Kronecker to Mittag-Leffler, 4 April 1886:

I promised Hermite I would not bring up again the circumstance that made me so angry last year. . . . I have newly worked out a great deal of the material [for lecture courses], and beyond this I have put the foundations of algebra in an entirely new form. . . . You will recall that I originally intended to give you my works on this subject for publication. . . . The so-called fundamental theorem of algebra is replaced by my new "fundamental theorem of general arithmetic." . . . I owe this beautiful and sure foundation of algebra to my sharp critique of the method of defining quantities that began with Heine and to the precious *Galois principle.* It will appear in the 100th volume of our journal.

This letter points to Kronecker's paper "Ein Fundamentalsatz der Allgemeinen Arithmetik" as his definitive statement of his *positive* criticism of the *Grossendefinitionen* that were becoming current at that time and that he associated with Heine.

Although Kronecker's views in this matter had scant influence on the development of algebra in the following decades, I believe they are worth our attention both because they bring to a successful conclusion (to my way of thinking) well over a century of thought about 'the fundamental theorem of algebra' and because they are central to Kronecker's approach to algebra, an approach that, valuable as it is, is in danger of remaining forever, in André Weil's words, "buried in the impressive but seldom opened volumes of his *Complete Works.*"

In the letter he also says that the "modern" method of defining quantities (his quotation marks) *cannot be used* for the definition of the coefficients of two polynomials if one intends to use the algorithm for finding their greatest common divisor. He does not elaborate, but he surely means that if, for example, you want to invert a nonzero element of the field $\mathbf{Q}[\sqrt[3]{2}]$, which involves finding the greatest common divisor of $x^3 - 2$ and a nonzero polynomial $f(x)$ of degree less than 3 as a linear combination of $x^3 - 2$ and $f(x)$, it won't do to know the coefficients of $f(x)$ as *real numbers;* they must be known *exactly* as rational numbers.

In other words, in arithmetic and algebra, which were Kronecker's greatest interests, real numbers are not only inappropriate but unacceptable.

As you all know, Gauss's doctoral dissertation of 1799 was devoted to what we call the fundamental theorem of algebra and what Kronecker called the so-called fundamental theorem of algebra. Gauss criticized earlier proofs of Euler, Lagrange and Laplace, saying that they were circular insofar as they used *computations with the roots* of the polynomial in the course of proving that the roots were complex numbers.

How, he asked, can you compute with the roots before you have proved that they are complex numbers?

This is in fact the key question that Kronecker's *Fundamentalsatz* answers. To put it more tersely:

How can you compute with the roots of a given polynomial?

In a peculiar way, *Galois* gave the pragmatic answer to this question. His answer was on the one hand unfounded, in a sense I will explain, at the same time that it was, paradoxically, the foundation of Galois theory.

The essential idea was what Kronecker was referring to when he wrote of "the precious Galois principle" (*der kostliche Galoisschen Princip*).

It is: *Make use of the fact that you can evaluate symmetric polynomials of the roots to find a quantity with the two properties that (1) each root of the given polynomial can be expressed rationally in terms of it, and (2) it is a root of a known polynomial.*

In modern terms: Find a primitive element for the splitting field of the given polynomial.

An example makes the process clear. Let the given polynomial be $x^3 - 2$. The three roots a, b, c of this equation of course satisfy $a + b + c = 0$, $ab + bc + ca = 0$ and $abc = 2$.

Let $t = a - b$. Then t is the root of a polynomial of degree 6 (fulfilling the second of the two properties we're requiring), namely, the polynomial $(X - a + b)(X + a - b)(X - b + c)(X + b - c)(X - c + a)(X + c - a)$, a polynomial in X of degree 6 whose coefficients are symmetric in a, b, c and can therefore be evaluated.

Here we are of course computing with a, b, c as if we knew how. And of course we do know how to compute with symmetric functions of them even if we don't know what they are! Galois seems never to have bothered himself with the question of what they were.

In fact, that polynomial of degree 6 in X is $X^6 + 108$. I'll indicate briefly how to arrive at this conclusion.

First combining the three pairs of factors, we find it is $(X^2 - (a-b)^2)(X^2 - (b-c)^2)(X^2 - (c-a)^2)$. Thus it is just a matter of finding the coefficients of X^4, X^2, and the constant term. The first of these is $-(a-b)^2 - (b-c)^2 - (c-a)^2 = -2(a^2+b^2+c^2) + 2(ab+bc+ca) = -2(a+b+c)^2 + 6(ab+bc+ca) = 0$. I'll skip the proof that the coefficient of X^2 is also 0. The proof that the constant term $-(a-b)^2(b-c)^2(c-a)^2 = 108$ is easy using a trick that is worth taking the 30 seconds that will be needed to show it.

