Improving the Fundamental Theorem of Algebra

JOSEPH SHIPMAN

The "algebraic part" of the Fundamental Theorem of Algebra says that under certain purely algebraic hypotheses, a field of characteristic 0 must be algebraically closed. In this article I will give a best possible version and extend the theorem to characteristic p. I will also give an algorithm for determining all finitary implications between "degree axioms" of the form "every polynomial of degree n has a root."

The Fundamental Theorem

The "Fundamental Theorem of Algebra" is the usual name for the theorem that the field of complex numbers is algebraically closed. However, all proofs of this fact involve, in addition to algebra, a certain amount of analysis, topology, or complex function theory. The less algebra there is in the proof, the more of other kinds of mathematics there must be. The more algebra there is in the proof, the more generally applicable it is and the easier the non-algebraic part of the proof is.

The book [FR] is an excellent summary of the known proofs of this theorem, which provides an illuminating introduction to many branches of modern mathematics. Hundreds of articles on the Fundamental Theorem of Algebra have been published, almost all of which involve new proofs or variations on old proofs.

Despite all this attention, I have something entirely new to demonstrate. I am going to improve, not simply a proof of the theorem, but *the theorem itself*: assuming less, and concluding more.

Most of the proofs in existence apply only to the complex number field, and contain very little actual algebra; some writers have therefore suggested that the theorem is misnamed. However, Gauss's 1815 "second proof" of the theorem [G], which was the first entirely rigorous proof, justifies the name. In this proof, Gauss showed by purely algebraic reasoning that every real polynomial resolves into factors of the first and second degree. A modernized and simplified version of Gauss's proof (due to E. Artin) is given by van der Waerden [vdW], who states the theorem as follows:

If in an ordered field K every positive element possesses a square root and every polynomial of odd degree at least one root, then the field $K(i)$ obtained by adjoining i is algebraically closed.

That the real field satisfies these conditions is a very easy piece of analysis; the algebra required is much harder, but as a reward the theorem is applicable to all "real closed" fields, not just the real and complex numbers.

An examination of the proof in [vdW] shows that it does not need K to be ordered, only that every element of K have a square root in $K(i)$ (which is an easy consequence of K's being ordered and having square roots for positive elements). The proof also implicitly uses that K has characteristic 0 (which follows from the original restriction to ordered fields), by applying the Primitive Element Theorem. We may therefore restate the theorem more generally:

If a field K has characteristic 0, if all odd-degree polynomials in $K[x]$ have roots in K, and if all elements of K have square roots in $K(i)$, then $K(i)$ is algebraically closed.

In this form, the theorem applies to fields which are not necessarily ordered, and we have the simple corollary:

If K has characteristic 0, and if all polynomials whose degree is 2 or an odd number have roots, then K is algebraically closed.

But we have not gone far enough towards finding the "algebraic essence" of the Fundamental Theorem of Algebra. The hypotheses actually needed for a field to be algebraically closed are much weaker; I shall optimize them.

"Degree Axioms"

Gauss proves the theorem by induction on the number of factors of 2 in the degree of the polynomial. Given a real polynomial $f(x)$ of even degree d, Gauss constructs another real polynomial of degree $\binom{d}{2} = d(d-1)/2$, which has one fewer power of 2, such that the new polynomial has a root in the complex numbers only if f does. Through repetition of the process, a polynomial of odd degree is eventually obtained, from a root of which we may obtain a root for f by solving a sequence of quadratic equations. From the existence of complex roots to real polynomials, we may obtain roots for any complex polynomial $g(x)$ via the real polynomial $g(x)g'(x)$, where g' is the "complex conjugate" of g.

The only properties of the real numbers that Gauss used were the existence of roots for equations of odd degree, and the existence of square roots for non-negative numbers. This "algebraic" proof is more useful than the proofs involving analysis or topology, because it applies to many more fields. Artin and Schreier's theory of "real closed fields" is built on this foundation. A field K is said to be "formally real" if -1 is not a sum of squares. Such K can be ordered, and have characteristic 0. K is "real closed" if every odd-degree polynomial has a root in K and every positive element has a square root. (The definition still applies to fields with no defined order relation, if -1 is not a sum of squares and every element is a square or the negative of a square.)

