^i, \sigma^j).$$

Since $m \in M^G$, the action of σ^i on the first term is trivial, so it may be omitted. After furthermore rearranging the equation, this means that f_m is a 2-cocycle if

$$f_m(\sigma^i, \sigma^j) + f_m(\sigma^{i+j}, \sigma^k) = f_m(\sigma^j, \sigma^k) + f_m(\sigma^i, \sigma^{j+k}) \text{ for all } 0 \leq i, j, k \leq n-1.$$

Consider the possibilities: First, if $i+j+k < n$, then also $i+j < n$ and $j+k < n$, so that all terms in question are, in fact, 0. So suppose that $i+j+k \geq n$. In the cases that both $i+j$ and $j+k$ are simultaneously either $< n$ or $\geq n$, the two sides of the equation are easily seen to match. So it remains to consider the case that $i+j < n$ but $j+k \geq n$, the opposite set of inequalities being symmetric. In this case, the left hand side is $0 + m = m$. As for the right hand side, observe that $f_m(\sigma^j, \sigma^k) = m$, and that $f_m(\sigma^i, \sigma^{j+k}) = f_m(\sigma^i, \sigma^{j+k-n})$. Since $i+j < n$ and $k \leq n-1$, $i+j+k-n < n$ and so this second term vanishes. Therefore the right hand side is $m + 0 = m$, matching the left.

The construction $m \mapsto f_m$ of (i) provides a homomorphism of abelian groups $f : M^G \to \mathrm{H}^2(G, M)$. We claim that f is surjective and that $\ker(f)$ is the image of the trace map $\mathrm{Tr} : M \to M^G$. First, to determine the kernel, that f_m is a 2-coboundary means that there is a function $\varphi : G \to M$ such that, for all $0 \leq i, j \leq n-1$,

$$f_m(\sigma^i, \sigma^j) = \delta^1(\varphi)(\sigma^i, \sigma^j) = \sigma^i \cdot \varphi(\sigma^j) - \varphi(\sigma^{i+j}) + \varphi(\sigma^i).$$

Taking $i = j = 0$ shows that $\varphi(1) = 0$; when $i = 1$ and $1 \leq j \leq n-2$, the equation $f_m(\sigma, \sigma^j) = 0$ may be rearranged to give the first equality in

$$\varphi(\sigma^{j+1}) = \sigma \cdot \varphi(\sigma^j) + \varphi(\sigma) = \sum\nolimits_{k=0}^{j} \sigma^k \cdot \varphi(\sigma).$$

Inductively applying the first equality then gives the second expression. Finally, taking $i = 1$ and $j = n-1$, and using the above expression shows that

$$m = f_m(\sigma, \sigma^{n-1}) = \sigma \cdot \varphi(\sigma^{n-1}) + \varphi(\sigma) = \sum\nolimits_{k=0}^{n-1} \sigma^k \cdot \varphi(\sigma) = \mathrm{Tr}(\varphi(\sigma)).$$

This shows that $\ker(f) \subseteq \mathrm{Tr}(M)$. The reverse inclusion $\mathrm{Tr}(M) \subseteq \ker(f)$ may be obtained by tracing backwards through these computations. This then shows that $\ker(f) = \mathrm{Tr}(M)$.

To see that $f : M^G \to \mathrm{H}^2(G, M)$ is surjective, suppose that $\psi : G \times G \to M$ is a 2-cocycle. The task is to show that there are some $\varphi : G \to M$ such that $\psi' := \psi + \delta^1(\varphi)$ matches f_m as 2-cocycles for some $m \in M^G$. Observe that the left hand side takes values, for $0 \leq i, j \leq n-1$,

$$\psi'(\sigma^i, \sigma^j) = \psi(\sigma^i, \sigma^j) + \sigma^i \cdot \varphi(\sigma^j) - \varphi(\sigma^{i+j}) + \varphi(\sigma^i).$$

