Wedderburn's Little Theorem

Gabriel Ribeiro

April 2021

The goal of these notes is to prove Wedderburn's little theorem, which states that a finite division ring is necessarily commutative, assuming some basic non-commutative algebra. Nevertheless, we explain in a first section everything from non-commutative algebra that is needed.

1 Basic non-commutative algebra

Let A be a finite division ring and k be its center. We observe that k is indeed a field since the inverse a^{-1} of an element $a \in k^\times$ is automatically in k. Indeed, clearly a^{-1} commutes with 0 and, if $b \in A^\times$, then $ab^{-1} = b^{-1}a$ implies

$$ba^{-1} = (ab^{-1})^{-1} = (b^{-1}a)^{-1} = a^{-1}b$$

and so $a^{-1} \in k$. Since A is finite, A is a finite-dimensional k-algebra. Moreover, as every non-zero element in A is invertible, A has no two-sided ideals other than $\{0\}$ and A itself. In other words, A is a finite-dimensional *simple*[1] k-algebra.

The main classification result about such algebras is the theorem below, which we won't prove but whose proof is not very difficult and can be found in [1].

Theorem 1 (Wedderburn)**.** *Let A be a finite-dimensional simple algebra over a field k. There exist an integer $n \geqslant 1$ and a division algebra D over k so that A is isomorphic to the matrix ring $M_n(D)$. Both n and D are uniquely determined up to isomorphism.*

Of course, since our ring A is already a division algebra over k, it suffices to take $n = 1$ and $D = A$. But we'll use this result in a non-trivial way. Indeed, fix an algebraic closure $\overline{k}$ of k and consider the $\overline{k}$-algebra $A_{\overline{k}} := A \otimes_k \overline{k}$. Since $\dim_k A = \dim_{\overline{k}} A_{\overline{k}}$, our new algebra is still finite-dimensional. Moreover, $A_{\overline{k}}$ is also simple as the following result shows.

Proposition 1. *If A and B are simple k-algebras, then so is $A \otimes_k B$.*

[1] A ring is said to be simple if it has no non-trivial ideals.

Proof. Let I be a nonzero two-sided ideal of $A \otimes_k B$. We begin by supposing that there is a pure nonzero tensor $a \otimes b$ in I. Since A is simple, the two-sided ideal AaA generated by $a \neq 0$ coincides with A. Hence $u_1 a v_1 + \ldots + u_m a v_m = 1$ for some $u_i, v_i \in A$. It follows that

$$1 \otimes b = \left(\sum_{i=1}^{m} u_i a v_i \right) \otimes b = \sum_{i=1}^{m} (u_i \otimes 1) \cdot (a \otimes b) \cdot (v_i \otimes 1) \in I.$$

Reversing the roles of A and B we conclude that $1 \otimes 1$ is in I as well and so $I = A \otimes_k B$.

Now, let $x = a_1 \otimes b_1 + \ldots + a_n \otimes b_n$ be a nonzero element of I\ with the smallest possible n. Both the sets $\{a_1, \ldots, a_n\}$ and $\{b_1, \ldots, b_n\}$ are linearly independent over k since otherwise we could rewrite this expression to make it shorter. Also, using the same trick as before we can suppose that $a_1 = 1$. Indeed, there are $u_i, v_i \in A$ such that $u_1 a_1 v_1 + \ldots + u_m a_1 v_m = 1$. Then

$$\sum_{i=1}^{m} u_i x v_i = \underbrace{\left(\sum_{i=1}^{m} u_i a_1 v_i \right)}_{=1} \otimes b_1 + \ldots + \left(\sum_{i=1}^{m} u_i a_n v_i \right) \otimes b_n$$

is an element in I of the desired form.

Suppose that $n > 1$. We have that $a_2 \notin k$ since otherwise a_1 and a_2 would be linearly dependent. Since the center of A is precisely k, there exists $a \in A$ such that $a a_2 \neq a_2 a$. Consider the element

$$(a \otimes 1) \cdot x - x \cdot (a \otimes 1) = (a a_2 - a_2 a) \otimes b_2 + \ldots + (a a_2 - a_2 a) \otimes b_2 \in I.$$

Since $\{b_1, \ldots, b_n\}$ is linearly independent over k and $a a_2 - a_2 a \neq 0$, this element is not zero, which contradicts the minimality of n. Ergo, $n = 1$ and so the result follows from the special case that was proved. $\square$

Before we apply Wedderburn's theorem to $A_{\overline{k}}$, we make one last observation. The only finite-dimensional division algebra D over $\overline{k}$ is $\overline{k}$ itself. Indeed, if $\overline{k}$ is strictly contained in D, let $a \in D \setminus \overline{k}$. Then $\overline{k}[a]$ is a finite, thus algebraic, proper extension of $\overline{k}$. This contradicts the hypothesis that $\overline{k}$ is algebraically closed.

