Bull. Aust. Math. Soc. **97** (2018), 382–385
doi:10.1017/S0004972718000035

A NOTE ON THE FUNDAMENTAL THEOREM OF ALGEBRA

MOHSEN ALIABADI

(Received 10 December 2017; accepted 31 December 2017; first published online 28 March 2018)

Abstract

The algebraic proof of the fundamental theorem of algebra uses two facts about real numbers. First, every polynomial with odd degree and real coefficients has a real root. Second, every nonnegative real number has a square root. Shipman [‘Improving the fundamental theorem of algebra’, *Math. Intelligencer* **29**(4) (2007), 9–14] showed that the assumption about odd degree polynomials is stronger than necessary; any field in which polynomials of prime degree have roots is algebraically closed. In this paper, we give a simpler proof of this result of Shipman.

2010 *Mathematics subject classification*: primary 12A55; secondary 12E05.

Keywords and phrases: fundamental theorem of algebra, fundamental theorem of Galois theory, perfect field.

1. Introduction

The *fundamental theorem of algebra*, abbreviated here as FTA, states that the field of complex numbers is algebraically closed. That is, every polynomial of degree n with real or complex coefficients has exactly n zeros (counting multiplicities) in the field of complex numbers. It is not possible to give a simple formula for the roots of polynomials of degree greater than four. Abel proved that there is no formula for the roots of a general fifth degree polynomial equation in terms of its coefficients that uses only the operations of addition, subtraction, multiplication, division and taking nth roots. That is, a fifth degree polynomial equation is not solvable by radicals. Galois gave conditions under which polynomial equations can be solved by radicals, originating what is now known as Galois theory.

Hundreds of proofs have been given for the FTA. There is a summary of the known proofs in [4]; see also [1, 3] for some recent accounts. Shipman [6] provided a new approach to the FTA. Not only did he improve the proof, but he also improved the theorem itself. The algebraic view of the FTA is that under certain algebraic hypotheses, a field of characteristic 0 must be algebraically closed. In [6], Shipman gives the optimal conditions and generalises the theorem to characteristic p. His main result is a necessary and sufficient (and straightforwardly computable) condition for a finite set of 'degree axioms' (that all polynomials of the given degrees have roots) to imply a further degree axiom in all fields. We give a simpler version of this strengthened FTA to show that all fields in which prime degree polynomials have roots are algebraically closed. Previous proofs only worked for characteristic 0 and needed assumptions for polynomials of degree two and all odd degrees rather than just prime degrees. Our main tools are the fundamental theorem of Galois theory and the primitive element theorem.

2. The alternative proof

A field K is said to be *perfect* if either K has characteristic 0, or K has characteristic $p > 0$ and every element of K is a pth power. The *primitive element theorem* states that if K is perfect, then every finite extension of K has the form $K(\alpha)$ for some α (see, for example, [5, Theorem 1.6.17]).

Throughout, K stands for a field for which all polynomials in $K[x]$ of prime degree have roots in K. Note that this condition implies that K is a perfect field because if $\operatorname{char} K = p > 0$, the polynomial $x^p - a$ has a root in K for any $a \in K$, and so $K^p = K$. Thus every finite extension of K has the form $K(\alpha)$, for some α.

The following two lemmas derive properties of the field K in case K is not algebraically closed.

Lemma 2.1. *Assume that K is not algebraically closed. Then, there exists a prime p which divides the degree of any nonlinear irreducible polynomial $p(x) \in K[x]$.*

Proof. Assume to the contrary that there is no such prime. Let $p(x) \in K[x]$ be a nonlinear irreducible polynomial and assume that $p_1, \ldots, p_n$ are the prime divisors of $\deg p(x)$. There exist nonlinear irreducible polynomials $f_1(x), f_2(x), \ldots, f_n(x) \in K[x]$ such that $p_i \nmid \deg f_i(x)$ for $1 \le i \le n$. Set $F(x) = p^{k_0}(x) f_1^{k_1}(x) \cdots f_n^{k_n}(x)$, where $k_0, \ldots, k_n$ are nonnegative integers and will be determined later. Clearly,

$$\gcd(\deg p(x), \deg f_1(x), \ldots, \deg f_n(x)) = 1$$

and $\deg F(x) = k_0 \deg p(x) + \sum_{i=1}^{n} k_i \deg f_i(x)$.

Choose $k_0, \ldots, k_n$ so that $\deg F(x)$ is a prime number. Such a choice of $k_0, \ldots, k_n$ is possible because of the fact that there are infinitely many primes and sums of integers with gcd = 1 generate all sufficiently large integers. Since $\deg F(x)$ is prime, $F(x)$ has a root in K which is a contradiction. □

Lemma 2.2. *Assume that K is not algebraically closed. Then K has no field extension of prime degree.*

Proof. Assume to the contrary that L is an extension of K with $[L : K] = p$, where p is a prime. Then, there exists $\alpha \in L \backslash K$ such that $L = K(\alpha)$. If $m(x) \in K[x]$ is the minimal polynomial of α, then $\deg m(x) = p$ and $m(x)$ has a root in K which contradicts the fact that $m(x)$ is irreducible in $K[x]$. □

https://doi.org/10.1017/S0004972718000035 Published online by Cambridge University Press

In the following lemma, we provide a simple proof of the existence of a Sylow p-subgroup of a finite group of order $p^r m$ (the first Sylow theorem). We will also show that p-groups have subgroups of index p. The main tool needed in the proof is the orbit-stabiliser theorem (see, for example, [2, Theorem 11.4]). We will use these results for finite groups in the proof of our main theorem to extract specific subgroups of Galois groups of some extensions of K.

