Lecture 5

Preparation for Kummer

As preparation for the general theory, I present a version of Euler's proof that is formulated within the domain $\mathbb{Z}(\alpha)$. This version is presented in several texts on number theory, no doubt in an effort to introduce the student to more advanced methods. I leave it to you to judge whether it is more or less comprehensible. It is, however, essential that it be comprehended for it is nothing but Kummer's proof in a special and simple case.

The element in Euler's proof that is still missing becomes here the statement that every number ξ in $\mathbb{Z}(\alpha)$ is a product $\epsilon\pi_1^{a_1}\pi_2^{a_2}\ldots$. The number ϵ is a unit, π_1 and π_2, and so on are essentially different primes, that is one is not obtained from another by multiplication with a unit. Moreover, this factorization is essentially unique. All others are obtained by multiplying each π_i by a unit ϵ_i, thus changing them in an inessential manner, and modifying ϵ as required.

For example, we have seen that $1+9\alpha$ and $3+11\alpha$ are primes. Then

$$\xi = -80+19\alpha = (1+9\alpha)(3+11\alpha) = \epsilon(-9-8\alpha)(-3-11\alpha), \quad \epsilon = -\alpha^2$$

because

$$\alpha(1+9\alpha) = -9-8\alpha, \alpha\alpha^2 = 1.$$

The presence of the units is nuisance, about which there is nothing to be done. We take the (essentially) unique factorization for granted for the moment. It will be treated later. I observe immediately that it is the failure of unique factorization in the domains $Z(\alpha)$ when

$$\alpha = \cos(2\pi/p) + i\sin(2\pi/p),$$

p being not 3 but a larger prime number, for example 23, that creates the initial bewilderment and forces the introduction of *ideal numbers*.

We shall prove a stronger statement than that of Fermat, namely that there is no solution of

$$\xi^3+\eta^3+\zeta^3 = 0, \quad \xi\eta\zeta \neq 0$$

in $\mathbb{Z}(\alpha)$. If any two of these numbers were divisible by a prime π then all three would be, and we could divide by it. So we may as well assume, when proving the theorem, that any two have no common divisor.

For convenience, I now introduce a modern notation. If ξ and η are two numbers in $\mathbb{Z}(\alpha)$ and ζ a third, then

$$\xi \equiv \eta \pmod{\zeta}$$

means that $\xi - \eta$ is a multiple of ζ. Recall that $\lambda = 1 - \alpha$ is a prime and that $3 = \rho\lambda^2$, where ρ is a unit.

Statement 1. *If ω is not divisible by λ then*

$$\omega^3 \equiv \pm 1 \pmod{\lambda^4}$$

If $\omega = a + b\alpha$, then $\omega + b\lambda = a + b$, so that

$$\omega \equiv a + b \pmod{\lambda}.$$

Since 3 is also a multiple of λ and any integer n is of the form $m + 3r$, $m = 0, \pm 1$, we may take $\omega \equiv 0, \pm 1 \pmod{\lambda}$. By hypothesis, 0 is excluded, and that leaves ± 1.

If the statement is true for ω then it is certainly true for $-\omega$ and conversely. Thus, multiplying ω by -1 if necessary, we suppose that $\omega \equiv 1 \pmod{\lambda}$ or that

$$\omega = 1 + \beta\lambda.$$

Then

$$\begin{aligned}\omega^3 - 1 &= (\omega - 1)(\omega - \alpha)(\omega - \alpha^2)\\ &= \beta\lambda(\beta\lambda + 1 - \alpha)(\beta\lambda + 1 - \alpha^2)\\ &= \beta\lambda^3(\beta + 1)(\beta - \alpha^2)\end{aligned}$$

Since

$$\alpha^2 = \alpha^2 - 1 + 1 \equiv 1 \pmod{\lambda},$$

the number

$$\beta(\beta + 1)(\beta - \alpha^2) \equiv \beta(\beta + 1)(\beta - 1)$$

is divisible by λ.

