Solutions to Exercises in Chapter 4 of "Noncommutative Algebra" by Benson Farb & Keith Dennis

1. Show that the following four conditions (one page 110) for two algebras to be similar are indeed equivalent. Let S and T be finite dimensional central simple k-algebras. Then $S \sim T$, i.e., S is similar to T if the following equivalent conditions hold:

   (a) If $S \sim M_n(D)$ and $T \sim M_m(E)$ for division rings D, E, then $D \sim E$

   (b) There exisits m, n such that $S \otimes M_m(k) \sim T \otimes M_n(k)$

   (c) There exists m, n such that $M_m(S) \sim M_n(T)$

   (d) If M is the unique simple S-module and N is the unique simple T-module, then $End_S(M) \sim End_T(N)$

   Solution: (a) $\implies$ (b): Let $S \sim M_n(D)$, $T \sim M_m(E)$. Then $S \otimes M_m(k) \sim M_{mn}(D)$ and $T \otimes M_n(k) \sim M_{mn}(E)$. So $D \sim E \implies$ (b).

   (b) $\implies$ (c): Follows from Lemma 4.1 (i) in the book.

   (c) $\implies$ (d): We first prove the following.

   Proposition 1. *Suppose $S \sim M_n(D)$ with $D^n = M$, the unique simple left S-module. Then $End_S(M) \sim D^{op}$. Similarly if N is the unique simple right S-module, then $End_S(N) \simeq D$.*

   Proof. Clearly, we have an injection

$$\begin{aligned} D^{op} &\hookrightarrow End_S(M) \\ d^{op} &\mapsto \phi_d : m \mapsto m.d \end{aligned}$$

   To show that the map is surjective, let $f \in End_S(M)$. Let $\{e_i\}$ denote the standard basis of M over D (acting from the left). Let E_{ij} denote the (i,j)-elementary matrix. Now for any

$m = Ae_1 \in M$ for some $A \in S$,

$$\begin{aligned} f(m) &= f(Ae_1), \text{for some} A \in S \\ &= Af(e_1) \\ &= Af(E_{11}e_1) \\ &= AE_{11}f(e_1) \\ &= AE_{11}\begin{bmatrix} d_1 \\ d_2 \\ \vdots \\ d_n \end{bmatrix} \\ &= A\begin{bmatrix} d_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} = (Ae_1)d_1 = m.d_1 = \phi_{d_1}(m) \end{aligned}$$

So $D^{op} \cong End_S(M)$. The proof for simple right S-modules is similar. □

Using the above claim let us prove (c) $\implies$ (d). Given that $Q := M_m(S) \sim M_n(T)$ for some m, n where $S \sim M_r(D)$ and $T \sim M_k(\Delta)$. Then by hypothesis $M_{mr}(D) \sim M_{nk}(\Delta)$. Let V be the unique simple Q-module. Then by the claim, $End_Q(V) \sim D^{op} \sim \Delta^{op}$, yielding $End_S(M) \sim D^{op} \sim \Delta^{op} \sim End_T(N)$.

(d) $\implies$ (a): By the claim, $D^{op} \sim End_S(M) \sim End_T(N) \sim \Delta^{op}$. So $D \sim \Delta$.

2. Let $A = [a_{ij}] \in M_n(k)$ and $B = [b_{kl}] \in M_m(k)$. The Kronecker product $A \otimes B$ is the $nm \times nm$ block matrix $[Ab_{kl}]1 \leq k, l \leq m$. Prove that the mapping

$$\begin{aligned} M_n(k) \otimes M_m(k) &\to M_{nm}(k) \\ (A, B) &\mapsto A \otimes B \end{aligned}$$

induces a k-algebra isomorphism.

Solution:

First note that the map is well-defined (Easy to check). To see that it is a k-algebra morphism, denote the i-th row of B_1 by $\mathbf{r_i}$ and the j-th column of B_2 by $\mathbf{s_j}$. Then

$$\begin{aligned} A_1A_2 \otimes B_1B_2 &= [A_1A_2\mathbf{r_i}\mathbf{s_j}]_{ij} \\ &= [A_1(\mathbf{r_i})]_i[A_2(\mathbf{s_j})]_j \\ &= (A_1 \otimes B_1)(A_2 \otimes B_2) \end{aligned}$$

where for $\mathbf{r_i} = [r_{i1}\ r_{i2} \cdots r_{im}]$, $A_1(\mathbf{r_i}) = [A_1r_{i1}\ A_1r_{i2} \cdots A_1r_{im}]$ and for $\mathbf{s_j} = \begin{bmatrix} s_{j1} \\ s_{j2} \\ \vdots \\ s_{jm} \end{bmatrix}$, $A_2(\mathbf{s_j}) = \begin{bmatrix} A_2s_{j1} \\ A_2s_{j2} \\ \vdots \\ A_2s_{jm} \end{bmatrix}$. The map is injective beacuse by definition if $A \otimes B = 0$ then $A = 0$ or $B = 0$. Since the dimension of both domain and codomain equals to n^2m^2, the map is surjective and hence an isomorphism.

3. Show that the set of isomorphism classes of finite dimensional central simple algebras over a field k actually forms a set. Estimate its cardinality.

4. (a) Show that $Br()$ is a functor from the category of fields and field homomorphisms to the category of abelian groups and group homomorphisms
   Solution: Consider
$$\begin{aligned} Br : Fields &\longrightarrow AbelianGroups \\ k &\rightsquigarrow Br(k) \\ i : k \to K &\rightsquigarrow Br(i) : Br(k) \to Br(K) \end{aligned}$$
   where $Br(i)$ takes a central simple algebra A over k to $A \otimes_k K$. Note that $Br(i)$ is a group homomorphism becuse it takes $A \otimes_k B$ to $A \otimes_k B \otimes_k K \simeq (A \otimes_k K) \otimes_K (B \otimes_k K)$. Clearly, $Br(id)$ is the identity. Moreover, if $k_1 \xrightarrow{f} k_2 \xrightarrow{g} k_3$ is a composition of maps then $Br(g) \circ Br(f)(A) = (A \otimes_{k_1} k_2) \otimes_{k_2} k_3 \simeq A \otimes_{k_1} k_3 = Br(g \circ f)$.

   (b) Let $i : k \to K$ and $j : k \to K$ be homomorphism of fields and let i_* and j_* be the induced maps from $Br(k)$ to $Br(K)$. Let $F = \{x \in k : i(x) = j(x)\}$ and assume that $K/i(F)$ is finite Galois. Prove that $i_* = j_*$.
   Solution: This is not true.

5. Give an example of two finite dimensional central fivision algebras over k whose tensor product (over k) is not a division algebra.
   Solution:
   Let $\mathbb{H}$ denote the real quarternions i.e., $H = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ with $ij = k, jk = i, ki = j, i^2 = j^2 = k^2 = -1$. Then $\mathbb{H}$ is a division algebra. So is $\mathbb{H}^{op}$. But $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}^{op} \simeq M_4(\mathbb{R})$ is not a division algebra.

   Digression: $\mathbb{H} \simeq \mathbb{H}^{op}$ since $[\mathbb{H}]$ has order 2 in $Br(\mathbb{R})$. The explicit isomorphism is given by
$$\begin{aligned} \mathbb{H} &\to \mathbb{H} \\ r &\mapsto r \\ i &\mapsto -j^{op} \\ j &\mapsto -r^{op} \\ k &\mapsto -i^{op} \end{aligned}$$
   It is easy to check that it is a $\mathbb{R}$-algebra isomorphism.

6. (a) Prove that $Br(k) = 0$ for any algebraic extension of finite fields
   Solution:
   Recall the definition of C_1-fields:
   A field k is *quasi-algebraically closed* or C_1 if for any homogeneous polynomial of degree d in $n > d$ variables, there exists a non-trivial solution.

   The result follows from the following lemmas:

   Lemma 2. *Finite fields are C_1.*

   Lemma 3. *Finite extensions of C_1-fields are C_1.*

   Lemma 4. *Algebraic extensions of C_1-fields are C_1.*

   Lemma 5. *If k is a C_1-field, then $Br(k) = 0$.*

(b) Prove that $Br(k) = 0$ for any field k of transcendence degree one over an algebraically closed field.

Solution:

This follows from the previous lemma and Tsen's theorem which states that such fields are C_1.

7. (a) Show that a k-algebra A is central simple over k if and only if there is a k-algebra B such that $A \otimes_k B \simeq M_n(k)$ as k-algebras for some n.

Solution:

The "only if " part follows by taking $B = A^{op}$. Now suppose $A \otimes B \simeq M_n(k)$ for some B. Now if A is not simple, then there is a non-trivial two sided ideal $I \subsetneq A$. This yields $I \otimes B$, a non-trivial two sided ideal in $A \otimes B \simeq M_n(k)$ which is simple. This is contradiction. Threfore A is simple.

Also

$$\begin{aligned} &Z(A) \otimes_k k \subseteq Z(A \otimes_k B) = Z(M_n(k)) = k \\ &\Rightarrow Z(A) \subseteq k \subseteq Z(A) \\ &\Rightarrow Z(A) = k \end{aligned}$$

Hence A is central simple over k.

(b) Let A, A' be central simple over k. Show that if $[A] = [A']$ in $Br(k)$ and $[A : k] = [A' : k]$ then $A \simeq A'$ as k-algebras

Solution:

Let $A \simeq M_n(D)$ and $A' \simeq M_r(D)$ for some division algebra D over k. Then

$$\begin{aligned} [A : k] = [A : D][D : k] = n^2[D : k] &= r^2[D : k] = [A' : k] \\ &\Rightarrow n^2 = r^2 \\ &\Rightarrow n = r \\ &\Rightarrow A \simeq A' \end{aligned}$$

8. Theorem 4.4 (in the book) may be interpreted as follows. Given $z \in Br(K/k)$, there is a pair (S, i) such that $z = [S]$ where S is central simple over k and $i : K \to S$ is a k-algebra homomorphism whose image is a maximal commutative subalgebra of S. Suppose that (S', i') is another such pair and $z = [S']$. Prove that ther eis a k-algebra isomorphism $\phi : S \to S'$ such that $\phi \circ i = i'$.

Solution:

$$[S : k] = [S : i(K)][i(K) : k]$$

Since $i(K)$ is a maximal subfield of S, its centralizer is itself. So by double centralizer theorem, $[S : k] = [K : k]^2$. Similarly, $[S' : k] = [K : k]^2$. Thus $[S : k] = [S' : k]$. Also it is given that $[S] = [S']$. Hence by Problem 7(b), there exists a k-isomorphism $\alpha : S \to S'$. Now $\alpha \circ i$ and i' are two homomorphisms from K to S'. By Skolem-Noether, there is an inner automorphism $\theta : S' \to S'$ such that $\theta \circ \alpha \circ i = i'$. Then $\phi = \theta \circ \alpha$ is the required k-isomorphism.

9. Let A be a central simple algebra over k with maximal commutative subalgebra K. Assume K/k is Galois with Galois group G. Let E be the normalizer of K^* in A^*. Find a homomorphism ϕ of E onto G such that $ker\phi = K^*$. E is an example of what is called a group extension of G by K^*.

Solution:
Define

$$\begin{aligned}\phi : E &\to G\\ \alpha &\mapsto \sigma_\alpha\end{aligned}$$

where σ_α is "conjugation by α". Now ϕ is surjective by Skolem-Noether and $ker\phi = C_A(K^*) = K^*$ since K is a maximal subfield.

10. Let A be a central simple k-algebra containing a field F. Let $C(F)$ be the centralizer of F in A. Show that the following equality holds in $Br(F)$: $[F \otimes_k A] = [C(F)]$.

Solution:
We first prove the following proposition which is the corrected version of Proposition 1.10 from "The Book of Involutions".

Proposition 6. *Every right module of finite type M over a central simple F-algebra A has a natural structure of left module over $E = End_A(M)$, so that M is an $A - E$ bimodule. If $M \neq \{0\}$, the algebra E is central simple over F and Brauer equivalent to A. Moreover,*

$$\begin{aligned}deg\ E &= rdim_A M\\ deg\ A &= rdim_E M\end{aligned}$$

Proof. Clearly M is an $A - E$ bimodule. Suppose $A = M_r(D)$ for some division algebra D. Then $N = D^r$ written as row vector is a simple right A-module. By Proposition 1 have an isomorphism of F-algebras:

$$D \to End_A(N)$$

Now $M \simeq (D^r)^s$ for some s. Therefore,

$$E = End_A(M) \simeq End_A((D^r)^s) \simeq M_s(End_A(D^r)) \simeq M_s(D)$$

This proves that E is central simple over F and is Brauer equivalent to A. Moreover,

$$degE = s.degD = rdim_A M$$

and

$$rdim_E M = \frac{rs(degD)^2}{s.degD} = r.degD = degA$$

□

Now $F \otimes_k A$ is a central simple algebra over F. Note that A is a right $F \otimes_k A$-module via the action given by $a \cdot (f \otimes a') = f \cdot a \cdot a'$. Consider the map

$$\begin{aligned}C(F) &\to End_{F\otimes_k K}(A) := B\\ h &\to \phi_h\end{aligned}$$

where ϕ_h is multiplication to the left by h. This map is clearly injective. Moreover, by Proposition 6,

$$degB = rdim_{F\otimes A}(A) = \frac{dim_F A}{deg(F \otimes A)} = \frac{(degA)^2}{[F : k] \cdot degA} = \frac{degA}{[F : k]}$$

Now by the double centralizer theorem

$$\begin{aligned} dim_F(C(F)) &= \frac{dim_k(C(F))}{[F:k]} = \frac{(degA)^2}{[F:k]^2} \\ \Rightarrow deg(C(F)) &= \frac{degA}{[F:k]} = degB \end{aligned}$$

So the map is surjective and $[C(F)] = [B] = [F \otimes_k K]$ by Proposition 6.

11. Let A be a central simple k-algebra. Prove the following

(a) If $[A : k] = n^2$, then $ind(A)/n$ and ind(A) = n iff A is a division algebra
Solution:
Let $A \simeq M_r(D)$. Then

$$\begin{aligned} [A:k] &= [A:D][D:k] \\ n^2 &= r^2 ind(A)^2 \\ \Rightarrow n &= r \cdot ind(A) \\ \Rightarrow ind(A)/n \end{aligned}$$

Moreover $ind(A) = n$ iff $r = 1$.

(b) If A' is a central simple algebra over k such that $[A'] = [A]$ in $Br(k)$, then $ind(A') = ind(A)$
Solution:
This is easy to see.

(c) A posseses a splitting field of degree $ind(A)$ over k.
Solution:
Let $A \simeq M_r(D)$ where $degD = ind(A) := n$. Let K be a maximal subfield of D. Then by the double centralizer theorem,

$$\begin{aligned} n^2 = [D:k] &= [K:k][C(K):k] = [K:k]^2 \\ \Rightarrow [K:k] &= n \end{aligned}$$

Since K splits D, it splits A too.

(d) If K is any splitting field of A, then $ind(A)/[K : k]$.
Solution:
Let $A \simeq M_r(D)$. Let K be a splitting field of A. Then by Theorem 4.4 in the book, thre exists S suchthat $[S] = [A]$ with $degS = [K : k]$. So $ind(A) = ind(S)$ and $ind(S)/deg(S)$. So $ind(A)/[K : k]$.

(e) $ind(A) = min\{[K : k] : K \text{ splits } A\}$
Solution:
Follows from (d) and (e).

