M561 - Noncommutative Algebra

Academic Year 2021/2022
preliminary version

Christian Lomp

U.PORTO
FACULDADE DE CIÊNCIAS
UNIVERSIDADE DO PORTO

Departamento de Matemática

April 8, 2022

Contents

1 Finite dimensional division algebras **2**

2 Commutativity of division algebras **11**

3 The tensor product of algebras **18**

4 The Brauer group of a field **32**

5 Maximal Subfields and Crossed products **41**

1

Finite dimensional division algebras

Any element d over a finite dimensional central division algebra D over $\mathbb{F}$ is algebraic over $\mathbb{F}$, because the suablgebra $\mathbb{F}[d]$ of D generated by $\mathbb{F}$ and d is actually a field extension over $\mathbb{F}$ as the elements of $\mathbb{F}$ are central and commute with d. Moreover $[\mathbb{F}(d) : \mathbb{F}] \mid [D : \mathbb{F}]$ is finite and hence d is algebraic over $\mathbb{F}$. In particular if $\mathbb{F}$ is algebraically closed, then $D = \mathbb{F}$. So there are no finite dimensional division algebras over $\mathbb{C}$. This does not mean that there are no field extensions over $\mathbb{C}$ at all. For instance the field of fractions $\mathbb{C}(x)$ of the polynomial ring $\mathbb{C}[x]$ is an infinite field extension over $\mathbb{C}$ and one could go on and construct more $\mathbb{C}(x_1, \ldots, x_n)$ field extensions of $\mathbb{C}$.

Note that the quaternions $\mathbb{H}$ are a 2-dimensional division algebra over $\mathbb{C}$, generated by 1 and j. However, $\mathbb{H}$ is not central over $\mathbb{C}$ as $Z(\mathbb{H}) = \mathbb{R}$. Over the real numbers $\mathbb{R}$, we will now prove a Theorem by Frobenius from 1877 (see [2])[1] that says that the $\mathbb{R}$ and $\mathbb{H}$ are the only finite dimensional central division algebras over $\mathbb{R}$:

Theorem 1.1 (Frobenius) *Let D be an algebraic division algebra over $\mathbb{R}$. Then D is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$ as $\mathbb{R}$-algebra.*

Proof: Without loss of generality we can assume that $\mathbb{R} \leq Z(D)$ is a central subfield of D. If $[D : \mathbb{R}] = 1$, then clearly $D = \mathbb{R}$. Hence suppose $[D : \mathbb{R}] \geq 2$ and let $\alpha \in D \setminus \mathbb{R}$. Then as D is an algebraic extension, α is algebraic over $\mathbb{R}$. Since $\alpha \notin \mathbb{R}$, the irreducible polynomial of α must have degree 2 and $\mathbb{R}(\alpha) \simeq \mathbb{C}$. Hence we can suppose that $\mathbb{C}$ also embeds into D and that there are elements $1, \imath \in D$ such that $\imath^2 = -1$. If $[D : \mathbb{R}] = 2$, then $D = \mathbb{C}$. Hence assume that $[D : \mathbb{R}] > 2$ and consider the centralizer of $\imath$ in D, i.e.

$$D^+ = \{d \in D \mid d\imath = \imath d\} = \mathrm{Cent}_D(\imath).$$

[1] Ferdinand Georg Frobenius (1849-1917), Biography: MacTutor

Then D^+ is a subalgebra of D that contains $\mathbb{C}$. Furthermore, the inverse of any non-zero element of D^+ will also commute with $\imath$, i.e. D^+ is a division algebra over $\mathbb{C}$ and by hypothesis algebraic. However, by the comment proceeding this Theorem, $\mathbb{C}$ is algebraically closed and therefore we must have $\mathbb{C} = D^+$. Set $D^- = \{d \in D : d\imath = -\imath d\}$. Then $D^-D^- \subseteq D^+ = \mathbb{C}$. For any $d \in D$,

$$d = \frac{1}{2\imath}(\imath d + d\imath) + \frac{1}{2\imath}(\imath d - d\imath) \tag{1.1}$$

where $\imath d + d\imath \in D^+ = \mathbb{C}$ and $\imath d - d\imath \in D^-$. This shows that $D = \mathbb{C} \oplus D^-$ as $\mathbb{C}$-vector spaces. Since $[D : \mathbb{C}] > 2$, there exists a non-zero element $z \in D^-$, which allows us to define the map

$$\mu : D^- \to \mathbb{C}, \qquad x \mapsto xz \in D^+ = \mathbb{C}. \tag{1.2}$$

Since z is algebraic over $\mathbb{R}$ and does not belong to $\mathbb{R}$, there exist $a, b \in \mathbb{R}$ such that

$$z^2 = az + b. \tag{1.3}$$

On the other hand $z^2 = \mu(z) \in \mathbb{C}$. Hence $z^2 \in \mathbb{C} \cap (\mathbb{R}z \oplus \mathbb{R}) = \mathbb{R}$, because $az = z^2 - b \subset D^- \cap D^+ = \{0\}$. Hence $z^2 = b$. If $b \geq 0$, then there exists $c \in \mathbb{R}$ such that $b = c^2$ and $z^2 = c^2$, which implies $z = \pm b \in \mathbb{R}$ and which contradicts $z \notin \mathbb{C}$. Hence $b < 0$ and $z^2 = -c^2$ for some $c \in \mathbb{R}$. Set $\jmath := \frac{1}{c}z$. Then $\jmath^2 = z^2/c^2 = -1$. Set $k = \imath\jmath$ and note that

$$\imath\jmath = \frac{1}{c}\imath z = -\frac{1}{c}z\imath = -\jmath\imath, \tag{1.4}$$

because $z \in D^-$. Furthermore, as μ is an isomorphism of $\mathbb{C}$-vector spaces,

$$D = \mathbb{C} \oplus \mathbb{C}z = \mathbb{R} \oplus \mathbb{R}\imath \oplus \mathbb{R}\jmath \oplus \mathbb{R}k \simeq \mathbb{H}. \tag{1.5}$$

□

Over the rational numbers there are infinitely many finite dimensional central division algebras. In what follows we will show how to construct so called quaternion algebras.

Definition 1.2 *Let A be a unital ring. A function $\sigma : A \to A$ is called an anti-algebra homomorphism if σ is a group homomorphism of $(A, +)$, such that*

$$\sigma(1) = 1 \qquad \text{and} \qquad \sigma(ab) = \sigma(b)\sigma(a), \ \ \forall a, b \in A. \tag{1.6}$$

An anti-algebra homomorphism $\sigma : A \to A$ is called an involution if $\sigma^2 = id$.

A typical examples for an involution is the transposition of matrices. Complex conjugation is another example of an involution.

Proposition 1.3 *Let A be a unital ring with involution σ such that $a\sigma(a)$ and $\sigma(a)a$ are invertible for all $a \in A \setminus \{0\}$. Then A is a division ring.*

Proof: For $a \in A \setminus \{0\}$ we have $a\left(\sigma(a)(a\sigma(a))^{-1}\right) = 1 = \left((\sigma(a)a)^{-1}\sigma(a)\right)a$. Hence a has a left and right inverse and is therefore invertible. □

Actually the Proposition above works for any map $\sigma : A \to A$ with $a\sigma(a)$ and $\sigma(a)a$ being invertible for $a \neq 0$.

Let R be a commutative ring, $a, b \in R$ two elements and consider $A = R[x]/\langle x^2 - a\rangle$. We can identify elements $r \in R$ with their coset $r + \langle x^2 - a\rangle$. Set $\imath := x + \langle x^2 - a\rangle$. Then 1 and $\imath$ form a basis of A as R-module such that

$$\imath^2 = a \tag{1.7}$$

This means for $\alpha = r + s\imath$ and $\beta = t + u\imath$ in A:

$$\alpha\beta = (r + s\imath)(t + u\imath) = (rt + sua) + (ru + st)\imath \tag{1.8}$$

The R-linear map $\overline{\ } : A \to A$ defined by $\overline{u + v\imath} := u - v\imath$, for all $u + v\imath \in A$ is an algebra homomorphism of order 2, because for $\alpha = r + s\imath$, $\beta = t + u\imath$ in A we calculate:

$$\overline{\alpha\beta} = (rt + sua) - (ru + st)\imath = rt - st\imath + sua - ru\imath = (r - s\imath)t - (r - s\imath)u\imath = \overline{\alpha}\overline{\beta}. \tag{1.9}$$

Clearly, $\overline{\overline{\alpha}} = \alpha$, for all $\alpha \in A$.

Consider the subset of 2×2-matrizes over A of the form

$$Q = \left\{ \begin{bmatrix} \alpha_0 & \alpha_1 \\ b\overline{\alpha_1} & \overline{\alpha_0} \end{bmatrix} \mid \alpha_0, \alpha_1 \in A \right\} \subseteq M_2(A). \tag{1.10}$$

which is a subring of $M_2(A)$, since it is closed under the multiplication:

$$\begin{bmatrix} \alpha_0 & \alpha_1 \\ b\overline{\alpha_1} & \overline{\alpha_0} \end{bmatrix} \begin{bmatrix} \beta_0 & \beta_1 \\ b\overline{\beta_1} & \overline{\beta_0} \end{bmatrix} = \begin{bmatrix} \alpha_0\beta_0 + b\alpha_1\overline{\beta_1} & \alpha_0\beta_1 + \alpha_1\overline{\beta_0} \\ b\overline{\alpha_1}\beta_0 + b\overline{\alpha_0}\overline{\beta_1} & b\overline{\alpha_1}\beta_1 + \overline{\alpha_0}\overline{\beta_0} \end{bmatrix} = \begin{bmatrix} \alpha_0\beta_0 + b\alpha_1\overline{\beta_1} & \alpha_0\beta_1 + \alpha_1\overline{\beta_0} \\ \overline{b\alpha_0\beta_1 + \alpha_1\overline{\beta_0}} & \overline{\alpha_0\beta_0 + b\alpha_1\overline{\beta_1}} \end{bmatrix}.$$

As A-module we can identify Q with $A \oplus A$ by sending a matrix $\begin{bmatrix} \alpha_0 & \alpha_1 \\ b\overline{\alpha_1} & \overline{\alpha_0} \end{bmatrix}$ to the pair(α_0, α_1). The multiplication on $A \oplus A$ has then the formula:

$$(\alpha_0, \alpha_1) \cdot (\beta_0, \beta_1) := (\alpha_0\beta_0 + b\alpha_1\overline{\beta_1}, \alpha_0\beta_1 + \alpha_1\overline{\beta_0}) \tag{1.11}$$

for all $\alpha_i, \beta_i \in A$ and $i = 0, 1$. We set $Q := Q(a, b, R) = A \oplus A$ with that multiplication. For any $\alpha, \beta_0, \beta_1 \in A$ we have

$$(\alpha, 0)(\beta_0, \beta_1) = (\alpha\beta_0, \alpha\beta_1) \qquad \text{and} \qquad (\beta_0, \beta_1)(\alpha, 0) = (\beta_0\alpha, \beta_1\overline{\alpha}) \tag{1.12}$$

which shows that $\epsilon : A \to Q$ given by $\epsilon(\alpha) := (\alpha, 0)$ is an injective ring homomorphism. Moreover the centre of Q is $\epsilon(R) = \{(r, 0) : r \in R\} \subset Z(Q)$, since $\alpha = \overline{\alpha}$ if and only if $\alpha \in R$. Thus Q is an R-algebra of rank 4, since Q has a basis as R-module consisting of

$$(1, 0), \qquad (\imath, 0), \qquad \jmath = (0, 1), \qquad k = (0, \imath). \tag{1.13}$$

Abusing notation we will simply write 1 for $(1, 0)$ and $\imath$ for $(\imath, 0)$. In matrix notation, these elements look like:

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \qquad \imath = \begin{bmatrix} \imath & 0 \\ 0 & -\imath \end{bmatrix}, \qquad \jmath = \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}, \qquad k = \begin{bmatrix} 0 & \imath \\ -b\imath & 0 \end{bmatrix}$$

Using that $\imath^2 = a$ we obtain $\jmath^2 = (b, 0)$, $k^2 = (-ab, 0)$, $\imath\jmath = (0, \imath) = k$ and $\jmath k = (0, a) = a\jmath$. In particular we obtain the following multiplication table:

	$\imath$	$\jmath$	k
$\imath$	a	k	$a\jmath$
$\jmath$	$-k$	b	$-b\imath$
k	$-a\jmath$	$b\imath$	$-ab$

(1.14)

The following Theorem shows that over a field $\mathbb{F}$ of characteristic different from 2 and for non-zero parameters a, b, $Q(a, b, \mathbb{F})$ is a central simple $\mathbb{F}$-algebra that is either a division ring or isomorphic to $M_2(\mathbb{F})$.

Theorem 1.4 *Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) \neq 2$, $a, b \in \mathbb{F}$ and $Q = Q(a, b, \mathbb{F})$.*

1. *If $a \neq 0$ or $b \neq 0$, then $\mathbb{F} = Z(Q)$, i.e. Q is a central $\mathbb{F}$-algebra.*
2. *If $ab \neq 0$, then Q is either a central division algebra or isomorphic to $M_2(\mathbb{F})$.*

Proof: As before, let $A = \mathbb{F}[x]/\langle x^2 - a\rangle$, $\imath = x + \langle x^2 - a\rangle$ and $Q = A \times A$ with the multiplication as in (1.11). Note that Q has the basis $\{1, \imath, \jmath, k\}$ as vector space over $\mathbb{F}$. As an A-module, Q has the basis $\{1, \jmath\}$. Moreover, if $\alpha = a + b\imath \in A$, then $\jmath\alpha = \overline{\alpha}\jmath$, since $\jmath\imath = -k = -\imath\jmath$. Similarly, $k\alpha = \imath\jmath\alpha = \imath\overline{\alpha}\jmath = \overline{\alpha}k$.

Denote by $[a, b] := ab - ba$ the (additive) commutator in a ring R. Let $\gamma = \alpha_0 + \alpha_1\jmath \in Q$, then the commutators with $\imath, \jmath$ and k are:

$$[\imath, \gamma] = \imath(\alpha_0 + \alpha_1\jmath) - (\alpha_0 + \alpha_1\jmath)\imath = 2\alpha_1 k \tag{1.15}$$

$$[\jmath, \gamma] = \jmath(\alpha_0 + \alpha_1\jmath) - (\alpha_0 + \alpha_1\jmath)\jmath = b(\overline{\alpha_1} - \alpha_1) + (\overline{\alpha_0} - \alpha_0)\jmath \tag{1.16}$$

$$[k, \gamma] = k(\alpha_0 + \alpha_1\jmath) - (\alpha_0 + \alpha_1\jmath)k = b\imath(\alpha_1 + \overline{\alpha_1}) + (\overline{\alpha_0} - \alpha_0)\imath\jmath \tag{1.17}$$

(1) Let $\gamma = \alpha_0 + \alpha_1\jmath \in Z(Q)$. Then $[\jmath, \gamma] = 0 = [\imath, \gamma]$ and hence by (1.15),

$$2\alpha_1 k = 0 \qquad b(\overline{\alpha_1} - \alpha_1) = 0 \qquad \text{and} \qquad \overline{\alpha_0} = \alpha_0.$$

Hence $\alpha_0 \in F$. If $b \neq 0$, then $\overline{\alpha_1} = \alpha_1$ and therefore, $\alpha_1 \in \mathbb{F}$. But then $2\alpha_1\imath = 0$ and $\mathrm{char}(\mathbb{F}) \neq 2$ imply $\alpha_1 = 0$. If $b = 0$, then $a \neq 0$ and $\imath$ is invertible, with inverse $a^{-1}\imath$. Hence the first equation $2\alpha_1\imath = 0$ and $\mathrm{char}(\mathbb{F}) \neq 2$ imply $\alpha_1 = 0$. In both cases $\gamma = \alpha_0 \in F$. It is clear that any element $\alpha_0 \in F$ is central in Q, which proves $\mathbb{F} = Z(Q)$.

(2) Note that if $a \neq 0 \neq b$, then $\imath, \jmath$ and k are units with inverses given by $a^{-1}\imath$, $b^{-1}\jmath$ and $-a^{-1}b^{-1}k$ respectively. Let I be an ideal of Q and assume $I \neq Q$. Let $\gamma = \alpha_0 + \alpha_1\jmath \in I$ be an element of I. From (1.15) we get that

$$[k, [\imath, \gamma]] = [k, 2\alpha_1 k] = 2(\overline{\alpha_1} - \alpha_1)k^2 = -2ab(\overline{\alpha_1} - \alpha_1) \in I \cap \mathbb{F}\imath,$$

which would be invertible if $\overline{\alpha_1} \neq \alpha_1$. Since $I \neq Q$, we must have $\overline{\alpha_1} = \alpha_1 \in \mathbb{F}$. But then $[\imath, \gamma] = 2\alpha_1\imath \in I \cap \mathbb{F}\imath$ would be invertible if $\alpha_1 \neq 0$. Thus we must have $\alpha_1 = 0$ and $\gamma = \alpha_0$. Then $[\jmath, \gamma] = (\overline{\alpha_0} - \alpha_0)\jmath \in I \cap \mathbb{F}k$ would be an invertible element if $\overline{\alpha_0} \neq \alpha_0$ and we must have $\gamma = \alpha_0 \in \mathbb{F}$. However this implies finally $\gamma = 0$, as otherwise $I = Q$.

We proved that the only proper ideal of Q is the zero ideal, i.e. Q is a central simple $\mathbb{F}$-algebra. In particular, any non-zero left Q-module M is faithful. This means in particular

that the canonical ring homomorphism $\lambda_M : Q \to \mathrm{End}_{\mathbb{F}}(M)$ is injective. In particular, $4 = \dim(Q) \leq \dim(M)^2$.

Suppose Q is not a division algebra there exists $0 \neq x \in Q$ without inverse element. Let $M = Qx$ be the left ideal of Q generated by x. Note that $M \neq Q$.[2] By the argument above, M and Q/M are non-zero faithful Q-modules $4 \leq \min(\dim(M)^2, (4 - \dim(M))^2)$ As $\dim(I) \in \{1, 2, 3\}$, the only choice is $\dim(M) = 2$. However, since $\lambda_M : Q \to \mathrm{End}_{\mathbb{F}}(M)$ is injective and $\mathrm{End}_{\mathbb{F}}(M) \simeq M_2(\mathbb{F})$ has the same dimension as Q, we must have that λ_M is an isomorphism of rings.

□

The last Theorem raises the immediate question as to how to decide whether $Q(a, b, \mathbb{F})$ is a division algebra or not. For that reason we define the conjugate of an arbitrary element $x = x_0 + x_1\imath + x_2\jmath + x_3k \in Q$ as

$$\overline{x} := x_0 - x_1\imath - x_2\jmath - x_3k \tag{1.18}$$

Note that $\overline{}$ is an involution of Q, because one can easily check that for $x, y \in Q$:

$$\overline{xy} = \overline{y}\,\overline{x} \qquad \text{and} \qquad \overline{x + y} = \overline{x} + \overline{y}.$$

These calculations are straightforward and rely on the simple observation that

$$\overline{\imath\jmath} = \overline{k} = -k = (-\jmath)(-\imath) = \overline{\jmath}\,\overline{\imath}.$$

For an element $x = x_0 + x_1\imath + x_2\jmath + x_3k \in Q$ we calculate

$$\begin{aligned} x\overline{x} &= (x_0 + x_1\imath + x_2\jmath + x_3k)(x_0 - x_1\imath - x_2\jmath - x_3k) \\ &= x_0^2 - x_0x_1\imath - x_0x_2\jmath - x_0x_3k \\ &\quad + x_1x_0\imath - ax_1^2 - x_1x_2k - ax_1x_3\jmath \\ &\quad + x_2x_0\jmath + x_2x_1k - bx_2^2 + bx_2x_3\imath \\ &\quad + x_3x_0k + ax_3x_1\jmath - bx_3x_2\imath + abx_3^2 = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 \in \mathbb{F} \end{aligned}$$

The norm on Q is then defined as the map

$$N : Q \to \mathbb{F}, \qquad N(x_0 + x_1\imath + x_2\jmath + x_3k) := x_0^2 - ax_1^2 - bx_2^2 + abx_3^2 \tag{1.19}$$

Note that $N(-)$ is a multiplicative map, because $Z(Q) = \mathbb{F}$, i.e. for all $x, y \in Q$:

$$N(xy) = xy\overline{xy} = xy\overline{y}\,\overline{x} = xN(y)\overline{x} = N(x)N(y)$$

Theorem 1.5 *Let $\mathbb{F}$ be a field with $\mathrm{char}(\mathbb{F}) \neq 2$ and $a, b \in \mathbb{F} \setminus \{0\}$. Then $Q = Q(a, b, \mathbb{F})$ is a division algebra if and only if $N(x) \neq 0$, for all $0 \neq x \in Q$.*

Proof: If $N(x) = x\overline{x} \neq 0$ for all non-zero $x \in Q$, then $N(x)$ is invertible and by Proposition 1.3, Q is a division algebra. The contrary is clear, since if Q is a division ring, then it has no zero divisors. Thus $x\overline{x} \neq 0$ for all $x \neq 0$. □

Taking $\mathbb{F} = \mathbb{R}$ and $a = b = -1$, we obtain $Q(-1, -1; \mathbb{R}) = \mathbb{H}$, which we already knew to be a division ring. We will prove that over $\mathbb{Q}$ there are infinitely non-isomorphic division

[2] Since x is not invertible, either $Qx \neq Q$ or $xQ \neq Q$. Without loss of generality we can assume $Qx \neq Q$.

algebras of the form $Q(a,b;\mathbb{Q})$. To do so we will recall some basic results of elementary number theory. In particular how to solve polynomial equations modulo an integer m. Suppose given $a,b \in \mathbb{Z}$ we want to solve $ax \equiv b(\bmod m)$, for some $x \in \mathbb{Z}$ then this is precisely possible if the Diophantine equation $ax + my = b$ has an integer solution $x, y \in \mathbb{Z}$, which is precisely possible if $\gcd(a,m) \mid b$. The solution is then of course given by the (extended) Euclidean Algorithm, as there exist $r, s \in \mathbb{Z}$ with $ra + sm = \gcd(a,m)$ and if $b = \gcd(a,m)b'$, then for $x = -rb'$ we have

$$ax = -arb' = \gcd(a,m)b' - sb'm \equiv b(\bmod m).$$

Theorem 1.6 *Let m be a positive integer such that $U(\mathbb{Z}/m\mathbb{Z})$ is cyclic. Let $a \in \mathbb{Z}$ be an integer that is relatively prime to m. Let $n \in \mathbb{N}^+$ and $d = \gcd(n, \varphi(m))$ Then the following are equivalent:*

(a) $x^n \equiv a(\bmod m)$ *has a solution.*

(b) $a^{\frac{\varphi(m)}{d}} \equiv 1(\bmod m)$.