This suggests that we inductively define the values $\varphi(\sigma^k)$. First, taking $i = j = 0$, we ought to have

$$\psi'(1, 1) = \psi(1, 1) + \varphi(1) = 0$$

so $\varphi(1) := -\psi(1, 1)$. Next, $\varphi(\sigma^{\ell+1})$ for $1 \leq \ell \leq n-2$ may may be expressed in terms of ψ and the yet-undefined $\varphi(\sigma)$: Take $i = \ell$ and $j = 1$, since $\ell + 1 \leq n-1$, we ought to have

$$\psi'(\sigma^\ell, \sigma) = \psi(\sigma^\ell, \sigma) + \sigma^\ell \cdot \varphi(\sigma) - \varphi(\sigma^{\ell+1}) + \varphi(\sigma^\ell) = 0.$$

Rearranging, we see that we should take $\varphi(\sigma^{\ell+1}) := \psi(\sigma^\ell,\sigma) + \sigma^\ell\cdot\varphi(\sigma) + \varphi(\sigma^\ell)$. Expanding this inductively shows that

$$\varphi(\sigma^{\ell+1}) = \sum_{k=1}^{\ell}\psi(\sigma^k,\sigma) + \sum_{k=0}^{\ell}\sigma^k\cdot\varphi(\sigma).$$

Even without choosing a value for $\varphi(\sigma)$, this already shows that $\psi'(\sigma^i,\sigma^j) = 0$ whenever $i+j<n$. When either $i=0$ or $j=0$, the cocycle condition on ψ shows that $\psi(1,\sigma^j) = \psi(1,1)$ and $\psi(\sigma^i,1) = \sigma^i\cdot\psi(1,1)$. Since $\varphi(1) := -\psi(1,1)$, we have

$$\psi'(1,\sigma^j) = \psi(1,\sigma^j) + \varphi(1) = 0 \text{ and } \psi'(\sigma^i,1) = \psi(\sigma^i,1) + \sigma^i\cdot\varphi(1) = 0.$$

When $i\neq 0$ and $j\neq 0$ but $i+j<n$, then

$$\begin{aligned}\psi'(\sigma^i,\sigma^j) = \psi(\sigma^i,\sigma^j) &+ \sum_{k=1}^{j-1}\sigma^i\cdot\psi(\sigma^k,\sigma) - \sum_{k=1}^{i+j-1}\psi(\sigma^k,\sigma) + \sum_{k=1}^{i-1}\psi(\sigma^k,\sigma)\\ &+ \sum_{k=0}^{j-1}\sigma^{i+k}\cdot\varphi(\sigma) - \sum_{k=0}^{i+j-1}\sigma^k\cdot\varphi(\sigma) + \sum_{k=0}^{i-1}\sigma^k\cdot\varphi(\sigma).\end{aligned}$$

The terms on the second line cancel out, whereas the first line reduces to

$$\begin{aligned}\psi'(\sigma^i,\sigma^j) &= \psi(\sigma^i,\sigma^j) - \psi(\sigma^i,\sigma) + \sum_{k=1}^{j-1}\big(\sigma^i\cdot\psi(\sigma^k,\sigma) - \psi(\sigma^{i+k},\sigma)\big)\\ &= \psi(\sigma^i,\sigma^j) - \psi(\sigma^i,\sigma) + \sum_{k=1}^{j-1}\big(\psi(\sigma^i,\sigma^k) - \psi(\sigma^i,\sigma^{k+1})\big) = 0\end{aligned}$$

where the second equality arises from the cocycle condition on ψ applied to each parenthesized term, and the final equality is the observation that the sum telescopes.