These assumptions are all expressible in the first-order language of fields. It follows from the work of Tarski [T] that all real closed fields satisfy the same first-order sentences, and the following axiomatization characterizes real closed fields:

Group i) AOF: The conjunction of the standard axioms for ordered fields.

Group ii) Axiom about existence of square roots:

SR: $\forall x_0\, \exists x_1\, ((x_1 * x_1 = x_0)$ or $((x_1 * x_1) + x_0 = 0))$.

Group iii) Degree Axioms (one for each odd integer):

[1]: $\forall x_0\, \exists x_1\, ((x_0 + x_1) = 0)$

[3]: $\forall x_0\, \forall x_1\, \forall x_2\, \exists x_3\, ((x_0 + (x_3 * (x_1 + (x_3 * (x_2 + x_3))))) = 0)$

[5]: $\forall x_0\, \forall x_1\, \forall x_2\, \forall x_3\, \forall x_4\, \exists x_5\, ((x_0 + (x_5 * (x_1 + (x_5 * (x_2 + (x_5 * (x_3 + (x_5 * (x_4 + x_5)))))))))) = 0)$

Etc.

Each "degree axiom" asserts the existence of roots for all polynomials of a given degree. Note that the first degree axiom [1] merely restates the existence of additive inverses and is true in all fields. Note also that the degree axiom [n] implies [d] for any d dividing n, because we can construct a rootless polynomial of degree n by taking a power of a rootless polynomial of degree d.

Since -1 is not a square in an ordered field, the polynomial $(x^2 + 1)$ has no roots. If there were a polynomial of odd degree $d > 1$ with no roots, then we could multiply it by powers of $(x^2 + 1)$ to construct rootless polynomials of degrees $d + 2$, $d + 4$, etc. Therefore, ANY infinite subset of Group iii) suffices to axiomatize real closed fields (together with the axioms AOF and SR).

This is as far as we can weaken the assumptions for an ordered field to be real closed. But the situation is much more interesting when we start with a field which is not necessarily "real."

In the preceding section, we saw that Gauss's proof, as adapted by Artin and van der Waerden, has the corollary

If K has characteristic 0, and if all polynomials whose degree is 2 or an odd number have roots, then K is algebraically closed.

This leads to a complete axiomatization for algebraically closed fields of characteristic 0 (all of which satisfy the same sentences as the complex numbers):

Group i) AF: The conjunction of the standard axioms for fields.

Group ii) Axioms for characteristic 0 (one for each prime):

$C0_2$: $\sim(1 + 1 = 0)$

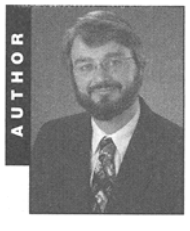
$C0_3$: $\sim(1 + 1 + 1 = 0)$

$C0_5$: $\sim(1 + 1 + 1 + 1 + 1 = 0)$

$C0_7$: $\sim(1 + 1 + 1 + 1 + 1 + 1 + 1 = 0)$

$C0_{11}$: $\sim(1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 + 1 = 0)$

Etc.



JOSEPH SHIPMAN was educated at MIT and Brandeis, where he got a PhD in Logic. In the years since then, he has worked in a variety of fields—biomedical research, software development, and more—while always continuing mathematical research pro bono. At present he is Director of Data Management at ALK Technologies of Princeton, NJ.

He is also devoted to chess, to singing in his church choir, and to his family: wife and four children.