A solution a of the equation $x^n \equiv a(\bmod m)$ is called an nth power residue modulo m. In case $n = 2$, a is called a quadratic residue modulo m.

Proof: Let g be a generator of $G = U(\mathbb{Z}/m\mathbb{Z})$. Then there exists $b \geq 0$ with $a = g^b$. Then

$$\begin{aligned}
\exists c \in \mathbb{N}:\ (g^c)^n \equiv a(\bmod m) &\Leftrightarrow \exists c \in \mathbb{N}:\ g^{cn} \equiv g^b(\bmod m)\\
&\Leftrightarrow \exists c \in \mathbb{N}:\ cn \equiv b(\bmod \varphi(m))\\
&\Leftrightarrow d = \gcd(n,\varphi(m)) \mid b\\
&\Leftrightarrow d \mid b \text{ and } a^{\frac{\varphi(m)}{d}} = g^{\frac{\varphi(m)b}{d}} = \left(g^{\varphi(m)}\right)^{\frac{b}{d}} \equiv 1(\bmod m)
\end{aligned}$$

□

As a technical tool we define the Legendre symbol of an integer a and a prime number p as

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & a \text{ is a quadratic residue modulo } p\\ 0 & p \text{ divides } a\\ -1 & a \text{ is not a quadratic residue modulo } p \end{cases}$$

By Theorem 1.6 we have in particular $\left(\frac{a}{p}\right) = 1$ if and only if $a^{\frac{p-1}{\gcd(2,p-1)}} \equiv 1(\bmod p)$. The special case $a = -1$ is important to us:

Corollary 1.7 *Let p be a prime number, then the following statements are equivalent:*

(a) -1 *is not a quadratic residue modulo p, i.e.* $\left(\frac{-1}{p}\right) = -1$

(b) $x^2 + 1$ *is an irreducible element in* $\mathbb{F}_p[x]$.

(c) $(-1)^{\frac{p-1}{2}} = -1$.

(c) $p \equiv 3(\bmod 4)$.

Proof: In case $p = 2$, none of the three conditions is true. Hence we can assume p to be odd. The equivalence of (a) and (b) is clear. By Theorem 1.6 (a) is equivalent to $(-1)^{\frac{p-1}{2}} \not\equiv 1(\mathrm{mod} p)$ and hence to $(-1)^{\frac{p-1}{2}} = -1$, which in turn is equivalent to $\frac{p-1}{2}$ being odd. This is equivalent to $p - 1 = 2(2n + 1) = 4n + 2$ for some $n \in \mathbb{Z}$ and hence to $p \equiv 3(\mathrm{\ mod\ } 4)$. □

As a consequence of the fact that $\mathbb{Z}$ is a unique factorization domain we conclude that there exist infinitely many prime numbers p that are congruent to 3 modulo 4.

Corollary 1.8 *There exist infinitely many prime numbers p with $p \equiv 3(\mathrm{\ mod\ } 4)$.*

Proof: The proof is by contradiction. Suppose that there are only finitely many prime numbers p of the form $p = 3 + 4n$, for some $n \in \mathbb{N}$. Let $\mathcal{P} = \{p_0, p_1, \ldots, p_m\}$ the set of all such prime numbers, where $p_i \neq p_j$, for $i \neq j$ and $p_0 = 3$. Let $x = 4p_1 \cdots p_m + 3$. Then since x is odd and must be divisible by some prime number. Since $x \equiv 3(\mathrm{\ mod\ } 4)$, not all prime factors of x can be of the form $1 + 4n$. Hence there must exist some prime factor of the form $q = 3 + 4n$, for some $n \in \mathbb{N}$. Hence $q \in \mathcal{P}$. If $q = p_0 = 3$, then $q = 3 \mid x$ implies $3 \mid p_i$ for some $i \geq 1$, which is impossible. Hence $q = p_i$ for some $1 \leq i \leq m$, but then $p_i \mid 3$, which is also impossible. This shows that we are lead to a contradiction and that there must be infinitely many prime numbers of the form $3 + 4n$. □

Now we will return to our construction of four dimensional division algebras over the rational numbers. Let $\mathbb{F} = \mathbb{Q}$ and let $b = p$ be a prime number in $\mathbb{Z}$. We will try to decide whether there exists $a \in \mathbb{Z}$ such that $Q = Q(a, p; \mathbb{Q})$ is a division algebra over $\mathbb{Q}$. Note that $A = \mathbb{Q}[x]/\langle x^2 - a\rangle$ is either isomorphic to $\mathbb{Q} \times \mathbb{Q}$ precisely in case a is a perfect square or $A \simeq \mathbb{Q}[\sqrt{a}]$ is a field extension of $\mathbb{Q}$ of degree 2. In the first case, Q will have zero divisors, since if $a = c^2$, then $(\imath - c)(\imath + c) = 0$. Hence we might assume that a is not a perfect square and that $A \simeq \mathbb{Q}[\sqrt{a}]$. Suppose $x = x_0 + x_1\imath + x_2\jmath + x_3k \in Q$ is a non-zero element, such that

$$N(x) = x_0^2 - ax_1^2 - p\left(x_2^2 - ax_3^2\right) = 0. \tag{1.20}$$

Multiplying by a common denominator, we can assume that all x_i are integers. Furthermore, we can also assume that at least one of the x_i's is not divisible by p (not all of them can be zero as $x \neq 0$). Hence modulo p, equation (1.20) becomes:

$$x_0^2 \equiv ax_1^2 \ (\mathrm{mod}\, p) \tag{1.21}$$

If $p \nmid x_1$, then $a \equiv (x_0x_1^{-1})^2(\mathrm{\ mod\ } p)$ and a is a perfect square modulo p, i.e. $\left(\frac{a}{p}\right) = 1$. If $p \mid x_1$, then also $p \mid x_0$ and we can cancel a multiple of p from equation (1.20) and obtain $p\left(x_0^2 - ax_1^2\right) - \left(x_2^2 - ax_3^2\right) = 0$. Hence, taking this equation again modulo p, we obtain $x_2^2 \equiv ax_3^2 \ (\mathrm{mod}\, p)$ and as either x_2 or x_3 are not divisible by p, none of them is. Hence, again we obtain $\left(\frac{a}{p}\right) = 1$ as $a \equiv (x_2x_3^{-1})^2 \ (\mathrm{mod}\, p)$. We have just proved the following Theorem:

Theorem 1.9 *For any $a \in \mathbb{Z}$ and prime number p such that $\left(\frac{a}{p}\right) = -1$, the quaternion algebra $Q(a, p; \mathbb{Q})$ is a four dimensional central division algebra over $\mathbb{Q}$. In particular, if p is a prime number, such that $p \equiv 3(\mathrm{\ mod\ } 4)$, then $Q(-1, p; \mathbb{Q})$ is a division algebra.*

Proof: By Corollary 1.7, $p \equiv 3(\bmod 4)$ is equivalent to $\left(\frac{-1}{p}\right) = -1$. Hence by Theorem 1.9, $Q(-1,p;\mathbb{Q})$ is a division algebra. □

The question arises when two of such quaternion division algebras are isomorphic. Suppose there exists an isomorphism $f : Q(a,b;\mathbb{F}) \to Q(a',b';\mathbb{F})$ of $\mathbb{F}$-algebras. Then the image of $f(\imath)$ satisfies $f(\imath)^2 = a$ like also the corresponding element $\imath' \in Q(a',b';\mathbb{F})$. Hence $f(\imath)$ and $\imath'$ are roots of the same (irreducible) polynomial $t^2 - a$. What the next Lemma will show is that roots in a division ring of an irreducible polynomial of degree 2 are conjugated. The reader should be aware that if x is a root of $t^2 - a$, then $-x$. However, this might not be all roots of $t^2 - a$. For instance in $\mathbb{H} = Q(-1,-1;\mathbb{R})$ all six elements $\pm\imath, \pm\jmath$ and $\pm k$ are roots of $t^2 + 1$. Even worse, for any $\lambda \in \mathbb{R}$ the element $\omega = \frac{1}{\sqrt{\lambda^2+1}}(\lambda\imath + \jmath)$ is a root of that polynomial as

$$\omega^2 + 1 = \frac{1}{\lambda^2+1}\left(\lambda^2\imath^2 + \lambda\imath\jmath + \lambda\jmath\imath + \jmath^2\right) = 0.$$

Hence the "innocent" looking polynomial $t^2 + 1$ has infinitely many roots in $\mathbb{H}$.

Lemma 1.10 *Let D be a division ring with $\mathbb{F} = Z(D)$ and $[D:\mathbb{F}] < \infty$. Then any two roots in D of an irreducible polynomial of degree 2 over $\mathbb{F}$ are conjugated in D.*

Proof: We need to show that if $x, y \in D$ are roots of some irreducible polynomial $f = t^2 + c_1 t + c_0 \in \mathbb{F}[t]$, then there exists $d \in D \setminus \{0\}$ such that $y = dxd^{-1}$. Note that as f is irreducible in $\mathbb{F}[t]$, it has no roots in $\mathbb{F}$ and therefore $x, y \in D \setminus \mathbb{F}$. Clearly, if $f(x) = 0$, then $(t-x)(t+x+c_1) = t^2 + (x + c_1 - x)t - x^2 - xc_1 = t^2 + c_1 t + c_0 = f$. Let us consider first the case $y = -x - c_1$. Then $xy = -x^2 - c_1 x = c_0 \in \mathbb{F} = Z(D)$ is central and $xy = yx$. Denote by $\mathrm{Cent}_D(x) = \{d \in D : [d,x] = 0\}$ the centralizer of x in D and define the $\mathbb{F}$-linear map $g : D \to D$ given by $g(d) = dx - yd$. Then $g(D) \subseteq \mathrm{Cent}_D(x)$, because, for all $d \in D$:

$$[x, g(d)] = x(dx - yd) - (dx - yd)x = xdx - dxy - dx^2 + ydx = xdx + dx^2 + dc_1 x - dx^2 - xdx - c_1 dx = 0.$$

As x is not central in D, $\mathrm{Cent}_D(x) \neq D$ and hence g is not surjective. Since $[D:\mathbb{F}] < \infty$ and g is $\mathbb{F}$-linear, g can also not be injective and there must exists a non-zero $d \in D$ with $dx - yd = g(d) = 0$, i.e. $dxd^{-1} = y$.

In case $y \neq -x - c_1$. then as $f(y) = 0$, we have $x^2 + c_1 x + c_0 = 0 = y^2 + c_1 y + c_0$. Hence $(x + c_1)x = y(y + c_1)$ and adding yx to both side, we obtain $(x + c_1 + y)x = y(x + c_1 + y)$. Since $d = x + c_1 + y \neq 0$, we obtain $y = dxd^{-1}$. □

Assume $\mathbb{F}$ is a field of characteristic not 2. An element $a \in \mathbb{F}$ is called a square in $\mathbb{F}$ if there exists $c \in \mathbb{F}$ with $a = c^2$, or equivalently if $x^2 - a$ is not irreducible in $\mathbb{F}[x]$.

Theorem 1.11 *Let $\mathbb{F}$ be a field of characteristic not 2, $a, b, b' \in \mathbb{F} \setminus \{0\}$. If a is not a square in $\mathbb{F}$ and $Q(a,b;\mathbb{F}) \simeq Q(a,b';\mathbb{F})$ as $\mathbb{F}$-algebras then $b/b' \in \mathrm{Im}(N_a)$, where*

$$N_a : \mathbb{F}[x]/\langle x^2 - a\rangle \to \mathbb{F}, \qquad N_a(c_0 + c_1\imath) = c_0^2 - ac_1^2.$$

Proof: Suppose $f : Q(a,b;\mathbb{F}) \to Q(a,b';\mathbb{F})$ is an isomorphism of $\mathbb{F}$-algebras. Denote the basis of $Q(a,b;\mathbb{F})$ by $1, \imath, \jmath, k$ and the basis of $D := Q(a,b',\mathbb{F})$ by $1, u, v, w$. Then

$$u^2 = a, \qquad v^2 = b', \qquad w = uv = -vu.$$

Note also that the subspace of elements that anti-commute with u is

$$D_u^- = \{d \in D \mid ud = -du\} = \mathbb{F}v \oplus \mathbb{F}w.$$

Set $u_0 = f(\imath)$ and $v_0 = f(\jmath)$. Then

$$u_0^2 = f(\imath^2) = a, \qquad v_0^2 = f(\jmath^2) = b, \qquad u_0 v_0 = -v_0 u_0.$$

In particular u and u_0 are elements of D and roots of the irreducible polynomial $x^2 - a \in \mathbb{F}[x]$. By Lemma 1.10, u and u_0 are conjugated, i.e. there exists $q \in D$ with $u = qu_0q^{-1}$. Set $\tilde{v} = qv_0q^{-1} \in D$. Then

$$u\tilde{v} = qu_0v_0q^{-1} = -qv_0u_0q^{-1} = -\tilde{v}u.$$

Hence $\tilde{v} \in D_u^-$ and there exists $c_0, c_1 \in \mathbb{F}$ such that $\tilde{v} = c_0v + c_1w$. Then

$$\begin{aligned} b = qv_0^2q^{-1} = \tilde{v}^2 &= (c_0v + c_1w)(c_0v + c_1w) \\ &= c_0^2v^2 + c_0c_1vw + c_0c_1wv + c_1^2w^2 \\ &= c_0^2b' - ab'c_1^2 \\ &= b'N_a(c_0 + \imath c_1) \end{aligned}$$

Hence $b/b' \in \mathrm{Im}(N_a)$. □

Corollary 1.12 *$Q(-1, p; \mathbb{Q}) \not\simeq Q(-1, q; \mathbb{Q})$ for all prime numbers $p \neq q$ congruent to 3 modulo 4.*

Proof: Clearly, $a = -1$ is not a square in $\mathbb{Q}$. Hence $A = \mathbb{Q}[x]/\langle x^2 + 1\rangle \simeq \mathbb{Q}(\imath)$ is a field and N_{-1} is the square of the usual norm on $\mathbb{C}$, i.e. $N_{-1}(c_0 + c_1\imath) = c_0^2 + c_1^2$. If $p/q \in \mathrm{Im}(N_{-1})$ then there exists $c_0, c_1 \in \mathbb{Q}$ with $p = q(c_0^2 + c_1^2)$. Write $c_0 = \frac{c_0'}{d}$ and $c_1 = \frac{c_1'}{d}$, with $c_0', c_1' \in \mathbb{Z}$ and d the common denominator of c_0 and c_1.Hence $d^2p = q(c_0'^2 + c_1'^2) \in \mathbb{Z}$. Since $p \equiv 3(\bmod 4)$, we have $\left(\frac{-1}{p}\right) = -1$ and therefore, $p \nmid c_0'^2 + c_1'2$. Hence $p = q$. □

Corollary 1.13 *There exist infinitely many non-isomorphic division algebras of dimension 4 over $\mathbb{Q}$.*

Let us finish this section with a comment on the construction of $Q(a, b; \mathbb{K})$. The two elements $\imath$ and $\jmath$ are algebra generators of $Q(a, b; \mathbb{K})$ and in particular we have a surjective map from the free algebra $\psi : \mathbb{K}\langle x, y\rangle \longrightarrow Q(a, b; \mathbb{K})$ to $Q(a, b; \mathbb{K})$ sending x to $\imath$ and y to $\jmath$. Looking at the kernel of ψ we see that $x^2 - a$, $y^2 - b$ and $yx + yx$ belong to it. On the other hand it is not hard to see that the free algebra modulo the ideal generated by these three elements is actually 4 dimensional and that therefore $Q(a, b; \mathbb{K})$ is actually isomorphic to $\mathbb{K}\langle x, y\rangle/\langle x^2 - a, y^2 - b, yx - xy\rangle$. The quantum plane at parameter q is defined as $\mathbb{K}_q[x, y] = \mathbb{K}\langle x, y\rangle/\langle yx - qxy\rangle$. Hence for $q = -1$ we have that

$$Q(a, b; \mathbb{K}) \simeq \mathbb{K}_{-1}[x, y]/\langle x^2 - a, y^2 - b\rangle$$

is a factor algebra of the quantum plane at parameter -1. Similarly, if q is a root of unity of index n and $a, b \in \mathbb{K}$ are non-zero elements, one can consider $\mathbb{K}_q[x, y]/\langle x^n - a, y^n - b\rangle$ and prove its centrality and simplicity.

2

Commutativity of division algebras

We have seen that there are infinitely many finite dimensional central division algebras over $\mathbb{Q}$, while there are only finitely many over $\mathbb{R}$. In this section we prove Wedderburn's theorem that says that any finite dimensional division algebra over a finite field is actually commutative. We also present Jacobson's result that extends Wedderburn's result to division algebras that are algebraic extensions over finite fields.

Before we start we need some facts about cyclotomic polynomials. Let $n \geq 1$ and consider the polynomial $x^n - 1 \in \mathbb{Z}[x]$. A complex primitive root of unity of index n is

$$\omega = \mathbf{e}^{\frac{2\pi\imath}{n}} = \cos\left(\frac{2\pi}{n}\right) + \imath \sin\left(\frac{2\pi}{n}\right)$$

and $x^n - 1$ decomposes into linear factors in $\mathbb{C}[x]$ as

$$x^n - 1 = \prod_{k=1}^{n} \left(x - \omega^k\right).$$

Recall that Euler's φ-function[1] is defined as

$$\varphi : \mathbb{N}^+ \to \mathbb{N}^+, \qquad \varphi(n) := |\{k : \gcd(k, n) = 1, 0 < k < n\}|, \ \forall n \in \mathbb{N}^+ \tag{2.1}$$

Lemma 2.1 *Let $n > 1$ and $C_n = \langle\omega\rangle \subset \mathbb{C}^\times$ be the multiplicative cyclic group of order n, where $\omega = \mathbf{e}^{\frac{2\pi\imath}{n}}$. Then*

$$\varphi(n) = |\{y \in C_n : y \text{ is a generator for } C_n\}| \tag{2.2}$$

[1] Leonhard Euler (1707-1783), Biography: MacTutor

Proof: Let $A = \{k : 0 < k < n, \gcd(k,n) = 1\}$ and $B = \{y \in C_n : y \text{ is a generator for } C_n\}$. We show that the mapping $f : A \to B$ with $f(k) = \omega^k$ is a bijection. Let $k \in A$ and consider $y = f(k) = \omega^k$. By the extended Euclidean Algorithm, there exist $s, t \in \mathbb{Z}$ such that $1 = sk + tn$. Thus

$$y^s = \omega^{sk} = \omega^{1-tn} = \omega(\omega^n)^{-t} = \omega. \tag{2.3}$$

This shows that $\omega \in \langle y \rangle$ and therefore $C_n = \langle y \rangle$. Let $k_1, k_2 \in A$ such that $f(k_1) = f(k_2)$. Without loss of generality we can assume $k_1 \geq k_2$, then

$$\omega^{k_1} = f(k_1) = f(k_2) = \omega^{k_2} \Rightarrow \omega^{k_1 - k_2} = 1. \tag{2.4}$$

Since ω has order n, $n \mid k_1 - k_2$. However, $0 \neq k_1 - k_2 < n$. Thus $k_1 = k_2$, showing that f is injective. To prove surjectivity, let $y \in B$. Then $y = \omega^m$ for some $m \in \mathbb{Z}$. By the division algorithm we can divide m by n and obtain $m = qn + k$, for $0 \leq k < n$. Since $\omega^n = 1$, $\omega^{qn} = 1$ and hence $y = \omega^m = \omega^{qn}\omega^k = \omega^k$. If $k = 0$, then $y = 1$ would be a generator, meaning $C_n = \langle 1 \rangle = \{1\}$, which is absurd as $n > 1$. Thus $0 < k < n$. Suppose $\gcd(k,n) = d$. Then there are $a, b \in \mathbb{N}$ such that $k = ad$ and $n = bd$. Hence

$$(\omega^k)^b = \omega^{adb} = \omega^{na} = 1 \tag{2.5}$$

and as the order of $y = \omega^k$ is n, we must have $n \mid b$. But then $n = bd$ and $n \mid b$ implies $1 \mid d$, i.e. $d = 1$. Therefore $k \in A$ and $y = f(k)$. □

The primitive roots of unity of index n are of the form ω^k for $1 \leq k \leq n$ and $\gcd(k,n) = 1$, because the generator of the cyclic group of order n, $C_n = \{\omega^k : k \in \mathbb{Z}\}$ are precisely of that form. The cyclotomic polynomial of index n is defined as

$$\Phi_n = \prod_{\gcd(k,n)=1} \left(x - \omega^k\right),$$

where it is understood that k runs between 1 and n. Note that if $n = de$, then ω^e is a root of unity of index d. Hence,

$$x^n - 1 = \prod_{e|n} \prod_{\gcd(n,k)=e} (x - \omega^k) = \prod_{n=de} \prod_{\gcd(d,k)=1} \left(x - ((\omega^e)^k\right) = \prod_{d|n} \Phi_d. \tag{2.6}$$

By induction we can show that $\Phi_n \in \mathbb{Z}[x]$, because for $n = 1$, we have $\Phi_1 = x - 1 \in \mathbb{Z}[x]$ and if $n \geq 1$ and we have already proven that $\Phi_d \in \mathbb{Z}[x]$ for all $d < n$. Then $g = \left(\prod_{d|n, d\neq n} \Phi_d\right) \in \mathbb{Z}[x]$ and hence $\Phi_n \in \mathbb{Z}[x]$ since $x^n - 1 = \Phi_n g \in \mathbb{Z}[x]$.

Theorem 2.2 (Wedderburn) *Any finite division algebra is commutative.*

Proof: Let $\mathbb{F} = Z(D)$ be the center of D. Then $\mathbb{F}$ is a finite field and has positive characteristic, say $p > 0$. In particular $|\mathbb{F}| = q = p^k$ for some $k \geq 1$. Since D is a finite dimensional vector space over $\mathbb{F}$, $|D| = q^n$, for some $n \geq 1$. We will show $n = 1$.