(f) For $m \geq 1$, $ind(A^{\otimes m})/ind(A)$
Solution:
Let K split A. Then K also splits $A^{\otimes m}$ since

$$A \otimes_k A \otimes_k \cdots \otimes_k A \otimes_k K \simeq (A \otimes_k K) \otimes_K (A \otimes_k K) \cdots \otimes_K (A \otimes_k K) \simeq M_r(K)$$

Moreover by (c), A has a splitting field K of degree $ind(A)$ over k which also splits $A^{\otimes m}$. By (d), $ind(A^{\otimes m})/[K : k]$. But $[K : k] = ind(A)$ so that we are done.

12. Let A be a central simple algebra over k and let K/k be a finite extension. Prove that

    (a) $ind(A_K)/ind(A)$
    Solution:
    We can asssume that A is a division algebra. Since the index of a central simple algebra divides its degree, $ind(A_K)/deg(A_K)$. But $deg(A_K) = deg(A) = ind(A)$ and we are done.

    (b) $ind(A)/[K : k]ind(A_K)$
    Solution:
    Let $A \simeq M_s(D)$. Write $D_K \simeq M_r(D')$ for some division algebra D'. Let K' be a mximal subfield of D'. Note that $[D'] = [A_K]$. Then K' splits D' and hence A_K. Moreover

    $$\begin{aligned} [K' : k]^2 &= [D' : K] = ind(A_K)^2 \\ ind(A_K) &= [K' : K] \end{aligned}$$

    Now

    $$A \otimes_k K' \simeq A \otimes_k K \otimes_K K' \simeq M_t(K')$$

    By the previous problem 11(d),

    $$\begin{aligned} &ind(A)/[K' : k] \\ \Rightarrow\ &ind(A)/[K' : K][K : k] \\ \Rightarrow\ &ind(A)/ind(A_K)[K : k] \end{aligned}$$

    (c) If $ind(A)$ and $[K : k]$ are relatively prime, then $ind(A_K) = ind(A)$; and if A is also a division algebra, then so is A_K.
    Solution:
    Follows from (a) and (b).

13. Let A and B be finite dimensionalcentral simple algebras over k. Let K/k be a finite field extension. Prove the following facts:

    (a) If $[A] = [B]$, then $exp(A) = exp(B)$
    Solution:
    This is easy to see because $A^{\otimes m}$ splits iff $D^{\otimes m}$ splits where D is the division algebra in the class of A in $Br(k)$.

    (b) $exp(A_K)/exp(A)$
    Solution:
    Let $n = exp(A)$. So $(A)^{\otimes n}$ splits. But $(A_K)^{\otimes n} = (A \otimes_k K) \otimes_K (A \otimes_k K) \cdots \otimes_K (A \otimes_k K) \simeq (A)^{\otimes n} \otimes_k K \simeq M_r(K)$. So $exp(A_k)/exp(A)$.

    (c) $exp(A)/[K : k]exp(A_K)$
    Solution:
    Let $exp(A_K) = n$. So $(A_K)^{\otimes n}$ splits. So $(A^{\otimes n})_K$ splits. This implies $[K : k]$ splits $A^{\otimes n}$. By 11 (d), this implies $ind(A^{\otimes n})/[K : k]$. Since $exp()/ind()$, $exp(A^{\otimes n})/[K : k]$ i.e., $(A^{\otimes n})^{[K:k]}$ splits. Therefore $exp(A)/n[K : k]$.

    (d) If $ind(A)$ is relatively prime to $[K : k]$, then $exp(A_K) = exp(A)$.
    Solution:
    $ind(A)$ relatively prime to $[K : k] \Leftrightarrow exp(A)$ relatively prime to $[K : k]$ since $ind(A)$ and $exp(A)$ have same prime factors. Now the result follows from (b) and (c).

(e) $exp(A \otimes B)$ divides the lcm of $exp(A)$ and $exp(B)$.
Solution:
Let n denote the lcm. Then $(A \otimes B)^{\otimes n} \simeq A^{\otimes n} \otimes B^{\otimes n}$ which is split. This means that $exp(A \otimes B)/n$.

(f) $exp(A^{\otimes m}) = exp(A)/n$ where n is the gcd of m and $exp(A)$.
Solution:
Let $exp(A^{\otimes m}) = r$. So $(A^{\otimes m})^r = A^{\otimes mr}$ splits. This means that $exp(A)/mr$. Here r is the least positive integer such that $exp(A)/mr$. So $r = \frac{exp(A)}{gcd(m, exp(A))}$.

(g) If $ind(A)$ and $ind(B)$ are relatively prime, then $ind(A \otimes B) = ind(A) \cdot ind(B)$ and $exp(A \otimes B) = exp(A) \cdot exp(B)$.
Solution:
WLOG we can assume that A and B are division algebras. By Lemma 4.18 in the book, $A \otimes B$ is a division algebra since their indices are coprime. Thus ,$ind(A \otimes B) = deg(A \otimes B) = deg(A)deg(B) = ind(A)ind(B)$.
By (e),

$$exp(A \otimes B)/(exp(A)exp(B)) \tag{1}$$

Let $m = exp(A \otimes B)$. WLOG assume A and B are division algebras. Then$[A \otimes B]^m = [A]^m[B]^m = 1$. By (f), $ind(A^{\otimes m})/exp(A)$ and $ind(B^{\otimes m})/exp(B)$. So $ind(A^{\otimes m})$ and $ind(B^{\otimes m})$ are relatively prime as well since $exp()$ and $ind()$ have same prime factors. Now let $[D] = [A]^n$ and $[E] = [B]^m$ where D, E are division algebras. Then from the above equation,

$$\begin{aligned} [A]^m[B]^m &= 1 \\ [D][E] &= 1 \\ [D \otimes E] &= 1 \end{aligned}$$

But $ind(D)$ and $ind(E)$ arerelatively prime. So by Lemma 4.8 in the book, $D \otimes E$ is division algebra over k. But that is possible only when $D = E = k$. So $A^{\otimes m}$ and $B^{\otimes m}$ are split i.e., $exp(A)/m$ and $exp(B)/m$. Since $exp(A)$ and $exp(B)$ are coprime, $exp(A)exp(B)/m$. This together with (3) finishes the proof.

14. Let A be a finite dimensional central simple algebraover k with $ind(A) = p^j n$, p prime, $j \geq 1$ and $p \nmid n$. Prove that there is a field extension K/k whose dimension is relatively prime to p, for which $ind(A_K) = p^j$.
Solution:
WLOG we can assume A is a division algebra. Then by Theorem 4.19, $A \simeq D_1 \otimes_k D_2 \otimes_k \cdots \otimes_k D_r$ where $ind(D_1) = p^j$ and $ind(D_t) = q_t^{i_t}$ where q_t are distinct primes and $p \neq q_t$ for $2 \leq t \leq r$. Now each D_t, $t \geq 2$ contains a maximal subfieldK_t of degree $ind(D_t)$ by the Centralizer theorem. Moreover K_t splits D_t. Let K be the composite of the fields in K_t in $\overline{k}$. Then $[K : k] = n = \prod_{t=2}^{r} q_t^{i_t}$. So $p \nmid [K : k]$. Moreover, $A \otimes k = (D_1 \otimes_k K) \otimes_K (D_2 \otimes_k K) \otimes_k \cdots \otimes_k (D_r \otimes_k K) = M_s(D_1 \otimes_k K)$. But $ind(D_1)$ and $[K : k]$ are coprime. So $D_1 \otimes_k K$ is division algebra by 12 (c). Therefore, $ind(A_K) = deg(D_1 \otimes_k K) = deg(D_1) = p^j$.

Generalized Quarternion Algebras

Let k be a field of characteristic not equal to 2. For $a, b\imath K^*$, let $(\frac{a,b}{k})$ denote the vector space of dimension 4 over k having the elements $1, i, j, k$ as a basis. Defining $i^2 = a, j^2 = b, ij = -ji = k$. This makes this into a k-algebra. Note that $k^2 = -ab, ki = -ik = -aj$ and $jk = -kj = -bi$. The algebra $(\frac{a,b}{k})$ is called the **generalized quarternion algebra**.

15. (a) Show that every 4-dimensional central simple algebra over k is isomorphic to $(\frac{a,b}{k})$, for some $a, b \in k^*$.

Solution:

Let A be a 4-dimensional central simple algerba over k. Then A is either $M_2(k)$ or a division algebra. By Problem 16, $M_2(k) \simeq (\frac{1,1}{k})$. So assume that A is a division algebra. Note that A contains a maximal subfield K. Then by the double centralizer theorem, K is a quadratic extension of k. Let $K = k(\sqrt{\alpha}), \alpha \in k/(k^*)^2$. Let σ be the non-trivial automorphism in $Gal(K/k)$. Then by Skolem-Noether, there exists $y \in A$ such that $\sigma(t) = yty^{-1} \forall t \in K$. Since $\sigma^2 = 1$, conjegation by y^2 is trivial on K . Since K is maximal, this implies $y^2 \in K$. Also $\sigma(y^2) = y^2 \Rightarrow y^2 \in k^*$. Let $y^2 = \beta \in k^*$ and $x^2 = \alpha \in k^*$. So the k-subalgebra in A generated by x and y is given by the following relations

$$\begin{aligned} x^2 &= \alpha, y^2 = \beta \\ \sigma(x) = yxy^{-1} \Rightarrow -x &= yxy^{-1} \Rightarrow xy = -yx \end{aligned}$$

The elements $\{1, x, y, xy\}$ forms a basis for A and $A \simeq (\frac{\alpha,\beta}{k})$.

(b) Using this description of the central simple algebra , explicitly give its factor sets.

Solution:

If $A \simeq M_2(k)$, its factor sets are $\{a_{1,\sigma} = a_{\sigma,1} = a_{1,1} = a_{\sigma,\sigma} = 1\}$. Now assume that A is a division algebra. Then from the proof of the previous prolem we note that $A \simeq (\frac{a,b}{k})$ where $i^2 = a, j^2 = b, k = ij = -ji$. Moreover, $a \notin (k^*)^2$. Then $K = k[i]$ is a mximal subfield of A. Let $\sigma \in Gal(K/k)$ be the non-trivial element. Then $\sigma(c + id) = c - id = j(c + id)j^{-1}$. So we can pick $x_\sigma = j$ and $x_1 = 1$. The the relation $x_1 x_\sigma = a_{1,\sigma} x_\sigma$, $x_\sigma x_1 = a_{\sigma,1} x_\sigma$ and $x_\sigma x_\sigma = a_{\sigma,\sigma} x_1$, yields the following factor set

$$\{a_{1,1} = a_{\sigma,1} = a_{1,\sigma} = 1, a_{\sigma,\sigma} = b\}$$

16. Show that $(\frac{1,1}{k}) \simeq M_2(k)$

Solution:

Since $(1 + i)(1 - i) = 1 - 1 = 0$, the ring has elements that do not have inverses. So it is not a division algebra and hence split.

17. Show that $(\frac{a,b}{k}) \simeq (\frac{b,a}{k})$

Solution:

The isomorphism is given by

$$\begin{aligned} (\frac{a,b}{k}) &\to (\frac{b,a}{k}) \\ 1 &\mapsto 1 \\ i &\mapsto -j \\ j &\mapsto -i \\ k &\mapsto -k \end{aligned}$$

18. Show that $(\frac{a,b}{k}) \simeq (\frac{ax^2,by^2}{k})$ for any $x, y \in k^*$

Solution:

The isomorphism is given by

$$\begin{aligned}(\frac{a,b}{k}) &\to (\frac{ax^2,by^2}{k})\\ 1 &\mapsto 1\\ i &\mapsto xi\\ j &\mapsto yj\\ k &\mapsto xyk\end{aligned}$$

19. Show that $(\frac{a,b}{k}) \otimes_k K \simeq (\frac{a,b}{K})$ for $k \subseteq K$.
<u>Solution:</u>
As a K-vector space $(\frac{a,b}{K})$ has basis $\{1 \otimes 1, i \otimes 1, j \otimes 1, k \otimes 1\}$. The explicit isomorphism is given by sending this ordered basis to the basis $\{1, i, j, k\}$ of $(\frac{a,b}{k})$.

20. Show that $(\frac{a,b}{k})$ is a central simple algebra.
<u>Solution:</u>
Let us first compute its center Z. Suppose $z = c + di + ej + fk \in Z$. Then the relation $iz = zi$ yields $e = f = 0$, so $z = c + di$. Using the relation $jz = zj$, we get $d = 0$, so that $z \in k$. Hence its center is k.
To show that it is simple, it suffices to show that $(\frac{a,b}{k}) \otimes_k \overline{k}$ is simple. Now

$$\begin{aligned}(\frac{a,b}{k}) \otimes_k \overline{k} &\simeq (\frac{a,b}{\overline{k}}) \quad \text{by Problem 19}\\ &\simeq (\frac{1.(\sqrt{a})^2, 1.(\sqrt{b})^2}{\overline{k}})\\ &\simeq (\frac{1,1}{\overline{k}}) \quad \text{by Problem 18}\\ &\simeq M_2(\overline{k}) \quad \text{by Problem 16}\end{aligned}$$

which is simple.

21. Show that $\frac{a,1-a}{k} \simeq M_2(k)$.
<u>Solution:</u>
Consider $z = (1 + i + j)$. Then $z \cdot (1 - i - j) = 0$, the algebra is split.

22. Show that $(\frac{1,b}{k}) \simeq (\frac{a,-a}{k}) \simeq M_2(k)$.
<u>Solution:</u> In $(\frac{1,b}{k})$, we have $(j + k)(-j - k) = 0$ and in $(\frac{a,-a}{k})$, $(i + j)(-i - j) = 0$. So they are isomorphic to $M_2(k)$.

23. Show that $A \simeq (\frac{a,b}{k})$ is isomorphic to its opposite algebra A^{op}.
<u>Solution:</u> This is because $exp(A)$ is either 1 or 2, so that $[A]^2 = 1$ in $Br(k)$. Hence $A \simeq A^{op}$. The explicit isomorphism is given by

$$\begin{aligned}(\frac{a,b}{k}) &\to (\frac{a,b}{k})^{op}\\ 1 &\mapsto 1^{op}\\ i &\mapsto -i^{op}\\ j &\mapsto -j^{op}\\ k &\mapsto -k^{op}\end{aligned}$$

24. Show that $(\frac{a,b}{k}) \simeq M_2(k)$ iff $a \in N_{E/k}(z)$, for some $z \in E = k(\sqrt{b})$ where $N_{E/k}(z)$ is the norm of z.
Solution:
$\underline{\Leftarrow}$: Let $a = u^2 - bv^2 = N(u + \sqrt{b}v)$. Then $(u + i + jv)(u - i - jv) = u^2 - a - bv^2 = 0$. So $(\frac{a,b}{k}) \simeq M_2(k)$

underline$\Rightarrow$: $(\frac{a,b}{k}) \simeq M_2(k)$. Then there exists $0 \neq z \in (\frac{a,b}{k})$ such that z is not invertble. Consider $z\overline{z}$ where $z = u - iv - jw - kx$ is the conjugate of $z = u + iv + jw + kx$. Then note that $N(z) = z\overline{z} = u^2 - av^2 - bw^2 + ab = 0$, since otherwise z will have an inverse given by $\overline{z}N(z)$. So we have

$$\begin{aligned} u^2 - av^2 - bw^2 + ab = 0 \\ u^2 - bw^2 &= av^2 - ab \\ u^2 - bw^2 &= a(v^2 - b) \end{aligned}$$

Now if $b = v^2$, then $k(\sqrt{b}) = k$ and $a = N(a)$ as $a \in k(\sqrt{b}) = k$. So assume $b \neq v^2$. Then

$$\begin{aligned} a &= \frac{u^2 - bw^2}{v^2 - b} \\ &= N(\frac{u + \sqrt{b}w}{v + \sqrt{b}}) \end{aligned}$$

25. Show that $(\frac{a,b}{k})$ is a division algebra if and inly if b is not the norm of an element of $k(\sqrt{a})$.
Solution:
This follows from Problem 17 and Problem 24.