Now suppose that $i+j\geq n$. Then

$$\begin{aligned}\psi'(\sigma^i,\sigma^j) = \psi(\sigma^i,\sigma^j) &+ \sum_{k=1}^{j-1}\sigma^i\cdot\psi(\sigma^k,\sigma) - \sum_{k=1}^{i+j-n-1}\psi(\sigma^k,\sigma) + \sum_{k=1}^{i-1}\psi(\sigma^k,\sigma)\\ &+ \sum_{k=0}^{j-1}\sigma^{i+k}\cdot\varphi(\sigma) - \sum_{k=0}^{i+j-n-1}\sigma^k\cdot\varphi(\sigma) + \sum_{k=0}^{i-1}\sigma^k\cdot\varphi(\sigma).\end{aligned}$$

Consider first the terms on the second line. Reindexing the first sum to range along $i\leq k\leq i+j-1$, breaking it at n, and combining the second and third sums gives the left hand side of:

$$\sum_{k=i}^{n-1}\sigma^k\cdot\varphi(\sigma) + \sum_{k=0}^{i+j-n-1}\sigma^k\cdot\varphi(\sigma) + \sum_{k=i+j-n}^{i-1}\sigma^k\cdot\varphi(\sigma) = \sum_{k=0}^{n-1}\sigma^k\cdot\varphi(\sigma) = \mathrm{Tr}(\varphi(\sigma)).$$

To deal with the first line of $\psi'(\sigma^i,\sigma^j)$, note first that the cocycle condition on ψ may be used to rewrite the first sum there as

$$\begin{aligned}\sum_{k=1}^{j-1}\sigma^i\cdot\psi(\sigma^k,\sigma) &= \sum_{k=1}^{j-1}\big(\psi(\sigma^{i+k},\sigma) - \psi(\sigma^i,\sigma^{k+1}) + \psi(\sigma^i,\sigma^k)\big)\\ &= -\psi(\sigma^i,\sigma^j) + \sum_{k=0}^{j-1}\psi(\sigma^{i+k},\sigma)\end{aligned}$$

The same manipulations with the summation indices as before then shows that the first line reduces to $\sum_{k=0}^{n-1}\psi(\sigma^k,\sigma)$. All together, this means that whenever $i+j\geq n$, we have

$$\psi'(\sigma^i,\sigma^j) = \sum_{k=0}^{n-1}\psi(\sigma^k,\sigma) + \mathrm{Tr}(\varphi(\sigma)) =: m.$$

In fact, this shows that we may take $\varphi(\sigma)$ to be an arbitrary element of M, at which point this shows that $\psi' = f_m$; one ought to check that $m\in M^G$, but this follows from a calculation using the cocycle condition on ψ, similar to the ones appearing several times now. In conclusion, since $\mathrm{Tr}(M)\subset\ker(f)$, this shows that an arbitrary 2-cocycle $\psi: G\times G\to M$ is cohomologous to the 2-cocycle f_m where

$$m := \sum_{k=0}^{n-1}\psi(\sigma^k,\sigma).$$

Thus $f: M^G\to \mathrm{H}^2(G,M)$ is surjective. ∎

Problem 7. — *With G and M as before, consider the map $D: M\to M$ given by $m\mapsto\sigma\cdot m - m$.*

(i) *Given $m \in M$ with $\mathrm{Tr}(m) = 0$, let $g_m : G \to M$ be the cochain given by*

$$g_m(\sigma^i) := \sum_{j=0}^{i-1} \sigma^j \cdot m.$$

Prove that g_m is a 1-cocycle.

(ii) *Prove that the map $m \mapsto g_m$ induces an isomorphism $\ker(\mathrm{Tr})/\operatorname{im}(D) \cong \mathrm{H}^1(G, M)$.*

Solution. To show that g_m is 1-cocycle, we must show that, for all $0 \le i, j \le n-1$,

$$\delta^1(g_m)(\sigma^i, \sigma^j) = \sigma^i \cdot g_m(\sigma^j) - g_m(\sigma^{i+j}) + g_m(\sigma^i) = 0.$$

When $i + j < n$, the right hand side expands to

$$\delta^1(g_m)(\sigma^i, \sigma^j) = \sum_{k=0}^{j-1} \sigma^{i+k} \cdot m - \sum_{k=0}^{i+j-1} \sigma^k \cdot m + \sum_{k=0}^{i-1} \sigma^k \cdot m = 0.$$