Consider the multiplicative group $G = D \setminus \{0\}$ and a set of representative of its conjugacy classes $\mathcal{C} = \mathbb{F}^\times \cup \{x_1, \ldots, x_m\}$, where the conjugacy classes of each non-zero central element

$z \in \mathbb{F}^\times$ are singletons and the elements x_i are non-central representatives of the remaining conjugacy classes $[x_i] = \{yx_iy^{-1} \mid y \in G\}$. In particular,

$$G = \mathbb{F}^\times \cup \bigcup_{i=1}^{m} [x_i] \tag{2.7}$$

Let x be an element, $[x]$ its conjugacy class and $\mathrm{Cent}_D(x) = \{y \in D : yx = xy\}$ the centralizer in D. Then $C_x := \mathrm{Cent}_D(x)^\times$ is a subgroup of $G = D^\times$ and the map

$$f : G/C_x \longrightarrow [x], \qquad yC_x \mapsto yxy^{-1}$$

is a bijection. Furthermore, the centralizer $\mathrm{Cent}_D(x)$ is a subdivision ring of D and contains $\mathbb{F} = Z(D)$. Hence $|\mathrm{Cent}_D(x)| = q^r$, for $r = \dim_{\mathbb{F}}(\mathrm{Cent}_D(x))$ that divides n. Thus,

$$|[x]| = \frac{|G|}{|C_x|} = \frac{q^n - 1}{q^r - 1}.$$

Applying this identity to (2.7) we obtain:

$$q^n - 1 = |D^\times| = |\mathbb{F}^\times| + \sum_{i=1}^{m} |[x_i]| = q - 1 + \sum_{i=1}^{m} \frac{q^n - 1}{q^{r_i} - 1}, \tag{2.8}$$

where $r_i = \dim_{\mathbb{F}}(\mathrm{Cent}_D(x_i))$. Since $\Phi_n \mid \frac{x^n-1}{x^{r_i}-1}$, for all i, we obtain

$$\Phi_n(q) \mid q^n - 1 - \sum_{i=1}^{m} \frac{q^n - 1}{q^{r_i} - 1} = q - 1.$$

Let $\omega = \cos\left(\frac{2\pi}{n}\right) + \imath \sin\left(\frac{2\pi}{n}\right)$, then $\Phi_n(q) = \prod_{\gcd(n,k)=1}(q - \omega^k)$ and

$$\begin{aligned}
\|\Phi_n(q)\|^2 &= \prod_{\gcd(n,k)=1} \|q - \omega^k\|^2 \\
&= \prod_{\gcd(n,k)=1} \left(\left(q - \cos\left(\frac{2\pi k}{n}\right) \right)^2 + \sin\left(\frac{2\pi k}{n}\right)^2 \right). \\
&= \prod_{\gcd(n,k)=1} \left(q^2 - 2q\cos\left(\frac{2\pi k}{n}\right) + 1 \right) \\
&\leq |q-1|^2 = q^2 - 2q + 1.
\end{aligned}$$

However, $q^2 - 2q\cos\left(\frac{2\pi k}{n}\right) + 1 \geq 1$ and $q^2 - 2q\cos\left(\frac{2\pi k}{n}\right) + 1 \leq q^2 - 2q + 1$ if and only if $\cos\left(\frac{2\pi k}{n}\right) \geq 1$ if and only if $k = n$. Hence we must have $n = k = 1$ and $D = Z(D) = \mathbb{F}$. □

Wedderburn's Theorem has some immediate consequences:

Corollary 2.3 *Any finite ring without zero divisors is a (commutative) field.*

Proof: In an Artinian ring, any non-zero divisor is invertible. Hence any finite ring without zero divisors is a division ring and by Wedderburn's Theorem a field. □

Using Euler's φ-function we will now prove that a finite groups is cyclic if it has for each divisor d of its order at most one subgroup of order d. This will be a key step to prove that the multiplicative group of a finite field is cyclic.

Theorem 2.4 *The following statements are equivalent for a finite group G of order n.*

(a) G is cyclic;

(b) for every divisor d of n, there exists exactly one subgroup H of G of order d;

(c) for every divisor d of n, there exists at most one subgroup H of G of order d.

Moreover, $n = \sum_{d|n} \varphi(d)$ holds.

Proof: Let G be a group of order n and denote by $\sim$ the equivalence relation $a \sim b$ if and only if $\langle a \rangle = \langle b \rangle$, for all $a, b \in G$. Then $\sim$ yields a partition of G into distinct equivalent classes, i.e.

$$G = \dot{\bigcup}_{a \in \Lambda} [a]_\sim \tag{2.9}$$

for some set of representatives $\Lambda \subset G$. Note that if $a \in \Lambda$, then $[a]_\sim$ is precisely the set of generators of the cyclic subgroup $C = \langle a \rangle$. Moreover, $|C| = d \mid n$ and $|[a]_\sim| = \varphi(d)$. For any divisor $d \mid n$, let c_d be the number of different cyclic subgroups of order d of G. Then the partition 2.9 yields:

$$n = |G| = \sum_{a \in \Lambda} |[a]_\sim| = \sum_{d|n} c_d \varphi(d). \tag{2.10}$$

$(a) \Rightarrow (b)$: Suppose G is cyclic, then we can assume $G = C_n$. Let $d \mid n$ be a divisor of n. Then there exist at least one subgroup H of order d, which is

$$H = \langle x^{n/d} \rangle = \{1, x^{n/d}, x^{2n/d}, \ldots, x^{(d-1)n/d}\}. \tag{2.11}$$

Hence $c_d \geq 1$, for all $d \mid n$. Supose there exists another subgroup of order d, say $H' = \langle x^k \rangle$, which is of course also cyclic, then $x^{kd} = 1 = x^n$. Hence $n \mid dk$ and $(n/d) \mid k$, i.e. $H' \subseteq H$. But since $|H'| = d = |H|$, both subgroups are equal. Hence $c_d = 1$, for all $d \mid n$ and (b) and (c) hold. Also from (2.10) we obtain the identity $n = \sum_{d|n} \varphi(d)$.

$(c) \Rightarrow (a)$: Let G be a group of order n, then by (c), $c_d \leq 1$, for all $d \mid n$. Hence by (2.10)

$$n = |G| = \sum_{d|n} c_d \varphi(d) \leq \sum_{d|n} \varphi(d) = n. \tag{2.12}$$

This shows $c_d = 1$ for all $d \mid n$ and in particular also $c_n = 1$, i.e. G is cyclic. □

As an application of Proposition 2.4 we can deduce that the multiplicative group of a finite field is cyclic. This is an important property and various modern cryptographic systems rely on this fact.

Theorem 2.5 *Let F be a field and $G = (F^\times, \cdot)$ its multiplicative group. Then any finite subgroup of G is cyclic.*

Proof: Let $H \leq G$ be a subgroup of order n. Suppose C_1 and C_2 are cyclic subgroups of H of the same cardinality, i.e. $|C_1| = |C_2| = d \mid n$. Any $x \in C_1 \cup C_2$ is a root of the polynomial $t^d - 1$, since $x^d = 1$. Since polynomials with coefficients in a field of degree d have at most d roots, we conclude that $C_1 \cup C_2$ has at most d elements. Thus $C_1 = C_2$. Therefore, H has at most one cyclic subgroup for each divisor $d \mid n$. By Proposition 2.4, H is cyclic. □

In particular, if R is a finite subring of a division ring, then it must be a field. This implies that we can generalize our result that any finite subgroup of the multiplicative group of a field is cyclic to domains of positive characteristic. Say that a domain D has characteristic $p > 0$ if $pd = 0$ for all $d \in D$. Hence $\mathbb{F}_p \simeq \mathbb{Z}1_D$ is a central subfield of D.

Corollary 2.6 *Let D be a domain of characteristic $p > 0$. Then any finite subgroup of the group of units $U(D)$ is cyclic.*

Proof: Identify $\mathbb{F}_p$ with the subring $\mathbb{Z}1_D$. Let $G \leq U(D)$ be a finite subgroup and consider the subring R of D generated by G and $\mathbb{F}_p$, i.e.

$$R = \left\{ \sum_{i=1}^{m} a_i g_i \mid a_i \in \mathbb{F}_p, g_i \in G \right\}.$$

Then $|R| \leq p^{|G|}$ is a finite subring of D and by the previous Corollary a field. By Theorem 2.5, $U(R)$ is a cyclic group and so is its subgroup G. □

Our aim is to show Jacobson's result which extends Wedderburn's Theorem from finite to algebraic division algebras over finite fields. In order to do so we will prove first several sufficient conditions for a division algebra to be commutative.

Lemma 2.7 *Let y be an element of a ring D without non-zero nilpotent elements. If y commutes with all (additive) commutators in D, then y is central.*

Proof: Note that for all $a, b, c \in D$ one has $[ab, c] = a[b, c] + [a, c]b$ and also $[a, ab] = a[a, b]$ as it is easily verified. Hence for $x, y \in D$:

$$[[x, xy], y] = [x[x, y], y] = x[[x, y], y] + [x, y]^2.$$

Thus, if y commutes with all commutators, then $[[x, xy], y] = 0 = [[x, y], y]$ and therefore $[x, y]^2 = 0$. By hypothesis $[x, y] = 0$, i.e. y commutes with x.□

Corollary 2.8 *Let D be a ring without non-zero nilpotent elements. Then D is commutative if and only if all additive commutators are central.*

Of course, a division ring is a domain and hence has no nilpotent elements. Thus if D is a non-commutative division ring and $x \in D \setminus Z(D)$, then there exists $y \in D$ with $[x, y] \neq 0$. Hence $x = x[x, y][x, y] = [x, xy][x, y]^{-1}$. This shows that any non-commutative division ring is generated as a $Z(D)$-division algebra by 1 and all of its non-zero additive commutators.

The next rather technical looking Lemma is a big step towards our goal and was first proved by I. Herstein.[2].

Lemma 2.9 (Herstein's Lemma) *Let D be a division ring of characteristic $p > 0$. Suppose $a \in D \setminus Z(D)$ is a torsion element in $D^\times$. Then there exists an additive commutator $y \in D^\times$ and some $i > 1$ such that*

$$yay^{-1} = a^i \neq a.$$

[2]Israel Nathan Herstein, 1925-1988, Biography: MacTutor

Proof: Let $\mathbb{F}_p$ be the prime subfield of $Z(D)$ and consider the field extension $\mathbb{K} = \mathbb{F}_p[a]$. Since a is a torsion element in $D^\times$, the field extension $\mathbb{K}$ is finite over $\mathbb{F}_p$ and there exists $n \geq 1$ such that $|\mathbb{K}| = p^n$. In particular, $a^{p^n} = a$. Consider the inner derivation $\delta = [a, -] : D \to D$ given by $\delta(x) = [a, x] = ax - xa$. Since $a \notin Z(D)$, $\delta \neq 0$. However, since $\mathbb{K}$ is commutative, $\delta(\mathbb{K}) = 0$. Thus δ is a $\mathbb{K}$-linear map, because $\delta(zx) = [a, zx] = [a, z]x + z[a, x] = z\delta(x)$, for all $z \in \mathbb{K}$ and $x \in D$. Our aim is now to show that δ has an eigenvector y in D. For this purpose, let $\lambda : D \to D$ denote the left multiplication by a, i.e. $\lambda(x) = ax$ and let $\rho : D \to D$ denote the right multiplication by a, i.e. $\rho(x) = xa$, for $x \in D$. Then $\delta = \lambda - \rho$. Note that λ and ρ are $\mathbb{K}$-linear and that the associativity of the multiplication implies that both maps commute, i.e. $\rho\lambda = \lambda\rho$. Furthermore, since $a^{p^n} = a$, we have that $\lambda^{p^n} = \lambda$ and $\rho^{p^n} = \rho$ and in particular,

$$\delta^{p^n} = (\lambda - \rho)^{p^n} = \sum_{i=0}^{p^n} \binom{p^n}{i} (-1)^i \lambda^{n-i} \rho^i = \lambda^{p^n} + (-1)^{p^n} \rho^{p^n} = \lambda - \rho = \delta,$$

because $p \mid \binom{p^n}{i}$ for all $0 < i < p^n$ and $(-1)^{p^n} = -1$ if p is odd. Thus δ is a root of the polynomial $t^{p^n} - t \in \mathbb{K}[t]$. As $|\mathbb{K}| = p^n$, we know that $\mathbb{K}$ is the splitting field of $t^{p^n} - t$ and therefore, $t^{p^n} - t = \prod_{b \in \mathbb{K}^\times} (t - b)t$. Since for any $\varphi \in \mathrm{End}_{\mathbb{K}}(D)$, the evaluation map

$$\Psi_\varphi : \mathbb{K}[t] \to \mathrm{End}_{\mathbb{K}}(D) \qquad \text{with } f \mapsto \Psi_\varphi(f) := f(\varphi)$$

is a ring homomorphism (with $1 \in \mathbb{K}$ being send to the identity map Id) we obtain

$$0 = \delta^{p^n} - \delta = \Psi_\delta\left(t^{p^n} - t\right) = \Psi_\delta\left(\prod_{b \in \mathbb{K}^\times} (t - b)t\right) = \prod_{b \in \mathbb{K}^\times} (\delta - b\mathrm{Id})\delta.$$

Note that the last "product" is actually a product of compositions of maps whose order is not relevant since the functions $\delta - b\mathrm{Id}$ mutually commute. As $\delta \neq 0$ and the $\prod_{b \in \mathbb{K}^\times} (\delta - b\mathrm{Id})\delta = 0$, there must exists some $b_0 \in \mathbb{K}^\times$ such that $\delta - b_0\mathrm{Id}$ is not injective. Hence, there exists $x \in D^\times$ such that $\delta(x) = b_0 x$. Spelled out, this means $(a - b_0)x = xa$. Since $b_0 \neq 0$, $a - b_0 \neq a$ and $xax^{-1} = a - b_0 \neq a$. The multiplicative order of xax^{-1} and the order of a are the same. Since $\mathbb{K}^\times$ is cyclic by Theorem 2.5, the elements xax^{-1} and a generate the same cyclic subgroup, as for each divisor there exists precisely one subgroup of that order. Hence $xax^{-1} = a^i$ for some i. In particular, $xa = a^i x$. As said before, $xax^{-1} = a - b_0 \neq a$ as $b_0 \neq 0$. Let $y = \delta(x) = [a, x]$. Then $ya = axa - xa^2 = a^{i+1}x - a^i xa = a^i[a, x] = a^i y$ and as $y = [a, x] \neq 0$, $a^i = yay^{-1}$. $\square$

Theorem 2.10 *A division ring is commutative if and only if all non-zero additive commutators have finite order.*

Proof: Clearly, if a division ring D is a field, then there are no non-zero additive commutators and the necessity holds vacuously. On the other hand, suppose that all non-zero additive commutators in D have finite order. Let $\mathbb{F} = Z(D)$ and suppose that D is non-commutative. Then there exists a non-zero non-central additive commutator, say $[x, y]$ in $D \setminus \mathbb{F}$. For any $z \in \mathbb{F}^\times$ we also have that $z[x, y] = [x, zy]$ is a non-zero non-central additive commutator. Hence by hypothesis, $[x, y]$ and $z[x, y]$ have finite order and there exists $k > 1$ such that $[x, y]^k = 1 = (z[x, y])^k$. But then $z^k = (z[x, y])^k = 1$ shows that all non-zero elements of

$\mathbb{F}$ have finite order. Thus $\mathbb{F}$ has a prime subfield of positive characteristic, say $p > 0$. By Herstein's Lemma, there exists a commutator $[u, v] \in D^\times$ such that

$$[u, v][x, y][u, v]^{-1} = [x, y]^i \neq [x, y] \tag{2.13}$$

for some $i > 0$. The multiplicative subgroup G of $D^\times$ generated by $[u, v]$ and $[x, y]$ is therefore finite, since both generators have finite order and $[u, v][x, y] = [x, y]^i[u, v]$ holds. Hence every element of G can be written as $[u, v]^a[x, y]^b$ for some a, b that are bound by the order of $[u, v]$ and the order of $[x, y]$ respectively. By Corollary 2.6, G is cyclic and hence Abelian. But then $[x, y]$ and $[u, v]$ would commute and equation (2.13) would imply $[x, y] = [x, y]^i$, contradicting Herstein's Lemma. Hence there cannot exists a non-zero non-central additive commutator. Thus all commutators are central and the commutativity of D follows by Corollary 2.8. □

Theorem 2.11 (Jacobson) *Any division algebra that is algebraic over a finite field is commutative.*

*P*roof: If $\mathbb{F}_p$ is the prime subfield of an algebraic division algebra D. Then by hypothesis any element $a \in D$ is algebraic over $\mathbb{F}_p$. The field extension $\mathbb{F}_p[a]$ is finite and hence a has finite order. By Theorem 2.10, D is commutative. □

3

The tensor product of algebras

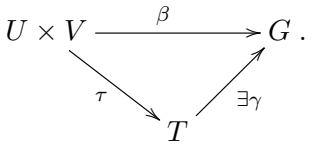
Let R be a ring, U_R a right R-module, ${}_RV$ a left R-module and T an Abelian group.

A map $\beta : U \times V \to T$ is called $\mathbb{Z}$-bilinear (or bilinear) if $\beta(u, -) : V \to T$ and $\beta(-, v) : U \to T$ are additive, i.e. $\mathbb{Z}$-linear, for all $u \in U$ and $v \in V$. The set of bilinear maps from $U \times V$ to an Abelian group T is denoted by $\mathrm{Bil}(U \times V, T)$.

A $\mathbb{Z}$-bilinear map $\beta : U \times V \to T$ is called R-balanced if

$$\beta(ur, v) = \beta(u, rv), \qquad \forall u \in U, v \in V, r \in R.$$

A pair (T, τ) of an Abelian group T and an R-balanced map $\tau : U \times V \to T$ is called a tensor product of U and V if it satisfies the universal property that for any R-balance map $\beta : U \times V \to G$ to some Abelian group G, there exist a unique $\mathbb{Z}$-linear map $\gamma : T \to G$ such that $\beta = \gamma \circ \tau$, i.e. the following diagram commutes:



Obviously, if a tensor product (T, τ) exists, then it is unique up to isomorphisms since for two pairs (T, τ) and (T', τ'), there are unique linear maps $\gamma : T \to T'$ and $\gamma' : T' \to T$ such that $\tau' = \gamma \circ \tau$ and $\tau = \gamma' \circ \tau'$. Thus $\tau = (\gamma' \circ \gamma) \circ \tau$ and $\tau' = (\gamma \circ \gamma') \circ \tau'$. By the uniqueness part of the definition of a tensor product, we have $id_T = \gamma' \circ \gamma$ and $id_{T'} = \gamma \circ \gamma'$. Hence, $\gamma : T \to T'$ is an isomorphism and $\tau' = \gamma \circ \tau$.

Tensor products exists: let $F = \mathbb{Z}^{(U \times V)}$ be the free Abelian group with basis $\{e_{u,v} \mid (u, v) \in U \times V\}$. Let N be the subgroup of F generated by all elements of the form

$$e_{u+u',v} - e_{u,v} - e_{u',v}, \qquad e_{u,v+v'} - e_{u,v} - e_{u,v'}, \qquad e_{ur,v} - e_{u,rv}$$

for all $u, u' \in U, v, v' \in V, r \in R$. Set $T := F/N$. Then the map

$$\tau : U \times V \to T, \qquad \text{with} \qquad (u, v) \mapsto e_{u,v} + N$$

is R-balanced, by the way N is generated, i.e. for instance

$$\tau(u + u', v) = e_{u+u',v} + N = e_{u,v} + e_{u',v} + N = \tau(u, v) + \tau(u', v).$$

for all $u, u' \in U, v \in V$ and moreover, for all $r \in R$:

$$\tau(ur, v) = e_{ur,v} + N = e_{u,rv} + N = \tau(u, rv).$$

Let $\beta : U \times V \to G$ be any other R-balanced map with Abelian group G. Then since homomorphisms on free objects are defined on their basis elements, we define a map $\gamma' : F \to G$ by setting $\gamma'(e_{u,v}) := \beta(u, v)$, for all $(u, v) \in U \times V$. Since β is R-balanced, the generators of the subgroup N belong to the kernel of γ' and we can lift γ' to a $\mathbb{Z}$-linear map $\gamma : T = F/N \to G$ given by

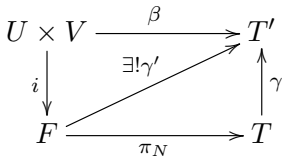
$$\gamma(e_{u,v} + K) := \beta(u, v), \qquad \forall (u, v) \in U \times V.$$

Thus, $\beta = \gamma \circ \tau$ and (T, τ) is indeed a tensor product of U and V.

Suppose there exists an R-balanced map $\beta : U \times V \to T'$ to some Abelian group T'. Then, as F is free, there exists a unique homomorphism of Abelian groups $\gamma' : F \to T$ such that

$$\gamma'(e_{u,v}) = \beta(u, v), \qquad \forall (u, v) \in U \times V.$$

As β is R-balanced, all generators of N, i.e. the elements of the form $e_{u+u',v} - e_{u,v} - e_{u',v}$, $e_{u,v+v'} - e_{u,v} - e_{u,v'}$ and $e_{ur,v} - e_{u,rv}$, belong to the kernel of γ'. Thus γ' can be lifted to a group homomorphism $\gamma : T = F/N \to T'$ and the following diagram comute:



where $i : U \times V \to F$ denotes the map $i(u, v) = e_{u,v}$. Then clearly $\beta = \gamma' i$ and $\gamma' = \gamma \pi_N$. Thus $\beta = \gamma \pi_N i = \gamma \tau$. Since γ' is unique and π_N is surjective, also γ is unique.

Since tensor products are unique up to isomorphism, we denote by $(U \otimes_R V, \tau)$ a tensor product of U and V and set $u \otimes v := \tau(u, v)$, for any $(u, v) \in U \times V$. An element of this form is called a pure tensor. Note that the elements of $U \otimes_R V$ are generated by pure tensors $u \otimes v$, but that linear combinations of the form $\sum_{i=1}^{n} u_i \otimes v_i$ are in general not unique. From the construction of the tensor product we can also deduce that

$$(u + u') \otimes v = u \otimes v + u' \otimes v, \qquad u \otimes (v + v') = u \otimes v + u \otimes v', \qquad ur \otimes v = u \otimes rv$$

holds, for all $u, u' \in U, v, v' \in V$ and $r \in R$.