26. Show that $(\frac{a,b}{k}) \otimes_k (\frac{a,c}{k}) \simeq (\frac{a,bc}{k}) \otimes_k (\frac{c,-a^2c}{k}) \simeq (\frac{a,bc}{k}) \otimes_k M_2(k)$
Solutions:
The last isomorphism is clear from Problem 18 and 22. Let $A = (\frac{a,b}{k}) \otimes_k (\frac{a,c}{k})$ and let

$$\begin{aligned} I &= i \otimes 1 \\ J &= j \otimes j' \\ K = IJ &= k \otimes j' \\ I' &= 1 \otimes j' \\ J' &= i \otimes k' \\ K' = I'J' &= -c(i \otimes i') \end{aligned}$$

Consider the k-linear map

$$\begin{aligned} (\frac{a,b}{k}) \otimes_k (\frac{a,c}{k}) \to (\frac{a,bc}{k}) \otimes_k (\frac{c,-a^2c}{k}) \\ I &\mapsto i \otimes 1 \\ J &\mapsto j \otimes 1 \\ K &\mapsto k \otimes 1 \\ I' &\mapsto 1 \otimes i \\ J' &\mapsto 1 \otimes j \\ K' &\mapsto 1 \otimes k \end{aligned}$$

It is easy to check that this map extends to k-algebra morphism. It is surjective since it maps onto the basis of the codomain. It is injective since the domain is simple. Hence it is an isomorphism.

27. Prove that an element of $Br(k)$ has the form $[(\frac{a,b}{k})]$ for some $a, b \in k$ if and only if it is in $Br(K/k)$ for some separable quadratic extension K/k.
Solution:
$\underline{\Rightarrow:}$ Let $K = k(\sqrt{b})$. Then $(\frac{a,b}{k}) \otimes_k K$ is split by Problem 18 and 22. Hence it is in $Br(K/k)$.
$\underline{\Leftarrow:}$ Suppose $[A] \in Br(K/k)$, i.e., K splits A where $[K : k] = 2$. Then by Theorem 4.4, there exists a central simple algebra of degree 2 (i.e., dimension 4) in the class of A which contains K as a maximal subfield. But every central simple algebra of dimension 4 is isomorphic to $(\frac{a,b}{k})$ for some a, b by Problem15(a). Hence $[A] = [(\frac{a,b}{k})]$.

28. **Power Norm Residue Symbols:**

(Reference: Milnor's Algebraic K-theory, Chapter 15, "Power Norm Residue Symbol" and Grayson's "On K-theory of fields") Let F be a field containing a primitive nth root of unity ω. For $a, b \in F^*$, let $A_w(a, b)$ be the F-algebra of dimension n^2 which is generated by elements x and y which satisfy $x^n = a$, $y^n = b$ and $yx = \omega xy$. A basis for $A_\omega(a, b)$ consists of $\{x^i y^j : 0 \leq i, j \leq n\}$. Check the following:

(a) $A_\omega(a, b)$ is central simple over F and thus gives a function

$$a_\omega : F^* \times F^* \to Br(F)$$

Solution:
Let $\sum c_{ij} x^i y^j$ be in the center. Then $(\sum c_{ij} x^i y^j)x = x(\sum c_{ij} x^i y^j)$ if and only if $c_i j = 0 \forall j \geq 1$. Similarly, $(\sum c_{ij} x^i y^j)y = y(\sum c_{ij} x^i y^j)$ if and only if $c_i j = 0 \forall i \geq 1$. Hence the center is F. Now let I be a non-zero two sided ideal in $A_\omega(a, b)$ and let $0 \neq \alpha = \sum c_{ij} x^i y^j \in I$. Suppose $c_{kl} \neq 0$. Then $x^{-k} \alpha y^{-l} \in I$ has a non-zero constant term. So WLOG we can assume that $c_{00} \neq 0$ in α. Let

$$\begin{aligned} T_x, T_y : A_\omega(a, b) &\to A_\omega(a, b) \\ T_x : z &\mapsto xzx^{-1} \\ T_y : z &\mapsto yzy^{-1} \end{aligned}$$

Then $T_x(x^i y^j) = \omega^{-j} x^i y^j$ and $T_y(x^i y^j) = \omega^i x^i y^j$. So $\beta = (T_x - \omega)(T_x - \omega^2) \cdots (T_x - \omega^{n-1})\alpha$ has no $x^i y^j$ term where $j \geq 1$. Hence WLOG assume that α has no term involving y. now for such an α, $\gamma = (T_y - \omega)(T_y - \omega^2) \cdots (T_y - \omega^{n-1})\alpha = (1-\omega)(1-\omega^2) \cdots (1-\omega^{n-1})c_{00} = nc_{00} \neq 0$ (Since F has primitive nth root of unity, $n \neq 0$ in F).

(b) The function

$$\begin{aligned} a_\omega : F^* \times F^* &\to Br(F) \\ (a, b) &\mapsto A_\omega(a, b) \end{aligned}$$

satisfies the following:

i. $a_\omega(a, bc) = a_\omega(a, b) a_\omega(a, c)$
Solution:
We will first prove the following lemma:

Lemma 7. *Let A be a central simple algebra of dimension n^2 over F and let $x \in A$ be an element which satisfies a polynomial equation over F of the form*

$$f(x) = x^n + \phi_1 x^{n-1} + \cdots + \phi_n 1 = 0$$

but no equation of smaller degree. If $f(x)$ splits into distinct linear factors over F, then A is siomorphic to the matrix algebra $M_n(F)$.

Proof. The subalgebra of A spanned by powers of x is clearly isomorphic to the quotient ring $F[x]/(f(x))$. By the Chinese Remainder theorem, $F[x]/(f(x))$ splits as a Cartesian product of n copies of F. Hence it contains mutually orthogonal idempotents $e_1, e_2, \cdots, e_n$ where

$$\begin{aligned} e_i e_j &= 0 \text{ iff } i \neq j \\ e_i^2 &= e_i \\ \sum_{i=1}^{n} e_i &= 1 \end{aligned}$$

Therefore A splits as a direct sum

$$A \simeq e_1 A \oplus e_2 A \oplus \cdots \oplus e_n A$$

of right ideals. Since $A \simeq M_r(D)$ for some division algebra D, every simple right ideal in A is given by a row vector in the matrix representation of A with the rest of the rows zero. So A decomposes as direct sum of r simple right ideals. Thus $n = r$ and hence $degD = 1 \Rightarrow D = F$. Therefore $A \simeq M_n(F)$. □

Using this lemma we proceed as follows. Consider $A_\omega(a, b) \otimes_F A_\omega(a, c)$. Let

$$\begin{aligned} X' &= x \otimes 1 \\ Y' &= y \otimes 1 \\ \Rightarrow Y'X' &= yx \otimes 1 = \omega xy \otimes 1 = \omega X'Y' \\ X &= 1 \otimes x \\ Y &= 1 \otimes y \\ \Rightarrow YX &= 1 \otimes yx = \omega(1 \otimes xy) = \omega XY \\ \Rightarrow X'^n &= a, Y'^n = b, X^n = a, Y^n = c \\ \text{Moreover, } X'X &= XX', X'Y = YX', XY' = Y'X, YY' = Y'Y \end{aligned}$$

Let B' be the subalgebra generated by X' and $Y'Y$. Let B'' be the subalgebra generated by $X'^{-1}X$ and Y. Then the generators of B' and B'' commute. We then have a map

$$\begin{aligned} \Phi : B' \otimes B'' &\to A_\omega(a, b) \otimes A_\omega(a, c) \\ X' \otimes 1 &\mapsto X' \\ Y'Y \otimes 1 &\mapsto Y'Y \\ 1 \otimes X'^{-1}X &\mapsto X'^{-1}X \\ 1 \otimes Y &\mapsto Y \end{aligned}$$

Note that $B' \simeq A_\omega(a, bc)$ and $B'' \simeq A_\omega(1, c)$. So $B' \otimes_F B''$ is simple and hence Φ is injective. By dimension count, it is surjective. So Φ is an isomorphism.

$$\begin{aligned} \Rightarrow A_\omega(a, b) \otimes A_\omega(a, c) &\simeq A_\omega(a, bc) \otimes A_\omega(a, c) \\ &\simeq A_\omega(a, bc) \otimes M_n(F) \\ \Rightarrow a_\omega(a, b) \otimes a_\omega(a, c) &\simeq a_\omega(a, bc) \text{ in Br(F)} \end{aligned}$$

Remark: By observing that $A_{\omega^{-1}}(a,b) \simeq A_\omega(b,a)$, we can also show that $a_\omega(a,b) \otimes a_\omega(c,b) \simeq a_\omega(ac,b)$ in Br(F).

ii. $a_\omega(a,b) = a_\omega(b,a)^{-1}$
Solution:
First we prove the following lemma.

Lemma 8. *Let $\xi = \omega^i$ where i is relatively prime to n (so that ξ is another primitive n-th root of unity), then*

$$a_\xi(a,b)^i = a_\omega(a,b)$$

Proof. The isomorphism is given by

$$\begin{aligned} A_{\omega_i}(a^i,b) &\to A_\omega(a,b) \\ x &\mapsto x^i \\ y &\mapsto y \end{aligned}$$

□

Since $a_\xi(a^i,b) = a_\xi(a,b)^i$ by (ii), we have $a_\omega(a,b) = a_\xi(a,b)^i = a_{\omega^i}(a,b)^i$. Now

$$\begin{aligned} a_{\omega^{-1}}(b,a)^{-1} &= a_\omega(b,a) \\ a_\omega(a,b) &= a_{\omega^{-1}}(b,a) = a_\omega(b,a)^{-1} \end{aligned}$$

iii. $a_\omega(a,1-a) = 1$ (Steinberg identity)
Solution:
We will first prove the following lemma:

Lemma 9. *Let x, y be arbitrary elements in a ring satisfying $yx = cxy$ where c is in the center, then*

$$(x+y)^n = \sum_{i=0}^{n} b_i^n(c) x^i y^{n-i}$$

where

$$b_i^n(c) = c^i b_i^{n-1}(c) + b_{i-1}^{n-1}(c)$$

Moreover,

$$\begin{aligned} b_i^n(c) &= \frac{f_n(c)}{f_i(c) f_{n-i}(c)} \text{ where} \\ f_0(c) = 1, f_n(c) &= (c-1)(c^2-1)\cdots(c^n-1) \end{aligned}$$

Proof. By induction on n. Clearly true for $n = 1$. Assume that the formNow

$$\begin{aligned} (x+y)^n &= (x+y)(x+y)^{n-1} \\ &= (x+y)(\sum_{i=0}^{n-1} b_i^{n-1}(c) x^i y^{n-1-i}) \end{aligned}$$

So the coefficient of $x^i y^{n-i}$ is $c^i b_i^{n-1}(c) + b_{i-1}^{n-1}(c)$. Hence

$$\begin{aligned} b_i^n(c) &= c^i b_i^{n-1}(c) + b_{i-1}^{n-1}(c) \\ &= c^i \frac{f_{n-1}(c)}{f_i(c) f_{n-1-i}(c)} + \frac{f_{n-1}(c)}{f_{i-1}(c) f_{n-i}(c)} \\ &= \frac{f_n(c)}{f_i(c) f_{n-i}(c)} \end{aligned}$$

□

Now I will prove that $a_\omega(a,b) = 1$ whenever $a+b=1$. Consider$A_\omega(a,b)$ where $a+b=1$. Then

$$\begin{aligned}(x+y)^n &= x^n + y^n \text{ by Lemma 9 since } b_i^n(\omega) = 0\ \forall i\\ &= a+b = 1\end{aligned}$$

Since $x+y$ satisfies the polynomial $z^n = 1$, that splits completely in F (as F contains primitive n-th root of unity) and no other polynomial of smaller degree over F, we conclude by Lemma 7 that $A_\omega(a,b) \simeq M_n(k)$ i.e.,$a_\omega(a,b) = 1$.

iv. $a_\omega(a,-a) = 1$

Solution:

Consider $A_\omega(a,-a)$ generated by x,y subjected to $x^n = a, y^n = -a, yx = \omega xy$ where ω is a primitive n-th root of unity. So

$$x^{-1}y = \omega y x^{-1}.$$

Now

$$\begin{aligned}yx^{-1} &= yx^{-1}yx^{-1}\cdots yx^{-1}\\ &= (\omega\omega^2\cdots\omega^{n-1})y^n(x^{-1})n\\ &= (-1)^{n+1}(-a)(a^{-1})\\ &= (-1)^n\end{aligned}$$

So the element yx^{-1} satisfies a polynomial of degree n over F that splits completely over F and no other polynomial of smaller degree. Therefore by Lemma 7, $a_\omega(a,-a) = 1$.

v. $a_\omega(a,b)^n = 1$

Solution:

First observe that $a_\omega(a,b)^n = a_\omega(a,b^n)$ by (i). Now the result follows from this and Lemma 7.

vi. Further, $a_\omega = 1$ iff a is a norm from $F(\sqrt[n]{b})$.

Solution:

Let $K := F(\sqrt[n]{b}) \simeq F[y]/(y^n - b) \subset A_\omega(a,b)$. Suppose $a = N_{K/F}(z)$ for some $z \in K$. Consider the map

$$\begin{aligned}\Phi : A_\omega(1,b) &\to A_\omega(a,b)\\ x &\mapsto z^{-1}x\\ y &\mapsto y\end{aligned}$$

This extends to an F-algebra morphism because $(z^{-1}x)^n = \frac{1}{N_{K/F}(z)}x^n = 1.$ and $y(z^{-1}x) = z^{-1}yx = z^{-1}\omega xy = \omega(z^{-1}x)y$. The map Φ obviously has an inverse. So it is an isomorphism. This gives $a_\omega(a,b) = a_\omega(1,b) = 1$.