Joseph Shipman
20 Montgomery Avenue
Rocky Hill, NJ 08553
USA
e-mail: JoeShipman@aol.com

Group iii) Degree Axioms ([2] and one for each odd integer)

[2]: $\forall x_0\, \forall x_1\, \exists x_2\, ((x_0 + (x_2 * (x_1 + x_2))) = 0)$

[3]: $\forall x_0\, \forall x_1\, \forall x_2\, \exists x_3\, ((x_0 + (x_3 * (x_1 + (x_3 * (x_2 + x_3))))) = 0)$

[5]: $\forall x_0\, \forall x_1\, \forall x_2\, \forall x_3\, \forall x_4\, \exists x_5\, ((x_0 + (x_5 * (x_1 + (x_5 * (x_2 + (x_5 * (x_3 + (x_5 * (x_4 + x_5)))))))))) = 0$

[7]: $\forall x_0\, \forall x_1\, \forall x_2\, \forall x_3\, \forall x_4\, \forall x_5\, \forall x_6\, \exists x_7\, ((x_0 + (x_7 * (x_1 + (x_7 * (x_2 + (x_7 * (x_3 + (x_7 * (x_4 + (x_7 * (x_5 + (x_7 * (x_6 + x_7)))))))))))))) = 0)$

[9]: $\forall x_0\, \forall x_1\, \forall x_2\, \forall x_3\, \forall x_4\, \forall x_5\, \forall x_6\, \forall x_7\, \forall x_8\, \exists x_9\, ((x_0 + (x_9 * (x_1 + (x_9 * (x_2 + (x_9 * (x_3 + (x_9 * (x_4 + (x_9 * (x_5 + (x_9 * (x_6 + (x_9 * (x_7 + (x_9 * (x_8 + x_9)))))))))))))))) = 0)$

Etc.

The key observation for improving the Fundamental Theorem of Algebra is that each degree axiom $[d]$, when d is an even number >2, is a consequence of *finitely many* of the degree axioms $\{[i] \mid i = 2$ or an odd integer$\}$, together with AF and the axioms for characteristic 0. This follows (nonconstructively) from the Compactness Theorem for first-order logic, but Gauss's proof provides an explicit reduction: $[d]$ follows from [2] and $[\binom{d}{2}] = [d(d-1)/2]$.

Thus, we can prove [6] from [2] and [15]. To prove [8] we can use [2] and [28], and to get [28] we use [2] and [378], and to get [378] we use [2] and [71253].

We will find a necessary and sufficient condition for a set of degree axioms to imply another degree axiom. This will allow us to find an optimal axiomatization of algebraically closed fields, where each axiom is independent of the others. As a bonus, it will turn out that the strengthened theorem is true in fields of all characteristics.

Degree Axioms and Galois Groups

Fix a field K. For now, require K to be of characteristic 0. For every polynomial $f(x)$ in $K[x]$, there is an associated splitting field L and an associated finite Galois group G. Suppose f has degree d and roots $r_1, r_2, \ldots, r_d$ (multiple roots appearing the appropriate number of times with different labels). G acts on the set $\{r_1, r_2, \ldots, r_d\}$, and this action has a fixed-point iff f has a root in K. If the degree axiom $[d]$ is true, then subgroups of S_d which act without fixed-points on the roots are ruled out as possible Galois groups for polynomials of degree d.

On the other hand, if $[d]$ is false, then there is a polynomial $f(x)$ of degree d, with irreducible factors $f_1, f_2, \ldots$, of degrees $d_1, d_2, \ldots$, with each $d_i > 1$ and $d_1 + d_2 + \cdots = d$. Since degrees of irreducible polynomials correspond to degrees of field extensions, there is a sequence of extension fields $K_1, K_2, \ldots$ which correspond to subgroups $G_1, G_2, \ldots$ of the Galois group G of f, where d_i is the degree of K_i over K and also the index of G_i in G. This restricts the possible G to groups such that d can be expressed as the sum of indexes of proper subgroups of G.

Denote by $<a,b,c, \ldots>$ the additive semigroup generated by the positive integers $a,b,c, \ldots$.

For any finite group G, let $<G>$ denote the additive semigroup generated by the indexes in G of its proper subgroups.

We are now ready for a sufficient condition for implications between "degree axioms."

THEOREM 1 *The statement*

$$(*) \qquad ([i_1]\&[i_2]\&\ \ldots\ \&[i_m]) \Rightarrow [n]$$

is true in all fields of characteristic 0 *if*

(**) *for every subgroup G of S_n which acts without fixed-points on* $\{1,2, \ldots, n\}$, *semigroup $<G>$ contains one of the i_j.*

Note that the condition in (**) is obviously computable.