Lemma 3.1 *Let R be a ring, $f : U \to U'$ a homomorphism of right R-modules and $g : V \to V'$ a homomorphism of left R-modules. Then there exists a unique homomorphism of Abelian groups*

$$f \underline{\otimes} g : U \otimes_R V \to U' \otimes_R V'$$

with $(f \underline{\otimes} g)(u \otimes v) = f(u) \otimes g(v)$. Moreover, for $f, f_1, f_2 : U \to U'$ and $g, g_1, g_2 : V \to V'$, $(f_1 + f_2) \underline{\otimes} g = f_1 \underline{\otimes} g + f_2 \underline{\otimes} g$ as well as $f \underline{\otimes} (g_1 + g_2) = f \underline{\otimes} g_1 + f \underline{\otimes} g_2$ hold.

Proof: Define $\beta : U \times V \to U' \otimes V'$ by $(u, v) \mapsto \beta(u, v) = f(u) \otimes g(v)$, which is R-balanced, because for example for $u, u_1, u_2 \in U$, $v, v_1, v_2 \in V$ and $r \in R$ we have

$$\begin{aligned}\beta(u_1 + u_2, v) = f(u_1 + u_2) \otimes g(v) = (f(u_1) + f(u_2) \otimes g(v) &= f(u_1) \otimes g(v) + f(u_2) \otimes g(v) \\ &= \beta(u_1, v) + \beta(u_2, v)\end{aligned}$$

and

$$\beta(ur, v) = f(ur) \otimes g(v) = f(u)r \otimes g(v) = f(u) \otimes rg(v) = \beta(u, rv)$$

By the universal property of the tensor product, there exists a unique group homomorphism $\gamma : U \otimes_R V \to U' \otimes_R V'$, such that

$$f(u) \otimes g(v) = \beta(u, v) = \gamma \circ \tau(u, v) = \gamma(u \otimes v), \qquad \forall (u, v) \in U \times V.$$

□

Since $f \otimes g$ is determined by f and g we have in particular $\mathrm{id}_{U \otimes V} = \mathrm{id}_U \otimes id_V$.

Lemma 3.2 *Let R be a ring U_R a right R-module and ${}_RV$ a left R-module. Then*

$$\lambda_V : R \otimes_R V \to V, \qquad \lambda_V(r \otimes v) = r \cdot v, \qquad \forall r \in R, v \in V$$

$$\rho_U : U \otimes_R R \to U, \qquad \rho_U(u \otimes r) = u \cdot r, \qquad \forall r \in R, u \in U.$$

are isomorphisms of Abelian groups.

A bimodule over R is a left R-module U such that U is also a right R-module and both scalar multiplications are compatible, i.e. $r \cdot (u \cdot r') = (r \cdot u) \cdot r'$, for all $r, r' \in R$ and $u \in U$. The most common examples we will consider stem from ring extensions: if R and S are associative untial rings and $f : R \to S$ is a ring homomorphism. Then S is an R-bimodule with scalar multiplication $r \cdot s = f(r)s$ and $s \cdot r = sf(r)$, for all $r \in R$ and $s \in S$. For instance if $S = M_n(R)$ is the $n \times n$ matrix ring with entries in R and $f : R \to M_n(R)$ is defined by $f(r) = r\mathbf{I}_n$, with $\mathbf{I}_n$ being the identity matrix of $M_n(R)$, then $M_n(R)$ is an R-bimodule. We denote an R-bimodule by ${}_RU_R$. In case R is commutative, any left R-module becomes naturally a right R-module with the same scalar multiplication and vice versa.

Given two R-bimodules ${}_RU_R$ and ${}_RV_R$, the tensor product $U \otimes_R V$ becomes naturally an R-bimodule by defining $r \cdot (u \otimes v) = ru \otimes v$ and $(u \otimes v) \cdot r = u \otimes vr$.

Proposition 3.3 *Let U, V, W be R-bimodules and $(U_i)_{i \in I}$ and $(V_i)_{i \in I}$ be families of R-bimodules.*

1. $\mathrm{Hom}_R(U \otimes_R V, W) \simeq \mathrm{Hom}_R(U, \mathrm{Hom}_R(V, W))$ *by* $f \mapsto [u \mapsto [v \mapsto f(u \otimes v)]]$.
2. $(U \otimes_R V) \otimes_R W \simeq U \otimes_R (V \otimes_R W)$ *with* $(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$.
3. $\tau_{U,V} : U \otimes_R V \simeq V \otimes_R U$ *with* $u \otimes v \mapsto v \otimes u$.
4. $\left(\bigoplus_{i \in I} U_i\right) \otimes_R V \simeq \bigoplus_{i \in I} (U_i \otimes_R V)$ *with* $(u_i)_{i \in I} \otimes v \mapsto (u_i \otimes v)_{i \in I}$
5. *If R is commutative, X resp. Y are bases for U resp. V as R-modules, then $\{x \otimes y \mid (x, y) \in X \times Y\}$ is a basis for $U \otimes_R V$ as R-module. In particular if $R = \mathbb{F}$ is a field, then* $\dim_{\mathbb{F}}(U \otimes_{\mathbb{F}} V) = \dim_{\mathbb{F}}(U) \dim_{\mathbb{F}}(V)$.

*P*roof: We leave (1-3) to the reader.

(4) For all $j \in I$ consider the inclusion respectively projection $\epsilon_j : U_j \to \bigoplus_{i\in I} U_i$ and $\pi_j : \bigoplus_{i\in I} U_i \to U_j$. Then $\mathrm{id}_{U_j} = \pi_j\epsilon_j$ as well as $\mathrm{id}_{\bigoplus_{i\in I} U_i} = \sum_{i\in I} \epsilon_i\pi_i$.

By Lemma 3.1,

$$(\pi_j \otimes \mathrm{id}_V) : \left(\bigoplus_{i\in I} U_i\right) \otimes V \to U_j \otimes V \qquad \text{and} \qquad (\epsilon_j \otimes \mathrm{id}_V) : U_j \otimes V \to \left(\bigoplus_{i\in I} U_i\right) \otimes V$$

are homomorphisms. Similarly, let $e_j : U_j \otimes V \to \bigoplus_{i\in I} U_i \otimes V$ and $p_j : \bigoplus_{i\in I} (U_i \otimes V) \to U_j \otimes V$ be the embedding and projection. Then there are homomorphisms

$$\alpha = \sum_{i\in I} e_i(\pi_i \otimes \mathrm{id}_V) : \left(\bigoplus_{i\in I} U_i\right) \otimes V \to \bigoplus_{i\in I} (U_i \otimes V)$$

and

$$\beta = \sum_{i\in I} (\epsilon_i \otimes \mathrm{id}_V)p_i : \bigoplus_{i\in I} (U_i \otimes V) \to \left(\bigoplus_{i\in I} U_i\right) \otimes V.$$

Using that $\pi_j\epsilon_i = 0 = p_je_i$ for $i \neq j$ we calculate:

$$\beta\alpha = \sum_{i,j\in I} (\epsilon_j \otimes \mathrm{id}_V)p_je_i(\pi_i \otimes \mathrm{id}_V) = \sum_{i\in I} (\epsilon_i \otimes \mathrm{id}_V)(\pi_i \otimes \mathrm{id}_V) = \left(\sum_{i\in I} \pi_i\epsilon_i\right) \otimes id_V = id_{(\bigoplus_{i\in I} U_i)\otimes V}.$$

Similarly one shows $\alpha\beta = id_{\bigoplus_{i\in I}(U_i\otimes V)}$.

(5) follows from (4), because if U and V are free, then $U \simeq \bigoplus_{x\in X} Rx$ and $V \simeq \bigoplus_{y\in Y} Ry$. Hence

$$U \otimes V \simeq \left(\bigoplus_{x\in X} Rx\right) \otimes V \simeq \bigoplus_{x\in X} (Rx \otimes V) \simeq \bigoplus_{x\in X} \bigoplus_{y\in Y} (Rx \otimes Ry) = \bigoplus_{(x,y)\in X\times Y} R\,(x \otimes y)$$

Since $Rx \simeq R \simeq Ry$, we conclude by Lemma 3.2 that

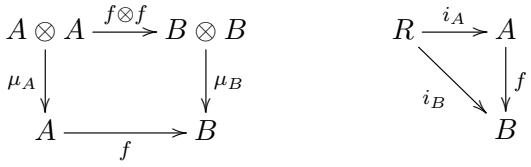
$$R(x \otimes y) = Rx \otimes Ry \simeq R \otimes Ry \simeq Ry \simeq R.$$

Hence $\{x \otimes y : (x, y) \in X \times Y\}$ is a basis for the R-module $U \otimes_R V$. □

In the sequel R will always denote a commutative, associative, unital and non-trivial ring. Recall that an R-algebra A is a ring with a ring homomorphism $i_A : R \to Z(A)$. As said before, A is naturally an R-bimodule. We usually will identify elements of R with their image in A under i_A. The multiplication $\mu : A \times A \to A$ of A is R-balanced and leads to a homomorphism $\mu : A \otimes_R A \to A$. The identity element of A is the image of the identity element of R under i_A. Hence $i_A(1) \cdot a = a = a \cdot i_A(1)$, or in a more diagrammatic language:

$$\begin{array}{ccc} A \otimes A \otimes A & \xrightarrow{\mu_A \otimes \mathrm{id}_A} & A \otimes A \\ {\scriptstyle \mathrm{id}_A \otimes \mu_A}\downarrow & & \downarrow{\scriptstyle \mu_A} \\ A \otimes A & \xrightarrow[\mu_A]{} & A \end{array} \qquad \begin{array}{ccccc} R \otimes A & \xrightarrow{i_A \otimes \mathrm{id}_A} & A \otimes A & \xleftarrow{\mathrm{id}_R \otimes \eta_A} & A \otimes R \\ & {\scriptstyle \lambda_A}\searrow & \downarrow{\scriptstyle \mu_A} & \swarrow{\scriptstyle \rho_A} & \\ & & A & & \end{array}$$

A homomorphism $f : A \to B$ of R-algebras is a ring homomorphism that satisfies $i_B = fi_A$. Equivalently this means that the following diagram commutes:



Or in other words, that f is an R-linear ring homomorphism, where A and B are considered R-modules using i_A and i_B respectively. The set of R-algebra homomorphisms from A to B is denoted by $\mathrm{Alg}_R(A, B)$.

The opposite algebra of A is denoted by A^{op} with $A = A^{op}$ as sets and

$$\mu_{A^{op}} = \mu_A \tau_{A,A}$$

where $\tau_{A,A} : A \otimes A \to A \otimes A$ sending $a \otimes b$ to $b \otimes a$ is the **flip** map. We clearly have $Z(A) = Z(A^{op})$.

Proposition 3.4 *Let A and B be R-algebras. Then $A \otimes_R B$ is an R-algebra with multiplication defined by*

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb', \qquad \forall a, a' \in A, b, b' \in B.$$

The R-algebra $A \otimes_R B$ is called the tensor product of algebras A and B.

Proof: All unadorned tensor products are taken over R, i.e. $\otimes = \otimes_R$. Let $\mu_A : A \otimes A \to A$ and $\mu_B : B \otimes B \to B$ denote the multiplications of A and B respectively. Let $\tau : B \otimes A \to A \otimes B$ be the flip map, sending $b \otimes a$ to $a \otimes b$. Then we define

$$\mu_{A\otimes B} : (A \otimes B) \otimes (A \otimes B) \to A \otimes B, \qquad \mu_{A\otimes B} := (\mu_A \otimes \mu_B)\,\tau$$

Then for any $a, a' \in A$ and $b, b' \in B$ we have

$$(a \otimes b)(a' \otimes b') = \mu_{A\otimes B}((a \otimes b) \otimes (a' \otimes b')) = (\mu_A \otimes \mu_B)(a \otimes a' \otimes b \otimes b') = aa' \otimes bb'.$$

The associativity condition hold because A and B are associative. The identity of $A \otimes B$ is given by $1_A \otimes 1_B$ and $A \otimes B$ becomes an R-algebra via $i_{A\otimes B} : R \to A \otimes B$ given by $i_{A\otimes B}(r) = i_A(r) \otimes i_B(r)$, for all $r \in R$. □

Some comments are in place. First of all, if $B = R$, then $A \otimes_R R \simeq A$ as R-algebras, by the isomorphism $A \otimes_R R \to A$ with $a \otimes r \mapsto ai_A(r)$. Similarly $R \otimes_R A \simeq A$ as R-algebras. Moreover if $a \in Z(A)$ and $b \in Z(B)$, then $a \otimes b \in Z(A \otimes B)$.

The tensor product of algebras has also the following universal property:

Proposition 3.5 *Let A, B, C be R-algebras, $f : A \to C$ and $g : B \to C$ be R-algebra homomorphisms. If $f(a)g(b) = g(b)f(a)$ for all $a \in A$ and $b \in B$, then there exists a unique R-algebra homomorphism*

$$f \underline{\otimes} g : A \otimes B \to C, \qquad \textit{such that} \qquad f \underline{\otimes} g(a \otimes b) = f(a)g(b), \qquad \forall a \in A, b \in B.$$

Proof: By Lemma 3.1, there exists an R-linear map $f \otimes g : A \otimes B \to C \otimes C$, such that $f \otimes g(a \otimes b) = f(a) \otimes g(b)$. Let μ_C denote the multiplication of C, then $f \underline{\otimes} g := \mu_C(f \otimes g)$ is the homomorphism we are looking for. since $f(a)$ and $g(b)$ commute in C, we obtain for any $a, a' \in A$ and $b, b' \in B$:

$$f \underline{\otimes} g(aa' \otimes bb') = f(aa')g(bb') = f(a)g(b)f(a')g(b') = (f \underline{\otimes} g(a \otimes b)) \left(f \underline{\otimes} g(a' \otimes b')\right)$$

□

One important case is when we tensor an R-algebra A with a matrix ring $M_n(R)$, which will produce the matrix ring $M_n(A)$ over A.

Lemma 3.6 *Let A be any R-algebra and $n \geq 1$. Then $A \otimes M_n(R) \simeq M_n(A)$ as R-algebras.*

Proof: The map $f : A \to M_n(A)$ with $f(a) = a\mathbf{I}_n$, for all $a \in A$ is an R-algebra homomorphism. Denote by E_{ij} the matrix unit of $M_n(A)$, which is a basis of $M_n(A)$ as (left) A-module. Then there exists an R-algebra homomorphism $g : M_n(R) \to M_n(A)$ sending rE_{ij} to $i_A(r)E_{ij}$, for any $r \in R$ and $1 \leq i, j \leq n$. In order to simplify notation, we will identify r with $i_A(r)$.[1] Note that the images of f and g commute, because $f(a)g(rE_{ij}) = arE_{ij} = rE_{ij}a = g(rE_{ij})f(a)$. By Proposition 3.5, there exists an R-algebra homomorphism such that $f \underline{\otimes} g : A \otimes M_n(R) \to M_n(A)$ with

$$f \underline{\otimes} g \left(\sum_{i,j} a \otimes r_{ij}E_{ij} \right) = \sum_{i,j} ar_{ij}E_{ij}.$$

Similarly, we can define an R-algebra homomorphism $h : M_n(A) \to A \otimes M_n(R)$ by

$$h \left(\sum_{i,j} a_{ij}E_{ij} \right) = \sum_{i,j} a_{ij} \otimes E_{ij}.$$

Then $h(f \underline{\otimes} g) \left(\sum_{i,j} a \otimes r_{ij}E_{ij} \right) = \sum_{i,j} ar_{ij} \otimes E_{ij} = \sum_{i,j} a \otimes r_{ij}E_{ij}$ and $(f \underline{\otimes} g)h \left(\sum_{i,j} a_{ij}E_{ij} \right) = \sum_{i,j} a_{ij}E_{ij}$ shows that h is the inverse of $f \underline{\otimes} g$. □

Note that the consequence of the last Lemma is that for any $n, m \geq 1$:

$$M_n(R) \otimes M_m(R) \simeq M_n(M_m(R)) = M_{nm}(R).$$

Note that for any R-algebra A and R-module M the tensor product $M \otimes_R A$ becomes an A-bimodule, by setting $a(m \otimes a') := m \otimes aa'$ and $(m \otimes a')a = m \otimes a'a$, for all $a, a' \in A$ and $m \in M$.

Proposition 3.7 *Let R be a commutative ring and S a commutative R-algebra.*

1. *$A \otimes_R S$ is an S-algebra, for any R-algebra A.*
2. *Any S-algebra A is also an R-algebra.*

[1] If R is not a field and i_A is not injective, then there might exist some non-zero element r in the kernel of i_A and $i_A(r) = 0$ while $r \neq 0$.

3. For any R-algebra A and S-algebras B we have a group isomorphism:

$$\mathrm{Alg}_S(A \otimes_R S, B) \simeq \mathrm{Alg}_R(A, B), \qquad f \mapsto \widetilde{f}(a) = f(a \otimes 1), \forall a \in A.$$

4. For any R-algebras A, B we have an isomorphism of S-algebras

$$(A \otimes_R B) \otimes_R S \simeq (A \otimes_R S) \otimes_S (B \otimes_R S), \qquad (a \otimes b) \otimes s \mapsto (a \otimes s) \otimes (b \otimes 1_S)$$

Proof: 1. If $i_S : R \to S$ and $i_A : R \to Z(A)$ are the ring homomorphisms, turning S and A into R-algebras, then $i_{A\otimes S} = i_A \underline{\otimes} i_S : R \to Z(A \otimes S)$ turns $A \otimes S$ into an R-algebra.

2. Clearly, if A is an S-algebra with $i_A : S \to Z(A)$, then $i_A \circ i_S$ turns A into an R-algebra.

3. If $f : A \otimes_R S \to B$ is an S-algebra homomorphism and $\widetilde{f}(a) = f(a \otimes 1)$, then $\widetilde{f}$ is clearly additive and for any $a, a' \in A$ and $r \in R$ we have

$$\widetilde{f}(aa') = f(aa' \otimes 1) = f(a \otimes 1)f(a' \otimes 1) = \widetilde{f}(a)\widetilde{f}(a')$$

as well as

$$\widetilde{f}(ra) = f(ra \otimes 1) = f(a \otimes r) = rf(a \otimes 1) = r\widetilde{f}(a)$$

where we use that the tensor product is taken over R and that the R-module action on A and S is determined by i_A and i_S respectively.

The inverse map associates to an R-algebra homomorphism $g : A \to B$ the R-algebra homomorphism $g \underline{\otimes} i_S : A \otimes_R S \to B$. Then for all $f \in \mathrm{Alg}_S(A \otimes_R S, B)$ and $a \in A$, $s \in S$:

$$(\widetilde{f} \otimes i_S)(a \otimes s) = f(a \otimes 1)i_S(s) = sf(a \otimes 1) = f(a \otimes s),$$

where the last equation uses that f is S-linear and acts on the last tensorand. Conversely if $g \in \mathrm{Alg}_R(A, B)$, then for any $a \in A$:

$$\widetilde{g \otimes i_S}(a) = (g \underline{\otimes} i_S)(a \otimes 1) = g(a).$$

4. The map $(A \otimes_R B) \times S \to (A \otimes_R S) \otimes_S (B \otimes_R S)$ given by $(a \otimes b, s) \mapsto (a \otimes s) \otimes (b \otimes 1)$ is S-balanced and shows that there exists a unique group homomorphism

$$\psi : (A \otimes_R B) \otimes_R S \to (A \otimes_R S) \otimes_S (B \otimes_R S), \qquad \psi((a \otimes b) \otimes s) = (a \otimes s) \otimes (b \otimes 1).$$

For elements $a, a' \in A$, $b, b' \in B$ and $s, s' \in S$ we calculate:

$$\begin{aligned} \psi((a \otimes b) \otimes s)((a' \otimes b') \otimes s')) &= \psi((aa' \otimes bb') \otimes ss') \\ &= (aa' \otimes ss') \otimes_S (bb' \otimes 1) \\ &= ((a \otimes s) \otimes_S (b \otimes 1))((a' \otimes s') \otimes_S (b' \otimes 1)) \\ &= \psi((a \otimes b) \otimes s)\psi((a' \otimes b') \otimes s'). \end{aligned}$$

It is also not difficult to see that ψ is R-linear. Hence ψ is an R-algebra homomorphism.

The inverse of ψ is given by

$$\psi^{-1}((a \otimes s) \otimes_S (b \otimes s')) = (a \otimes b) \otimes ss'.$$

Its existence can be shown again by the universal property of the tensor product. □

By passing from A to $A \otimes_R S$, one speaks of extension of scalars, while restricting the scalar multiplication and viewing an S-algebra as an R-algebra is called restriction of scalars.

Central Algebras

From now on we will reduce to algebras over a field K and all unadorned tensor products are taken over K, i.e. $\otimes = \otimes_K$. Recall that a K-algebra A is called central if $Z(A) = K$, where we now stop mentioning the homomorphism $i_A : K \to Z(A)$ and identify elements of K with elements of A. We have seen already that $Q(a, b; K)$ if $a \neq 0$ or $b \neq 0$ is a central K-algebra. Similarly, $Z(M_n(K)) = K\mathbf{I}_n \simeq K$ shows that $M_n(K)$ is a central K-algebra.

We want to show that for any central K-algebras A and B, also $A \otimes B$ is a central K-algebra. In order to do so, recall that $\mathrm{Cent}_A(M) = \{a \in A : am = ma, \forall m \in M\}$ is the centralizer subalgebra of a subset $M \subseteq A$. The centralizer is easily seen to be an $\mathbb{F}$-subalgebra of A.

Lemma 3.8 *Let A and B be K-algebras with subsets $M \subseteq A$ and $N \subseteq B$.*

1. $\mathrm{Cent}_{A\otimes B}(M \otimes N) = \mathrm{Cent}_A(M) \otimes \mathrm{Cent}_B(N)$.
2. $Z(A \otimes B) = Z(A) \otimes Z(B)$
3. *If A and B are central K-algebras, then $A \otimes B$ is a central K-algebra.*

Proof: Clearly (3) follows from (2) and (2) follows from (1) for $M = A$ and $N = B$. Hence we only need to prove (1). Without loss of generality we can assume that M and N are $\mathbb{F}$-subspaces of A and B respectively, since the centralizer of a subset is equal to the centralizer of the subspace generated by that subset. Hence $M \otimes N$ is a subspace of $A \otimes B$. Furhtermore, we can assume that $1_A \in M$ and $1_B \in N$, since both elements are central and will not change the centralizers. Clearly $\mathrm{Cent}_A(M) \otimes \mathrm{Cent}_B(N) \subseteq \mathrm{Cent}_{A\otimes B}(M \otimes N)$. Let $0 \neq z = \sum_{i=1}^{n} x_i \otimes y_i \in \mathrm{Cent}_{A\otimes B}(M \otimes N)$. If the $x_1, \ldots, x_n$ were linearly dependent, then we could write some x_i as linear combination of the others, say $x_n = \sum_{i=1}^{n-1} \lambda_i x_i$ and $\lambda_i \in \mathbb{F}$. Hence $z = \sum_{i=1}^{n-1} x_i \otimes (y_i - \lambda_i y_n)$ is a representation of z with fewer summands. Hence we can assume that n is minimal and that the elements $\{x_1, \ldots, x_n\}$ are linearly independent.