The proof of the converse follows along the one in Milnor's book on "Algebraic K-theory", Chapter 15. Sippose $A_\omega(a,b) \simeq M_n(F)$. Then, $A_\omega(a,b) \simeq Hom_F(V,V)$ for some n-dimensional vector psace V over F.Thus the genrators x,y of $A_\omega(a,b)$ correspond to linear transformations X and Y of V. The minimal polynomial $y^n - b$ of Y has degree n. Hence we can choose a basis $v_1, v_2, \cdots, v_n$ for V so as to put Y in "companion matrix" normal form. In other words,

$$Y(V_i) = V_{i+1}\ \forall i < n, Y(v_n) = bV_1$$

(So the rational canonical form of Y has one block). Consider the F- linear transformation

$$\begin{aligned} Hom_F(V,V) &\to Hom_F(V,V) \\ z &\mapsto T_Y(Z) = YZY^{-1} \end{aligned}$$

The element Z defined by

$$Z(V_i) = \omega^i V_i$$

is clearly an eigen vector of T_Y with eigen vector ω^{-1}. Since the ω^{-1} eigen space is spanned by the elements $X^{-1}, X^{-1}Y, \cdots, X^{-1}Y^{n-1}$, it follows that we can write

$$Z = X^{-1}f(Y)$$

for some polynomial f. Now

$$Z^n(V_i) = (\omega^i)^n V_i = V_i \; \forall i$$

So $Z^n = I$. This yields,

$$\begin{aligned} X^{-1}f(Y)X^{-1}f(Y)\cdots X^{-1}f(Y) &= f(\omega Y)f(\omega^2 Y)\cdots f(\omega^n Y)X^{-n} = I \\ \Rightarrow \prod_{i=1}^{n} f(\omega^i Y) &= X^n = aI \end{aligned}$$

Now consider the extension field $F(\eta)$ where $\eta^n = b$. Mapping Y to η, proves that

$$\prod_{i=1}^{n} f(\omega^i \eta) = a$$

If $F(\eta)/F$ has degree n, then clearly this product is the norm of $f(\eta)$. If $F(\eta)/F$ has degree d,

$$\begin{aligned} a &= \prod_{i=1}^{d} \sigma^i(f(\omega\eta)f(\omega^2\eta)\cdots f(\omega^{n/d}\eta)) \text{ where } \sigma^i(\eta) = (\omega^{n/d})^i\eta \\ a &= N(f(\omega\eta)f(\omega^2\eta)\cdots f(\omega^{n/d}\eta)). \end{aligned}$$

29. An involution of k-algebra A is a k-module automorphism $\phi : A \to A$ such that $\phi(xy) = \phi(y)\phi(x)$ and $\phi^2(x) = x \; \forall x, y \in A$.

    (a) Show that if there is an involution of A, then $A^{op} \simeq A$.
    Solution:
    The isomorphism is given by

    $$\begin{aligned} A &\to A^{op} \\ a &\mapsto \phi(a)^{op} \\ ab &\mapsto \phi(ab)^{op} = (\phi(b)\phi(a))^{op} = \phi(a)^{op}\phi(b)^{op} \end{aligned}$$

    (b) Find involutions of the k-algebras $M_n(k)$ and $(\frac{a,b}{k})$, thus concluding that $M_n(k) \simeq M_n(k)^{op}$ and thus $(\frac{a,b}{k}) \simeq (\frac{a,b}{k})^{op}$.

Solution:
The involution on $M_n(k)$ is given by

$$\begin{aligned} \phi : M_n(k) &\to M_n(k) \\ A &\mapsto A^T \end{aligned}$$

The involution on $(\frac{a,b}{k})$ is given by

$$\begin{aligned} \phi : (\frac{a,b}{k}) &\to (\frac{a,b}{k}) \\ i &\mapsto -i \\ j &\mapsto -j \\ k &\mapsto -k \end{aligned}$$

(c) Let A be a finite dimensional central simple k-algebra. Prove that if there is an involution ϕ of A, then $[A]^2 = 1$ in $Br(k)$. Deduce that $[A]^2 = 1$ for every quarternion algebra.
Solution:
From (a), if there exists an involution on A, then $A \simeq A^{op}$. But $[A^{op}] = [A]^{-1}$ in $Br(k)$. The rest follows.

30. (a) Let $k \subseteq K$ be a finite separable field extension and let Lbe a splitting field for K relative to k (i.e., any irreducible polynomial in $k[x]$ which has a root in K splits completely in L). For example, L could be an algebraic closure of k, or if K/k is Galois, then L could be K. Let $\sigma_1, \sigma_2 \cdots \sigma_n$ be the distince k-algebra maps form K to L and let $\sigma : K \to L^n$ be the maps with components $\sigma_1, \cdots \sigma_n$. Let $\sigma_L : K_L \to L^n$ be the unique L-algebra map extending σ.

$$\begin{aligned} \sigma_L : K \otimes_k L &\to L^n \\ x \otimes a &\mapsto a\sigma(x) \end{aligned}$$

Prove that σ_L is an isomorphism. Thus the k-algebra K "splits completely" when the scalars are extended to L.
Solution:
Since K/k is separable, by primitve element theorem, there exists $\alpha \in K$ such that $K \simeq k(\alpha)$. Then $K \simeq k[x]/f(x)$, where $f9x)$ is the minimal polynomial of α. Note that if $\alpha = \alpha_1, \alpha_2, \cdots, \alpha_n$ are the distinct roots of $f(x)$ and since L contains all the roots, then the distinct embeddings $\sigma_i isgivenby \sigma_i(\alpha) = \alpha_i \ \forall i = 1, \cdots, n$. In particular, the number n of distinct embeddings of K in L is equal to the degree of $f(x)$ which is $[K : k]$. It is now clear that σ_L is an isomorphism. In fact, it is given by the following composition of isomorphisms

$$\begin{aligned} K \otimes_k L \overset{\cong}{\to} k[x]/f(x) \otimes_k L \overset{\cong}{\to} L[x]/f(x) \overset{\cong}{\to} \oplus_{i=1}^n L[x]/(x - \alpha_i) \overset{\cong}{\to} \oplus_{i=1}^n L \\ t \otimes a \mapsto (\sum_i c_i x^i) \otimes a \mapsto \sum_i a c_i x^i \mapsto (\sum_i a c_i \alpha_1^i, \sum_i a c_i \alpha_2^i, \cdots, \sum_i a c_i \alpha_{n-1}^i) \\ = (a\sigma_1(t), a\sigma_2(t), \cdots, a\sigma_n(t)) \\ = \sigma_L(t \otimes a) \end{aligned}$$

(b) Let K and L be as in (a). Show that if D is a central simple k-algebra with maximal subfield K, then L splits D.
Solution:
This is clear since a maximal subfield of D splits D and $D \otimes_k L \simeq D \otimes_k K \otimes_K L$.

(c) If L spits D and if K is a maximal separable subfield of D, does L split K relative to k i.e., is $L \otimes_k K \simeq L^n$ where $n = [K : k]$.

Solution:

No. Let K/k be an extension of degree $n \geq 2$. Then from Theorem 4.4 from the book, $M_n(k)$ contains K as a maximal subfield. Now take $D = M_n(k)$ which is already split. Now let $L = k$. Then $L \otimes_k K \simeq k \otimes_k K \simeq K \not\simeq L^n$.

31. Another Proof that $Br(K/k) \simeq H^2(Gal(K/k), K^*)$:

Let K/k be a Galos extension with Galois grop G. The fact that $Br(K/k) \simeq H^2(G, K^*)$ boils down to the fact that for factor sets a and b, $[(K, G, a)][(K, G, b)] = [(K, G, ab)]$. The roof (of chase) given in the text exhibits a "magic module" on which both $(K, G, a) \otimes_k (K, G, b)$ and (K, G, ab) act. A more direct approach is to choose a basis for the first two algebras which give cocycles a and b respectively and then try to find a corresponding basis for their tensor product. Their tensor product is not unfortunately, (K, G, ab), but rather is matrices over this ring. Hence we must find an appropriate subring of the matrix ring $M_n((K, G, ab)) \simeq (K, G, ab) \otimes_k M_n(k)$ which is isomorphic to (K, G, ab). This is where Exercise 30 comes in: we now want to list explicitly the idempotents (and their properties) from that exercise. Complete the following outline, which gives the "classical" proof that $Br(K/k) \simeq H^2(G, K^*)$.

(a) Prove that it if A is a central simple algebra over k and if $e \neq 0$ is an idempotent element in A, then $[A] = [eAe]$ in $Br(k)$.

Solution:

Let $A \simeq M_n(D)$. Since e is idempotent, e is diagonalizable with 1's and 0's along the diagonal. So there exists an invertible matrix $P \in A$ such that PeP^{-1} is diagonal with 1's and 0's along the diagonal. After conjugating with a permutation matrix, we assume that

$$PeP^{-1} = \begin{bmatrix} 1 & & & & & & \\ & 1 & & & & & \\ & & \ddots & & & & \\ & & & 1 & & & \\ & & & & 0 & & \\ & & & & & \ddots & \\ & & & & & & 0 \end{bmatrix}$$

with r 1's along the diagonal Now note that as k-algebras, $eAe \simeq PeAeP^{-1}$. The explicit isomorphism is given by sending eae to $PeaeP^{-1}$ $\forall a \in A$ (It is easy to check that this map is infact a k-algebra isomorphism). So we get

$$\begin{aligned} eAe = PeAeP^{-1} &= (PeP^{-1})PAP^{-1}(PeP^{-1}) \\ &= \begin{bmatrix} D & D\cdots & D & 0 & 0\cdots 0 \\ D & D\cdots & D & 0 & 0\cdots 0 \\ \vdots & & \vdots & & \\ D & D\cdots & D & 0 & 0\cdots 0 \\ 0 & 0\cdots & 0 & 0 & 0\cdots 0 \\ \vdots & & \vdots & & \\ 0 & 0\cdots & 0 & 0 & 0\cdots 0 \end{bmatrix} \\ &\simeq M_r(D) \end{aligned}$$

Thus $[A] = [D] = [eAe]$ in $Br(k)$.

(b) Prove that

$$K \otimes_k K \simeq \oplus_{\sigma \in G} e_\sigma (K \otimes_k 1) = \oplus_{\sigma \in G} e_\sigma (1 \otimes_k K)$$

where e_σ are orthogonal idempotents such that $e_\sigma(z \otimes 1) = e_\sigma(1 \otimes \sigma(z))\ \forall z \in K$.
Solution:
Since K/k is separable, $K = k(a)$ for some a by primitive element theorem. Let $p(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_0$ be the minimal polynomial of a over k. Now since K/k is Galois,

$$K \otimes_k K \simeq K\left[x\right]/p\left(x\right) = K\left[x\right]/\left(x - c_1\right)\ldots\left(x - c_n\right) \simeq \bigoplus_{i=1}^{n} K$$

For $\sigma \in G$, let

$$b_{\sigma,m} = a^m \otimes 1 + a^{m-1} \otimes \sigma\left(a\right) + \ldots + 1 \otimes \sigma\left(a\right)^m.$$

Now $\left\{1, \sigma\left(a\right), \ldots, \sigma\left(a\right)^{m-1}\right\}$ is linearly independent over k for each fixed σ, where $0 \le m \le n-1$ since $p(x)$ is the minimal polynomial for $\sigma(a)$.
Claim: $\{b_{\sigma,0}, b_{\sigma,1} \cdots b_{\sigma,n-1}\}$ is independent over k in $K \otimes_k K$.

Proof. Suppose $\alpha_0 b_{\sigma,0} + \alpha_1 b_{\sigma,1} + ... + \alpha_{n-1} b_{\sigma,n-1} = 0$ for some $\alpha_{0,}\alpha_1, \ldots \alpha_{n-1} \in k$. Then,

$$\begin{aligned}&\left(a^{n-1} \otimes 1\right)\left[1 \otimes \alpha_{n-1}\right] + \left(a^{n-2} \otimes 1\right)\left[1 \otimes \left(\alpha_{n-2} + \alpha_{n-1}\sigma\left(\alpha\right)\right)\right] + \ldots \\ &\ldots + \left(a \otimes 1\right)\left(1 \otimes \left[\alpha_1 + \alpha_2\sigma\left(a\right) + \ldots + \alpha_{n-1}\sigma\left(a\right)^{n-2}\right]\right) \\ &+ \left(1 \otimes 1\right)\left(1 \otimes \left[\alpha_0 + \alpha_1\sigma\left(a\right) + \ldots + \alpha_{n-1}\sigma\left(a\right)^{n-1}\right]\right) = 0\end{aligned}$$

But $S = \{a^i \otimes 1 : 1 \le i \le n-1\}$ form a basis over$1 \otimes k$. So S islinearly independent. Hence we get

$$\alpha_0 + \alpha_1\sigma\left(a\right) + \alpha_2\sigma\left(a\right)^2 + \ldots + \alpha_{n-1}\sigma\left(a\right)^{n-1} = 0$$

But $\{\sigma(a) : 1 \le i \le n-1\}$ is linearly independent. This implies $\alpha_0, \alpha_1, \cdots, \alpha_{n-1} = 0$. Hence $\{b_{\sigma,m} : 1 \le m \le n-1\}$ is linearly independent over k in $K \otimes_k K$. □

Now,

$$\left(a \otimes 1 - 1 \otimes \sigma\left(a\right)\right) b_{\sigma,m} = a^{m+1} \otimes 1 - 1 \otimes \sigma\left(a\right)^{m+1}$$

So,

$$\begin{aligned}&\left(a \otimes 1 - 1 \otimes \sigma\left(a\right)\right)\left(b_{\sigma,n-1} + \alpha_{n-1}b_{\sigma,n-2} + \ldots + \alpha_1 b_{\sigma,0}\right) \\ &\qquad = \left(p\left(a\right) \otimes 1 - \alpha_0 \otimes 1\right) - \left(1 \otimes p\left(\sigma\left(a\right)\right) - 1 \otimes \alpha_0\right) = 0\end{aligned}$$

Since $\{b_{\sigma,m} : 1 \le m \le n-1\}$ is linearly independent, $b_{\sigma,n-1} + \alpha_{n-1}b_{\sigma,n-2} + \ldots + \alpha_1 b_{\sigma,0} \neq 0$. Therefore $t_\sigma = a \otimes 1 - 1 \otimes \sigma(a)$ is a non-zero zero-divisor in $K \otimes K$. Consider the following isomorphism

$$\phi : K \otimes_k K \xrightarrow{\simeq} \bigoplus_{i=1}^{n} K$$

Let $e_j = \phi^{-1}(r_j)\ \forall \sigma \in G$, where $r_j = (0, 0, \cdots, 1, \cdots, 0) \in \oplus_{\tau \in G} K$ is the vector with 1 at j-th position and zero everywhere else. Then e_j is a non-trivial minimal idempotent in $K \otimes K$ (An idempotent e is minimal if whenever $e = e_1 + e_2$ for some commuting idempotents e_1 and e_2, then $e = e_1$ or $e = e_2$). Now since t_σ is a zero divisor in $K \otimes K$, there exists a minimal idempotent $e_\sigma \in K \otimes K\ \forall \sigma \in G$ such that

$$\begin{aligned} &e_\sigma t_\sigma = 0 \\ \Rightarrow &e_\sigma(a \otimes 1 - 1 \otimes \sigma(a)) = 0 \\ \Rightarrow &e_\sigma(a \otimes 1) = e_\sigma(1 \otimes \sigma(a)) \end{aligned}$$

Since $\{1, a, a^2, \cdots a^{n-1}\}$ form a basis for K/k, for any $z = \sum_{i=0}^{n-1} c_i a^i \in K$, we have

$$\begin{aligned} e_\sigma (z \otimes 1) &= e_\sigma \left[\left(c_0 + c_1 a + c_2 a^2 + \dots c_{n-1} a^{n-1} \right) \otimes 1 \right] \\ &= \sum_{i=0}^{n-1} c_i e_\sigma (ai \otimes 1) \\ &= \sum c_i e_\sigma (a \otimes 1)^i \\ &= \sum c_i \left[e_\sigma (a \otimes 1) \right]^i \\ &= \sum c_i e_\sigma (1 \otimes \sigma(a))^i \\ &= \sum c_i e_\sigma \left(1 \otimes \sigma(a)^i \right) \\ &= e_\sigma \left[1 \otimes \left(\sum c_i \sigma(a)^i \right) \right] \\ &= e_\sigma (1 \otimes \sigma(z)) \qquad (2) \end{aligned}$$

Now I claim that $e_\sigma \neq e_\tau$ if $\sigma \neq \tau$. Suppose not. Then $e_\sigma = e_\tau$ for some $\sigma \neq \tau$. Then since $e_\sigma(a \otimes 1) = e_\sigma(1 \otimes \sigma(a))$ and $e_\tau(a \otimes 1) = e_\tau(1 \otimes \tau(a))$, we get

$$e_\sigma[1 \otimes (\sigma(a) - \tau(a))] = 0$$

But $s = \sigma(a) - \tau(a) \neq 0$ and hence $1 \otimes s$ is invertible. This implies $e_\sigma = 0$, which is contadiction. Thus we have shown that $e_\sigma \neq e_\tau$ if $\sigma \neq \tau\ \forall \sigma, \tau \in G$.
Let $S = \{e_\sigma : \sigma \in G\}$. Then $|S| = |G| = n$. But $K \otimes K \simeq \oplus_{i=1}^n K$ has exactly n nontrivial minimal idempotents given by the coordinate vectors $(0, 0, \cdots, 1, 0, \cdots 0)$. So we conclude that if $\sigma \neq \tau$, $e_\sigma e_\tau = 0$. Hence S is a set of orthogonal idempotents such that $\sum_{\sigma \in G} e_\sigma = 1$. This yields

$$\begin{aligned} K \otimes K &= (\sum_{\sigma \in G} e_\sigma)(K \otimes K) \\ &= \sum_{\sigma \in G} e_\sigma(K \otimes K) \\ &\simeq \bigoplus_{\sigma \in G} e_\sigma(K \otimes 1) \\ &\simeq \bigoplus_{\sigma \in G} e_\sigma(1 \otimes K) \text{ (by (2))} \end{aligned}$$

(c) Use parts (a) and (b) to prove that for factor sets a and b,

$$(K, G, a) \otimes_k (K, G, b) \simeq (K, G, ab) \otimes_k M_n(k)$$

Solution:

Let $R = (K, G, a) \otimes_k (K, G, b)$. Since $R \supseteq K \otimes K$, part (b) gives $e_\sigma \in R$ as above. Let $e = e_1$. Choose a basis $\{x_\sigma\}_{\sigma \in G}$ and $\{y_\sigma\}_{\sigma \in G}$ for (K, G, a) and (K, G, b) which give cocycles a and b respectively.