Statement 2. *If $\xi^3 + \eta^3 + \zeta^3 = 0$, then one of ξ, η, ζ is divisible by λ.*

If not, then

$$0 = \pm 1 \pm 1 \pm 1 \pmod{\lambda^4}.$$

Thus, either

$$\pm 1 \equiv 0 \pmod{\lambda^4}$$

or

$$\pm 3 \equiv 0 \pmod{\lambda^4}.$$

The first possibility is certainly out of the question. The second possibility is out of the question because 3 is equal to a unit times λ^2 and thus not a multiple of λ^4 – because of unique factorization!

Suppose then that $\xi^3 + \eta^3 + \zeta^3 = 0$ and that λ divides ζ, so that

$$\zeta = \lambda^n \gamma,$$

where $n > 0$ and where λ does not divide γ. So we are to prove the impossibility of

$$(A) \qquad \xi^3 + \eta^3 + \lambda^{3n}\gamma^3 = 0,$$

in which neither ξ nor η is divisible by λ and in which the greatest common divisor of $\xi \neq 0$ and $\eta \neq 0$ is 1. As is often the case in mathematics, it is better to prove a stronger assertion, the impossibility under the same conditions of

$$(B), \qquad \xi^3 + \eta^3 + \epsilon\lambda^{3n}\gamma^3 = 0,$$

where ϵ is a unit. This we prove with two assertions.

Statement 3. *If (B) is satisfied with the conditions specified then $n > 1$.*

Statement 4. *If (B) is possible with the conditions specified for a given $n = m > 1$, then it is possible for $n = m - 1$.*

The first of these statements is easy to verify. (B) means that

$$-\epsilon\lambda^{3n}\gamma^n \equiv \pm 1 \pm 1 \pmod{\lambda^4}$$

The signs cannot be the same because λ does not divide 2. (Otherwise its norm could not be 3.) Thus we have

$$-\epsilon\lambda^{3n}\gamma^n \equiv 0 \pmod{\lambda^4}.$$

This requires that $3n \geq 4$ or that $n > 1$.

It is the final statement that is difficult to prove. Its proof exploits a very important technique in number theory, that of descent. We show that when a statement is true for one number, then it is true for a smaller number, and continue in this way until we reach a very small number for which we easily show it is impossible. This technique, introduced by Fermat, remained until recently the most powerful one available.

We begin by factoring.

$$(C) \qquad -\epsilon\lambda^{3m}\gamma^n = \xi^3 + \eta^3 = (\xi+\eta)(\xi+\alpha\eta)(\xi+\alpha^2\eta).$$

Just to be certain, we explicitly verify the second equation by expanding the right-hand side.

$$\xi^3 + \xi^2\eta(1+\alpha+\alpha^2) + \xi\eta^2(1+\alpha+\alpha^2) + \eta^3 = \xi^3+\eta^3.$$

The differences of the terms on the left side of (C) are $\eta\lambda$, $\alpha\eta\lambda$, $\alpha^2\eta\lambda$, all associates of $\eta\lambda$ Thus each of them is divisible by λ but not by λ^2, because λ does not divide η. One of the three factors on the left of (C) must be divisible by λ^2 because $m \geq 2$. Since we can replace η by $\alpha\eta$ or by $\alpha^2\eta$ without changing (B), thereby permuting the three factors on the left of (C), we might as well suppose that $\xi+\eta$ is divisible by λ^2. The other factors are then divisible by λ but not by λ^2.

So we express these factors as follows.

$$(D) \qquad \xi+\eta = \lambda^{3m-2}\kappa_1, \quad \xi+\alpha\eta = \lambda\kappa_2, \quad \xi+\alpha^2\eta = \lambda\kappa_3,$$

in which none of κ_1, κ_2 and κ_3 is divisible by λ.

We have next to verify that these three numbers, κ_1, κ_2 and κ_3 are relatively prime to each other. Observe that

$$\lambda(\kappa_2 - \kappa_3) = \alpha(1-\alpha)\eta = \alpha\lambda\eta,$$
$$\lambda(\alpha\kappa_3 - \alpha^2\kappa_2) = \alpha\xi - \alpha_2\xi = \alpha\lambda\xi$$

or cancelling the λ,

$$\kappa_2 - \kappa_3 = \alpha\eta,$$
$$\alpha\kappa_3 - \alpha^2\kappa^2 = \alpha\xi,$$

so that any divisor of κ_2 and κ_3 is also a divisor of η and ξ and must therefore be a unit. Consequently κ_2 and κ_3 are relatively prime.