For any $v \in N$ we have $1 \otimes v \in M \otimes N$ and $z(1 \otimes v) = (1 \otimes v)z$. But then

$$0 = z(1 \otimes v) - (1 \otimes v)z = \sum_{i=1}^{n} x_i \otimes (y_i v - v y_i).$$

As the x_i were linearly independent we deduce, for instance by extending $\{x_1, \ldots, x_n\}$ to a basis of A and projecting onto the x_i-component, that $y_i v = v y_i$, for all i. Thus $y_i \in \mathrm{Cent}_B(N)$.

Without loss of generality, we might assume that $\{y_1, \ldots, y_m\}$ is a maximal linearly independent subset of $\{y_1, \ldots, y_n\}$ and z can be represented as $z = \sum_{i=1}^{m} x_i' \otimes y_i$ for some x_i'. A similar argument as the one above, forces now the x_i' to belong to the centralizer of M in A, while the $y_1, \ldots, y_m$ are still in the centralizer of N in B. Hence we have shown $z \in \mathrm{Cent}_A(M) \otimes \mathrm{Cent}_B(N)$ and have proven (1). □

Corollary 3.9 *Let $K \leq L$ be a field extension. If A is a central K-algebra, then $A \otimes_K L$ is a central L-algebra.*

Simple Algebras

Recall that a ring is simple if the only ideals are the trivial ones. We know already that $M_n(A)$ is a simple ring whenever A is simple. Hence we conclude that $A \otimes M_n(K) \simeq M_n(A)$ is a simple K-algebra whenever A is a simple K-algebra. We will show under which conditions the tensor product of two simple algebras is simple. Note that this need not be true in general and for tensor products of fields, there is a connection with inseparable field extensions.

Let $\mathbb{F}_2$ be the finite field with 2 elements and consider the polynomial ring $R = \mathbb{F}_2[t]$. The polynomials in $x = t^2$ form a subring of R denoted by $S = \mathbb{F}_2[x]$. Consider their fraction fields $L = \mathrm{Frac}(R) = \mathbb{F}_2(t)$ and $K = \mathrm{Frac}(S) = \mathbb{F}_2(x)$. Then L is a finite field extension of K and $L = K(t)$ with $t^2 = x$. The element $t \otimes 1 - 1 \otimes t \in L \otimes_K L$ is nilpotent, because

$$(t \otimes 1 - 1 \otimes t)^2 = t^2 \otimes 1 - 2t \otimes t + 1 \otimes t^2 = 2x \otimes 1 = 0.$$

Thus the ideal $I = \langle t \otimes 1 - 1 \otimes t \rangle \leq L \otimes_K L$ is a proper non-zero nilpotent ideal and $L \otimes L$ is not simple. The problem with this example is that L/K is not a separable field extension.

Let us denote the algebraic closure of a field K by $\overline{K}$. Let $K \subseteq L$ be a field extension. An element $a \in L$ is called a separable element over K if its minimal polynomial $\mathrm{minpoly}_K(a)$ has only simple roots, i.e. it is irreducible in $\overline{K}[x]$. A field extension $K \subseteq L$ is called a separable extension if every element of L is separable over K.

Theorem 3.10 *Let K be a field with algebraic closure $\overline{K}$ and L a finite dimensional simple field extension of K. Then L is separable over K if and only if $\overline{K} \otimes_K L$ is a semisimple $\overline{K}$-algebra.*

Proof: Let $L = K(a)$, for some algebraic element a and minimal polynomial $f = \mathrm{minpoly}_K(a)$ with $n = \deg(f)$. Then $1, a, \cdots, a^{n-1}$ form a basis of $L \simeq K[x]/\langle f \rangle$. Consider the homomorphism

$$\phi : \overline{K} \otimes_K L \longrightarrow \overline{K}[x]/\langle f \rangle \qquad \text{with} \qquad \phi\left(\sum_{i=0}^{n-1} \alpha_i \otimes a^i\right) = \sum_{i=0}^{n-1} \alpha_i \overline{x}^i$$

where $\overline{x} = x + \langle f \rangle$ denotes the image of x under the canonical projection. Since the powers $1, a, a^2, \cdots, a^{n-1}$ form a basis of L, ϕ is well-defined. Since $1, \overline{x}, \cdots, \overline{x}^{n-1}$ are linearly independent, ϕ is injective and hence an isomorphism of K-algebras as

$$\dim_{\overline{K}}(\overline{K} \otimes L) = \dim_{\overline{K}}(\overline{K}[x]/\langle f \rangle) = n.$$

Over $\overline{K}$, f decomposes into linear factors, let's say

$$f = p_1^{m_1} \cdots p_k^{m_k}$$

where $\deg(p_i) = 1$ and $m_i \geq 1$. By the Chinese remainder theorem we have an isomorphism of algebras:

$$\overline{K} \otimes_K L \simeq \overline{K}[x]/\langle f \rangle \simeq \prod_{i=1}^{k} \overline{K}[x]/\langle p_i^{m_i} \rangle$$

Note that $\overline{K}[x]/\langle p_i^{m_i} \rangle$ contains a nilpotent element if and only if $m_i > 1$ if and only if a is separable over K. $\square$

A K-algebra A is called a separable algebra if $A \otimes L$ is semisimple, for any field extension L of K. In particular, any separable algebra is semisimple itself.

Let us recall that if A is an K-algebra, its dual algebra A^{op} is also an K-algebra, since $i_A : K \to Z(A) = Z(A^{op})$. Hence $A \otimes A^{op}$ is an K-algebra as well.

Let λ_a and ρ_b denote the left and right action of $a \in A$ on A respectively. Then the map $A \times A^{op} \to \mathrm{End}({}_K A)$ with $(a, b) \mapsto \lambda_a \circ \rho_b$ is K-balanced and yields the existence of an algebra homomorphism

$$A \otimes A^{op} \to \mathrm{End}({}_K A), \qquad a \otimes b \mapsto \lambda_a \circ \rho_a.$$

This shows that A becomes naturally a (left) $A \otimes A^{\overline{\phi}}$-module by setting

$$(a \otimes b) \cdot x = \lambda_a \circ \rho_b(x) = axb, \qquad \forall a, b, x \in A.$$

Hence (twosided) ideals of A corresponds to $A \otimes A^{op}$-submodules of A and A is a simple algebra if and only if A is a simple $A \otimes A^{op}$-module.

Let $B \leq A$ be a subalgebra of A. Then A is also an $A \otimes B^{op}$-module, $B \otimes A^{op}$-module and $B \otimes B^{op}$-module. The ring of endomorphisms $\mathrm{End}({}_{B \otimes A^{op}} A)$ is a K-algebra where each $\lambda \in K$ is identified with $\lambda \mathrm{id}_A$.

Recall that the centralizer of B in A is defined as $\mathrm{Cent}_A(B) = \{a \in A \mid ab = ba, \forall b \in B\}$.

Lemma 3.11 *Let $B \leq A$ be a subalgebra of A. Then*

$$\Phi : \mathrm{End}({}_{B \otimes A^{op}} A) \longrightarrow \mathrm{Cent}_A(B), \qquad f \mapsto \Phi(f) := f(1)$$

is an isomorphism of K-algebras with inverse given by $\Phi^{-1}(x) = \lambda_x$, for all $x \in \mathrm{Cent}_A(B)$.

Proof: Let $f \in \mathrm{End}({}_{B \otimes A^{op}} A)$ and $b \in B$. Then

$$bf(1) = (b \otimes 1)f(1) = f(\lambda_b(1)) = f(b) = f(\rho_b(1)) = (1 \otimes b)f(1) = f(1)b.$$

This means $\Phi(f) = f(1) \in \mathrm{Cent}_A(B)$.

Furthermore, for $f, g \in \mathrm{End}({}_{B \otimes A^{op}} A)$ we calculate:

$$\Phi(f \circ g) = (f \circ g)(1) = f(g(1)) = f(\rho_{g(1)}(1)) = (1 \otimes g(1))f(1) = f(1)g(1)$$

Since Φ is clearly an K-linear map it is a K-algebra homomorphism.

For any $f \in \mathrm{End}({}_{B \otimes A^{op}} A)$ and $a \in A$ we have

$$\lambda_{\Phi(f)}(a) = \Phi(f)a = (1 \otimes a)f(1) = f(\rho_a(1)) = f(a).$$

Thus $\lambda_{\Phi(f)} = f$.

Furthermore, if $x \in \mathrm{Cent}_A(B)$, we have first of all that $\lambda_a \in \mathrm{End}({}_{B \otimes A^{op}} A)$, because for any $a \in A$ and $b \otimes a' \in B \otimes A^{op}$:

$$\lambda_x((b \otimes a')a) = xbaa' = bxaa' = (b \otimes a')\lambda_x(a)$$

shows that $\lambda_x \in \mathrm{End}({}_{B \otimes A^{op}} A)$. The associativity of A shows also that $\lambda_{x'} \circ \lambda_x = \lambda_{x'x}$, for all $x, x' \in \mathrm{Cent}_A(B)$ and therefore $\lambda : \mathrm{Cent}_A(B) \to \mathrm{End}({}_{B \otimes A^{op}} A)$ is a homomorphism of K-algebras, that satisfies $\Phi(\lambda_x) = x$, i.e. $\Phi^{-1} = \lambda_{|_{\mathrm{Cent}_A(B)}}$. $\square$

Analogously one proves the isomorphisms of K-algebras

$$\mathrm{End}({}_{A\otimes B^{op}}A) \simeq \mathrm{Cent}_A(B)^{op}, \qquad \text{and} \qquad \mathrm{End}({}_{A\otimes A^{op}}A) \simeq \mathrm{Cent}_A(A) = Z(A),$$

where an endomorphism f is send to $f(1)$.

Furthermore, A is also naturally a left B^e-module and there exists an isomorphism of K-vector spaces given in the same way, namely by evaluating f at 1:

$$\mathrm{Hom}_{B\otimes B^{op}}(B, A) \simeq \mathrm{Cent}_A(B).$$

Lemma 3.12 *Let $B \leq A$ be a subalgebra of a K-algebra A. If B is a central simple K-algebra, then the linear map*

$$m : \mathrm{Cent}_A(B) \otimes B \longrightarrow A, \qquad x \otimes b \mapsto xb$$

is an injective homomorphism of K-algebras.

Proof: To ease the notation, let us write $B^e := B \otimes B^{op}$.

The linear map m exists, because the images of $\lambda : \mathrm{Cent}_A(B) \to A$ and the embedding of B into A commute. As K-vector spaces we have

$$\mathrm{Cent}_A(B) \simeq \mathrm{Hom}({}_{B^e}B, A)$$

by sending $x \in \mathrm{Cent}_A(B)$ to λ_x. Hence we get a linear map

$$m' : \mathrm{Hom}_{B^e}(B, A) \otimes B \simeq \mathrm{Cent}_A(B) \otimes B \longrightarrow A, \qquad f \otimes b \mapsto f(1) \otimes b \mapsto f(1)b = f(b),$$

which is the evaluation map. In particular m is injective if and only if m' is injective.

By hypothesis B is a simple algebra, hence B is a simple B^e-module and we consider the B^e-submodule of A:

$$M = \sum \{U \leq A \mid U \simeq B \text{ as } B^e\text{-submodule }\}.$$

Since a sum of isomorphic simple modules is semisimple and a direct sum of some of these simples:

$$M = \bigoplus_{i\in I} E_i, \qquad \text{with} \qquad E_i \simeq B \text{ as } B^e - \textit{module}.$$

Since B is a central K-algebra, we have for all $i \in I$:

$$\mathrm{Hom}_{B^e}(B, E_i) \simeq \mathrm{End}({}_{B^e}B) \simeq Z(B) = K$$

Moreover, the image of any non-zero $f \in \mathrm{Hom}_{B^e}(B, A)$ is isomorphic to B as B^e-module. Hence $\mathrm{Im}(f) \subseteq M$ and

$$\mathrm{Hom}_{B^e}(B, A) = \mathrm{Hom}_{B^e}(B, M) = \mathrm{Hom}_{B^e}\left(B, \bigoplus_{i\in I} E_i\right) = \bigoplus_{i\in I} \mathrm{Hom}_{B^e}(B, E_i) \simeq K^{(I)}.$$

For each $i \in I$ choose an isomorphism $\varphi_i \in \mathrm{Hom}_{B^e}(B, E_i)$. Then $\mathrm{Hom}_{B^e}(B, E_i) = K\varphi_i$ and $\{\varphi_i \mid i \in I\}$ forms a basis of $\mathrm{Hom}_{B^e}(B, A)$. In particular, any element of $\mathrm{Hom}_{B^e}(B, A) \otimes B$ can be uniquely written as $\gamma = \sum_{i\in I} \varphi_i \otimes b_i$ for some $b_i \in B$. Thus if $m'(\gamma) = 0$, then

$$0 = m'(\gamma) = \sum_{i\in I} \varphi_i(b_i) \in \bigoplus_{i\in I} E_i \qquad \Rightarrow \qquad \varphi_i(b_i) = 0, \forall i \in I$$

As the φ_i were isomorphisms, $b_i = 0$ for all $i \in I$ and hence $\gamma = 0$. This shows that m' and thus m is injective. $\square$

The following technical Lemma is also needed for the next Theorem:

Lemma 3.13 *Let $f : U \to U'$ and $g : V \to V'$ be linear maps of vector spaces. If f and g are surjective, then $f \underline{\otimes} g : U \otimes V \to U' \otimes V'$ is surjective and*

$$\mathrm{Ker}(f \underline{\otimes} g) = \mathrm{Ker}(f) \otimes V + U \otimes \mathrm{Ker}(g).$$

Proof: Clearly, if f and g are surjective, then so is $f \underline{\otimes} g$. For $u \in \mathrm{Ker}(f)$, $v \in \mathrm{Ker}(g)$ and $a \in V, b \in U$ one has

$$(f \underline{\otimes} g)(u \otimes a + b \otimes v) = 0 \cdot g(a) + g(b) \cdot 0 = 0_{U' \otimes V'}.$$

Hence $J := \mathrm{Ker}(f) \otimes V + U \otimes \mathrm{Ker}(g) \subseteq \mathrm{Ker}(f \underline{\otimes} g)$ and $f \underline{\otimes} g$ factors through J, i.e. there exists a (surjective) linear map $\phi : (U \otimes V)/J \to U' \otimes V'$ such that $f \underline{\otimes} g = \phi \pi_J$, where π_J is the canonical projection. Define a map from $U' \otimes V' \to (U \otimes V)/J$ as follows: For each pair $(x, y) \in U' \times V'$ choose a pair $(u, v) \in U \times V$ such that $f(u) = x$ and $g(v) = y$ and define the map $\psi : U' \times V' \to (U \otimes V)/J$ by $\psi(x, y) = u \otimes v + J$. This map is independent of the choice we made, because if (u_2, v_2) is another pair such that $f(u_2) = x$ and $g(v_2) = y$, then

$$u \otimes v - u_2 \otimes v_2 = (u - u_2) \otimes v + u_2 \otimes (v - v_2) \in \mathrm{Ker}(f) \otimes V + U \otimes \mathrm{Ker}(g) = J.$$

Since this map is balanced, by the universal property of the tensor product, there exists a (unique) map $\psi : U' \otimes V' \to (U \otimes V)/J$, such that $\psi(x \otimes y) = u \otimes v$ if and only if $f(u) = x$ and $g(v) = y$. This map satisfies $\pi_J = \psi(f \underline{\otimes} g)$. Thus $\mathrm{Ker}(f \otimes g) = \mathrm{Ker}(\pi_J) = J$. $\square$

Theorem 3.14 *Let A and B be K-algebras. If B is central simple then the following function is a bijection*

$$\{ \textit{ ideals of } A\} \longrightarrow \{\textit{ideals of } A \otimes B\} \qquad I \mapsto I \otimes B$$

whose inverse function is given by

$$\{ \textit{ ideals of } A \otimes B\} \longrightarrow \{\textit{ideals of } A\} \qquad J \mapsto \{a \in A \mid a \otimes 1 \in J\}.$$

Proof: If I is an ideal of A, then it is easy to see that $I \otimes B$ is also an ideal of $A \otimes B$. And if $J \leq A \otimes B$ is an ideal and $I = \{a \in A \mid a \otimes 1 \in J\}$, then I is a subspace of A, because for any $a, a' \in I$ also $(a + a') \otimes 1 = a \otimes 1 + a' \otimes 1 \in J$, thus $a + a' \in I$. And for $x \in I$ and $a, a' \in A$ one has $axa' \otimes 1 = (a \otimes 1)(x \otimes 1)(a' \otimes 1) \in J$, i.e. $axa' \in I$.

Starting with an ideal I of A, forming $I \otimes B$ and looking at $I' = \{a \in A \mid a \otimes 1 \in I \otimes B\}$, we see $I \subseteq I'$ and choosing a basis of B that contains 1, we can easily also conclude $I = I'$.

Let J be an ideal of $A \otimes B$ and $I = \{a \in A : a \otimes 1 \in J$. If $J = A \otimes B$, then $1 \otimes 1 \in J$ and hence $1 \in I$ and $I = A$. Suppose $J \neq A \otimes B$, consider $T = (A \otimes B)/J$ and the following homomorphisms of K-algebras:

$$\begin{aligned} \pi : A \otimes B &\to T, & a \otimes b &\mapsto a \otimes b + J \\ \epsilon_1 : A &\to T, & a &\mapsto a \otimes 1 + J \\ \epsilon_2 : B &\to T, & b &\mapsto 1 \otimes b + J \end{aligned}$$

Since B is simple and $J \neq A \otimes B$, we conclude that ϵ_2 is injective. The images of the maps ϵ_1 and ϵ_2 are subalgebras of T. Denote by $A' = \epsilon_1(A)$ and $B' = \epsilon_2(B)$. Since ϵ_2 is injective, B' is a central simple K-algebra. Consider also the algebra homomorphism

$$\epsilon_1 \underline{\otimes} \epsilon_2 : A \otimes B \to A' \otimes B'.$$

By Lemma 3.13 and using that ϵ_2 is injective we have

$$\mathrm{Ker}(\epsilon_1 \underline{\otimes} \epsilon_2) = \mathrm{Ker}(\epsilon_1) \otimes B = I \otimes B.$$

Moreover, $A' \subseteq \mathrm{Cent}_T(B')$, because

$$\epsilon_1(a)\epsilon_2(b) = a \otimes b + J = \epsilon_2(b)\epsilon_1(a),$$

for all $a \in A$ and $b \in B$. Hence by Lemma 3.11, the multiplication map $m : A' \otimes B' \to T$ is injective. Note that $\pi = m \circ (\epsilon_1 \underline{\otimes} \epsilon_2)$. Hence

$$J = \mathrm{Ker}(\pi) = \mathrm{Ker}(m \circ (\epsilon_1 \underline{\otimes} \epsilon_2)) = \mathrm{Ker}((\epsilon_1 \underline{\otimes} \epsilon_2)) = I \otimes B.$$

□

The correspondence Theorem 3.14 implies that if B is central simple, then $A \otimes B$ is simple if and only if A is simple. Together with Lemma 3.8 we can summarize our findings as follows:

Corollary 3.15 *Let B be a central simple K-algebra (CSA) and A a K-algebra.*

1. *$A \otimes B$ is a simple K-algebra if and only if A is a simple K-algebra.*
2. *$Z(A \otimes B) = Z(A) \otimes Z(B) \simeq Z(A)$.*
3. *$A \otimes B$ is a central simple K-algebra if and only if A is a central simple K-algebra.*

An immediate consequence of Corollary 3.15 we can prove that $A \otimes A^{op}$ is isomorphic to a full matrix ring over K, if A is a finite dimensional central simple K-algebra.

Corollary 3.16 *If A is an n-dimensional central simple K-algebra A, then $A \otimes_K A^{op} \simeq M_(K)$.*

Proof: Let $\psi : A \otimes_K A^{op} \to \mathrm{End}(_K R) \simeq M_n(K)$ be given by $a \otimes b \mapsto \lambda_a \circ \rho_b$. Since A is central simple, A^{op} is central simple and hence $A \otimes A^{op}$ is central simple by Corollary 3.15. Thus ψ is injective and as $\dim A \otimes A^{op} = n^2 = \dim M_n(K)$ it must be also surjective. □

We will strength now Lemma 3.12.

Corollary 3.17 *Let $B \leq A$ be a subalgebra of a K-algebra A. If B is a finite dimensional central simple K-algebra, then the linear map*

$$m : \mathrm{Cent}_A(B) \otimes B \longrightarrow A, \qquad x \otimes b \mapsto xb$$

is an isomorphism of K-algebras.

Proof: We have already seen in Lemma 3.12 that m is injective and that its image is equal to the sum of all simple B^e-submodules of A that are isomorphic to B, where $B^e = B \otimes B^{op}$. By Corollary 3.16, $B^e \simeq M_n(K)$, with $n = \dim B$. Thus B^e is a semisimple, simple K-algebra, any left B^e-module is semisimple and a direct sum of a unique (up to isomorphism) simple B^e-module. Hence A is isomorphic toa direct sum of copies of B as left B^e-module and m is surjective. □

Corollary 3.18 (Double Centralizer Theorem) *Let A be a finite dimensional central simple K-algebra with subalgebra $B \leq A$. If B is a central simple algebra, then*

1. $\mathrm{Cent}_A(B)$ *is central simple and*
2. $\mathrm{Cent}_A(\mathrm{Cent}_A(B)) = B$.

Proof: By Corollary 3.17, the multiplication $m : \mathrm{Cent}_A(B) \otimes B \simeq A$ is an isomorphism. Hence $\mathrm{Cent}_A(B) \otimes B$ is simple and central and therefore also $\mathrm{Cent}_A(B)$ by Corollary 3.15.

Moreover, $n = \dim A = \dim \mathrm{Cent}_A(B) \dim B$.