Lemma 10. *For every $\tau \in G$, we have*

$$(1 \otimes y_\tau)e(1 \otimes y_\tau^{-1}) = e_\tau$$
$$(x_\tau^{-1} \otimes 1)e(x_\tau \otimes 1) = e_\tau$$

Proof. First note that $(1 \otimes y_\tau)e(1 \otimes y_\tau^{-1})$ is a nontrivial minimal idempotent since e is. Since $K \otimes_k K$ has exactly n nontrivial minimal idempotents given by $\{e_\sigma\}_{\sigma \in G}$, $(1 \otimes y_\tau)e(1 \otimes y_\tau^{-1})$ must be one of them. Now note that e_σ is the unique minimal idempotent such that

$$e_\sigma[(a \otimes 1) - (1 \otimes \sigma(a))] = 0$$

for if $e_\tau[(a \otimes 1) - (1 \otimes \sigma(a))] = 0$, then

$$\begin{aligned} e_\tau\left(1 \otimes \tau\left(a\right)\right) = e_\tau\left(a \otimes 1\right) &= e_\tau\left(1 \otimes \sigma\left(a\right)\right) \\ &\Rightarrow e_\tau\left(1 \otimes \left(\tau - \sigma\right)\left(a\right)\right) = 0 \end{aligned}$$

If $\tau \neq \sigma$, them $\tau(a) - \sigma(s)$ is invertible which yields $e_\tau = 0$, a contradiction. Hence it suffices to show that

$$(1 \otimes y_\tau)e(1 \otimes y_\tau^{-1})(a \otimes 1 - 1 \otimes \tau(a)) = 0$$

Write $e = \sum_{i=1}^n a_i \otimes b_i$. Then

$$\begin{aligned} (1 \otimes y_\tau)e(1 \otimes y_\tau^{-1}) &= \sum a_i \otimes \tau(b_i)(1 \otimes y_\tau)(1 \otimes y_\tau^{-1}) \\ &= \sum a_i \otimes \tau(b_i) \end{aligned}$$

Therefore

$$\begin{aligned} (1 \otimes y_\tau)e(1 \otimes y_\tau^{-1})(a \otimes 1 - 1 \otimes \tau(a) &= [\sum a_i \otimes \tau(b_i)][a \otimes 1 - 1 \otimes \tau(a)] \\ &= \phi_\tau(e(a \otimes 1 - 1 \otimes a)) = \phi_\tau(0) = 0 \end{aligned}$$

where $\phi_\tau : K \otimes_k K \to K \otimes_k K$ is the k- algebra homomorphism given by $\phi_\tau(a \otimes b) = a \otimes \tau(b)$. This proves $(1 \otimes y_\tau)e(1 \otimes y_\tau^{-1}) = e_\tau$. The proof for $(x_\tau^{-1} \otimes 1)e(x_\tau \otimes 1) = e_\tau$ is similar. □

Let $w_\sigma = x_\sigma \otimes y_\sigma$. Now

$$w_\sigma e = \left(x_\sigma \otimes 1\right)\left(1 \otimes y_\sigma\right)e = \left(x_\sigma \otimes 1\right)e_\sigma\left(1 \otimes y_\sigma\right) = ew_\sigma$$

Observe that $u_\sigma = ew_\sigma = w_\sigma e = ew_\sigma e \in eRe$ is invertible with inverse ew_{sigma}^{-1}. We have

$$\begin{aligned} u_\sigma u_\tau = ew_\sigma ew_\tau &= ew_\sigma w_\tau \\ &= e(x_\sigma \otimes y_\sigma)(x_\tau \otimes y_\tau) \\ &= e(x_\sigma x_\tau \otimes y_\sigma y_\tau) \\ &= e(a_{\sigma,\tau} x_{\sigma\tau} \otimes b_{\sigma,\tau} y_{\sigma\tau}) \\ &= e(a_{\sigma,\tau} \otimes b_{\sigma,\tau})(x_{\sigma\tau} \otimes y_{\sigma\tau}) \\ &= e(a_{\sigma,\tau} \otimes 1)e(b_{\sigma,\tau} \otimes 1)(x_{\sigma\tau} \otimes y_{\sigma\tau}) \text{ by definition of } e = e_1 \\ &= e(a_{\sigma,\tau} b_{\sigma,\tau} \otimes 1)w_{\sigma\tau} \\ &= e(a_{\sigma,\tau} b_{\sigma,\tau} \otimes 1)ew_{\sigma\tau} \end{aligned}$$

Therefore,

$$u_\sigma u_\tau = e(a_{\sigma,\tau} b_{\sigma,\tau} \otimes 1) u_{\sigma\tau} \tag{3}$$

Now for $x \in K$,

$$\begin{aligned} u_\sigma e(x \otimes 1) u_\sigma^{-1} &= e(x_\sigma \otimes y_\sigma) e(x \otimes 1) e(x_\sigma^{-1} \otimes y_\sigma^{-1}) \\ &= e(x_\sigma x \otimes y_\sigma) e(x_\sigma^{-1} \otimes y_\sigma^{-1}) \\ &= e(\sigma(x) x_\sigma \otimes y_\sigma) e(x_\sigma^{-1} \otimes y_\sigma^{-1}) \end{aligned}$$

Thus,

$$u_\sigma e(x \otimes 1) u_\sigma^{-1} = e(\sigma(x) \otimes 1) \tag{4}$$

Lemma 11. *$K \simeq e(K \otimes 1)$ as G-modules where the G-action on $e(K \otimes 1)$ is given by $\sigma \cdot e(c \otimes 1) = e(\sigma(c) \otimes 1)$.*

Proof. Define

$$\begin{aligned} \phi : K &\to e(K \otimes 1) \\ c &\mapsto e(c \otimes 1) \end{aligned}$$

It is easy to check ϕ is an isomorphism of k-algebras as well as of G- modules. □

Lemma 12. *$\{u_\sigma\}_{\sigma \in G}$ is linearly independent over $e(K \otimes 1)$.*

Proof. Suppose $\sum_{\sigma \in G} e(a_\sigma \otimes 1) e(x_\sigma \otimes y_\sigma) = 0$ in $R = (K, G, a) \otimes (K, G, b)$. Then

$$\sum_{\sigma \in G} e(a_\sigma \otimes 1)(x_\sigma \otimes 1)(1 \otimes y_\sigma) = 0$$

But $\{1 \otimes y_\sigma\}$ form a basis for R as $(K, G, a) \otimes 1$-module.

$$\begin{aligned} \Rightarrow e(a_\sigma \otimes 1)(x_\sigma \otimes 1) &= 0 \ \forall \sigma \in G \\ e(a_\sigma \otimes 1) &= 0 \end{aligned}$$

since $x_\sigma \otimes 1$ is invertible. □

From Eqn (3), (4) and Lemma 12, we conclude that

$$eRe \supseteq (e(K \otimes 1), G, e(ab \otimes 1)) \tag{5}$$

with basis $\{u_\sigma\}_{\sigma \in G}$.

Lemma 13. *$eRe \subseteq \sum_{\sigma \in G} e(K \otimes 1) u_\sigma$.*

Proof. Since $\{x_\sigma\}$ and $\{y_\sigma\}$ span (K, G, a) and (K, G, b) over K resectively, $\{x_\sigma \otimes y_\tau\}$ span R over $K \otimes K$. So any element $r \in R$ can be written as

$$r = \sum_{\sigma, \tau \in G} (a_\sigma \otimes b_\tau)(x_\sigma \otimes y_\tau)$$

Now

$$\begin{aligned} ere &= \sum_{\sigma,\tau\in G} e(a_\sigma \otimes b_\tau)(x_\sigma \otimes 1)(1 \otimes y_\tau)e \\ &= \sum_{\sigma,\tau\in G} (a_\sigma \otimes b_\tau)e(x_\sigma \otimes 1)e_\tau(1 \otimes y_\tau) \\ &= \sum_{\sigma,\tau\in G} (a_\sigma \otimes b_\tau)(x_\sigma \otimes 1)e_\sigma e_\tau(1 \otimes y_\tau) \end{aligned}$$

□

But $e_\sigma e_\tau = 0$ for $\sigma \neq \tau$ by part (b). So

$$\begin{aligned} ere &= \sum_{\sigma\in G} e(a_\sigma \otimes b_\sigma)(x_\sigma \otimes y_\sigma) \\ &= \sum (a_\sigma b_\sigma \otimes 1)u_\sigma \end{aligned}$$

So eRe is generated by $\{u_\sigma\}$ over $e(K \otimes 1)$.

$$\Rightarrow eRe \subseteq (e(K \otimes 1), G, e(ab \otimes 1)) \subseteq eRe$$

where the last containment comes from (5). Therefore

$$eRe = (e(K \otimes 1), G, e(ab \otimes 1)) \simeq (K, G, ab)$$

By part (a), we finally conclude

$$[(K, G, a) \otimes (K, G, b)] = [R] = [eRe] = [(K, G, ab)]$$

32. Norms and Traces:
Let R be a finite dimensional algebra over a field k. If $x \in R$, then left multiplication by x is a k-endomorphism of R. The norm of this k- endomorphism, i.e., the determinant of the associated linear transformation, is called the **norm** of x, denoted by $N_{R/k}(x)$ or $N(x)$ if the underlying algebra is understood.
Let R be a finite dimensional algebra over a field k and let $x \in R$. Show that the following properties hold.

(a) $N(x) = 0$ iff x is invertible.
Solution:
Define

$$\begin{aligned} \phi : R &\to End_k(R) \\ x &\mapsto \phi_x : r \mapsto xr \end{aligned}$$

where for an element $x \in R$, ϕ_x denotes left multiplication by x. Clearly ϕ is a homomorphism of k-algebras. Note that $N(x) = det(\phi_x)$ and hence $N(x_1x_2) = det(\phi_{x_1x_2}) = det(\phi_{x_1}\phi_{x_2}) = N(x_1)N(x_2)$. So the norm map

$$N : R \to k$$

is multiplicative. Therefore if x is invertible, we have $1 = N(xx^{-1}) = N(x)N(x^{-1})$. This implies $N(x) \neq 0$.
Conversely suppose $N(x) \neq 0$. Then x is not a zero divisor in R as $N()$ is multiplicative. Now the result follows from the following lemma.

Lemma 14. *In an Artinian ring R, an element $x \in R$ is invertible if it is not a zero divisor.*

Proof. Let $x \in R$ be an element that is not a zero divisor. Consider the descending chain of ideals $(x) \supseteq (x^2) \supseteq (x^3) \supseteq \cdots$. Since R is Artinian , there exists an integer n such that $(x^n) = (x^{n+1})$. So $x^n = yx^{n+1}$ for some $y \in R$. This implies $x^n(yx - 1) = 0$. But x is not a zero divisor, so $yx = 1$ and thus x is invertible. □

(b) $N : R^* \to k^*$ is a homomorphism.
Solution:
With notations as in (a), this follows from the fact that ϕ is a homomorphism and determinant is multiplicative.

(c) $N(a) = a^n$ if $a \in k$ where $n = [R : k]$.
Solution:
This is because for any basis of R, the matrix ϕ_a is diagonal with a along the diagonal.

(d) $T : R \to k$ is k-linear where T is the trace map i.e., $T(x) = Tr(\phi_x)$.
Solution:
Let $a, b \in k$ and $x, y \in R$.Then it is easy to see that $\phi_{ax+by} = \phi_a\phi_x + \phi_b\phi_y$. Since ϕ_a and ϕ_b are diagonal matrices with a and b along the diagonal respectively, we have $T(ax + by) = Tr(\phi_{ax+by}) = Tr(\phi_a\phi_x + \phi_b\phi_y) = aTr(\phi_x) + bTr(\phi_y) = aT(x) + bT(y)$.

(e) $T(xy) = T(yx)$.
Solution:
This follows from the properties of trace of product of matrices.

(f) $T(a) = na$ for $a \in k$.
Solution:
This follows from the fact that ϕ_a is a diagonal matrix with a along the diagonal.

33. Prove the following:

(a) Norm and trace are invariant under extension of scalars. That is if $S = R_K$ for a field K containing k, then $\forall x \in R$

$$N_{S/K}(x) = N_{R/k}(x)$$
$$T_{S/K}(x) = T_{R/k}(x)$$

This is because for $x \in R$, left multiplication by $(x \otimes 1)$ is the endomorphism given by $\phi_x \otimes 1 \in End_K(S)$ where ϕ_x is defined as in the previous problem (which is multiplication by x in R). Therefore $N_{S/K}(x) := N_{S/K}(x \otimes 1) = det(\phi_x \otimes 1) = det(\phi_x) = N_{R/k}(x)$. Similar argument shows $T_{S/K}(x) = T_{R/k}(x)$.

(b) Norm and trace are compatible with direct products i.e., if $R = R_1 \times R_2$, then

$$N_{R/k}(x_1, x_2) = N_{R_1/k}(x_1) \cdot N_{R_2/k}(x_2) T_{R/k}(x_1, x_2) = T_{R_1/k}(x_1) + T_{R_2/k}(x_2)$$

Solution:
This is because the linear transformation ϕ_x in R induced by left multiplication by $x = (x_1, x_2)$ is given by the direct sum $\phi_{x_1} \oplus \phi_{x_2}$.