Applying this observation to Wedderburn's theorem, we have that $A_{\overline{k}}$ is isomorphic to $M_n(\overline{k})$ for some integer $n \geqslant 1$. This integer is said to be the *degree* of A. In particular, $\dim_k A = \dim_{\overline{k}} A_{\overline{k}} = n^2$.

By composing the base change $A \to A \otimes_k \overline{k} \cong M_n(\overline{k})$ with the determinant, we obtain a multiplicative map $N : A \to k$, called the *reduced norm*. The fact that its image is contained in k follows from Galois descent and it is independent of the choice of the isomorphism $A_{\overline{k}} \cong M_n(\overline{k})$ by the Noether-Skolem theorem. Since it is multiplicative, it maps $A^\times$ to $k^\times$. In particular, if $A \neq k$, we get a homogeneous polynomial of degree n in n^2 variables that has no non-trivial root.

2 The Chevalley-Warning theorem

In order to prove that our ring A is commutative, we have to prove that it is equal to its center. That is, we want to prove that its dimension over k, the integer we called n^2, is equal to 1. This will follow from our next result, which is incredible by itself.

Theorem 2 (Chevalley-Warning)**.** *Let k be a finite field of characteristic p and let $P \in k[x_1, \dots, x_m]$ be a polynomial whose degree is strictly inferior to m. Then, the number of solutions in k^m of $P(x_1, \dots, x_m) = 0$ is divisible by p. In particular, if P is homogeneous, then this equation has a non-trivial solution.*

Proof. We begin the proof by observing that, if k has q elements, the map $x \mapsto x^{q-1}$ is the indicator function on k. It follows that the number of solutions to our equation is congruent modulo p to

$$N := \sum_{x \in k^n} \left(1 - P(x)^{q-1}\right).$$

We'll show that every monomial of $1 - P^{q-1}$ sums to zero modulo p. Consider one such monomial $ax_1^{e_1} \dots x_m^{a_m}$. Since its degree is strictly less than $(q-1)m$, we have $a_i < q-1$ for at least one i. Let j be this index. As

$$\sum_{(x_i) \in k^n} ax_1^{e_1} \dots x_m^{a_m} = a \prod_{i=1}^{m} \left(\sum_{x_i \in k} x_i^{a_i} \right),$$

it suffices to show that $\sum_{x_j \in k} x_j^{a_j} \equiv 0 \pmod{p}$. If $a_j = 0$, this is clear. Else, let y be a generator of $k^\times$. Then,

$$\sum_{x_j \in k} x_j^{a_j} \equiv \sum_{x_j \in k^\times} x_j^{a_j} \equiv \sum_{k=0}^{q-2} (y^m)^{a_j} \equiv \sum_{k=0}^{q-2} (y^{a_j})^m \equiv \frac{1 - (y^{a_j})^{q-1}}{1 - y^{a_j}} \equiv 0 \pmod{p},$$

concluding our proof. □

Corollary 1 (Wedderburn's little theorem)**.** *Every finite division ring is commutative.*

Proof. As in the previous section, let A be a finite division ring and k be its center, which is a finite field. Suppose that the dimension of A over k is strictly bigger than 1. If $e_1, \dots, e_{n^2}$ is a basis for A over k, the map given by the reduced norm

$$P(x_1, \dots, x_{n^2}) := N(x_1 e_1 + \dots + x_{n^2} e^{n^2})$$

is an homogeneous polynomial of degree n in n^2 variables that has no non-trivial root. Since $n < n^2$, the Chevalley-Warning applies and contradicts our supposition that $n > 1$. It follows that $A = k$. □

3 Related stuff

An important invariant of a field k is its *Brauer group*, composed by the finite-dimensional division algebras over k with a natural operation, which is well described in [1]. A restatement of Wedderburn's little theorem is the fact that the Brauer group of a finite field is trivial. Our proof of this result was based on the affirmation that every homogeneous polynomial of degree d with n variables has a non-trivial root whenever $d < n$. The fields satisfying such property are said to be *quasi-algebraically closed* or C_1.

As we saw, algebraically closed fields and finite fields are C_1. Moreover, C_1 fields have trivial Brauer group. Another interesting class of C_1 fields are those of transcendence degree 1 over an algebraically closed field, for example $\mathbb{C}(x)$. This result is called *Tsen's theorem*. The number-theoretic reader may be interested in knowing that the maximal unramified extension of a complete field with a discrete valuation and a perfect residue field is C_1. Moreover, a complete field with a discrete valuation and an algebraically closed residue field is also C_1. These latter results may be found in the classic [2].

References

[1] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*. Vol. 165. Cambridge University Press, 2017.

[2] Jean-Pierre Serre. *Local fields*. Vol. 67. Springer Science & Business Media, 2013.