PROOF. Assume the condition (**) is true for $i_1, i_2, \ldots i_m, n$. Choose a field K of characteristic 0, and suppose there is a polynomial f in $K[x]$ of degree n with no roots in K; since degree axiom $[n]$ fails, we now need to falsify one of the degree axioms $[i_j]$.

The Galois group G of the splitting field of f over K acts without fixed-points on the roots of f (if f has multiple roots, we add extra copies of the roots of f to the set G is acting on to get a fixed-point-free action on a set of size n). Every subgroup of index h corresponds to a field extension of K of degree h; in characteristic 0, these extensions have primitive elements, so we can get irreducible polynomials of all those degrees, and multiply them together to get rootless polynomials of all degrees contained in the semigroup $<G>$. By assumption, i_j is in the semigroup for some j in $\{1, \ldots m\}$, and the corresponding rootless polynomial counterexemplifies $[i_j]$, as required. □

COROLLARY 1 $[n]$ *follows from the conjunction of* $[p]$ *for primes dividing n with* $[m]$ *for any sufficiently large m.*

PROOF. For any finite group G, for each prime p dividing $|G|$, G's Sylow-p subgroups have indexes not divisible by p. If $|G|$ is not a prime power, then the gcd of these indexes is 1, and $<G>$ contains all sufficiently large integers; only finitely many G are relevant, so any sufficiently large m causes (**) to be satisfied for all those G. If G is a p-group and p doesn't divide n, then G can't act without fixed-points on $\{1, \ldots, n\}$, because all orbits must have size 1 or a power of p, so (**) is vacuously satisfied. If p does divide n, then we already have $[p]$ on the left-hand side of (**); this suffices, because p-groups have subgroups of index p, so $<G> = <p>$. □

The Fundamental Theorem of Algebra, Improved

These ideas make possible much better versions of the Fundamental Theorem of Algebra: not only do fields of characteristic 0 no longer need degree axioms for composite degrees, but the theorem now applies to fields of all characteristics.

COROLLARY 2 *If a field K has characteristic* 0, *if all odd-prime-degree polynomials in $K[x]$ have roots in K, and if all elements of K have square roots in $K(i)$, then $K(i)$ is algebraically closed.*

PROOF. We are able to replace "odd" with "odd prime" by applying Corollary 1: for any odd composite $[d]$, the primes dividing d are odd and there is a sufficiently large odd prime.

For completeness, I give an argument which does not depend on the proof in [vdW]. Assume $K(i)$ has square roots for all elements and K has roots for polynomials of odd prime degree. Applying Corollary 1, all odd-degree polynomials have roots. If f in $K[x]$ has even degree, its Galois group G has order $2^r m$ for m odd. Corresponding to the 2-Sylow subgroup, which has index m, is an extension of degree m; but there are no irreducible polynomials of odd degree, so $m = 1$ and $|G| = 2^r$. Since p-groups have subgroups of index p, we can build a chain of extensions of degree 2 to reach the splitting field of f; but since $K(i)$ has square roots for all elements, each extension comes from a degree-2 polynomial with coefficients in K, so f splits into linear and quadratic factors. Any polynomial in $K(i)[x]$ can be multiplied by its "conjugate" to get a polynomial in $K[x]$, and from the resulting factorization into linear and quadratic factors we can get a complete split into linear factors in $K(i)[x]$. □

THEOREM 2 *Any field which satisfies [p] for all primes p satisfies [n] for all natural numbers n.*

PROOF. If the field K has characteristic 0, this follows directly from Corollary 1 and the existence of infinitely many primes. The only place where the assumption of characteristic 0 was needed in the proof of Theorem 1 was to obtain primitive elements for algebraic extensions of K; but we have [p] for all primes p, so every element of K has a p-th root in K; this holds in particular for the characteristic of the field, so K is a perfect field, and all algebraic extensions are separable and they have primitive elements anyway. □

Theorem 2 allows us to delete all axioms [n] for composite n from our axiomatization of algebraically closed fields. Can we go further? No!