When $i + j \ge n$, then

$$\begin{aligned}\delta^1(g_m)(\sigma^i, \sigma^j) &= \sigma^i \cdot g_m(\sigma^j) - g_m(\sigma^{i+j-n}) + g_m(\sigma^i) \\ &= \sum_{k=0}^{j-1} \sigma^{i+k} \cdot m - \sum_{k=0}^{i+j-n-1} \sigma^k \cdot m + \sum_{k=0}^{i-1} \sigma^k \cdot m = \sum_{k=i+j-n}^{i+j-1} \sigma^k \cdot m.\end{aligned}$$

Factoring out σ^{i+j-n} from the last expression shows that $\delta^1(g_m)(\sigma^i, \sigma^j) = \sigma^{i+j-n} \cdot \mathrm{Tr}(m) = 0$, and so g_m still satisfies the cocycle condition in this case.

The construction (i) provides a homomorphism of abelian groups $g : \ker(\mathrm{Tr}) \to \mathrm{H}^1(G, M)$. We will now show that g is surjective and that its kernel is the image of the map $D : M \to M$. To determine the kernel, suppose that $g_m = \delta^0(a)$ for some $a \in M$. Then

$$g_m(\sigma) = m = \sigma \cdot a - a = D(a).$$

Conversely, if $m = D(a)$, then

$$g_m(\sigma^i) = \sum_{j=0}^{i-1} \sigma^i \cdot m = \sum_{j=0}^{i-1} (\sigma^{i+1} \cdot a - \sigma^i \cdot a) = \sigma^i \cdot a - a = \delta^0(a)(\sigma^i)$$

is the 1-coboundary associated with $a \in M$. Thus $\ker(g) = D(M)$. To see that g is surjective, let $\varphi : M \to G$ be any 1-cocycle, and note that the cocycle condition implies

$$\varphi(\sigma^i) = \sigma^{i-1} \cdot \varphi(\sigma) + \varphi(\sigma^{i-1}) = \sum_{j=0}^{i-1} \sigma^j \cdot \varphi(\sigma)$$

where the second equality comes from inductively applying the first identity. Thus $\varphi = g_m$ for $m := \varphi(\sigma)$. It remains to check that $\mathrm{Tr}(m) = 0$:

$$\mathrm{Tr}(m) = \sum_{j=0}^{n-1} \sigma^j \cdot \varphi(\sigma) = \varphi(\sigma^n) = \varphi(1) = 0$$

where $\varphi(1) = 0$ may be deduced directly from the cocycle condition. Thus every 1-cocycle is of the form g_m for some $m \in \ker(\mathrm{Tr})$, so $g : \ker(\mathrm{Tr}) \to \mathrm{H}^1(G, M)$ is surjective. ∎

Problem 8. — *Let L/K be a finite Galois extension with group G. Fix a function $f : G \times G \to L^\times$ and define a K-algebra as follows: Let*

$$V_f := \bigoplus_{g \in G} L e_g$$

be the $\#G$-dimensional L-vector space with basis $\{e_g\}_{g \in G}$ and define a product $\star : V_f \times V_f \to V_f$ using f by, for all $\sigma, \tau \in G$ and $a, b \in L$,

$$a e_\sigma \star b e_\tau := a\sigma(b) f(\sigma, \tau) e_{\sigma\tau}.$$

(i) *Prove $\star$ defined above makes V_f into an associative algebra if and only if f is a 2-cocycle.*

(ii) *Prove that if further $f(\sigma, \tau) = 1$ for all $\sigma, \tau \in G$, then this algebra is isomorphic to $\mathrm{M}_n(K) \cong \mathrm{End}_K(L)$, where $n = \#G$.*

(iii) *Prove that if g is another 2-cocycle that differs from f by a 2-coboundary, then $V_g \cong V_f$.*