Lemma 2.3. *Let G be a finite group of order $p^r m$, where p is prime, r is a positive integer and* $\gcd(m, p) = 1$.

(i) *G has at least one Sylow p-subgroup.*

(ii) *If $m = 1$, then G has a subgroup of order p^{r-1}, that is, p-groups have subgroups of index p.*

Proof. (i) Let G act on subsets of G of size p^r by left multiplication. The number of such subsets is $\binom{p^r m}{p^r}$, which is not divisible by p. Consequently, since the orbits partition the set on which a group acts, there is at least one orbit S whose size is not divisible by p. If P is the stabiliser of S, then by the orbit-stabiliser theorem, the size of the orbit is $[G : P] = |G|/|P| = p^r m/|P|$. For this to fail to be divisible by p, we must have $p^r \mid |P|$, and therefore $p^r \le |P|$. But for any fixed $x \in S$, the map of P into S given by $g \to gx$ is injective. (Indeed g belongs to the stabiliser of S, so that $gS = S$.) Thus $|P| \le |S| = p^r$. We conclude that $|P| = p^r$, hence P is a Sylow p-subgroup.

(ii) By a similar argument, the number of subsets of G of size p^{r-1} is $\binom{p^r}{p^{r-1}}$ which is exactly divisible by p but not divisible by p^2. Under the action of left multiplication all orbits have size dividing p^r and also have size at least p, therefore at least one orbit has size exactly p (because p^2 does not divide the number of subsets of G of size p^{r-1}). In an orbit of size p the subset containing the group identity has size p^{r-1} and is its own stabiliser subgroup and the other subsets are its cosets. □

Now we are ready to prove our main theorem. For axiomatisation of algebraically closed fields, this is the best possible result, as there are counterexamples if a single prime is excluded (see [6, Theorem 3]). The theorem is a corollary of the more general results in [6], but we use a different and simpler technique to prove it.

Theorem 2.4. *K is algebraically closed.*

Proof. Assume to the contrary that K is not algebraically closed. By Lemma 2.2, K has no field extension of degree p, where p is the prime obtained in Lemma 2.1. Let L be a Galois extension of K with $[L : K] = p^r m$, where $r, m \in \mathbb{N}$ and $\gcd(m, p) = 1$. By the fundamental theorem of Galois theory and Lemma 2.3, there is an intermediate subfield L' of K/L such that $[L : L'] = p^r$, and so $[L' : K] = m$. If $m > 1$, choose $\alpha \in L' \backslash K$ and assume that $m(x)$ is the minimal polynomial of α over K. Then $\deg m(x) \mid m$. Since $m(x)$ is irreducible, Lemma 2.1 implies that $p \mid \deg m(x)$. Therefore $p \mid m$ and this contradicts $\gcd(m, p) = 1$. Thus, $m = 1$ and $[L : K] = p^r$. Again, by the fundamental theorem of Galois theory and Lemma 2.3, there is an intermediate subfield L' of K/L for which $[L : L'] = p^{r-1}$. Then $[L' : K] = p$. But this contradicts

https://doi.org/10.1017/S0004972718000035 Published online by Cambridge University Press

Lemma 2.2. Thus K has no Galois extension and since K is a perfect field, it must be algebraically closed. □

Remark 2.5. Note that the primitive element theorem is only proven for fields of characteristic 0. There are fields of characteristic $p > 0$, which have an extension of degree p^2 that cannot be generated by adjoining a single element, so we cannot always find an element whose minimal polynomial has degree p^2. However, this case cannot occur in the proof of Theorem 2.4, because K is a perfect field. (All elements have pth roots, which follows from the assumption that polynomials of degree p have roots.) Perfect fields always have primitive elements.

Acknowledgements

I am grateful to Professor Shmuel Friedland for many instructive conversations and encouragement. I thank Dr. Joseph Shipman for his useful suggestions and comments especially providing a nice direction to prove Lemma 2.3 and detecting several mistakes in the earlier version of the proof of Theorem 2.4. I also thank the referees for making several useful comments.

References

[1] S. Basu and D. J. Velleman, 'On Gauss's first proof of the fundamental theorem of algebra', *Amer. Math. Monthly* **124**(8) (2017), 688–694.

[2] J. B. Carrell, *Groups, Matrices and Vector Spaces. A Group Theoretic Approach to Linear Algebra* (Springer, New York, 2017).

[3] M. Eisermann, 'The fundamental theorem of algebra made effective: an elementary real-algebraic proof via Sturm chains', *Amer. Math. Monthly* **119**(9) (2012), 715–752.

[4] B. Fine and G. Rosenberger, *The Fundamental Theorem of Algebra* (Springer, New York, 1997).

[5] A. Levin, *Difference Algebra*, Algebra and Applications, Vol. 8 (Springer, Netherlands, 2008).

[6] J. Shipman, 'Improving the fundamental theorem of algebra', *Math. Intelligencer* **29**(4) (2007), 9–14.

MOHSEN ALIABADI,
Department of Mathematics, Statistics and Computer Science,
University of Illinois, 851 S. Morgan St, Chicago, IL 60607, USA
e-mail: maliab2@uic.edu

https://doi.org/10.1017/S0004972718000035 Published online by Cambridge University Press