THEOREM 3 *Theorem 2 is not true if we omit any single prime from the hypothesis.*

PROOF. Let K be the field generated by all algebraic numbers whose degree over Q is not divisible by a given prime p. This K contains no numbers of degree p over Q, because we can write K as an expanding union of fields of finite degree over Q, where each field is obtained from the previous one by adjoining the "next" algebraic number whose degree is not divisible by p—at each stage we have a finite extension whose degree over Q is not divisible by p, so no number of degree p can ever get in. Therefore there are polynomials of degree p in $Q[x]$ (and so also in $K[x]$) with no roots in K. For any other prime q, every polynomial in $K[x]$ of degree q has an irreducible factor of degree not divisible by p, and so has a root r whose degree over K is not divisible by p. But r has the same degree over the subfield of K generated by the coefficients of its irreducible polynomial, which has a finite degree over Q that is not divisible by p; so r also has such a degree and is therefore in K by construction. □

We have thus obtained an "optimal" axiomatization for algebraically closed fields: ACF = {AF, [2], [3], [5], [7], [11], . . . }, where each axiom is independent of the others. Adding the axioms {$C0_2$, $C0_3$, $C0_5$, $C0_7$, . . . } gives an optimal axiomatization for algebraically closed fields of characteristic 0, while adding the single axiom $\sim C0_p$ gives an optimal axiomatization for algebraically closed fields of characteristic p.

However, omitting any set of primes is no worse than omitting one, as long as we still have infinitely many "good degrees" for which all polynomials have roots:

THEOREM 4 *For any field K, if there are arbitrarily large "good degrees" d such that all polynomials of degree d have roots, then either K is algebraically closed, or there is exactly one "bad prime" which is the degree of a rootless polynomial, and a degree is "good" if and only if it is not a multiple of that prime.*

PROOF. We know there can be at most one "bad prime," because if two primes were bad then all sufficiently large degrees could be expressed as a sum of those primes and so would have a rootless polynomial, contradicting the assumption of arbitrarily large "good degrees." Corollary 1 implies that if infinitely many primes are "good degrees" then any number only divisible by "good primes" is a "good degree." If there are no bad primes, the proof goes through to show that K is algebraically closed. □

Sufficiency for Characteristic *p*

Theorem 1 gives us the best possible version of the Fundamental Theorem of Algebra, but it can itself be made stronger: the sufficient condition is also necessary, and the characteristic 0 assumption can be dropped.

First, let's look at some examples. Suppose n is odd. We know the alternating group A_n is a possible Galois group, and it contains subgroups of index n, $\binom{n}{2}$, $\binom{n}{3}$, . . . , $\binom{n}{d}$, where $d = (n-1)/2$. These subgroups are intransitive and arise from partitioning {1, . . . , n} into two pieces. When $n = 2k$ is even, there is also a transitive imprimitive subgroup of index $\binom{n}{k}/2$ containing those even permutations which permute {1, . . . , k} and {$k+1$, . . . , n} independently OR switch the two blocks. It is not difficult to prove (see [DM, section 5.2]) that, with a few small exceptions where $n < 10$, any other subgroup of A_n is smaller than these or is contained in one of them.

What degree axioms do we need to ensure [15]? The largest subgroups of A_{15} have indexes 15, 105, 455, 1365, 3003, 5005, 6435. The semigroup $<A_{15}>$ is therefore generated by these numbers plus some others larger than 6435. However, it is not hard to see that <15, 455, 3003> includes 105, 1365, 5005, 6435, and all larger indexes of subgroups of A_{15}, so $<A_{15}>$ = <15, 455, 3003>. This means that to derive the degree axiom [15], we will need either [15k] for some k, or at least [455]. And [455] by itself isn't enough, because it only eliminates the possibility of A_{15} as a Galois group, but we also need to get rid of the prime 3. It turns out (I omit the details of the derivation from Theorem 1) that [15] follows from any set of degree axioms where the degrees include a multiple of 3, a multiple of 5, and an element of the semigroup <15, 455, 3003> (of which 3533 is the first prime).