In the same way,

$$\lambda(\kappa_3 - \lambda^{3m-3}\kappa_1) = \alpha^2\lambda\eta,$$
$$\lambda(\kappa_3 - \alpha^2\lambda^{3m-3}\kappa_1) = -\alpha^2\lambda\eta,$$

so that, cancelling the λ, we see that κ_1 and κ_3 must be relatively prime. A similar calculation will show that κ_1 and κ_2 have to be relatively prime.

We substitute (D) in (C). The result is

$$-\epsilon\gamma^3 = \kappa_1\kappa_2\kappa_3.$$

When we factor each of κ_1, κ_2 and κ_3 as well as γ and γ^3 into a product of primes and remember that if a prime factor appears, for example, in κ_1 then it cannot appear in κ_2 or in κ_3, then we see that every prime factor that appears in κ_1 appears to a power that is a multiple of 3.

$$(E) \qquad \kappa_1 = \epsilon_1\pi_1^{3a_1}\pi_2^{3a_2}\ldots = \epsilon_1\theta^3, \quad \theta = \pi_1^{a_1}\pi_2^{a_2}\ldots.$$

For similar reasons,

$$(F) \qquad \begin{aligned}\kappa_2 &= \epsilon_2\phi^3,\\ \kappa_3 &= \epsilon_3\psi^3.\end{aligned}$$

We substitute (E) and (F) in (D). The result is

$$\xi + \eta = \epsilon_1\lambda^{3m-2}\theta^3, \quad \xi + \alpha\eta = \epsilon_2\lambda\phi^3, \quad \xi + \alpha^2\eta = \epsilon_3\lambda\psi^3.$$

Consequently

$$(G) \qquad \begin{aligned}0 &= (1+\alpha+\alpha^2)(\xi+\eta)\\ &= \xi + \eta + \alpha(\xi+\alpha\eta) + \alpha^2(\xi+\alpha^2\eta)\\ &= \epsilon_1\lambda^{3m-2}\theta^3 + \epsilon_2\alpha\lambda\phi^3 + \epsilon_3\alpha^2\lambda\psi^3.\end{aligned}$$

If we cancel a λ from the right-hand side of (G), then we are almost back to an equation of the form (B), but with m replaced by $m-1$ and that was our goal. To be precise, we have

$$\phi^3 + \epsilon_4\psi^3 + \epsilon_5\lambda^{3m-3}\theta^3 = 0, \quad \epsilon_4 = \epsilon_3\alpha/\epsilon_2, \quad \epsilon_5 = \epsilon_1/\epsilon_2\alpha.$$

This is at first sight not quite right, because of the ϵ_4

The process is completed as follows. As $m \geq 2$,

$$\phi^3 + \epsilon_4 \psi^3 \equiv 0 \pmod{\lambda^2}.$$

We had already seen that

$$\phi^3 \equiv \pm 1 \pmod{\lambda^2}, \quad \psi^3 \equiv \pm 1 \pmod{\lambda^2}.$$

Indeed the λ^2 can even be replaced by λ^4. Thus

$$\pm 1 \pm \epsilon_4 \equiv 0 \pmod{\lambda^2}.$$

There are six choices for ϵ_4, either ± 1, $\pm\alpha$ or $\pm\alpha^2$. The first is fine, for we just replace ψ by $\pm\psi$ and the ϵ_4 is absorbed. On the other hand

$$\pm(1+\alpha) = \mp\alpha, \quad \pm(1-\alpha) = \lambda,$$

and

$$\pm(1+\alpha^2) = \mp\alpha, \quad \pm(1-\alpha^2) = \mp\alpha^2\lambda,$$

so that these numbers are either units or associates of λ. Consequently $\epsilon_4 = \pm 1$.