(c) If $x \in J(R)$, then $N(1 + x) = 1$ and $T(x) = 0$ where $J(R)$ is the Jacobson radical of R
Solution:
Since $x \in J(R)$, x is nilpotent. So $T(x) = 0$. Now choose a k-basis of R such that the matrix $[\phi_x]$ with respect to this basis is in rational canonical form. Since the characteristic polynomial of ϕ_x is t^n where $n = [R : k]$, $[\phi_x]$ has zeros along diagonal entries.

$$N(1 + x) = det(1 + [\phi_x]) = det([\phi_x] - \lambda I)|_{\lambda=-1} = (-1)^n t^n|_{\lambda=-1} = 1$$

(d) In the notation of Exercise 30,

$$N_{K/k}(x) = \prod_i \sigma_i(x)$$

Let $p(z)$ be the minimal polynomial of $x \in K$ of degree m. Let $F = k(x)$, so that $[F : k] = m$. Let $[K : F] = n$ so that $[K; k] = mn$. Since K is separable, $K = k(\alpha)$ and the number of distince embeddings of $K \hookrightarrow L$ in its splitting field is equal to the degree of the minimal polynomial of α over k which is equal to mn. Let $q(z)$ be the minimal polynomial of α over F. Then $deg\ q(z) = [K : F] = n$. Note that $\{1, x, \cdots x^{m-1}\}$ forms a basis for F over k and $\{1, x, \cdots, x^{m-1}, \alpha, \alpha x, \cdots, \alpha x^{m-1}, \cdots, \alpha^{n-1}, \alpha^{n-1}x, \cdots, \alpha^{n-1}x^{m-1}\}$ form a basis for K/k. With respect to this basis, multiplication by x is an $n \times n$ block diagonal matrix of the form

$$[\phi_x] = \begin{bmatrix} C & 0 & 0 & \cdots & 0 \\ 0 & C & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 0 & 0 & 0 & \cdots & C \end{bmatrix}$$

where C is the $m \times m$ companion matrix for $p(z)$. Now $N(x) = det(\phi_x) = det(C)^n$. Since the characteristic polynomial of the companion matrix of a polynomial is the polynomial itself, we see that the characteristic polynomial of C is $p(z)$ and hence its determinant is equal to the constant term p_0 of $p(z)$ which is nothing but the product of its roots i.e., $p_0 = \prod_{j=1}^m \gamma_j(x)$ where $\{\gamma_j(x)\}_{j=1}^m$ are the (distinct) roots of $p(x)$. Here γ_j give distinct embeddings of F into L and hence are elements of G/H where H is the subgroup of G that fixes F. Now

$$\begin{aligned} N(x) &= det(C)^n \\ &= \prod_{j=1}^m \gamma_j(x)^n \\ &= \prod_{j=1}^m \prod_{\theta \in H} \gamma_j\theta(x) \\ &= \prod_{i=1}^{mn} \sigma_l(x) \end{aligned}$$

Similarly

$$\begin{aligned} T_{K/k}(x) = n \cdot T_{F/k} &= n(\sum_{j=1}^m \gamma_j(x)) \\ &= \sum_{j=1}^m \sum_{\theta \in H} \gamma_j\theta(x) \\ &= \sum_{i=1}^n \sigma_i(x) \end{aligned}$$

(e) If $R = M_n(k)$, then

$$\begin{aligned} N_{R/k}(x) &= det(x)^n \\ T_{R/k}(x) &= n \cdot Tr(x) \end{aligned}$$

Solution:
Let e_{ij} denote the matrix with 1 at the (i,j)-th entry and 0 everywhere else. Then the set $\{e_{ij} : 1 \leq i,j \leq n\}$ forms a basis for $M_n(k)$. It is now easy to see that with respect to some ordering of the basis, the linear operator associated to left multiplication by a matrix x is just $n^2 \times n^2$ the block diagonal matrix with x along the diagonal. Hence $N(x) = det(x)^n$ and $T(x) = n \cdot Tr(x)$.

34. A bilinear form $B(x,y)$ on a finite dimensional vector space V over a field $k$is a function $B : V \times V \to k$ which is linear as a function of one variable when the other is kept fixed. B is said to be non-degenerateif the following equivalent criteria hold:

   (a) If $x \in V$ satisfies , $B(x,y) = 0 \forall y \in V$, then $x = 0$.

   (b) The map $f : V \to V^* = Hom_k(V,k)$ defined by $f(x)(y) = B(x,y)$ is an isomorphism.

   (c) For any basis $\{e_1, \cdots e_n\}$ of V, the matrix $[B(e_i,e_j)]$ is invertible.

   (d) For some basis $\{e_1, \cdots e_n\}$ of V, the matrix $[B(e_i,e_j)]$ is invertible.

Show that the four conditions are equivalent. Recall that a finite dimensional algebra R over k is called **separable** over k if its center is a product of separable field extensions of k. Prove that if $char(k) = 0$ or if R is commutative, then R is separable iff the bilinear form $B(x,y) = T_{R/k}(xy)$ is non-degenerate.

Solution: First I will show that the conditions are equivalent.

(a) ⇒ (b): By (a) for a given x, $B(x,y) = 0 \ \forall y$ implies $x = 0$. This means that the map

$$\begin{aligned} f : V &\to V^* = Hom_k(V,k) \\ x &\mapsto f(x)(y) = B(x,y) \end{aligned}$$

is injective. Since $dimV = dimV^*$, f is surjective and hence is an isomorphism.

(b) ⇒ (c): Suppose the matrix $M = [(B(e_i,e_j)]$ is not invertible for some basis $\{e_i\}$. of V. Then the rows of M are linearly dependent over k. So there exists $c_1, c_2, \cdots, c_n \in k$, not all zero, such that

$$\begin{aligned} &\sum_j c_j B(e_j,e_i) = 0 \ \forall i \\ \Rightarrow\ & B(\sum_j c_j e_j, e_i) = 0 \ \forall i \\ \Rightarrow\ & B(\sum_j c_j e_j, y) = 0 \ \forall y \\ \Rightarrow\ & f(\sum_j c_j e_j) = 0 \end{aligned}$$

This means that f is not injective and hence is not an isomorphism.

(c) ⇒ (d): Trivial.

(d) ⇒ (a): Suppose $[B(e_i,e_k)]$ is invertible for some basis $\{e_i\}$. Let $x \in V$ be such that $B(x,y) = 0 \ \forall y \in V$.Write $x = \sum_j c_j e_j$. Then

$$\begin{aligned} & B(\sum_j c_j e_j, e_i) = 0 \ \forall i \\ \Rightarrow\ & \sum_j c_j B(e_j,e_i) = 0 \ \forall i \end{aligned}$$

This means that the rows of $[B(e_i, e_j)]$ are linearly dependent unless $c_j = 0\ \forall j$ i.e, $x = 0$.
Now I will prove the second part of the problem.
Remark:To do this we need the additional hypothesis that R is also semisimple because finite dimensional k-algebras whose center is a product of separable field extensions of k need not be semisimple. Here is an example:
Example: Let $R = k[x, y]/(x^n = 0, y^n = a, yx = \zeta xy)$ where $a \in k, \zeta \in k^*$ is a primitive n-th root of unity.Clearly R is finite dimensional k-algebra that is not semisimple as it has nilpotents. Moreover note that the set $\{x^i y^j\}_{0\le i,j\le n-1}$ forms a basis for R. Let us order the basis as $(i_1, j_1) > (i_2, j_2)$ if $(i_1 > i_2)$ or $(i_1 = i_2$ and $j_1 > j_2)$. With respect to this ordered basis, it is now easy to see that $Tr(x^{i+1}y^j) = B(x, x^i y^j) = 0\ \forall i, j$. So $B(x, v) = 0\ \forall v \in R$. This implies that $B(v, w) = Tr(vw)$ is degenerate. Therefore the assumption that R is semisimple is necessary for the statement of the problem to be true.
So we will proceed with the additional assumption that semisimplicity is part of the definition of a separable algebra.
$\Rightarrow$: Suppose R is separable (and hence semisimple by the above Remark). So $R \simeq R_1 \times R_2 \times \cdots R_m$ where R_i is a simple k-algebra. Let K_i be the center of R_i. Then it is easy to check that K_i is a field. The center of R is thus $K_1 \times K_2 \times \cdots \times K_m$. Since R is separable K_i/k is a separabe field extension . Since R is finite dimensional, K_i/k is a finite dimensional separable field extension. By Structure theorem for simple rings, $R_i \simeq M_{n_i}(D)$ where D_i is a division ring with center K_i. Let

$$\begin{aligned} B' : (R \otimes_k \overline{k}) \times (R \otimes_k \overline{k}) &\to \overline{k} \\ (v \otimes a, w \otimes b) &\mapsto abB(v, w) \end{aligned}$$

be obtained by extending B to $\overline{k}$ linearly. Then B' is a bilinear form on the $\overline{k}$-vector space $R \otimes_k \overline{k}$. Note that if $\{e_1, \cdots, e_l\}$ is abasis for R, then $\{e_1 \otimes 1, \cdots e_l \otimes 1\}$ is a $\overline{k}$-basis for $R \otimes_k \overline{k}$. Moreover, for any two vectors $v = \sum e_i \otimes a_i, w = \sum e_i \otimes b_i \in R \otimes_k \overline{k}$, we have

$$\begin{aligned} B'(v, w) &= B'(\sum e_i \otimes a_i, \sum e_i \otimes b_i) \\ &= \sum_{i,j} a_i b_j B'(e_i \otimes 1, e_j \otimes 1) \\ &= \sum_{i,j} a_i b_j B(e_i, e_j) \\ &= \sum_{i,j} a_i b_j T_{R/k}(e_i e_j) \\ &= \sum_{i,j} a_i b_j T_{S/\overline{k}}(e_i \otimes 1)(e_j \otimes 1) \\ &\text{(where } S = R \otimes_k \overline{k} \text{ since trace is invariant under extension of scalars by 33(a))} \\ &= T_{S/\overline{k}}(\sum_i (e_i \otimes a_i) \sum_j (e_j \otimes b_j) \text{ (since trace is linear by 32(a))} \\ &= T_{S/\overline{k}}(vw) \end{aligned} \tag{6}$$

Lemma 15. *B' is non-degenrate iff B is.*

Proof. This is easy to see because the matrix $[(B(e_i, e_j))]$ is invertible iff $[(B'(e_i \otimes 1, e_j \otimes 1))]$ is. □

Now $[(B'(e_i \otimes 1, e_j \otimes 1)]$ is invertible iff $[(B'(f_i, f_j)]$ is invertible for *any* basis$\{f_i\}$ of S over $\overline{k}$. But by (6), $B'(f_i, f_j) = T_{S/\overline{k}}(f_i f_j)$. So to show that $B(e_i, e_j)$ is invertible it suffices to show that the matrix $[(B'(f_i, f_j))] = [(T_{S/\overline{k}}(f_i f_j))]$ is invertible for some basis $\{f_i\}$ of S.

Remark 1. *Suppose $R \simeq R_1 \times \cdots \times R_m$ then the matrix $[(T_{S/\overline{k}}(f_i f_j))]$ decomposes as direct sum of m matrix blocks. So the invertibility of $[(T_{S/\overline{k}}(f_i f_j))]$ is equivalent to the invertibility of each block. Hence , we can assume that R is simple. Moreover,*

$$\begin{aligned} S = R \otimes_k \overline{k} &\simeq (R \otimes_K K) \otimes_k \overline{k} \textit{ where } K \textit{ is the center of R} \\ &\simeq R \otimes_K (K \otimes_k \overline{k}) \\ &\simeq R \otimes_K (\oplus_{i=1}^r \overline{k}) \textit{ since } K/k \textit{ is separable by hypothesis} \\ &\simeq \oplus R \otimes_K \overline{k} \simeq M_n(\overline{k}) \end{aligned}$$

Therefore to show invertibility of $[(B'(f_i, f_j))]$, we can assume without loss of generality that $S = M_n(\overline{k})$.

Consider the matrix $[(T(e_{ij}e_{rs})]$ where e_{ij} is the matrix in $M_n(\overline{k})$ with 1 at the (i, j)-th position and zero everywhere else. Note that $e_{ij}e_{rs}$ is non zero and is equal to e_{is} if $j = r$ and that $T(e_{ij}) = n \cdot Tr(e_{ij})$ by Problem 33(e) which equal n if $i = j$ and 0 else. This means that with respect to some ordering of the basis $\{e_{ij}\}$, the matrix $[(T(e_{ij}e_{rs}))]$ equals nI. If $char\ k = 0$, then this matrix is clearly invertible. If R is commutative, so is S. By Remark 1, we can assume $S = \overline{k}$ whose associated bilinear form given by trace is clearly non-degenrate. Therefore we are done whenever $char\ k = 0$ or if R is commutative.
Warning: This is not true if $char\ k = p \neq 0$, for $T_{R/k} = 0$ where $R = M_p(k)$ by Problem 33(e).
($\Leftarrow$:) For the converse, suppose that R is not separable. Let C be its center. Then C is a finite dimensional commutative k-algebra.

Lemma 16. *$C \otimes_k K$ has nilpotent elements for some field extension K/k.*

Proof. Suppose C has no nilpotents. So the Jacobson radical of C is trivial. By Corollary 2.3 from the book, C is semisimple. But C is also commutative. So $C \simeq K_1 \times \cdots \times K_n$ where K_i/k are fintie field extensions of k. By hypothesis, R is not separable, so K_i/k is inseparable for some i. Let $\alpha \in K_i$ be an inseparable element and let K be the splitting field for the minimal polynomial of α. Then $C \otimes_k K \supseteq K_i \otimes_k K \supseteq k(\alpha) \otimes_k K$ clearly contains nilpotents. □

Since $C \otimes_k K$ is in the center of $R \otimes_k K$, we conclude that the center of $S := R \otimes_k K$ contains nilpotents for some field extension K/k. Let $B' : S \times S \to K$ be the bilinear form obtained by extending K-linearly the bilinear for m$B : R \times R \to k$ over K i.e., $B'(r_1 \otimes a, r_2 \otimes b) = abB(r_1, r_2) = abT_{R/k}(r_1 r_2)$. Recall that by (6), $B'(v, w) = T_{S/k}(vw)$ and by Lemma 15, B' is non-degenerate iff B is. Now pick a nilpotent δ in the center of S. Then $B'(\delta, x) = T_{S/k}(\delta x)$. Since δ is in the center, δx is also nilpotent $\forall x \in S$ yielding $T_{S/k}(\delta x) = B'(\delta, x) = 0\ \forall x \in S$. So B' and hence B is degenerate. We are done.