Now let's see if the proof of Theorem 1 can fail in characteristic p. If a "degree implication" $[i_1]\& \ldots \& [i_m] \Rightarrow [n]$ holds in characteristic 0, we know that it holds in characteristic p also if p divides one of the i_j, because the proof fails only in the case of "inseparable extensions," which cannot occur in characteristic p when every element has a p-th root. But if p does not divide any of the i_j, it doesn't divide n either, for in the preceding section, "The Fundamental Theorem of Algebra Improved," we constructed a characteristic-0 field in which $[n]$ was true iff n was not a multiple of p.

So we may assume p does not divide n. If n divides any of the i_j, the degree implication is trivially true, so we may rule out this possibility. Purely inseparable extensions have degrees that are powers of the characteristic, which means we may assume there is an irreducible polynomial of degree p^r for some r; furthermore, p^r must be $< n$ if we are going to have a degree-n polynomial give an inseparable extension. So if there is a counterexample, we have rootless polynomials of degree p^r and degree n. This means we can construct rootless polynomials of all degrees in $<p^r, n>$, and since p doesn't divide n, this semigroup includes all sufficiently large degrees, in particular, all degrees $n(n-1)$ or greater. If n is even, then p^r is odd, and $<p^r, n>$ includes $n(n-1)/2$ as well, because $n(n-1)/2 = (n/2)*(n-1) = (n/2)*(n-3) + n = (n/2)*(n-5) + 2n = \cdots = (n/2)*p^r + ((n+1-p^r)/2)*n$.

But we saw above that, for $n > 9$, the smallest element of $<A_n>$ that is not a multiple of n is $n(n-1)/2$, if n is even, and for odd n is at least $\binom{n}{3} = n(n-1)(n-2)/6$, which is greater than $n(n-1)$ since $n > 9$. Therefore, $<p^r, n>$ contains the entire semigroup $<A_n>$, so at least one of the i_j must be in $<p^r, n>$ and there is a rootless polynomial of that degree. Thus we can't get a counterexample to our degree implication, because one of the degree axioms on the left-hand side must fail.

We can deal with the remaining cases $n < 10$ by direct calculation. When n is prime, the only valid degree implications have a multiple of n on the left-hand side, and they are trivially valid in all characteristics. For $n = 4, 6, 8, 9$, we calculate the following semigroups:

$$<A_4> = <3, 4>$$
$$<A_6> = <6, 10, 15>$$
$$<A_8> = <8, 15, 28, 35>$$
$$<A_9> = <9, 84, 280>.$$

In each case, for any prime power p^r less than n and not dividing n, the generators of the semigroup (and so the whole semigroup) are in $<p^r, n>$, so we can't get a counterexample to the degree implication. Therefore the characteristic 0 assumption in Theorem 1 can be eliminated.

COROLLARY 3 ([3]&[10]) $\Rightarrow$ [6] *is true in all fields.*

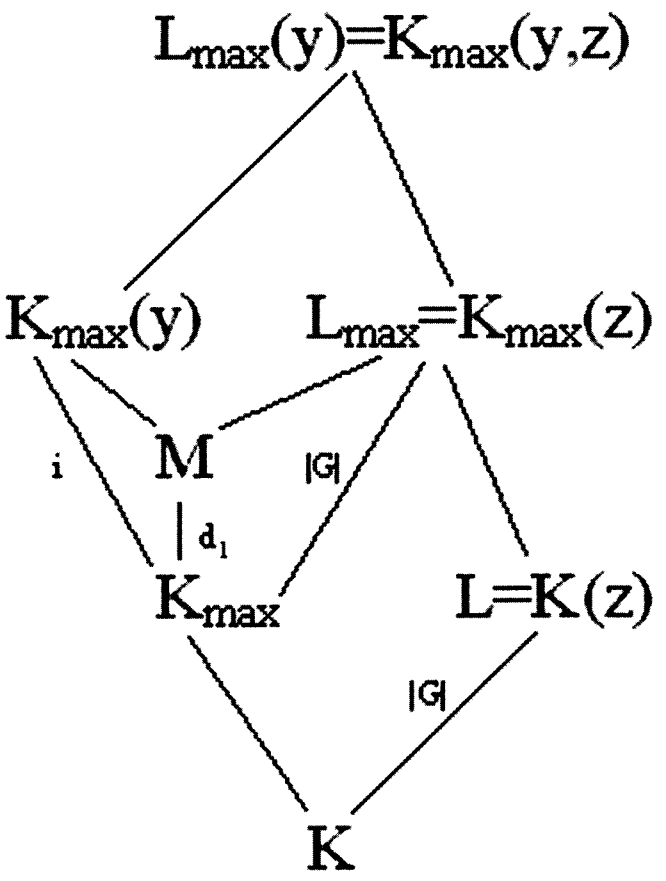
COROLLARY 4 ([2]&[15]) $\Rightarrow$ [8] *is true in all fields.*