Applying Corollary 3.17 to the subalgebra $\mathrm{Cent}_A(B)$, we also get that $n = \dim A = \dim \mathrm{Cent}_A(\mathrm{Cent}_A(B)) \dim \mathrm{Cent}_A(B)$. Hence $\dim B = \dim \mathrm{Cent}_A(\mathrm{Cent}_A(B))$. Now the result follows as $B \subseteq \mathrm{Cent}_A(\mathrm{Cent}_A(B))$. □

4

The Brauer group of a field

We have seen that in general the tensor product of division rings is not necessarily a division ring. If $K \leq L$ is an inseperable field extension, then we have seen that $\overline{K} \otimes_K L$ contains a nilpotent element and hence cannot be a division algebra. But even for separable field extensions the tensor product of two fields might not be a division algebra. For example, $\mathbb{Q}(\imath) \otimes_{\mathbb{Q}} \mathbb{Q}(\imath)$ contains zero divisors:

$$(\imath \otimes 1 + 1 \otimes \imath)(\imath \otimes 1 - 1 \otimes \imath) = (-1) \otimes 1 - 1 \otimes (-1) = 0.$$

More generally, if D is any K-algebra that contains an element $a \in D \setminus K$ satisfying $a^n = 1$, for some even number $n \geq 1$, then

$$\begin{aligned}(a \otimes 1 + 1 \otimes a)\left(\sum_{i=0}^{n-1}(-1)^i a^i \otimes a^{n-i}\right) &= \sum_{i=0}^{n-1}(-1)^i a^{i+1} \otimes a^{n-i} + \sum_{i=0}^{n-1}(-1)^i a^i \otimes a^{n+1-i} \\ &= (-1)^{n-1} 1 \otimes a + 1 \otimes a = 0.\end{aligned}$$

On the other hand, the tensor product of two central simple algebras is central simple. Hence if D and D' are finite dimensional central division algebras, then their matrix rings $M_n(D) \simeq D \otimes M_n(K)$ and $M_m(D')$ are finite dimensional central simple K-algebras and so is their tensor product $M_n(D) \otimes M_m(D')$. What is the relation between finite dimensional central simple algebras and division algebras? The short answer is given by the Wedderburn-Artin Theorem. The uniqueness of that Theorem is important.

Lemma 4.1 *Let D and E be two division algebras such that $M_n(D) \simeq M_m(E)$ as rings, for some $n, m \geq 1$. Then $n = m$ and $D \simeq E$ as rings.*

Proof: Let $A = M_n(D)$, $B = M_m(E)$ and $f : A \to B$ an isomorphism of rings. The first column of $A = M_n(D)$ is the unique (up to isomorphism) simple left A-module M and $D \simeq \mathrm{End}_A(M)^{op}$. Analogously, the first column of $B = M_m(D)$ is the unique simple left B-module N and $E \simeq \mathrm{End}_B(N)^{op}$. Since f induces an equivalence of categories between A and B, any left B-module N is uniquely a left A-module by $a \cdot n = f(a)n$, for all $a \in A$ and $n \in N$. Moreover, the submodule lattice of ${}_BN$ and ${}_AN$ are equal and there exists an isomorphism between $\mathrm{End}_B(N)$ and $\mathrm{End}_A(N)$. Hence the unique simple B-module N is isomorphic to M as left A-module and $E \simeq \mathrm{End}_B(N)^{op} \simeq \mathrm{End}_A(M)^{op} \simeq D$. Furthermore, M has rank n over D and N has rank m over $E \simeq D$. Thus, $n = m$. □

Corollary 4.2 *Let A be a finite dimensional central simple K-algebra. Then there exists a unique finite dimensional central division K-algebra D and a number n such that $A \simeq M_n(D)$ as K-algebras.*

Proof: By the Wedderburn-Artin Theorem any finite dimensional simple algebra A is semisimple and hence a finite direct product of matrix rings over division rings, i.e. $A \simeq M_{n_1}(D_1) \times \cdots \times M_{n_t}(D_t)$. As A is simple we must have $t = 1$, i.e. $A \simeq M_n(D)$, with D a division ring. The first column of $M_n(D)$ is a simple left A-module and $D \simeq \mathrm{End}(D)^{op}$. If A was a central K-algbera, then D is also a finite dimensional central division algebra over K. □

Last Corollary and the uniqueness of the Wedderburn-Artin decomposition allows us to conclude that the tensor product of two finite dimensional central division algebras is in fact a division algebra if their dimensions are relatively prime.

Proposition 4.3 *Let C e D be finite dimensional central division algebras over. If $\dim_K(C)$ and $\dim_K(D)$ are relatively prime, then $C \otimes D$ is a central division algebra over K.*

Proof: We know that $C \otimes D$ is a finite dimensional central simple K-algebra. Hence by Corollary 4.2 there exists a finite dimensional central division K-algebra E and number $r \geq 1$ such that $C \otimes D \simeq M_r(E)$. Let $n = \dim_K(C)$. Then $M_n(K) \simeq C \otimes C^{op}$ and

$$M_n(D) \simeq D \otimes M_n(K) \simeq D \otimes C \otimes C^{op} \simeq M_r(E) \otimes C^{op} \simeq M_r(E \otimes C^{op}).$$

Since $E \otimes C^{op}$ is a finite dimensional central simple algebra, again Corollary 4.2 shows that there exist a finite dimensional central division algebra E' and a number $s \geq 1$ such that $E \otimes C^{op} \simeq M_s(E')$. Hence $M_n(D) \simeq M_{rs}(E')$. By the uniqueness of the Wedderburn-Artin decomposition $n = rs$ and $D \simeq E'$.

Similarly for $m = \dim_K(D)$ we have $D \otimes D^{op} \simeq M_m(K)$ and

$$M_m(C) \simeq C \otimes M_m(K) \simeq C \otimes D \otimes D^{op} \simeq M_r(E) \otimes D^{op} \simeq M_r(E \otimes D^{op})$$

Againm $E \otimes D^{op} \simeq M_t(E'')$ for some number $t \geq 1$ and a division algebra E''. Thus $M_m(C) \simeq M_{rt}(E'')$ and by the uniqueness of the Wedderburn-Artin Theorem, $m = rt$ and $C \simeq E''$. Hence r is a divisor of n and m and by hypothesis $r = 1$. Thus $C \otimes D \simeq E$. □

When extending the scalars of a central simple algebra, we can apply Corollary 3.15 again and conclude that the dimension of a finite dimensional central simple algebras is a square number. In particular the dimension of any finite dimensional central division algebra over a field is a square.

Lemma 4.4 *Let A be a central simple K-algebra and $\overline{K}$ the algebraic closure of K.*

1. *If $K \leq L$ is a field extension of K, then $A \otimes_K L$ is a central simple L-algebra.*
2. *If $\dim_K(A) = n$, then $n = d^2$ and $A \otimes_K \overline{K} \simeq M_d(\overline{K})$ as $\overline{K}$-algebras, for some $d \geq 1$.*

Proof: (1) follows directly from Corollary 3.15.

(2) By (1) $A \otimes \overline{K}$ is a central simple $\overline{K}$-algebra. By Corollary 4.2, $A \otimes \overline{K} \simeq M_d(D)$ for some finite dimensional central division algebra D over $\overline{K}$. Since any element of D is algebraic over $\overline{K} = Z(D)$, we must have $D = \overline{K}$. Moreover, if $n = \dim_K(A)$ and $\{a_1, \ldots, a_n\}$ is a K-basis for A, then $a_1 \otimes 1, \ldots, a_n \otimes_1$ is a $\overline{K}$-basis for $A \otimes \overline{K}$. Thus $A \otimes \overline{K} \simeq M_d(\overline{K})$ and $n = \dim_K(A) = \dim_{\overline{K}}(A \otimes \overline{K}) = \dim_{\overline{K}}(M_d(\overline{K})) = d^2$. $\square$

Definition 4.5 *The degree of a finite dimensional central simple K-algebra A is defined as*

$$\deg_K(A) := \sqrt{\dim_K(A)}.$$

The Brauer group will be defined on the set of equivalence classes of finite dimensional central simple algebras over a field.

Definition 4.6 *Let A and B be finite dimensional central simple K-algebra. Then A and B are called similar, in symbol $A \sim B$ if and only if there exist numbers $n, m \geq 1$ and an isomorphism of K-algebras*

$$A \otimes M_n(K) \simeq B \otimes M_m(K).$$

The relation $\sim$ is obviously reflexive and symmetric. Let $A \sim B$ and $B \sim C$, for finite dimensional central simple K-algebras A, B, C. Then there exist n_1, n_2, m_1, m_2 such that

$$A \otimes M_{n_1}(K) \simeq B \otimes M_{m_1}(K) \qquad \text{and} \qquad B \otimes M_{n_2}(K) \simeq C \otimes M_{m_2}(K).$$

Then

$$\begin{aligned} A \otimes M_{n_1 n_2}(K) \simeq (A \otimes M_{n_1}(K)) \otimes M_{n_2}(K) &\simeq (B \otimes M_{m_1}(K)) \otimes M_{n_2}(K) \\ &\simeq B \otimes M_{n_2}(K) \otimes M_{m_1}(K) \\ &\simeq (C \otimes M_{m_2}(K)) \otimes M_{m_1}(K) \simeq C \otimes M_{m_1 m_2}(K) \end{aligned}$$

Thus, $A \sim C$.

Let us denote by $[A] = [A]_\sim$ the equivalence class of a finite dimensional central simple K-algebra. We have already seen that any such algebra A is isomorphic to $M_n(D)$ for some finite dimensional central division algebra D over K. Hence $A \sim D$ shows that any equivalence class contains a finite dimensional central division algebra. The uniqueness of the Wedderburn-Artin decomposition shows that any two finite dimensional central division algebra contained in the same equivalence class must be isomorphic.

Lemma 4.7 *Let D and E be finite dimensional central division algebras over K. Then D and E are similar if and only if D and E are isomorphic K-algebras.*

Proof: Suppose $D \sim E$. Then there are numbers $n, m \geq 1$ such that $M_n(D) \simeq D \otimes M_n(K) \simeq E \otimes M_m(K) \simeq M_m(E)$. By Lemma 4.1 $E \simeq D$. □

We conclude that for any finite dimensional central simple K-algebra A there exists a uniquely determined finite dimensional central division algebra D over K such that $[A] = [D]$. Moreover, D determines the equivalence class of A, i.e. $[A] = \{M_n(D) : n \geq 1\}$.

Definition 4.8 *The Schur index of a finite dimensional central simple K-algebra A is defined as*

$$\mathrm{Ind}_K(A) := \deg_K(D) = \sqrt{\dim_K(D)}$$

if $A \simeq M_r(D)$ for some finite dimensional central division K-algebra D and $r \geq 1$.

Theorem 4.9 (The Brauer group of a field) *Let K be a field. The set of equivalence classes of finite dimensional central simple K-algebras*

$$\mathrm{Br}(K) = \{[A] : A \text{ is a finite dimensional central simple } K\text{-algebra}\}$$

is a group with product given by the tensor product

$$[A] \cdot [B] := [A \otimes B] \qquad \forall [A], [B] \in \mathrm{Br}(K)$$

neutral element given by $[K]$ such that $[A]^{-1} = [A^{op}]$ for all $[A] \in \mathrm{Br}(K)$.

Proof: Firstly we have to show that the product is independent of the representatives of the classes. Hence let $A \sim A'$ and $B \sim B'$ be finite dimensional central simple K-algebras. Then there are $n_1, n_2, m_1, m_2 \geq 1$ such that

$$A \otimes M_{n_1}(K) \simeq A' \otimes M_{n_2}(K) \qquad \text{and} \qquad B \otimes M_{m_1}(K) \simeq B' \otimes M_{m_2}(K).$$

Hence

$$\begin{aligned} (A \otimes B) \otimes M_{n_1 m_1}(K) &\simeq A \otimes M_{n_1}(K) \otimes B \otimes M_{m_1}(K) \\ &\simeq A' \otimes M_{n_2}(K) \otimes B' \otimes M_{m_2}(K) \simeq \left(A' \otimes B'\right) \otimes M_{n_2 m_2}(K) \end{aligned}$$

shows $A \otimes B \sim A' \otimes B'$.

The isomorphism $K \otimes A \simeq A \simeq A \otimes K$ shows that $[K][A] = [A] = [A][K]$. Furthermore, from 3.16 we know that $A \otimes A^{op} \simeq M_n(K)$, with $n = \dim_K(A)$. Hence $A \otimes A^{op} \sim K$, i.e. $[A][A^{op}] = [K]$.

□

We have already characterised the finite dimensional central division algebras over several fields. For instance if $K = \overline{K}$ is algebraically closed, then $\mathrm{Br}(K) = \{[K]\}$ is the trivial group, e.g. $\mathrm{Br}(\mathbb{C}) = \{[\mathbb{C}]\}$. Similarly, if K is a finite field, then $\mathrm{Br}(K) = \{[K]\}$.

Then we have also $\mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$. In particular

$$\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \simeq M_4(\mathbb{R})$$

as $\dim_{\mathbb{R}}(\mathbb{H}) = 4$ and $\mathbb{H} = \mathbb{H}^{op}$. Hence $\mathrm{Br}(\mathbb{R}) \simeq (\mathbb{Z}_2, +)$ is the cyclic group of order 2.

Consider a field K and a finite dimensional central simple K-algebra A that admits a K-linear involution, i.e. an anti-isomorphism $* : A \to A$ such that $a^{**} = a$ for all $a \in A$. Then $*$ is an isomorphism between A and its opposite algebra A^{op}. Thus $[A]^2 = [A][A^{op}] = [K]$ shows that $[A]$ has order 2 in the Brauer group $\mathrm{Br}(K)$. For example if the Quaternion algebra $Q = Q(a, b; K)$ is a division algebra, then the conjugation $\overline{\ }$ (see equation 1.18) of Q is an involution and Q is an element of order 2 in $\mathrm{Br}(K)$.

We will show that any element of the Brauer group has finite order, i.e. $\mathrm{Br}(K)$ is a torsion group, but first we will see how to reduce the study of the Brauer group to Galois extensions of K.

Theorem 4.10 *Let L/K be a field extension. The following map*

$$\tau_{L/K} : \mathrm{Br}(K) \to \mathrm{Br}(L), \qquad [A] \mapsto [A \otimes L]$$

is a group homomorphism, such that if $K \leq L \leq F$ is an extension of fields, then

$$\tau_{F/K} = \tau_{F/L} \circ \tau_{L/K}.$$

Proof: We need to show that $\tau_{L/K}$ is well-defined. Hence if $A \sim B$ are similar finite dimensional central simple K-algebras, then there are numbers $n, m \geq 1$ and an isomorphism of K-algebras $A \otimes M_n(K) \simeq B \otimes M_m(K)$. Hence

$$(A \otimes L) \otimes_L M_n(L) \simeq A \otimes M_n(K) \otimes L \simeq B \otimes M_n(K) \otimes L \simeq (B \otimes L) \otimes_L M_m(L)$$

shows that $\tau_{L/K}$ is well-defined. By Proposition 3.7 $(A \otimes B) \otimes L \simeq (A \otimes L) \otimes_L (B \otimes L)$ as L-algebras shows

$$\tau_{L/K}([A][B]) = [(A \otimes B) \otimes L] = [(A \otimes L) \otimes_L (B \otimes L)] = [A \otimes L][B \otimes L] = \tau_{L/K}([A])\tau_{L/K}([B]).$$

We also have $\tau_{L/K}([K]) = [L]$, which shows that $\tau_{L/K}$ is a group homomorphism.

Let $K \leq L \leq F$ be a field extension and A a central simple K-algebra. Then we have an isomorphism of F-algebras

$$(A \otimes_K L) \otimes_L F \longrightarrow A \otimes_K F, \qquad (a \otimes_K x) \otimes_L y \mapsto a \otimes_K xy.$$

Hence

$$\tau_{F/L}(\tau_{L/K}([A])) = [(A \otimes_K L) \otimes_L F] = [A \otimes_K F] = \tau_{F/K}([A]).$$

□

We make a remark about the index and the degree of a finite dimensional central simple K-algebra A. We have seen that there exists a finite dimensional central division algebra D over K such that $A \simeq M_r(D)$. Hence

$$\deg_K(A) = \sqrt{\dim_K(A)} = r\sqrt{\dim_K(D)} = r\mathrm{Ind}_K(D) = r\mathrm{Ind}_K(A).$$

Moreover we have seen that then $[A] = [D]$ and if $[B] = [A]$, then $B \sim D$ and hence $\mathrm{Ind}_K(B) = \mathrm{Ind}_K(A) = \deg_K(D)$. Moreover, for any field extension L/K, if $A \otimes L \sim D \otimes L \simeq M_s(E)$ for some finite dimensional central division algebra E over L. Then

$$\mathrm{Ind}_K(A) = \sqrt{\dim_K(D)} = \sqrt{\dim_L(D \otimes L)} = s\sqrt{\dim_L(E)} = s \deg_L(E) = s\mathrm{Ind}_L(A \otimes L).$$

This means $\mathrm{Ind}_L(A \otimes L) \mid \mathrm{Ind}_K(A)$.

Definition 4.11 *Let A be a finite dimensional central simple K-algebra. A field extension L of K is called a splitting field for A if $[A] \in \mathrm{Ker}(\tau_{L/K})$.*

Lemma 4.12 *Let A be a finite dimensional central simple K-algebra and L a field extension of K. Then L is a splitting field for A if and only if there exists a number $n \geq 1$ and an isomorphism of L-algebras $A \otimes L \simeq M_n(L)$.*

Proof: By Corolary 4.2, there exists a finite dimensional central division K-algebra D, a number $r \geq 1$ and an isomorphism of K-algebras $A \simeq M_r(D)$. Hence

$$A \otimes L \simeq M_r(D) \otimes L \simeq M_r(K) \otimes D \otimes L \simeq M_r(D \otimes L)$$

as L-algebras. Since $D \otimes L$ is a finite dimensional central simple L-algebra, there exists again by Corollary 4.2 a finite dimensional central division L-algebra E, a number $s \geq 1$ and an isomorphism of L-algebras $D \otimes L \simeq M_s(E)$. Hence

$$A \otimes L \simeq M_r(D \otimes L) \simeq M_{rs}(E).$$

If L is a splitting field for A. Then $[A \otimes L] = [L]$ and there are numbers $n, m \geq 1$ and an isomorphism of L-algebras $(A \otimes L) \otimes_L M_n(L) \simeq M_m(L)$. Hence

$$M_m(L) \simeq (A \otimes L) \otimes_L M_n(L) \simeq M_{rs}(E) \otimes_L M_n(L) \simeq M_{rsn}(E).$$

By the uniqueness of the Wedderburn-Artin Theorem Lemma 4.1, we must have $E = L$ and $m = rsn$. Hence $D \otimes L \simeq M_s(L)$ and $A \otimes L \simeq M_{rs}(L)$.

Conversely, if $A \otimes L \simeq M_n(L)$, then clearly $A \otimes L \sim L$ and therefore $[A \otimes L] = [L]$, i.e. $[A] \in \mathrm{Ker}(\tau_{L/K})$.

□

If L is a splitting field for A, then so is any field extension F/L, because $A \otimes F \simeq (A \otimes L) \otimes_L F \simeq M_n(L) \otimes_L F \simeq M_n(F)$. In particular $\overline{K}$ is a splitting field for any A and the next Proposition will show that any finite dimensional central simple K-algebra A admits a finite dimensional splitting field.

Proposition 4.13 *Any finite dimensional central simple algebra has a finite dimensional splitting field.*

Proof: Let $n = \dim_K(A)$. We have already seen that there exists an isomorphism of algebras $f : A \otimes_K \overline{K} \to M_d(\overline{K})$, with $d^2 = n$. For $1 \leq i, j \leq d$, denote by E_{ij} the matrix units of $M_d(\overline{K})$. Let $\{b_1, \ldots, b_n\}$ be a K-basis of A. Then there exist elements $\mu_{ijk} \in \overline{K}$ for $1 \leq i, j \leq d$ and $1 \leq k \leq n$ such that

$$f(b_k \otimes 1) = \sum_{i,j=1}^{n} \mu_{ijk} E_{ij} \in M_d(\overline{K}).$$

Let L be the subfield of $\overline{K}$ generated by all elements μ_{ijk} and K. Then f restricts to an isomorphism of L-algebras $f : A \otimes L \to M_d(L)$. Hence L is a finite dimensional splitting field for A. □

The kernel of $\tau_{L/K}$ is called a relative Brauer group, denoted by $\mathrm{Br}(L/K) := \mathrm{Ker}(\tau_{L/K})$ and we have just seen that any $[A] \in \mathrm{Br}(K)$ belongs to a relative Brauer group, i.e.

$$\mathrm{Br}(K) = \bigcup \{\mathrm{Br}(L/K) \mid L/K \text{ is a finite field extension}\}.$$

We will see soon, that L can be assumed to be a finite Galois extension of K, but first of all we need another technical Lemma:

Theorem 4.14 (Skolem-Noether) *Let A and B be finite dimensional simple K-algebras and $f, g : A \to B$ two K-algebra homomorphisms. If B is central, then there exists an invertible element $u \in B$ such that*

$$g(a) = uf(a)u^{-1}, \qquad \forall a \in A.$$

Proof: Let $T = A \otimes B^{op}$. Then T is a finite dimensional simple K-algebra. By the Wedderburn-Artin Theorem, $T \simeq M_n(D)$ for some finite dimensional division K-algebra D. Recall that up to isomorphism, there exist only one simple left T-module, say E, and that $\mathrm{End}({}_TE) \simeq D^{op}$ and $\dim(E) = n[D : K]$. Moreover, any non-zero finitely generated left T-module M is isomorphic to E^r, for some $r \geq 1$, and $\dim(M) = r \dim(E) = rn[D : K]$. In particular, two non-zero finitely generated left T-modules are isomorphic if and only if they have the same dimension.