35. Let K be a Galois extension of k with Galois group G which is cyclic of order n. Prove that $Br(K/k) \simeq k^*/N_{K/k}(K^*)$.
Solution: Given any class $T \in Br(K/k)$, pick a central simple algebra A of degree n in the class (you can do this by Theorem 4.4 in Benson-Farb). Moreover K is a maximal subfiels of A and $[K : k] = n$. Fix $\sigma \in G = Gal(K/k)$ a generator. By Skolem-Noether, there exists $x_\sigma \in A$ such that

$$x_\sigma c x_\sigma^{-1} = \sigma(c)\ \forall c \in K$$

For $j \geq 2$, pick $x_{\sigma^j} = x_\sigma x_\sigma \cdots x_\sigma = x_\sigma^j$. Now $x_1 = x_{\sigma^n} = x_\sigma^n$. Note that $x_1 \in C(K) = K$. Moreover,

$$x_1 x_{\sigma^j} = x_\sigma^n x_\sigma^j = x_\sigma^{n+j} = x_\sigma^j x_\sigma^n = x_{\sigma^j} x_{\sigma^n} = x_{\sigma^j} x_1$$

By Proposition 4.8 in the book, $\{x_\sigma\}$ forms a K-basis for A. So x_1 commutes with all elements in A. So $x_1 \in k^*$. Picking a different x'_σ implies that

$$x'_\sigma = f x_\sigma$$

for some $f \in K^*$, so

$$\begin{aligned} x'_1 = x'^n_\sigma &= f\sigma(f)\cdots\sigma^{n-1}(f)x_\sigma^n \\ &= N(f)x_1 \end{aligned}$$

So x_1 and x'_1 differ by $N(K^*)$.
Now $[A] = [(K, G, \{a\})]$, where the factor set $\{a\}$ is given by $a_{1,1} = a_{\sigma,1}, a_{1,\sigma} = x_1$ (this is because $x_1 x_\sigma = a_{1,\sigma} x_\sigma$) and $a_{\sigma^i,\sigma^j} = 1$ if $i, j \neq 0 \; mod \; n$ (this is because $x_{\sigma^i} x_{\sigma^j} = x_{\sigma^{i+j}}$). Let us call such factor sets 'special' and denote the set with a subscript s, i.e, by $\{a\}_s$. This means that for K/k cyclic Galois, any element in $Br(K/k)$ is represented by $[(K, G, \{a\})]$ where the factor set $\{a\}$ is special. So there is a well-defined map

$$\begin{aligned} \Phi : Br(K/k) &\to k^*/N(K^*) \\ [(K, G, \{a\}_s)] &\mapsto a_{1,1} \end{aligned}$$

Suppose we have $[A], [B] \in Br(K/k)$ such that $[A] = [(K, G, \{a\}_s)], [B] = [(K, G, \{b\}_s)]$. Then note that the factor set $\{ab\}$ is special since $\{a\}$ and $\{b\}$ are special. Since $[(K, G, \{ab\}_s)] = [(K, G, \{a\}_s)] \otimes [(K, G, \{b\}_s)]$, we conclude that Φ is a homomorphism of groups. Now I will show that ϕ is am isomorphism.
<u>Injecctivity:</u> Suppose $[(K, G, \{a\}_s)]$ and $[(K, G, \{ab\}_s)]$ both go to the same element under Φ.Then $a_{1,1} = cb_{1,1}$ for some $c \in N(K^*)$. Let $c = N(\alpha)$, for some $d \in K^*$. Then we have a k-isomorphism

$$[(K, G, \{a\}_s)] \to [(K, G, \{b\}_s)] x_\sigma \qquad\qquad \to \alpha y_\sigma$$

<u>Surjectivity:</u> Let $r \in k^*/N(K^*)$. Then we define A as follows. As a K-vector space,

$$A = \bigoplus_{i=1}^{n-1} K x_{\sigma^i}$$

with algebra operation as follows

$$\begin{aligned} x_{\sigma^i} x_{\sigma^j} &= x_{\sigma^{i+j}} \text{ if } i, j \geq 1 \\ &= r x_{\sigma^{i+j}} \text{ if } \; i = 0 \; \text{ or } \; j = 0 \\ \alpha x_{\sigma^i} \beta x_{\sigma^j} &= \alpha \sigma^i(\beta) x_{\sigma^i} x_{\sigma^j} \end{aligned}$$

Then $[A] = [(K, G, \{a\})]$ where $a_{1,1} = a_{1,\sigma} = a_{\sigma,1} = r$ and $a_{\sigma^i,\sigma^j} = 0$ if $i, j \neq 0$. Clearly A maps to r under Φ. So Φ is surjective and hence is an isomorphism.

36. Use the preceeding problem to give another proof of the Frobenius theorem that the only finite dimensional central division algebras over $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{H}$. Also give another proof of Wedderburn's theorem that all finite division rings are commutative.

Solution:

Proof of Frobenius Theorem:

Any finite dimensional central division algebra over $\mathbb{R}$ is an element of $Br(\mathbb{C}/\mathbb{R}) \simeq \mathbb{C}^*/N_{\mathbb{C}/\mathbb{R}}(C^*) \simeq \mathbb{Z}_2$. This proves the claim.

Proof of Weddernburn's theorem:

Let D be a finite division ring with maximal subfield K. Clearly K is a finite field. Also the center of D is $\mathbb{F}_q$ where q is a prime power. and $K/\mathbb{F}_q$ is a finite extension so that $K = \mathbb{F}_{q^r}$. Since the maximal subfield splits a central simple algebra, $D \in Br(K/\mathbb{F}_q) = Br(\mathbb{F}_{q^r}/\mathbb{F}) = \mathbb{F}_q^*/N_{\mathbb{F}_{q^r}/\mathbb{F}}(\mathbb{F}_{q^r}^*)$ by the previous problem. The result follows from the following claim.

Claim: $\mathbb{F}_q^*/N_{\mathbb{F}_{q^r}/\mathbb{F}}(\mathbb{F}_{q^r}^*) = 1$.

Proof of the Claim: Let $\mathbb{F}_{q^r} = \mathbb{F}_q(a)$ and let $p(t)$ be the minimal polynomial of a. Then the roots of $p(t)$ are $\{a, a^q, \cdots a^{q^{r-1}}\}$. Moreover, the matrix M associated to left multiplication by a is just the companion matrix of $p(t)$. Therefore $N(a) = det(M) = a \cdot a^2 \cdots a^{q^{r-1}} = a^{\frac{q^r-1}{q-1}} \in \mathbb{F}_q^*$. Observe that since a has order $q^r - 1$, $a^{\frac{q^r-1}{q-1}}$ has order $q - 1$and hence $N(a)$ generates $\mathbb{F}_q^*$. This proves the claim.

37. Cohomology and Applications:

Prove Proposition 4.11 from the book i.e., $\delta^2 = 0$.

Solution:

Let $f \in C^n(G, M)$, so $f : G^n \to M$.

$$\delta^2(f)(g_1, g_2, \cdots g_{n+2}) =$$

$$\underbrace{g_1 \cdot \delta f(g_2, \cdots g_{n+2})}_{A} + \underbrace{\sum_{i=1}^{n+1}(-1)^i \delta f(g_1, \cdots, g_i g_{i+1}, \cdots, g_{n+2})}_{B} + \underbrace{(-1)^{n+2}\delta f(g_1, \cdots, g_{n+1})}_{C}$$

Now it is easy to check that

$$A = g_1 g_2 f(g_3, \cdots, g_{n+2}) + \sum_{i=2}^{n+1}(-1)^{i-1} f(g_2, \cdots, g_i g_{i+1}, \cdots g_{n+2}) + (-1)^{n+1} g_i g(g_2, \cdots, g_{n+1})$$

$$B = \sum_{i=1}^{n+1} \underbrace{(-1)^i \delta f(g_1, \cdots, g_i g_{i+1}, \cdots, g_{n+2})}_{B_i}$$

Let us compute each B_i,

$$\begin{aligned} B_1 &= (-1)\delta f(g_1 g_2, g_3 \cdots, g_{n+2}) \\ &= (-1)[g_1 g_2 \cdot f(g_3, \cdots, g_{n+2}) - f(g_1 g_2 g_3, g_4, \cdots, g_{n+2}) + \\ &\sum_{j=3}^{n+1}(-1)^{j-1} f(g_1 g_2, \cdots, g_j g_{j+1}, g_{n+2}) + (-1)^{n+1} f(g_1 g_2, \cdots, g_{n+1})] \end{aligned}$$

For $2 \leq i \leq n$,

$$\begin{aligned}
B_i &= (-1)^i \delta f(g_1, \cdots, g_ig_{i+1}, \cdots, g_{n+2}) \\
&= (-1)^i [g_i f(g_2, \cdots, g_ig_{i+1}, \cdots g_{n+2}) + \sum_{j=1}^{i-2} f(g_1, \cdots, g_jg_{j+1}, \cdots, g_ig_{i+1}, \cdots, g_{n+2}) \\
&+ (-1)^{i-1} f(g_1, g_2, \cdots, g_{i-1}g_ig_{i+1}, \cdots g_{n+2}) + \sum (-1)^i f(g_1, g_2, \cdots, g_ig_{i+1}g_{i+2}, \cdots g_{n+2}) \\
&+ \sum_{j=i+2}^{n+1} (-1)^{j-1} f(g_1, g_2, \cdots, g_ig_{i+1}, \cdots g_jg_{j+1}, \cdots g_{n+2}) + (-1)^{n+1} f(g_1, g_2, \cdots, g_ig_{i+1}, \cdots, g_{n+1})]
\end{aligned}$$

$$\begin{aligned}
B_{n+1} &= (-1)^{n+1} \delta f(g_1, g_2, \cdots, g_{n+1}g_{n+2}) \\
&= (-1)^{n+1} [g_1 f(g_2, \cdots, g_{n+1}g_{n+2}) + \sum_{j=1}^{n-1} f(g_1, \cdots g_jg_{j+1}, \cdots, g_{n+1}g_{n+2}) \\
&+ (-1)^n f(g_1, \cdots g_{n-1}, g_ng_{n+1}g_{n+2}) + (-1)^{n+1} f(g_1, \cdots, g_n)]
\end{aligned}$$

$$\begin{aligned}
C &= (-1)^{n+2} \delta f(g_1, \cdots, g_{n+1}) \\
&= (-1)^{n+2} [g_1 \cdot f(g_2, \cdots, g_{n+1}) + \sum_{j=1}^{n} (-1)^j f(g_1, \cdots, g_jg_{j+1}, \cdots g_{n+1}) + (-1)^{n+1} f(g_1, g_2, \cdots g_n)]
\end{aligned}$$

After painful suffering one can check that $\delta^2 = A + B + C = 0$.

38. Let G be a finite group and let M be a G-module. Show by a direct argument that every element of $H^n(G, M)$ is annihilated by $|G|$ for $n \geq 1$.
Solution:
Let $f \in H^n(G, M) \Rightarrow \delta f = 0$.

$$\begin{aligned}
&\delta f(g_1, \cdots, g_{n+1}) = 0 \; \forall g_1, \cdots, g_{n+1} \\
&\Rightarrow g_1 f(g_2, \cdots g_{n+1}) + \sum_{i=1}^{n} (-1)^i f(g_1, \cdots g_ig_{i+1}, \cdots g_{n+1}) + (-1)^{n+1} f(g_1, \cdots, g_n) = 0 \\
&\Rightarrow (-1)^n f(g_1, \cdots, g_n) = g_1 f(g_2, \cdots g_{n+1}) + \sum_{i=1}^{n} f(g_1, \cdots g_ig_{i+1}, \cdots g_{n+1})
\end{aligned}$$

Summing over all g_{n+1},

$$\begin{aligned}
(-1)^n \sum_{g_{n+1} \in G} f(g_1, \cdots g_n) &= \sum_{g_{n+1} \in G} g_1 \cdot f(g_2, \cdots, g_{n+1}) + \sum_{g_{n+1} \in G} \sum_{i=1}^{n} (-1)^i f(g_1, \cdots, g_ig_{i+1}, \cdots g_{n+1}) \\
(-1)^n |G| f(g_1, \cdots, g_n) &= \sum_{g_{n+1} \in G} g_1 \cdot f(g_2, \cdots, g_{n+1}) + \sum_{g_{n+1} \in G} \sum_{i=1}^{n-1} (-1)^i f(g_1, \cdots, g_ig_{i+1}, \cdots, g_{n+1}) \\
&+ \sum_{g_{n+1} \in G} (-1)^n f(g_1, g_2, \cdots, g_ng_n + 1)
\end{aligned}$$

Let $h(g_1, g_2, \cdots g_{n-1}) = \sum_{g_n \in G} f(g_1, \cdots g_{n-1}, g_n)$. Note that

$$\sum_{g_{n+1} \in G} f(g_1, g_2, \cdots g_n g_{n+1}) = \sum_{g_n \in G} f(g_1, g_2, \cdots, g_n) = h(g_1, g_2, \cdots g_{n-1})$$

So we get,

$$\begin{aligned}(-1)^n |G| f(g_1, \cdots, g_n) &= g_1 h(g_2, \cdots, g_n) + \sum_{i=1}^{n-1} (-1)^i h(g_1, \cdots g_i g_{i+1}, \cdots, g_n) \\ &\quad + (-1)^n h(g_1, g_2, \cdots, g_{n-1}) \\ &= \delta h(g_1, g_2, \cdots g_n) \Rightarrow |G| f = 0 \text{ in } H^n(G, M)\end{aligned}$$

39. Try to understand the following argument, checking statements and filling in details as needed. By Theorem 4.13, $H^2(G, K^*) \simeq Br(K/k)$ and hence classifies central simple algebras. By an entirely similar argument, one can show that for a G-module M, $H^2(G, M)$ classifies extensions

$$1 \to M \to E \to G \to 1$$

inducing the given G-action on M (See K.Brown, Cohomology of Groups). If M is finite and $|M|$ is prime to $|G|$, then note that

(a) Multiplication by $|G|$ is an automorphism of M and so induces an automorphism of $H^2(G, M)$.

Solution:

Since $gcd(|G|, |M|) = 1$, there exists $n, r \in \mathbb{Z}$ such that $n|G| + r|M| = 1$. For an integer k, let ϕ_k denote multiplication by k in M. Then it is easy to see that ϕ_n is the inverse of $\phi_{|G|}$. In particular, $\phi_{|G|}$ is an automorphism of M.In fact, it is a G-invariant automorphism of M. Now a G-invariant automorphism ϕ of M, induces an automorphism of $H^(G, M)$ via

$$\begin{aligned}\Phi : H^2(G, M) &\to H^2(G, M) \\ f &\to \phi \circ f\end{aligned}$$

The above map is well defined because $\delta\phi \circ f = \phi\delta f$ and hence Φ takes boundaries to boundaries and co-cycles to co-cycles. Its inverse is given by $f \mapsto \phi^{-1} \circ f$.

(b) Multiplication by $|G|$ kills $H^2(G, M)$ by the previous problem. So the only possibility is aht $H^2(G, M) = 0$, that is there is only one extension $1 \to M \to E \to G \to 1$, the split one. Put another way, if E is a group and M is an abelian normal subgroup such that $G = E/M$ has order prime to $|M|$, then E is a semi-direct product, $E = M \rtimes G$. Finally, by suitable cleverness one can reduce the arbitrary case (M non-abelian) to the case of M abelian, thus giving the following:

Theorem 17 (Schur-Zehhenhaus)**.** *If G is a finite group, $H \lhd G$ a normal subgroup with $|H|$ prime to $[G : H]$, then G is a semi-direct product $G = H \rtimes (G/H)$. In other words, any normal Hall subgroup H of a finite group G has a complement in G.*

Proof. The case when H is abelian is clear as proved above using cohomology. Now let us prove Schur-Zehhenhaus for arbitrary H. The following proof is developed based on the outline given in Wikipedia.