PROOF OF NECESSITY. Reversing the direction of Theorem 1 is trickier. Suppose (**) is false, so we have G acting on $<1, \ldots, n>$ with none of the i's in $<G>$. We need to falsify (*), so we must construct a field where $[i_1], \ldots [i_m]$ are true but $[n]$ is false.

Begin by constructing fields K and L such that L is the splitting field over K of a polynomial $f(x)$ of degree n, with Galois group $\mathrm{Gal}(L/K) = G$. (This can be done so K and L are both algebraic over Q.) Let z be a primitive element for this extension, so $L = K(z)$ and z satisfies an irreducible polynomial of degree $|G|$ over K. Let $K_{\max}$ be a *maximal* algebraic extension of K with the property that $L_{max} = K_{max}(z)$ has degree $|G|$ over K_{max}. (We can construct this by successively adjoining algebraic numbers that don't kill any of G, because there is an enumeration of the algebraic numbers.)

Since we haven't disturbed G, $f(x)$ still has G as its Galois group, and no roots in K_{max}, but any further algebraic extension of K_{max} will fail to extend L_{max} by the same degree—that is, for any new algebraic number y, $K_{max}(y,z) = L_{max}(y)$ has a degree over $K_{max}(y)$ that is smaller than $|G|$. We need to show that all the degree axioms $[i_1], \ldots [i_m]$ are true for K_{max}—then, since $f(x)$ is still rootless, $[n]$ is false and thus (*) is also false, as required.

So suppose that we have a polynomial $g(x)$ of degree i_j over K_{max}, where by assumption i_j is not in the semigroup $<G>$. g is a product of irreducible polynomials, and at least one of these must not have a degree in $<G>$ (for if they all did, their product would). So we now have an irreducible polynomial $h(x)$ whose degree i is not in $<G>$. Let y be a root of h. Then $K_{max}(y)$ has degree i over K_{max}, since h is irreducible. Consider the intersection M of $K_{max}(y)$ and $L_{max} = K_{max}(z)$. Let d_1 be the degree of this field over K_{max}. Since M is a subfield of L_{max}, the subgroup of G fixing it must have index d_1, so either $d_1 = 1$ or d_1 is in $<G>$.



Fields defined in proof of Theorem 5

But d_1 also divides i because M is a subfield of $K_{max}(y)$, which means we must have $d_1 = 1$, because we know i is not in $<G>$. Thus $M = K_{max}$: the extension fields $K_{max}(y)$ and $K_{max}(z)$ have only K_{max} in common.

But this means that every automorphism of L_{max} fixing K_{max} extends to an automorphism of $L_{max}(y)$ fixing $K_{max}(y)$, because it doesn't matter which of the $|G|$ conjugates of z we use when forming $K_{max}(y,z) = K_{max}(z,y) = L_{max}(y)$. Therefore the Galois group of $L_{max}(y)$ over $K_{max}(y)$ is still G; but we constructed K_{max} so that any algebraic extension would collapse some of G. Therefore $K_{max}(y)$ is not really an extension: y must already be in K_{max}, which means that $h(x)$ is of degree 1, and $g(x)$ has a root, as was to be shown.

We have now established Theorem 5.