$$(a-b)(b-c)(c-a) = \begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix}$$

because both sides are polynomials of degree 3 that contain bc^2 and are zero whenever two of a, b, c are equal. Therefore, the square of this determinant is the determinant of the product

$$\begin{aligned}
&\begin{bmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{bmatrix} \begin{bmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{bmatrix} \\
&= \begin{bmatrix} 1+1+1 & a+b+c & a^2+b^2+c^2 \\ a+b+c & a^2+b^2+c^2 & a^3+b^3+c^3 \\ a^2+b^2+c^2 & a^3+b^3+c^3 & a^4+b^4+c^4 \end{bmatrix} \\
&= \begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 2+2+2 \\ 0 & 2+2+2 & 2a+2b+2c \end{bmatrix} \\
&= \begin{bmatrix} 3 & 0 & 0 \\ 0 & 0 & 6 \\ 0 & 6 & 0 \end{bmatrix} = -108.
\end{aligned}$$

Thus, the difference $t = a - b$ of any two roots of $x^3 - 2$ is a root of $X^6 + 108$. But that is of course the easy part. The hard part is to express a, b and c rationally in terms of t.

I will spend a moment on this because Peter Neumann called my reconstruction of Galois' proof "far-fetched", and I feel that I have new evidence for it in the form of the following sentence of Abel, published a few years before Galois' work:

"When a quantity satisfies, at the same time, two given algebraic equations, these equations have a common factor of the first degree. When one supposes that they have no other common factor than this one, one can always, *as one knows,* express the unknown as a rational function of the coefficients of the two equations." (Emphasis added.)

Galois' basic construction uses the formula

$$(V-b)(V-c) = \frac{(V-a)(V-b)(V-c)}{V-a}$$
$$= \frac{V^3-2}{V-a} = \frac{V^3-a^3}{V-a} = V^2+aV+a^2$$

or, more generally,

$$(V-b)(V-c)\cdots(V-e) = \frac{f(V)-f(a)}{V-a}$$

(where V is a new unknown) to express the elementary symmetric polynomials (and therefore all symmetric polynomials) in b, c, ... , as polynomials in a. With $V=-t+a$, we have $(-t+a-b)(-t+a-c) = (-t+a)^2+a(-t+a)+a^2 = t^2-2at+a^2-at+a^2+a^2 = t^2-3at+3a^2$.

But the first factor on the left is zero by the definition of t, so we have the two relations $a^3 - 2 = 0$ and $t^2 - 3at + 3a^2 = 0$ to determine a rationally in terms of t. Explicitly, $0 = (t+a)(t^2-3at+3a^2)-3(a^3-2) = -2at^2 + t^3 + 6$, from which we find $a = \frac{t^3+6}{2t^2}$. Then $b = a - t = \frac{t^3+6-2t^3}{2t^2} = \frac{-t^3+6}{2t^2}$ and $c = -a - b = -\frac{6}{t^2}$ gives the expressions of *all three* roots of $x^3 - 2$ rationally in terms of a root t of $t^6 + 108$.

Kronecker thought that true scientific value lay in *formulas.* The mathematical truth just derived is

$$x^3 - 2 \equiv (x - \frac{t^3+6}{2t^2})(x - \frac{-t^3+6}{2t^2})(x + \frac{6}{t^2}) \\ \bmod t^6 + 108,$$

or, if you prefer it without denominators,

$$8t^6(x^3-2) \equiv (2t^2x - t^3 - 6)(2t^2x + t^3 - 6)(2t^2x + 6) \\ \bmod t^6 + 108.$$

The same method exactly can be used to derive, for a given polynomial $f(x)$ (the case in which $f(x)$ is monic and irreducible with integer coefficients is the natural one to consider first) a formula of the same form

$$f(x) \equiv (x-\rho_1(t))(x-\rho_2(t))\cdots(x-\rho_n(t)) \bmod G(t)$$

where $G(t)$ is an irreducible, monic polynomial with integer coefficients and where $\rho_1(t)$, $\rho_2(t)$, $\ldots$, $\rho_n(t)$ are rational functions in t with integer coefficients.

The construction is: (1) Set $t = Aa+Bb+\cdots+Ee$ where a, b, $\ldots$, e are the roots of the given $f(x)$ and where A, B, $\ldots$, E are strategically chosen integers. (In the example, $A = 1$, $B = -1$, $C = 0$.)

(2) Multiply $t-(Aa+Bb+\cdots+Cc)$ by the $(n-1)!$ polynomials in t, a, b, … , e obtained by permuting b, c, … , e in all possible ways.

The result is on the one hand 0 (the first factor is zero by the definition of t) and on the other hand, since it is symmetric in b, $c\ldots$, e, it can be expressed as a polynomial in t and a, say $F(t,a)=0$.

(3) Use the two relations $f(a)=0$ and $F(t,a)=0$ to express a rationally in terms of the coefficients of the two relations and therefore as a rational function of t, call it $\rho_a(t)$.

Since you can do the same for all roots, not just for a, you get, when $G(t)$ is the irreducible polynomial of which t is a root,

$$f(x)=(x-\rho_a(t))\cdots(x-\rho_e(t)) \bmod G(t).$$

You will of course be uneasy about the requirement that the integer multipliers A, B, $\ldots$, E be ‘chosen strategically,’ but this is easily explained. Galois requires that the $n!$ quantities $Aa+Bb+\cdots+Ee$ obtained by permuting the roots a, b, $\ldots$, e be distinct, and this is easy (in theory, not computationally) to guarantee: The product of the $n!(n!-1)$ differences of these quantities is symmetric in the roots and is therefore a known known polynomial in A, B, $\ldots$, E with integer coefficients.