The proof is by induction on $|G|$.

i. Base case: If $|G|$ is prime, then clearly the claim is true as $H = 1, G/H = G$ or $H = G, G/H = 1$. In both cases, $G \simeq H \times G/H$. So assume that the claim is true for any smaller group.

ii. Case when H is abelian: If H is abelian, the claim is true as argued above using cohomology.

iii. Case when H is solvable: Let H be a non-trivial solvable subgroup. This means that the derived series eventually goes to 1 i.e.,

$$H \rhd H^{(1)} = [H, H] \rhd H^{(2)} = [H^{(1)}, H^{(1)}] \rhd \cdots \rhd H^{(n)} = 1$$

Note tha in the above series $H^{(n-1)}$ is a non-trivial abelian subgroup of H that is characteristic in H. Since H is normal in G, $H^{(n-1)}$ is stable under conjugation by elements in G and thus is a non-trivial abelian normal subgroup in G. For simplicity, call $A := H^{(n-1)}$. Now H/A is a normal Hall subgroup of G/A. So by induction hypothesis, there is a subgroup F/A in G/A that is complement of H/A. Thus we get subgroups F, H in G such that $F \cap H = A$ and $FH = G$. Now F contains A as a normal abelian subgroup. I claim that A is a Hall subgroup of F i.e., $|F/A|$ and $|A|$ are coprime. Because otherwise let p be a prime dividing both. Then F contains an element of order p that is not in A. Since $F \cap H = A$, this means that G contains an element of order p not in H. Now since $|A|$ divides $|H|$, p divides $|H|$.This contradicts the assumption that H is a normal subgroup of G. So A is an abelian normal Hall subgroup of F and F contains a complement of A. Call it E. Now $G = FH = EAH = EH$. Moreover since $F \cap H = A$ and $E \cap A = 1$, we get $E \cap H = 1$. So E si complement to H in G and we are done.

iv. If the normalizer of every p-Sylow subgroup P of H equals G, then P is normal in H and by Sylow theory, H is a direct product of p-Sylow subgroups and hence is nilpotent. In particular, H is solvable and we are done by previous step.

v. Suppose the normalizer $N = N_G(P)$ of some p-Sylow subgroup P of H is smaller than G.
Claim: G=NH
Proof of the Claim: Pick $g \in G$. Then gPg^{-1} is a Sylow p-subgroup and hence P and gPg^{-1} are conjugate by an element of H. So there exists $h \in H$ such that $gPg^{-1} = hPh^{-1}$. So $g \in hN \Rightarrow G = HN$. But $H \lhd G \Rightarrow G = NH$.
Since N is smaller than G and $N \cap H$ is a normal Hall subgroup of N, by induction, $N \cap H$ has a complement E in N so that $N = E(N \cap H)$ and $(N \cap H) \cap E = 1$. But $G = NH = E(N \cap H)H = EH$. Moreover, since $E \subseteq N$, $E \cap H = E \cap (N \cap H) = 1$, so that E is complement to H and we are done.

□

40. Prove the following corollary to the above discussion.

Corollary 1. *Let A be a finite dimensional central simple algebra over k with Galois splitting field L and let $n = [L : k]$. Then*

$$\underbrace{A \otimes_k A \otimes_k \cdots \otimes_k A}_{n} = M_m(k)$$

for some m.

Proof. Since $Br(L/k) \simeq H^2(G, L^*)$ where $G = Gal(L/k)$ and $|G|$ annihilates $H^2(G, L^*)$ by the previous discussion, we have for every $[A] \in Br(L/k)$, $|G|[A] = n[A] = [A^{\otimes n}] = [k]$. □

41. Prove Hilbert's so called 'Theorem 90': If K/k is a Galois extension and $G = Gal(K/k)$, then $H^0(G, K^*) = k^*$ and $H^1(G, K^*) = 1$.

Proof of Hilbert Theoren 90:

Let $f \in H^0(G, K^*)$ i.e., $f \in K^*$ such that $\delta f(g) = g \cdot f = f \ \forall g \in G$. Then f is fixed by G. So $f \in k^*$. This proves the first part.Now let us prove the second part.

Case 1: G is finite i.e., K/k is a finite Galois extension. Now let $f \in H^1(G, K^*)$ i.e., $f : G \to K^*$ that satisfies $(\delta f)(\tau\sigma) = 1 \ \forall \sigma, \tau \in G$.

Claim1: There exists $c \in K^*$ such that

$$\sum_{\sigma \in G} f(\sigma)\sigma(c) \neq 0$$

Proof of Calim1: Since K/k is finite Galois, by primitive element theorem, we have $K = k(a)$ for some a. Let $G = \{1 = \sigma_1, \sigma_2, \cdots, \sigma_n\}$. Consider the matrix

$$M = \begin{bmatrix} 1 & 1 & \cdots & 1 \\ a & \sigma_2(a) & \cdots & \sigma_n(a) \\ a^2 & \sigma_2(a)^2 & \cdots & \sigma_n(a)^2 \\ \vdots & \vdots & \cdots & \vdots \\ a & \sigma_2(a)^{n-1} & \cdots & \sigma_n(a)^{n-1} \end{bmatrix}$$

This is full rank Vandermonde matrix. Hence it has trivial null space. Therefore,

$$M \begin{bmatrix} f(\sigma_1) \\ f(\sigma_2) \\ \vdots \\ f(\sigma_n) \end{bmatrix} \neq 0$$

$$\Rightarrow \sum_{\sigma \in G} f(\sigma)\sigma(a^r) \neq 0$$

for some r. Take $c = a^r$.

Claim2: With c as above, let $b = \sum_{\sigma \in G} f(\sigma)\sigma(c) \neq 0$. Then $\tau(b) = f(\tau)^{-1}b \ \forall \tau \in G$.

Proof of Calim2:

$$\begin{aligned} f(\tau)^{-1}b &= f(\tau)^{-1} \sum_{\sigma \in G} f(\sigma)\sigma(a) \\ &= f(\tau^{-1}) \sum_{\sigma \in G} f(\tau\sigma)\tau\sigma(a) \\ &= \sum_{\sigma \in G} f(\tau)^{-1} f(\tau\sigma)\tau\sigma(a) \end{aligned}$$

But since $\delta f(\tau, \sigma) = 1$ we have $f(\tau)^{-1} f(\tau\sigma) = \tau f(\sigma)$. So we get,

$$\begin{aligned} f(\tau)^{-1}b &= \sum_{\sigma \in G} \tau(f(\sigma))\tau\sigma(a) \\ &= \tau(\sum_{\sigma \in G} f(\sigma)\sigma(a)) \\ &= \tau(b) \end{aligned}$$

Therefore

$$\begin{aligned} f(\tau) &= \tau(b)^{-1}b \\ &= \tau(b^{-1})(b^{-1})^{-1} \\ &= (\delta b^{-1})(\tau)\ \forall \tau \in G \end{aligned}$$

So $f = 0$ in $H^1(G, K^*)$.
Case 2: G is infinite.
In this case

$$\begin{aligned} G &= \varprojlim_{E/k finite\ Galois,\ E \subseteq K} Gal(E/k) \\ \Rightarrow H^1(G, K^*) &= \varprojlim_{E/k finite\ Galois,\ E \subseteq K} H^1(Gal(E/k), E^*) = 0 \end{aligned}$$

42. (a) Let G be a group and H be a subgroup. Let M be a G-module. Show that by restricting a function from $G \times G \times \cdots \times G \to M$ to be a function to a function $H \times H \times \cdots \times H \to M$, we obtain a homomorphism of co-chain groups

$$Res_H^G : C^n(G, M) \to C^n(H, M)$$

"Res" stands for restriction. The map is called this for obvious reasons. Show that Res_H^G maps $Z^n(G, M)$ to $Z^n(H, M)$ and $B^n(G, M)$ to $B^n(H, M)$ and hence induces a homomorphism

$$Res_H^G : H^n(G, M) \to H^n(H, M)$$

Solution:
It is clear that restriction induces a homomorphism on co-chain groups. Now let $f \in Z^n(G, M)$ so that $\delta f = 0$. Then

$$\delta f|_{H \times H \times \cdots \times H} = (\delta f)|_{H \times H \times \cdots \times H} = 0$$

So Res_H^G maps $Z^n(G, M)$ to $Z^n(H, M)$. Similarly if $f = \delta g$, then

$$f|_{H \times H \times \cdots \times H} = (\delta g)|_{H \times H \times \cdots \times H} = \delta g|_{H \times H \times \cdots \times H}$$

So Res_H^G maps $B^n(G, M)$ to $B^n(H, M)$ and hence induces a homomorphism between cohomologies.

(b) Let $k \subseteq F \subseteq K$ be fields. Show that extension of scalars induces a map

$$\begin{aligned} Br(K/k) &\to Br(K/F) \\ [A] &\mapsto [F \otimes_k A] \end{aligned}$$

Solution:
This is because if $A \sim B$, then $A \otimes_k F \sim B \otimes_k F$ and $A \otimes_k B \otimes_k K = (A \otimes_k K) \otimes_K (B \otimes_k K)$

(c) Let K/k be a Galois extension with Galois group G. Let H be a subgroup of G and F be the corresponding fixed field. Let f be a factor set satisfying the cocycle condition. Let $A = (K, G, f)$ be the central simple algebra corresponding to f. Let $\{x_\sigma : \sigma \in G\}$ be the ususal K-basis of A, that is, $x_\sigma u = \sigma(u)x_\sigma$ and $x_\sigma x_\tau = f_{\sigma,\tau} x_{\sigma\tau}$. Prove that $\{x_\sigma : \sigma \in H\}$ is a K- basis for $A' = (K, H, f|_H)$.
Solution: This is clear.

(d) Let $k \subseteq F \subseteq K$ and H a subgroup of G as in part (c). Show that the following diagram commutes.

$$\begin{tikzcd}
H^2(G, K^*) \arrow[r, "\simeq"] \arrow[d, "Res_H^G"] & Br(K/k) \arrow[d, "Res_k^F"] \\
H^2(H, K^*) \arrow[r, "\simeq"] & Br(K/F)
\end{tikzcd}$$

Solution:
Recall from the above notation that $A' = (K, H, f|_H)$. To show that the above diagram commutes one needs to show that $[A'] = [A \otimes_k F]$. Since A' is a subalgebra of A, we have a right module action of A' on A via multiplication on the right. Now consider the natural map

$$\begin{aligned} A \otimes_k F &\to End_{A'}(A) := E \\ \alpha x_\sigma \otimes c &\mapsto \phi_{\alpha x_\sigma \otimes c} \end{aligned}$$

where $\phi_{\alpha x_\sigma \otimes c}(e x_\tau) = \alpha x_\sigma (e x_\tau) c$. This map is A'-invariant because H and hence all $\{x_\tau : \tau \in H\}$ fix F.This map is clearly a homomorphism of F-algebras and is easy to see that it is injective. Moreover by Proposition 6 as proved before,

$$\begin{aligned} dim_F(E) = (deg\ E)^2 = (rdim_{A'} A)^2 &= \left(\frac{deg\ A \cdot [K:F]}{deg\ A'}\right)^2 \\ &= [K:k][K:F]^2[K:f]^2 \\ &= [K:k] \\ &= dim_F A \otimes_k F \end{aligned}$$

So the map is surjective and hence is an isomorphism. From Proposition 6 we also conclude that $[A'] = [E] = [A \otimes_k F]$.

43. (a) Let G be a group, H a normal subgroup and M a G-module. Show that $M^H = \{m \in M : \sigma(m) = m\ \forall \sigma \in H\}$ is a G/H-module. Show that there is a homomorphism

$$Inf_H^G : H^2(G/H, M^H) \to H^2(G, M)$$

which sends a cocycle f to the function defined by

$$(\sigma, \tau) \mapsto f(\sigma H, \tau H)$$

"Inf" stands for inflationbecause it gives a map from the cohomology of a quotient group G/H into the cohomology ofthe (inflated) full group G.
Solution:
It is easy to see that the map

$$\begin{aligned} &Inf_H^G : C^2(G/H, M^H) \to C^2(G, M) \\ &\qquad\qquad f \mapsto f \circ \pi \text{ (where } \pi : G \times G \to G/H \times G/H \text{ is the projection)} \end{aligned}$$

is a homomorphism and takes cocycles to cocyles and coboundaries to coboundaries, thus inducing a map between the cohomologies.

(b) Let $k \subseteq F \subseteq K$ be fields such that $[K : k] < \infty$. Let B be a central simple algebra over k with maximal commutative subring F. Considering $K \otimes_F B$ as right B-module, show that $C := End_B(K \otimes_F B)$ is a central simple algebra over k with maximal commutative subring K. Further show that $[C] = [B]$ in $Br(k)$.
<u>Solution:</u>
The fact that $[C] = [B]$ is clear by Proposition 6. Now note that $B \simeq (F, G/H, f)$ for some factor set f. Let A be the central simple algebra over k given by inflating f i.e, $A = (K, G, f')$ where $f' = Inf_H^G(f)$. So A is generated as a K-basis by $\{x_\sigma : \sigma \in G\}$ with multiplication given by

$$\alpha x_\sigma \beta x_\tau = \alpha\sigma(\beta) f_{\sigma H, \tau H} x_{\sigma\tau}$$

Consider the map

$$\begin{aligned} A &\to End_B(K \otimes_F B) = C \\ \alpha x_\sigma &\mapsto \phi_{\alpha x_\sigma} \end{aligned}$$

where $\phi_{\alpha x_\sigma}(c \otimes x_{\tau H}) = \alpha\sigma(c) \otimes x_{\sigma H} x_{\tau H}$. It is easy to see that this map is a k-algebra homomorphism that is injective. Moreover, by Proposition 6, C is central simple over k and

$$\begin{aligned} deg\ C &= rdim_B(K \otimes_F B) \\ &= \frac{dim_k K \otimes_F B}{deg\ B} \\ &= \frac{dim_F K dim_F B}{deg\ B} \\ &= dim_F K = deg\ A \end{aligned}$$

So the map is surjective and hence is an isomorphism. Therefore the maximal subfield of $C =$ maximal subfield of $A = K$.

(c) Show that the following diagram commutes:

$$\begin{tikzcd}
H^2(G/H, F^*) \arrow[r, "\simeq"] \arrow[d, "Inf_H^G"] & Br(F/k) \arrow[d, "Id : B \mapsto B"] \\
H^2(G, K^*) \arrow[r, "\simeq"] & Br(K/k)
\end{tikzcd}$$

With the notations as before, the diagram commutes if $[B] = [A]$ which is proved in part (b). So we are done.

44. Show that the following sequence is exact:

$$0 \to H^2(G/H, F^*) \xrightarrow{Inf_H^G} H^2(G, K^*) \xrightarrow{Res_H^G} H^2(H, K^*)$$

<u>Warning:</u> The map Res_H^G is not necessarily surjective as claimed incorrectly in the book.
<u>Solution:</u> From previous two exercises,

$$\begin{tikzcd}
0 \arrow[r] & H^2(G/H, F^*) \arrow[r, "Inf_H^G"] \arrow[d, "\simeq"] & H^2(G, K^*) \arrow[r, "Res_H^G"] \arrow[d, "\simeq"] & H^2(H, K^*) \arrow[d, "\simeq"] \\
0 \arrow[r] & Br(F/k) \arrow[r, "I"] & Br(K/k) \arrow[r, "R"] & Br(K/F)
\end{tikzcd}$$

where $I : A \mapsto A$ and $R : A \mapsto A \otimes_k F$. Since the squares commute as proved in previous problems, to show exactness of the top sequence, it suffices to show exactness of the bottom sequence.We will show that now:

<u>I is injective:</u>

This is clear since $I(A) = A$.

<u>$R \circ I = 0$:</u>

Let $A \in Br(F/k)$, then F splits A. So we have $R \circ I(A) = R(A) = [A \otimes_k F] = [k] = 0$.

<u>$Ker\ R = Im\ I$:</u>

Suppose $R(A) = 0$ where $A \in Br(K/k)$. Then $A \otimes_k F \simeq M_n(F)$. This means that A is split by F. So $A \in Br(F/k)$.

We have shown that the sequence is exact.

DONE!!!