Since B is simple algebra, it is a simple $B \otimes B^{op}$-module. Note that as A is simple, f and g are injective. For each of the ring homomorphisms, we have a $T = A \otimes B^{op}$-module structure on B, namely by

$$(a \otimes b) \cdot x = f(a)xb, \qquad \forall a \in A, b, x \in B.$$

and

$$(a \otimes b) \cdot x = g(a)xb, \qquad \forall a \in A, b, x \in B.$$

Thus the two left T-module structures on B must be isomorpic. Hence there exists an isomorphism $\varphi : B \to B$ of left T-modules such that

$$\varphi(f(a)x) = \varphi(a \cdot xb) = a \cdot \varphi(x)b = g(a)\varphi(x)b, \qquad \forall a \in A, x, b \in B.$$

Thus, for $a = 1_A$, $x = 1_B$ we have $\varphi(b) = \varphi(1_B)b$, for all $b \in B$. As φ is bijective, there exists $b \in B$ with $1 = \varphi(b) = \varphi(1_B)b$. Hence $u = \varphi(1_B) \in U(B)$ is invertible. Moreover,

$$g(a)u = g(a)\varphi(1_B) = \varphi(f(a)1_B) = \varphi(f(a)) = \varphi(1_B)f(a) = uf(a), \qquad \forall a \in A$$

This shows, $g(a) = uf(a)u^{-1}$ for all $a \in A$.

□

Corollary 4.15 *Let A be a finite dimensional central simple K-algebra and B_1, B_2 simple K-subalgebras of A. If $g : B_1 \to B_2$ is an isomorphism of K-algebras, then there exists $u \in U(A)$ such that $f(x) = uxu^{-1}$, for all $x \in B_1$. Moreover,*

$$u^{-1}\mathrm{Cent}_A(B_1)u = \mathrm{Cent}_A(B_2).$$

Proof: Let $f = \mathrm{id}_{|_{B_1}} : B_1 \to A$ be the restriction of the identity map to B_1. By the Skolem-Noether Theorem, 4.14, there exists $u \in U(A)$ such that $g(x) = uxu^{-1}$ for all $x \in B_1$.

Furthermore, let $y \in A$. Then for any $x \in B_1$ we have

$$yg(x) = g(x)y \qquad \Leftrightarrow \qquad yuxu^{-1} = uxu^{-1}y \qquad \Leftrightarrow \qquad \left(u^{-1}yu\right)x = x\left(u^{-1}yu\right)$$

As g is surjective andy element if B_2 is of the form $g(x)$ for some $x \in B_1$. Thus $y \in \mathrm{Cent}_A(B_2)$ if and only if $u^{-1}yu \in \mathrm{Cent}_A(B_1)$. □

An automorphism σ of a ring R is called an inner automorphism if there exists an invertible element $u \in U(R)$ such that $\sigma(x) = uxu^{-1}$. The inner automorphisms form a subgroup $\mathrm{Inn}(A)$ of the group of automorphisms $\mathrm{Aut}(A)$ of A. The map $U(R) \to \mathrm{Inn}(A)$ given by $u \mapsto [x \mapsto uxu^{-1}]$ is a surjective group homomorphism. By Corollary 4.15 we have that

Corollary 4.16 *Any automorphism of a finite dimensional central simple K-algebra is inner.*

The following so-called Centralizer Theorem will generalise the Double Centralizer Theorem.

Theorem 4.17 (Centralizer Theorem) *Let A be a finite dimensional central simple K-algebra with simple K-subalgebra $B \leq A$. Then*

1. *there exists an isomorphism of K-algebras $A \otimes B^{op} \to \mathrm{Cent}_A(B) \otimes \mathrm{End}_K(B)$;*
2. $\dim(A) = \dim(B) \cdot \dim(\mathrm{Cent}_A(B))$*;*
3. $\mathrm{Cent}_A(B)$ *is simple with center* $Z(\mathrm{Cent}_A(B)) = Z(B)$ *such that* $\mathrm{Cent}_A(\mathrm{Cent}_A(B)) = B$.

Proof: (1) As B is finite dimensional, say $n = \dim(B)$, its endomorphism ring $\mathrm{End}(B) \simeq M_n(K)$ is central simple and so is $A \otimes \mathrm{End}(B)$ as A is central simple. The map $f : B \to A \otimes \mathrm{End}(B)$ sending b to

$$f(b) = b \otimes \mathrm{id}_B, \qquad \forall b \in B.$$

is an injective algebra homomorphism.

Denote by $\lambda_b \in \mathrm{End}(B)$ the endomorphism $\lambda_b(x) = bx$. Then $l : B \to \mathrm{End}(B)$ with $l(b) = \lambda_b$ is an injective algebra homomorphism The map $g : B \to A \otimes \mathrm{End}(B)$ sending b to

$$g(b) = 1 \otimes \lambda_b, \qquad \forall b \in B$$

is also an injective algebra homomorphism.

Hence $f(B) \simeq B \simeq g(B)$ as K-algebras, showing that the subalgebras $f(B)$ and $g(B)$ of $A \otimes \mathrm{End}(B)$ are isomorphic. By the Skolem-Noether Theorem there exist an invertible element $u \in U(A \otimes \mathrm{End}(B))$ such that

$$g(b) = uf(b)u^{-1}, \qquad \forall b \in B.$$

As seen before, this implies $\mathrm{Cent}_{A\otimes\mathrm{End}(B)}(g(B)) = u^{-1}\mathrm{Cent}_{A\otimes\mathrm{End}(B)}(f(B))u$ and hence

$$\mathrm{Cent}_{A\otimes\mathrm{End}(B)}(g(B)) \simeq \mathrm{Cent}_{A\otimes\mathrm{End}(B)}(f(B)).$$

By Lemma 3.8, we have

$$\mathrm{Cent}_{A\otimes \mathrm{End}(B)}(f(B)) = \mathrm{Cent}_{A\otimes \mathrm{End}(B)}(B\otimes \mathrm{id}_B) = \mathrm{Cent}_A(B)\otimes \mathrm{End}(B).$$

Similarly we calculate

$$\mathrm{Cent}_{A\otimes \mathrm{End}(B)}(g(B)) = \mathrm{Cent}_{A\otimes \mathrm{End}(B)}(1\otimes l(B)) = A\otimes \mathrm{Cent}_{End(B)}(l(B)).$$

In order to conclude, we need to determine $\mathrm{Cent}_{\mathrm{End}(B)}(l(B))$. Denote by $r : B^{op} \to \mathrm{End}(B)$ the map $r(b) = \rho_b$, where $\rho_b(x) = xb$ is the right multiplication of an element x by b.

Then for any $\varphi \in \mathrm{End}(B)$

$$\begin{aligned}
\varphi \in \mathrm{Cent}_{\mathrm{End}(B)}(l(B)) &\Leftrightarrow \forall b\in B:\ \varphi\circ\lambda_b = \lambda_b\circ\varphi \\
&\Leftrightarrow \forall b\in B: \forall x\in B:\ \varphi(bx) = b\varphi(x) \\
&\Leftrightarrow \forall b\in B:\ \varphi(b) = b\varphi(1) \\
&\Leftrightarrow \varphi \in r(B^{op})
\end{aligned}$$

Hence $\mathrm{Cent}_{\mathrm{End}(B)}(l(B)) = r(B^{op})$ and since B^{op} is simple, r is injective and therefore, $B^{op} \simeq r(B^{op}) \simeq \mathrm{Cent}_{\mathrm{End}(B)}(l(B))$. Thus

$$A\otimes B^{op} \simeq A\otimes \mathrm{Cent}_{\mathrm{End}(B)}(l(B)) \simeq \mathrm{Cent}_{A\otimes \mathrm{End}(B)}(g(B)) \simeq \mathrm{Cent}_{A\otimes \mathrm{End}(B)}(f(B)) = \mathrm{Cent}_A(B)\otimes \mathrm{End}(B).$$

(2) follows from (1) and the following calculations

$$\dim(A)\dim(B) = \dim(A\otimes B^{op}) = \dim(\mathrm{Cent}_A(B))\dim(\mathrm{End}(B)) = \dim(\mathrm{Cent}_A(B))\dim(B)^2.$$

(3) Since A and B^{op} are simple, so is $A\otimes B^{op}$. By (1) also $\mathrm{Cent}_A(B)\otimes \mathrm{End}(B)$ is simple and therefore also $\mathrm{Cent}_A(B)$.

Applying (2) to $\mathrm{Cent}_A(B)$ instead of B yields $\dim(B) = \dim(\mathrm{Cent}_A(\mathrm{Cent}_A(B)))$ and therefore $\mathrm{Cent}_A(\mathrm{Cent}_A(B)) = B$. Then $Z(\mathrm{Cent}_A(B)) = \mathrm{Cent}_A(B)\cap B = Z(B)$.

□

Corollary 4.18 *Let A be a finite dimensional central simple K-algebra and $K \le L \le A$ a subfield of A containing K. Then*

1. *$A\otimes L \simeq \mathrm{Cent}_A(L)\otimes M_n(K)$ as L-algebras, with $n = [L:K]$;*
2. *$\dim(A) = [L:K]\dim(\mathrm{Cent}_A(L))$*
3. *$[L:K] \mid \deg(A) = \sqrt{\dim(A)}$.*

Proof: Take $B = L$ in the Centralizer Theorem 4.17. Then (1) and (2) follow from the same Theorem, having in mind that $\mathrm{End}({}_KL) \simeq M_n(K)$. Furthermore, $L \subseteq \mathrm{Cent}_A(L)$ turns $\mathrm{Cent}_A(L)$ into an L-algebra. Therefore $\dim(C_A(L)) = \dim({}_LC_A(L))[L:K]$, where $\dim({}_LC_A(L))$ denotes the dimension of $C_A(L)$ as L-space. Hence $[L:K]$ divides $\dim(C_A(L))$ and therefore $[L:K]^2 \mid [L:K]\dim(C_A(L)) = \dim(A)$ by 4.17(2). Thus $[L:K] \mid \deg(A)$. □

5

Maximal Subfields and Crossed products

A subfield L of a K-algebra A is a K-subalgebra $L \leq A$ that is a field and contains K. Recall that a finite field extension L/K is a Galois extension if L/K is separable and normal, where L/K is called a normal extension if any polynomial $f \in K[x]$ that has a root in L will decompose over L in linear factors. Given any finite field extension L/K with $L = K(a_1, \ldots, a_n)$, we can consider the product f of minimal polynomials $min_{a_i,K}$ of the $a_1, \ldots, a_n$ and consider the splitting field F over K. It is a fact from Galois Theory that F/K is a normal extension, called the normal closure of L and generated by all the (finitely many) roots of f. Let A be finite dimensional central simple K-algebra with finite splitting field L of A and F the normal closure of L, then F is also a splitting field of A.

A maximal subfield L of a central simple K-algebra A is a subfield such that $\text{Cent}_A(L) = L$. Our aim will be to show that any finite dimensional central simple K-algebra is similar to a finite dimensional central simple K-algebra that contains a splitting field L as maximal subfield such that L is a finite Galois extension of K.

Lemma 5.1 *A subfield L of a division algebra D over K is maximal if and only if it is maximal in the lattice of subfields of D.*

Proof: Any subfield L is commutative and hence satisfies $L \subseteq \text{Cent}_D(L)$. Hence if $L \subseteq L'$ is a chain of subfields of D and L is maximal, then $L \subseteq L' \subseteq \text{Cent}_D(L) = L$.

On the other hand, if L is maximal in the lattice of subfields of D, then for any non-zero $x \in \text{Cent}_D(L)$, the subfield $L' = L(x)$ generated by L and x is an extension of L and hence $x \in L' = L$. Thus $L = \text{Cent}_D(L)$. $\square$

While Lemma 5.1 shows that maximal subfields do exist in finite dimensional central division algebras, they might not exist in a finite dimensional central simple algebra as we will see soon. However, if they exist, then they are splitting fields for the algebra in question.

Theorem 5.2 *Any maximal subfield L of a finite dimensional central simple K-algebra A is a splitting field for A and satisfies $[L:K] = \deg_K(A)$.*

Proof: Let L be a maximal subfield of A and $n = \deg_K(A)$. Then Corollary 4.18 yields $n^2 = [L:K]\dim_K(\mathrm{Cent}_D(L)) = [L:K]^2$. Thus $n = [L:K]$. Moreover, by the same Corollary, $A \otimes L = \mathrm{Cent}_A(L) \otimes M_n(K) = L \otimes M_n(K) \simeq M_n(L) \sim L$. Hence $[A] \in \mathrm{Ker}(\tau_{L/K})$. □

The following technical Lemma will be important to show that we can reduce our study to separable splitting fields. Recall that an element of a division K-algebra $a \in D$ is not separable over K if it is a multiple root of its minimal polynomial f. In other words, if $f = (x-a)^m g$, for some $g \in \overline{K}[x]$ and $m \geq 2$. Then the formal derivative $f' = (x-a)^{m-1}((x-a)g' + mg)$ has still a as a root and f divides f'. Since the degree of f is larger than that of f' we must have $f' = 0$. This of course cannot happen if $\mathrm{char}(K) = 0$. If $\mathrm{char}(K) = p > 0$, the condition $f' = 0$ implies that $f = h(x^p)$ for some $h \in K[x]$. Let $n \geq 1$ be the largest number such that there exists $f \in K[x^{p^n}]$ and $f \notin K[x^{p^{n+1}}]$. Then there exist $g \in K[x]$ with $f = g(x^{p^n})$. Note that $g' \neq 0$ since otherwise $g = h(x^p)$ and $f = h(x^{p^{n+1}})$ which contradicts our choice of n. Thus, g is irreducible in $K[x]$ and in particular the minimal polynomial of a^{p^n} as $g(a^{p^n}) = f(a) = 0$. Thus we showed that for any non-separable element a of a division K-algebra D over a field of characteristic p, there exists $n \geq 1$ such that a^{p^n} is separable over K.

Theorem 5.3 (Noether-Jacobson) *Any noncommutative algebraic central division algebra D over K contains a separable subfield $K \subsetneq L$.*

Proof: If $a \in D \setminus K$ is separable over K, then we can choose the subfield $L = K(a) \leq D$ generated by a and K, which is possible since the elements of K commute with a and since non-zero elements of D are invertible in K. In case $\mathrm{char}(K) = 0$, we can choose any element $a \in D \setminus K$, since any element is separable. Hence assume $\mathrm{char}(K) = p > 0$.

We will prove the result by contradiction: Suppose that no element of $D \setminus K$ is separable over K. Let $a \in D \setminus K$ be any element. By the previous comment, there exists a minimal $n \geq 1$ such that a^{p^n} is separable over K and $a^{p^{n-1}}$ is not. We can substitute a by $a^{p^{n-1}}$ and obtain that $a \notin K$, while a^p is separable and hence by assumption belongs to $K = Z(D)$.

Consider the additive commutator $\delta = [-, a] : D \to D$. Then $\delta \neq 0$ since $a \notin K = Z(D)$ and $\delta^p = 0$, as $a^p \in Z(D)$ and $\delta^p(b) = ba^p - a^p b = 0$. Let $m \geq 1$ be the least positive integer such that $\delta^m \neq 0$ and $\delta^{m+1} = 0$. Then there exists $0 \neq w \in D$ such that

$$\delta(w) = wa - aw \neq 0 \qquad \text{and} \qquad \delta^2(w) = \delta(w)a - a\delta(w) = 0.$$

Thus $\delta(w)^{-1}a = a\delta(w)^{-1}$ and $\delta(w) + aw = wa$. For $u = wa\delta(w)^{-1}$ we calculate:

$$aua^{-1} + 1 = awa\delta(w)^{-1}a^{-1} + 1 = aw\delta(w)^{-1} + 1 = (aw + \delta(w))\delta(w)^{-1} = wa\delta(w)^{-1} = u.$$

If u is not separable, then there exists $m \geq 1$ such that u^{p^m} is separable and hence $u^{p^m} \in K$. If u is separable, then $u \in K$ and we can take $m = 0$. But then

$$u^{p^m} = \left(aua^{-1} + 1\right)^{p^m} = (aua^{-1})^{p^m} + 1 = au^{p^m}a^{-1} + 1 = u^{p^m} + 1,$$

which leads to the contradiction $0 = 1$. Hence there must exist some element of $D \setminus K$ that is separable over K. □

Theorem 5.4 *Let D be a finite dimensional central division algebra over K. Then D contains a maximal subfield L such that L/K is separable.*

Proof: Let L be a subfield of D such that L/K is separable and $[L:K]$ is maximal. Such a subfield exists, since K is a subfield of D with K separable over K.

We will show that $L = \mathrm{Cent}_D(L)$. Clearly $\mathrm{Cent}_D(L)$ is a central division algebra over L by 4.17. If $L \neq \mathrm{Cent}_D(L)$, then by the Noether-Jacobson Theorem 5.3 there exists a subfield $L' \subseteq \mathrm{Cent}_D(L)$ with $L \subsetneq L'$ and L/L' separable. But then L' is also a subfield of D and L'/K is separable as L'/L and L/K are separable field extensions. As $[L':K] > [L:K]$, we obtain a contradiction to the choice of L. Therefore, $\mathrm{Cent}_D(L) = L$, i.e. L is maximal. □

Theorem 5.5 *Any finite dimensional central simple K-algebra has a finite dimensional splitting field L such that L/K is Galois.*

Proof: Let D be a finite dimensional central division algebra over K. By Theorem 5.4, D contains a maximal separable subfield L. Substituting L by its normal closure F, shows that F is a Galois and a splitting field of D. □

Corollary 5.6 *For any field K we have*

$$BrK = \bigcup \{\mathrm{Br}(L/K) : L/K \text{ is a finite Galois extension } \}$$

The last Corollary allows us to reduce our classification of finite dimensional central division algebras over a field to those that have a finite Galois extension as splitting field. We will classify $\mathrm{Br}(L/K)$ with the help of so called crossed products.

Assume that L/K is a finite Galois extension with Galois group

$$G = \mathrm{Gal}(L/K) = \{\sigma \in \mathrm{Aut}(L) : \sigma_{|_K} = id_K\}.$$

Consider $A = \mathrm{End}_K(L) \simeq M_n(K)$, where $n = [L:K]$. Then each $g \in G$ can be considered a K-linear endomorphism of A, i.e. $g \in A$, by $x \mapsto g(x)$, for all $x \in L$. We need the following fact about the linear independence of automorphisms of L:

Lemma 5.7 (Dedekind's Lemma) *The elements of* $\mathrm{Gal}()L/K)$ *form a linearly independent set of* $\mathrm{End}_K(L)$ *considered as vector space over L.*

Proof: $A = \mathrm{End}_K(L)$ is a vector space over L with scalar multiplication given by $\lambda \cdot f : [x \mapsto \lambda f(x)]$ for all $f \in A$ and $\lambda \in L$. We wish to prove that any set $\{\sigma_1, \ldots, \sigma_m\} \subseteq G$ is linearly independent. If $m = 1$, then $\lambda\sigma_1 = 0$, means $\lambda = 0$ since $\sigma_1 \neq 0$. Suppose we have proven our claim for some $m \geq 1$. Let $\{\sigma_1, \ldots, \sigma_{m+1}\} \subseteq G$ be $m+1$ distinct elements such that there exist $\lambda_1, \ldots, \lambda_{m+1} \in L$ with

$$\lambda_1\sigma_1 + \cdots + \lambda_{m+1}\sigma_{m+1} = 0 \tag{5.1}$$

Note that equation 5.1 is an equation of functions. If one of the $\lambda_i = 0$, then all are equal to zero by induction hypothesis. Thus we suppose $\lambda_{m+1} \neq 0$ and by dividing equation 5.1 by

λ_{m+1} we actually can suppose that $\lambda_{m+1} = 1$. In other words, without loss of generality we can assume that we have an equation:

$$\lambda_1\sigma_1 + \cdots + \lambda_m\sigma_m + \sigma_{m+1} = 0 \tag{5.2}$$

Since $\sigma_{m+1} \neq \sigma_1$, there exists $y \in L$ such that $\sigma_1(y) \neq \sigma_{m+1}(y) \neq 0$. Hence for all $x \in L$:

$$\lambda_1\sigma_1(xy) + \cdots + \lambda_m\sigma_m(xy) + \sigma_{m+1}(xy) = 0.$$

Multiplying by the inverse of σ_{m+1}^{-1} yields

$$\left(\lambda_1\sigma_1(y)\sigma_{m+1}(y)^{-1}\right)\sigma_1(x) + \cdots + \left(\lambda_m\sigma_m(y)\sigma_{m+1}(y)^{-1}\right)\sigma_m(x) + \sigma_{m+1}(x) = 0.$$

By setting $\mu_i := \lambda_i\sigma_i(y)\sigma_{m+1}(y)^{-1}$ for all $1 \leq i \leq m$ we re-write the last equation:

$$\mu_1\sigma_1 + \cdots + \mu_m\sigma_m + \sigma_{m+1} = 0. \tag{5.3}$$

Subtrating equations 5.3 from 5.2 yields:

$$(\lambda_1 - \mu_1)\sigma_1 + \cdots + (\lambda_m - \mu_m)\sigma_m = 0. \tag{5.4}$$

The induction hypothesis then shows $\lambda_i = \mu_i$, for all i. But then $\lambda_1 = \mu_1 = \lambda_1\sigma_1(y)\sigma_{m+1}(y)^{-1}$ and $\sigma_1(y) \neq \sigma_{m+1}(y)$ implies $\lambda_1 = 0$ - a contradiction. □

Since $[|G|^2 = [L : K]^2 = \dim_K(A) = [L : K]\dim_L(A)$, we have $\dim_L(A) = |G|$ and therefore that the elements of G form a basis of A as vector space over L.

Not all finite dimensional central simple algebras contain a maximal subfield. Consider the real quaternions $\mathbb{H}$ and the central simple $\mathbb{R}$-algebra $A = M_n(\mathbb{H})$. Then $\dim_{\mathbb{R}}(A) = 4n^2$. If there existed a maximal subfield $L \subseteq A$ of A, then by Corollary 4.18, $4n^2 = [L : \mathbb{R}]^2$. Hence $[L : \mathbb{R}] = 2n$. However, any finite field extension of $\mathbb{R}$ has degree at most 2. Thus if $n > 1$, then A cannot have a maximal subfield, e.g. $A = M_4(\mathbb{H})$.

However, we will prove now that any finite dimensional central simple K-algebra with finite dimensional splitting field L is similar to a finite dimensional central simple K-algebra that contains (up to isomorphism of course) L as a maximal subfield.

Theorem 5.8 *For any finite field extension L/K and $[A] \in \mathrm{Br}(L/K)$ there exists $[B] = [A]$ such that L is a maximal subfield of B and $\deg_K(B) = [L : K]^2$.*

Proof: Let D be a finite dimensional central division K-algebra, such that $[A] = [D]$. Then $D \otimes L \simeq M_n(L)$, for $n^2 = \dim_K(D)$. The algebra $M_n(L)$ is simple and semisimple. Hence there exists a unique simple left $M_n(L)$-module V such that $M_n(L) \simeq V^n$.