So all we need to do to find our ‘Galois resolvent’ t is to assign integer values to A, B, $\ldots$, E that give this polynomial a nonzero value (so the $n!$ values are distinct). (Clearly this polynomial in A, B, $\ldots$, E is nonzero provided the roots a, b, $\ldots$, e are distinct.)

What one needs to be uneasy about is the very concept of *computing with the roots of the given polynomial.* Once again, in my opinion the truly fundamental theorem of algebra is the statement that there is a valid way to compute with the roots of a polynomial as though they were numbers. (And by 'numbers' I mean the most elementary kind 1, 2, 3, …).

Galois proved—or at least sketched a fully satisfactory proof—that *if there is any valid way to compute* with the roots of a given polynomial $f(x)$, then the splitting field can be represented *explicitly* as the field $\mathbf{Q}[t]$ mod $G(t)$ obtained by adjoining to the rationals $\mathbf{Q}$ a single root t of an explicitly computable (in theory) irreducible and monic polynomial $G(t)$ with integer coefficients.

Again, the theorem constructs for a given $f(x)$ with integer coefficients a formula

$$f(x) = (x - \rho_a(t)) \cdots (x - \rho_e(t)) \bmod G(t)$$

where G is irreducible and monic with integer coefficients. This not only constructs a splitting field $\mathbf{Q}[t] \bmod G(t)$ of $f(x)$, it also constructs the roots $\rho_a(t)$, ... within it.

Galois deduced this theorem from the tacit assumption that the use of the algebra of symmetric polynomials is a valid way to find a polynomial of which $t = Aa + Bb + \cdots + Ee$ is a root and to find a polynomial relation $F(a,t) = 0$, which, combined with $f(a) = 0$, makes it possible to express a rationally in terms of t.

Kronecker's 'Fundamental Theorem of General Arithmetic' is essentially this same statement, but freed from reliance on any tacit assumptions.

However Kronecker's theorem, and Galois' theorem too, is more general than the one I have stated. I have been assuming $f(x)$ has *integer* coefficients, but once the theorem has been formulated in this way it is quite natural to allow the coefficients of $f(x)$ to contain *letters* as well as numbers.

Galois had this very much in mind because, among other things, he wanted to prove that the roots of $x^5+Ax^4+Bx^3+Cx^2+Dx+E$, a polynomial whose coefficients are 'letters', cannot be expressed by radicals.

Kronecker in fact *defined* 'general arithmetic' as the algebra of such polynomials.

Kronecker's Fundamental Theorem of General Arithmetic. *Given a polynomial $F(x)$ whose coefficients are polynomials in some set of letters r, r', r'', $\ldots$ with integer coefficients, you can construct an explicit congruence relation relation on the ring of polynomials in x, r, r', r'', $\ldots$ with integer coefficients such that the ring of congruence classes is an integral domain, and some nonzero multiple $q \cdot F(x)$ of $F(x)$, where q does not contain x, is congruent to a product of factors linear in x.*

Confession: I don't understand the details of Kronecker's proof.

Defense: I can prove it in a very clear, simple, constructive way. The heart of the method is a Kroneckerian algorithm for factoring polynomials whose coefficients are in a fixed algebraic number field.

Then the construction of the splitting field of $F(x)$ can follow the naïve step-by-step construction in which one adjoins at each step a root of a factor of degree greater than 1 that is irreducible over the field that has been constructed so far, until all the factors have degree 1.

(I suspect Kronecker would not have liked this approach because it does not put the Galois group in evidence.)

In conclusion, I would like to justify my statement at the outset that Kronecker's theorem can be regarded as bringing to a successful conclusion the study of the so-called fundamental theorem of algebra.

In short, the idea is that a polynomial $F(x)$ with integer coefficients has n roots that can be expressed rationally in terms of a root t of a polynomial (which can in fact be assumed to be monic and irreducible) $G(t)$ with integer coefficients. Thus, to find n complex roots of $F(x)$ we have only to find *one* complex root t of $G(t)$.

It is easy to construct one complex root of $G(t)$ in two steps:

(1) The integral of $d \log |G(z)|$ around the boundary of any square in the complex z-plane on which $|G(z)|$ is bounded away from zero is zero because $\log |G(z)|$ is single-valued on such a square. Using this, and using the fact that the integral of $d \log |G(z)|$ around the boundary of a very large square is nearly the same as the integral of $d \log |z^n|$ around the same boundary, which is $2\pi ni$, one can find small squares on which $|G(z)|$ is nearly zero.

(2) Given a value of z for which $G(z)$ is nearly zero, you can use an iteration to construct a sequence that converges to an actual zero. (Note that this convergent sequence encapsulates the part of the theorem that is *not algebra*.)