(iv) *Let now $K = \mathbf{R}$ and $L = \mathbf{C}$. Find $[f] \in \mathrm{H}^2(\mathbf{Z}/2\mathbf{Z}, \mathbf{C}^\times)$ such that $V_f \cong \mathbf{H}$.*

Solution. Item (i) asks us to verify associativity for the operation $\star$; this means that, given $a, b, c \in L$ and $\sigma, \tau, \rho \in G$, we need to compare the two quantities

$$(ae_\sigma \star be_\tau) \star ce_\rho = a\sigma(b)f(\sigma,\tau)e_{\sigma\tau} \star ce_\rho = a\sigma(b)f(\sigma,\tau)\sigma(\tau(c))f(\sigma\tau,\rho)e_{\sigma\tau\rho}, \text{ and}$$
$$ae_\sigma \star (be_\tau \star ce_\rho) = ae_\sigma \star b\tau(c)f(\tau,\rho)e_{\tau\rho} = a\sigma(b\tau(c)f(\tau,\rho))f(\sigma,\tau\rho)e_{\sigma\tau\rho}.$$

Since $\sigma : L \to L$ is a field homomorphism, $\sigma(b\tau(c)f(\tau,\rho)) = \sigma(b)\sigma(\tau(c))\sigma(f(\tau,\rho))$, so comparing the coefficients shows that $\star$ is associative if and only if

$$f(\sigma,\tau)\cdot f(\sigma\tau,\rho) = \sigma(f(\tau,\rho))\cdot f(\sigma,\tau\rho)$$

and this is precisely the condition that f is a 2-cocycle, just written in multiplicative notation.

Suppose now that $f(\sigma,\tau) = 1$ for all $\sigma, \tau \in G$. This certainly satisfies the 2-cocycle condition, so $\star$ is associative by (i), and the operation is simply

$$ae_\sigma \star be_\tau = a\sigma(b)e_{\sigma\tau}.$$

This expression may remind one of a linearized form of the action of G on L. In fact, we may define a K-action of V_f on L by letting the basis element $e_\sigma \in V_f$ act on $y \in L$ by $e_\sigma \cdot y := \sigma(y)$, and then extending L-linearly. That this is indeed defines an action comes from the identity

$$ae_\sigma \cdot (be_\tau \cdot y) = ae_\sigma \cdot b\tau(y) = a\sigma(b)\sigma(\tau(y)) = (ae_\sigma \star be_\tau)\cdot y.$$

This action gives rise to a K-algebra homomorphism $\varphi : V_f \to \mathrm{End}_K(L)$ which is furthermore a map of L-vector spaces. Dedekind's lemma on independence of characters implies that the basis $\{e_\sigma : \sigma \in G\}$ of V_f is mapped to a set of L-linearly independent operators on L, and so φ is injective and, as a map of L-vector spaces, has rank n. To compute the dimension of $\mathrm{End}_K(L)$ as an L-vector space, note that it is also a K-vector space and that a choice of K-basis of L of size n identifies endomorphism algebra $\mathrm{End}_K(L)$ with the algebra $\mathrm{M}_n(K)$ of $n \times n$ matrices with entries in K. Thus

$$\dim_L \mathrm{End}_K(L) = \frac{1}{n}\dim_K \mathrm{End}_K(L) = \frac{1}{n}\dim_K \mathrm{M}_n(K) = \frac{n^2}{n} = n.$$

Therefore $\varphi : V_f \to \mathrm{End}_K(L)$ is also surjective as a map of L-vector spaces, whence an isomorphism.