The isomorphism between $D \otimes L$ and $M_n(L)$ yields both a left D- and a left L-module structure on V. Considering $B = \mathrm{End}_D(V)$, the algebra of left D-linear endomorphisms of V, we have that $D \sim B$, since for $m = \dim_D(V)$ we have

$$D \otimes M_m(K) \simeq M_m(D) \simeq \mathrm{End}_D(V) = B.$$

Moreover, since the left D- and left L-action on V commute, we obtain an embedding of K-algebras of L into $\mathrm{End}_D(V)$ by

$$x \mapsto [v \mapsto (1 \otimes x) \cdot v], \qquad \forall x \in L.$$

We calculate

$$[L:K] = \dim_D(D \otimes L) = \dim_D(M_n(L)) = \dim_D(V^n) = n \dim_D(V) = nm$$

and deduce

$$\dim_K(B) = \dim_K(\mathrm{End}_D(V)) = \dim_K(D) \dim_D(V)^2 = n^2 m^2 = [L:K]^2.$$

Furthermore, by Corollary 4.18, $[L:K]^2 = \dim_K(B) = [L:K] \dim_K(\mathrm{Cent}_B(L))$ shows, $\dim_K(\mathrm{Cent}_B(L)) = [L:K]$. Since $L \subseteq \mathrm{Cent}_B(L)$, we obtain equality, i.e. L is a maximal subfield of B. □

Definition of crossed products

Lemma 5.9 *Let L/K be a Galois extension with Galois group G. Then $L \star_\gamma G$ is associative if and only if γ satisfies $\gamma(g,h)\gamma(gh,k) = \gamma(g,hk)g(\gamma(h,k))$, for all $g,h,k \in G$.*

Proof: **...still to come ...** □

Definition of 2-cocycle:

$$Z^2(G, L^\times) = \{\gamma : G \times G \to L^\times : \gamma(g,h)\gamma(gh,k) = \gamma(g,hk)g(\gamma(h,k)), \forall g,h,k \in G\}$$

For $\gamma \in Z^2(G, L^\times)$ we conclude (setting $g = h = id$) that $\gamma(id,id)\gamma(id,k) = \gamma(id,k)\gamma(id,k)$ holds for all $k \in G$. Similarly, setting $h = k = id$, yields $\gamma(g,id)\gamma(g,id) = \gamma(g,id)g(\gamma(id,id))$. Hence

$$\gamma(id,g) = \gamma(id,id) \qquad \text{and} \qquad \gamma(g,id) = g(\gamma(id,id)), \qquad \forall g \in G.$$

Set $u = \gamma(id,id)$.

Theorem 5.10 *Let L/K be a Galois extension with Galois group G. Then for any $\gamma \in Z^2(G, L^\times)$, $L \star_\gamma G$ is a central simple K-algebra of dimension $[L:K]^2$ and L as maximal subfield.*

Proof: **...still to come ...** □

Theorem 5.11 *Let L/K be a Galois extension with Galois group G. For any $[A] \in \mathrm{Br}(L/K)$, there exists $\gamma \in Z^2(G, L^\times)$ such that $[A] = [L \star_\gamma G]$.*

Proof: **...still to come ...** □

Group structure on $Z^2(G, L^\times)$. Neutral element $\hat{\epsilon}(g,h) = 1$, for all $g,h \in G$. Definition of 2-coboundary. Given $\delta : G \to L^\times$ define $\hat{\delta} \in Z^2(G, L^\times)$ by

$$\hat{\delta}(g,h) := \delta(g)g(\delta(h))\delta(gh)^{-1}.$$

The set of 2-coboundaries

$$B^2(G, L^\times) := \{\hat{\delta} : \delta : G \to L^\times\}$$

is a subgroup of $Z^2(G, L^\times)$ and the second cohomology group of G with coefficients in $L^\times$ is defined to be

$$H^2(G, L^\times) = Z^2(G, L^\times)/B^2(G, L^\times)$$

Theorem 5.12 *Let L/K be a Galois extension with Galois group G. Then*

$$\beta : H^2(G, L^\times) \to \mathrm{Br}(L/K), \qquad [\gamma] \mapsto [L \star_\gamma G]$$

is an isomorphism of Abelian groups.

Proof: **...still to come ...** □

Lemma 5.13 *Let R be a ring and e a non-zero idempotent of R. Then $eRe \simeq \mathrm{End}({}_R Re)^{op}$ as rings.*

Proof: **...still to come ...** □

Lemma 5.14 *Let A be a finite dimensional central simple K-algebra with non-zero idempotent $e \in A$. Then $[A] = [eAe]$.*

Proof: **...still to come ...** □

A set of idempotents $\{e_1, \ldots, e_n\}$ of a ring R is called a complete set of orthogonal idempotents of R if $1 = \sum_{i=1}^n e_i$ and $e_i e_j = 0$ for all $i \neq j$.

Lemma 5.15 *Let L/K be a finite Galois extension with Galois group G. Then there exits a unique complete set of central orthogonal idempotents $\{e_g : g \in G\}$ of $L \otimes L$ satisfying:*

$$(a \otimes b)e_g = (1 \otimes g(b)a)e_g = e_g(a \otimes b), \qquad \forall a, b \in L, g \in G.$$

Proof: **...still to come ...** □

Recall the construction of $L \star_\gamma G$ which had basis $\{\overline{g} : g \in G\}$ subject to the multiplication rule

$$(a\overline{g})(b\overline{h}) = ag(b)\gamma(g,h)\overline{gh}.$$

The identity element of $L \star_\gamma G$ was $u^{-1}\overline{id}$ where $u = \gamma(id, id)$. Recall that $u = \gamma(id, id) = \gamma(id, g)$ for all $g \in G$ holds.

And there was an inclusion $i : L \to L \star_\gamma G$ with $i(a) = au^{-1}\overline{id}$.

$$\overline{g}i(a) = \overline{g}(au^{-1}\overline{id}) = g(a)g(u)^{-1}\gamma(g, id)\overline{g} = g(a)\overline{g} = i(g(a))\overline{g}.$$

We shall identify $a \in L$ with $i(a) \in L \star_\gamma G$ and set $u_g := \overline{g}$. Then u_g satisfies

$$u_g a = g(a)u_g, \qquad u_g u_h = \gamma(g,h)u_{gh} \qquad \forall a \in L, g, h \in G \tag{5.5}$$

Note that $1_{L\star_\gamma G} = u^{-1}u_{id}$ and that u_g is invertible with inverse

$$(u_g)^{-1} = g^{-1}\left(\gamma(g, g^{-1})^{-1}u^{-1}\right)u_{g^{-1}},$$

because

$$u_g g^{-1}\left(\gamma(g, g^{-1})^{-1}u^{-1}\right)u_{g^{-1}} = \gamma(g, g^{-1})^{-1}u^{-1}u_g u_{g^{-1}} = \gamma(g, g^{-1})^{-1}u^{-1}\gamma(g, g^{-1})u_{id} = 1_{L\star_\gamma G}.$$

Lemma 5.16 *Let L/K be a finite Galois extension with Galois field G. Let $\{e_g : g \in G\}$ be the idempotents of $L \otimes L$ as in Lemma 5.15 and set $e = e_{id}$. Then*

$$L \star_{\gamma\gamma'} G \simeq e\,(L \star_\gamma G) \otimes_K \big(L \star_{\gamma'} G\big)\, e$$

as K-algebras and in particular $\beta([\gamma\gamma']) = \beta([\gamma])\beta([\gamma'])$.

Proof: Let $\{e_g : g \in G\}$ be the idempotents of $L \otimes L$ as in Lemma 5.15. Set $e = e_{id}$. We identify $L \otimes L$ with its image in $(L \star_\gamma G) \otimes_K (L \star_\gamma G)$.

Denote by $\{u_g : g \in G\}$ the L-basis of $L \star_\gamma G$ of invertible elements that satisfies

$$u_g a = g(a) u_g \qquad \text{and} \qquad u_g u_h = \gamma(g,h) u_{gh} \qquad\qquad \forall g,h \in G, a \in L.$$

Then $(u_g^{-1} \otimes 1)e(u_g \otimes 1)$ is an idempotent of $L \star_\gamma G$ and lies actually in $L \otimes L$, because for any $a, b \in L$ and $g \in G$ we have $(u_g^{-1} \otimes 1)(a \otimes b)(u_g \otimes 1) = g^{-1}(a) \otimes b \in L \otimes L$. Thus $(u_g^{-1} \otimes 1)e(u_g \otimes 1) \in L \otimes L$. Since $u_g a = g(a) u_g$, we also have $a u_g^{-1} = u_g^{-1} g(a)$ and we calculate, for all $a, b \in L$ and $g \in G$:

$$\begin{aligned}(a \otimes b)(u_g^{-1} \otimes 1)e(u_g \otimes 1) &= (u_g^{-1} \otimes 1)(g(a) \otimes b)e(u_g \otimes 1) \\ &= (u_g^{-1} \otimes 1)(1 \otimes g(a)b)e(u_g \otimes 1) = (1 \otimes g(a)b)(u_g^{-1} \otimes 1)e(u_g \otimes 1)\end{aligned}$$

Hence the idempotent $(u_g^{-1} \otimes 1)e(u_g \otimes 1) \in L \otimes L$ satisfies the same identity as e_g and must be equal to e_g be the uniqueness of it, i.e. $(u_g^{-1} \otimes 1)e(u_g \otimes 1) = e_g$ or equivalently

$$e(u_g \otimes 1) = (u_g \otimes 1)e_g. \tag{5.6}$$

Similarly, if $\{v_g : g \in G\}$ denotes an L-basis of $L \star_{\gamma'} G$ of invertible elements that satisfies

$$v_g a = g(a) v_g \qquad \text{and} \qquad v_g v_h = \gamma'(g,h) u_{gh} \qquad\qquad \forall g,h \in G, a \in L,$$

then $(1 \otimes v_g)e(1 \otimes v_g^{-1} \otimes 1)$ is an idempotent of $L \star_\gamma G$ and lies actually in $L \otimes L$, because for any $a, b \in L$ and $g \in G$ we have: $(1 \otimes v_g)(a \otimes b)(1 \otimes v_g^{-1}) = a \otimes g(b) \in L \otimes L$. Thus $(1 \otimes v_g)e(1 \otimes v_g^{-1}) \in L \otimes L$. Since $v_g b = g(b) v_g$, we also have $b v_g = g^{-1}(b) v_g$ and we calculate, for all $a, b \in L$ and $g \in G$:

$$\begin{aligned}(a \otimes b)(1 \otimes v_g)e(1 \otimes v_g^{-1}) &= (1 \otimes v_g)(a \otimes g^{-1}(b))e(1 \otimes v_g^{-1}) \\ &= (1 \otimes v_g)(1 \otimes a g^{-1}(b))e(1 \otimes v_g^{-1}) = (1 \otimes g(a)b)(1 \otimes v_g)e(1 \otimes v_g^{-1})\end{aligned}$$

Hence the idempotent $(1 \otimes v_g)e(1 \otimes v_g^{-1}) \in L \otimes L$ also satisfies the same identity as e_g and must be equal to e_g, i.e. $(1 \otimes v_g)e(1 \otimes v_g^{-1}) = e_g$ or equivalently

$$(1 \otimes v_g)e = e_g(1 \otimes v_g). \tag{5.7}$$

Let $\{w_g : g \in G\}$ an analogous L-basis for $L \star_{\gamma\gamma'} G$ satisfying

$$w_g a = g(a) w_g \qquad \text{and} \qquad w_g w_h = \gamma(g,h)\gamma'(g,h) w_{gh} \qquad\qquad \forall g,h \in G, a \in L$$

and define the map

$$\psi : L \star_{\gamma\gamma'} G \to e\,\big(L \star_\gamma G \otimes L \star_{\gamma'} G\big)\, e, \qquad \psi(a w_g) = (1 \otimes a)e(u_g \otimes v_g)e, \qquad \forall g \in G, a \in L.$$

Since $(1 \otimes a)e = e(1 \otimes a)$, the image of ψ belongs certainly to $e\left(L \star_\gamma G \otimes L \star_{\gamma'} G\right) e$. For any $g, h \in G$ and $a, b \in L$, using equations (5.6) and (5.7) yields:

$$\begin{aligned}
\psi(aw_g)\psi(bw_g) &= (1 \otimes a)e(u_g \otimes v_g)e(1 \otimes b)e(u_h \otimes v_h)e \\
&= (1 \otimes ag(b))e(u_g \otimes v_g)e(u_h \otimes v_h)e \qquad \text{using the property of } e \text{ and } v_g \\
&= (1 \otimes ag(b))e(u_g \otimes 1)e_g(u_h \otimes v_g v_h)e \qquad \text{using (5.7)} \\
&= (1 \otimes ag(b))e(u_g u_h \otimes v_g v_h)e \qquad \text{using (5.6)} \\
&= (1 \otimes ag(b))e(\gamma(g,h)u_{gh} \otimes \gamma'(g,h)v_{gh})e \qquad \text{using properties of } u_g \text{ and } v_g \\
&= (1 \otimes ag(b)\gamma(g,h)\gamma'(g,h))e(u_{gh} \otimes v_{gh})e \qquad \text{using the property of } e \\
&= \psi(ag(b)\gamma(g,h)\gamma'(g,h)w_{gh}) \\
&= \psi((aw_g)(bw_h))
\end{aligned}$$

Note also that the identity of $L \star_{\gamma\gamma'} G$ is mapped to e, because for $u = \gamma(id, id)$ and $v = \gamma'(id, id)$, we have $1_{L\star_{\gamma\gamma'}G} = (uv)^{-1}w_{id}$ and hence

$$\begin{aligned}
\psi(1_{L\star_{\gamma\gamma'}G}) &= (1 \otimes u^{-1}v^{-1})e(u_{id} \otimes v_{id})e \\
&= (u^{-1} \otimes v^{-1})e(u_{id} \otimes v_{id})e = e(1_{L\star_\gamma G} \otimes 1_{L\star_{\gamma'}G})e = e.
\end{aligned}$$

Since $L \star_{\gamma\gamma'} G$ is a simple algebra, ψ is injective. Let $a, b \in L$ and $g, h \in G$. If $g \neq h$, then $e(au_g \otimes bv_h)e = 0$, because by equations (5.6) and (5.7) we have

$$e(au_g \otimes bv_h)e = (a \otimes b)e(u_g \otimes v_h)e = (a \otimes b)e(u_g \otimes 1)e_g e_h(1 \otimes v_h)e = 0,$$

since $e_g e_h = 0$ if $g \neq h$. On the other hand, any element of the form $e(au_g \otimes bv_g)e$ is equal to

$$e(au_g \otimes bv_g)e = (1 \otimes ab)e(u_g \otimes v_g)e = \psi(abw_g).$$

Thus, ψ is also surjective and hence an isomorphism. □

Corollary 5.17 *The Brauer group of a field is a torsion group.*

Proof: We have seen that any $[A] \in \mathrm{Br}(K)$ belongs to some $\mathrm{Br}(L/K)$, with L/K a finite Galois extension and Galois group G. Then we have seen that $H^2(G, L^\times) \simeq \mathrm{Br}(L/K)$ and that $[A] = [L \star_\gamma G] = \beta([\gamma])$, for some $\gamma \in Z^2(G, L^\times)$. Hence we only need to show that $H^2(G, L^\times)$ is a torsion group for each Galois group G of a finite Galois extension L/K. Let $\gamma \in Z^2(G, L^\times)$. Using the defining relation of a 2-cocyles,

$$\gamma(g,h)\gamma(gh,k) = \gamma(g,hk)g(\gamma(h,k)), \qquad \forall g, h, k \in G$$

we calculate:

$$\gamma(g,h)^n \prod_{k\in G} \gamma(gh,k) = \prod_{k\in G} (\gamma(g,hk)g(\gamma(h,k)))$$

Define $\delta : G \to L^\times$ by

$$\delta(g) := \prod_{k\in G} \gamma(g,k).$$

Then we obtain

$$\begin{aligned}\gamma(g,h)^n &= \prod_{k\in G}\left(\gamma(g,hk)g(\gamma(h,k))\gamma(gh,k)^{-1}\right)\\ &= \left(\prod_{k\in G}\gamma(g,hk)\right)g\left(\prod_{k\in G}\gamma(h,k)\right)\left(\prod_{k\in G}\gamma(gh,k)\right)^{-1}\\ &= \delta(g)g\left(\delta(h)\right)\delta(gh)^{-1} = \hat{\delta}(g,h).\end{aligned}$$

Thus, $\gamma^n = \hat{\delta} \in B^2(G, L^\times)$, i.e. $[\gamma]$ has finite order.

□

We finish with an example.

Let L/K be a Galois extension with Galois group G. Then for any $\gamma \in Z^2(G, L^\times)$ we can define $\delta : G \to L^\times$ as $\delta(g) = \gamma(id, id)^{-1}$, for all $g \in G$ and conclude that

$$\hat{\delta}(g,h) = \delta(g)g(\delta(h))\delta(gh)^{-1} = g\left(\gamma(id,id)^{-1}\right), \qquad \forall g, h \in G.$$

In particular $\gamma' = \hat{\delta}$ satisfies

$$\gamma'(id, g) = \gamma'(id, id) = 1 = g(1) = g(\gamma'(id, id)) = \gamma'(g, id), \qquad \forall g \in G.$$

Therefore, any class $[\gamma] \in H^2(G, L^\times)$ can be represented by some $\gamma \in Z^2(G, L^\times)$ with $\gamma(id, id) = \gamma(id, g) = \gamma(g, id) = 1$ for all $g \in G$.

We assume now that $[L : K] = 2$ and $G = \{id, \sigma\}$. For any $[\gamma] \in H^2(G, L^\times)$ with $\gamma(id, id) = \gamma(id, \sigma) = \gamma(\sigma, id) = 1$ we also have by the the 2-cocycle condition with all three parameters equal to σ:

$$\gamma(\sigma,\sigma) = \gamma(\sigma,\sigma)\gamma(\sigma^2,\sigma) = \gamma(\sigma,\sigma^2)\sigma(\gamma(\sigma,\sigma)) = \sigma(\gamma(\sigma,\sigma)) \in L^\sigma = K$$

Hence $\gamma(\sigma, \sigma) \in K^\times$. Define $\psi : K^\times \to H^2(G, L^\times)$ with $b \mapsto \psi(b) = [\gamma_b]$, where

$$\gamma_b(\sigma,\sigma) = b \qquad \text{and} \qquad \gamma_b(id,id) = \gamma_b(id,\sigma) = \gamma_b(\sigma,id) = 1.$$

Then ψ is a surjective group homomorphism, because for any $b, b' \in K^\times$ we have $\psi(bb') = [\gamma_{bb'}]$ with

$$\gamma_{bb'}(\sigma,\sigma) = bb' = \left(\gamma_b\gamma_{b'}\right)(\sigma,\sigma).$$

Hence $\psi(bb') = \psi(b)\psi(b')$.

Recall the norm $n_{L/K} : L \to K$ defined by $n_{L/K}(x) = x\sigma(x)$, for all $x \in L$. The norm is multiplicative and in particular, $n_{L/K}(L^\times)$ is a multiplicative subgroup of $K^\times$. We will show that $\mathrm{Ker}(\psi) = n_{L/K}(L^\times)$. For any $b = n_{L/K}(x) = x\sigma(x)$, we can define $\delta : G \to L^\times$ with $\delta(id) = 1$ and $\delta(\sigma) = x$ and conclude:

$$\begin{aligned}\hat{\delta}(id,id) &= \delta(id)^2\delta(id)^{-1} = 1 = \gamma_b(id,id)\\ \hat{\delta}(\sigma,id) &= \delta(\sigma)\sigma(\delta(id))\delta(\sigma)^{-1} = 1 = \gamma_b(\sigma,id)\\ \hat{\delta}(id,\sigma) &= \delta(id)\delta(\sigma)\delta(\sigma)^{-1} = 1 = \gamma_b(id,\sigma)\\ \hat{\delta}(\sigma,\sigma) &= \delta(\sigma)\sigma(\delta(\sigma))\delta(id)^{-1} = x\sigma(x) = b = \gamma_b(\sigma,\sigma).\end{aligned}$$

Hence $n_{L/K}(L^\times) \subseteq \mathrm{Ker}(\psi)$. On the other hand, if $b \in \mathrm{Ker}(\psi)$, then $\gamma_b = \hat{\delta}$, for some $\delta : G \to L^\times$. Hence, $1 = \gamma_b(id, id) = \delta(id)^2\delta(id)^{-1} = \delta(id)$ and

$$b = \gamma_b(\sigma, \sigma) = \delta(\sigma)\sigma(\delta(\sigma))\delta(\sigma^2)^{-1} = n_{L(K}(\delta(\sigma)) \in n_{L/K}(L^\times).$$

Thus we proved,

$$K^\times/n_{L/K}(L^\times) \simeq H^2(G, L^\times) \simeq \mathrm{Br}(L/K).$$

Index

R-balanced, 18
$\mathbb{Z}$-bilinear, 18
nth power residue modulo m, 7

anti-algebra homomorphism, 3

bimodule, 20

centralizer, 9
cyclotomic polynomial of index n, 12
cyclotomic polynomials., 11

extension of scalars, 24

involution, 3

Legendre symbol, 7

norm, 6

opposite algebra, 22

primitive roots of unity, 12
pure tensor, 19

quadratic residue modulo m, 7

restriction of scalars, 24

separable algebra, 27
separable element, 26
separable extension, 26

tensor product, 18
tensor product of algebras, 22

Bibliography

[1] Benson Farb and R. Keith Dennis, *Noncommutative algebra*, Graduate Texts in Mathematics, vol. 144, Springer-Verlag, New York, 1993. MR1233388

[2] F.G. Frobenius, *Über lineare Substitutionen und bilineare Formen*, J. Reine Angew. Math. **84** (1878), 1–63, DOI 10.1515/crelle-1878-18788403. MR1581640

[3] T. Y. Lam, *A first course in noncommutative rings*, 2nd ed., Graduate Texts in Mathematics, vol. 131, Springer-Verlag, New York, 2001. MR1838439

[4] ———, *Lectures on modules and rings*, Graduate Texts in Mathematics, vol. 189, Springer-Verlag, New York, 1999. MR1653294

[5] Joseph Rotman, *Galois theory*, 2nd ed., Universitext, Springer-Verlag, New York, 1998. MR1645586