THEOREM 5. *The statement*

(*) $$([i_1]\&[i_2]\& \ldots \&[i_m]) \Rightarrow [n]$$

is true in all fields iff

(**) *for every subgroup G of S_n which acts without fixed-points on $\{1,2, \ldots ,n\}$, the semigroup $<G>$ contains one of the i_j.*

(Compared with Theorem 1, Theorem 5 eliminates the characteristic 0 hypothesis and works in both directions.)

Conclusion

Theorems 2 and 3 establish the minimum algebraic conditions necessary for a field to be algebraically closed, and they can therefore be said to "optimize" the Fundamental Theorem of Algebra. But each specific "degree implication" is a first-order consequence of the axioms for fields, and could have been discovered two centuries ago; the existence of these finitary relationships appears to have been unsuspected by practically everyone, with one important exception.

The inspiration for Theorem 1 was the work done by John H. Conway on "Finite Choice Axioms" in 1970, detailed in [Co]. Conway, building on earlier work of Mostowski and Tarski, identified a necessary and sufficient condition for effective implications between axioms of the form "Every collection of n-element sets has a choice function." Conway's group-theoretic condition is very similar to (**), the difference being that one could use the semigroup $<H>$ for any subgroup H of a group G acting fixed-point-freely on $\{1, \ldots , n\}$, rather than requiring $G = H$. The present article also borrows some terminology, notational conventions, and proof ideas from Conway's work.

Theorem 2 was originally proved by a difficult combinatorial argument that generalized Gauss's original proof. Corollaries 3 and 4 emerged during discussions with Conway, and led ultimately to the formulation of Theorem 1 (which is not hard to prove once it is formulated just right!).

Although Theorem 5 may appear definitive, there are several directions for further investigation.

The algorithm implicit in (**) is slow, but it can be sped up by making certain assumptions about permutation groups; however, verifying these assumptions will require careful analysis of the O'Nan/Scott Theorem on maximal subgroups of A_n (see [DM]) and the Classification of Finite Simple Groups.

There is also a rich theory for several kinds of *weakened degree axioms*, such as

$[n]'$: "all polynomials of degree n are reducible," or

$[n_k]$: "all polynomials of degree n have a factor of degree k" (when $k = 1$ this is the standard degree axiom $[n]$).

These weakened axioms are still expressible in the language of field theory, but they translate differently into the language of Galois groups.

Finally, the "finite choice axioms" deserve further investigation. The great progress in finite group theory over the last 35 years ought to make it easier to calculate the relationships between these axioms, including weakened versions which identify subsets or partitions of $\{1, \ldots , n\}$ instead of elements.

ACKNOWLEDGMENTS

I am grateful to Dan Shapiro, Alison Pacelli, Harvey Friedman, Frank Morgan, Simon Kochen, Noam Elkies, and Jonathan Cohen for verifications, suggestions, and encouragement.

I would especially thank Professor John Conway for many instructive and enjoyable conversations over the last 20 years, as well as for his inexhaustibly inspiring writings and personality.

REFERENCES

[Co] Conway, John H., "Effective Implications between the 'Finite' Choice Axioms," in *Cambridge Summer School in Mathematical Logic* (eds. A. R. D. Mathias, H. Rogers), Springer Lecture Notes in Mathematics 337, 439–458 (Springer-Verlag, Berlin 1971).

[DM] Dixon, John D., and Brian Mortimer, *Permutation Groups*, Springer Graduate Texts in Mathematics 163, Springer-Verlag, 1996.

[FR] Fine, Benjamin, and Gerhard Rosenberger, *The Fundamental Theorem of Algebra*, Springer-Verlag, New York 1997.

[G] Gauss, Carl Friedrich, *Werke*, Volume 3, 33–56 (In Latin; English translation available at http://www.cs.man.ac.uk/~pt/misc/gauss-web.html).

[T] Tarski, Alfred, *A Decision Method for Elementary Algebra and Geometry*, University of California Press, Berkeley and Los Angeles, 1951.

[vdW] van der Waerden, B. L., *Algebra* (7th edition, Vol. 1), Frederick Ungar Publishing, U.S.A., 1970.