Suppose now that f and g are 2-cocycles that differ by a 2-coboundary, say $g = f \cdot \delta^1(\varphi)$ for a function $\varphi : G \to L^\times$. Multiplication in V_g, denoted by $\star_g$ for clarity, then takes the form

$$ae_\sigma \star_g be_\tau = a\sigma(b)g(\sigma,\tau)e_{\sigma\tau} = a\sigma(b)f(\sigma,\tau)\sigma(\varphi(\tau))\varphi(\sigma\tau)^{-1}\varphi(\sigma)e_{\sigma\tau}.$$

Since φ takes values in $L^\times$, each $\varphi(\sigma) \neq 0$, so this may be rearranged to the identity

$$a\frac{e_\sigma}{\varphi(\sigma)} \star_g b\frac{e_\tau}{\varphi(\tau)} = a\sigma(b)f(\sigma,\tau)\frac{e_{\sigma\tau}}{\varphi(\sigma\tau)}.$$

Equivalently, consider the L-linear map $\psi : V_f \to V_g$ determined by $\psi(e_\sigma) := e_\sigma/\varphi(\sigma)$. The identity above is equivalent to the identity

$$\psi(ae_\sigma \star_f be_\tau) = \psi(ae_\sigma) \star_g \psi(be_\tau),$$

which means that ψ is an algebra homomorphism. Since ψ but scales basis elements, it is an isomorphism of L-vector spaces, and so V_f and V_g are isomorphic as K-algebras.

Finally, Hamilton's quaternion algebra $\mathbf{H}$ may be realized as an $\mathbf{R}$-algebra as a twist of the complex numbers $\mathbf{C}$ by an appropriate 2-cocycle $f : \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \to \mathbf{C}^\times$. First, as a vector space over $\mathbf{R}$,

$$\mathbf{H} = \mathbf{R}\cdot 1_{\mathbf{R}} \oplus \mathbf{R}\cdot i \oplus \mathbf{R}\cdot j \oplus \mathbf{R}\cdot k$$

and the multiplication is determined by the relations $i^2 = j^2 = k^2 = ijk = -1_{\mathbf{R}}$. The complex numbers $\mathbf{C}$ may be identified with the subspace $\mathbf{C} = \mathbf{R} \cdot 1 \oplus \mathbf{R} \cdot i \subset \mathbf{H}$. Since $ij = k$, the quaternions $\mathbf{H}$ may be viewed as a vector space over $\mathbf{C}$ by writing

$$a \cdot 1_{\mathbf{R}} + b \cdot i + c \cdot j + d \cdot k = (a + bi) \cdot 1_{\mathbf{C}} + (c + di) \cdot j$$

where $a, b, c, d \in \mathbf{R}$, but we view $a + bi$ and $c + di$ as elements of $\mathbf{C}$. Multiplication in $\mathbf{H}$ of the two $\mathbf{C}$-basis elements now behaves as follows:

$$\begin{aligned}
(a + bi) \cdot 1_{\mathbf{C}} \times (c + di) \cdot 1_{\mathbf{C}} &= (a + bi)(c + di) \cdot 1_{\mathbf{C}}, \\
(a + bi) \cdot 1_{\mathbf{C}} \times (c + di) \cdot j &= (a + bi)(c + di) \cdot j, \\
(a + bi) \cdot j \times (c + di) \cdot 1_{\mathbf{C}} &= (a + bi)(c - di) \cdot j, \\
(a + bi) \cdot j \times (c + di) \cdot j &= -(a + bi)(c - di) \cdot j,
\end{aligned}$$

where we have used the relation $ji = -ij$ in the last two lines. Write σ for the generator of $\mathrm{Gal}(\mathbf{C} \mid \mathbf{R}) \cong \mathbf{Z}/2\mathbf{Z}$, which acts by complex conjugation $a + ib \mapsto a - ib$. Consider the function $f : \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z} \to \mathbf{C}^\times$ given by

$$f(1,1) = f(1,\sigma) = f(\sigma,1) = 1 \text{ and } f(\sigma,\sigma) = -1.$$

The $\mathbf{C}$-linear map $\mathbf{C}e_1 \oplus \mathbf{C}e_\sigma \to \mathbf{H}$ determined by $e_1 \mapsto 1_{\mathbf{C}}$ and $e_\sigma \mapsto j$ matches the operation $\star_f$ with multiplication in the quaternions, showing that $\mathbf{H} \cong V_f$ as $\mathbf{R}$-algebras. ■