FERMAT'S LAST THEOREM FOR REGULAR PRIMES

Contents

1. Introduction 1
2. Discriminants of number fields 1
3. Cyclotomic fields 3
4. Fermat's Last Theorem for regular primes 5
References 7

1. Introduction

We prove Fermat's Last Theorem for regular primes and give some of the necessary background. It uses [Sam70, Mar18, Was82].

2. Discriminants of number fields

We recall basic facts about the discriminant.

Lemma 2.1. *Let K be a number field, $\alpha \in K$ and let σ_i be the embeddings of K into $\mathbb{C}$. Then*

$$N_{K/\mathbb{Q}}(\alpha) = \prod_i \sigma_i(\alpha)$$

.

Proof. The proof is standard. □

Lemma 2.2. *Let K be a number field, $\alpha \in K$ and let σ_i be the embeddings of K into $\mathbb{C}$. Then*

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_i \sigma_i(\alpha).$$

Proof. The proof is standard. □

Definition 2.3. Let A, K be commutative rings with K and A-algebra. let $B = \{b_1, \dots, b_n\}$ be a set of elements in K. The discriminant of B is defined as

$$\Delta(B) = \det \begin{pmatrix} \mathrm{Tr}_{K/A}(b_1 b_1) & \cdots & \mathrm{Tr}_{K/A}(b_1 b_n) \\ \vdots & & \vdots \\ \mathrm{Tr}_{K/A}(b_n b_1) & \cdots & \mathrm{Tr}_{K/A}(b_n b_n) \end{pmatrix}.$$

Lemma 2.4. *Let L/K be an extension of fields and let $B = \{b_1, \dots, b_n\}$ be a K-basis of L. Then $\Delta(B) \neq 0$.*

Proof. The proof is standard. □

Lemma 2.5. *Let K be a number field and B, B' bases for $K/\mathbb{Q}$. If P denotes the change of basis matrix, then*

$$\Delta(B) = \det(P)^2 \Delta(B').$$

Proof. The proof is standard. □

Lemma 2.6. *Let K be a number field with basis $B = \{b_1, \ldots, b_n\}$ and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of K into $\mathbb{C}$. Now let M be the matrix*

$$\begin{pmatrix} \sigma_1(b_1) & \cdots & \sigma_1(b_n) \\ \vdots & & \vdots \\ \sigma_n(b_1) & \cdots & \sigma_n(b_n) \end{pmatrix}.$$

Then

$$\Delta(B) = \det(M)^2.$$

Proof. By Lemma 2.2 we know that $\mathrm{Tr}_{K/\mathbb{Q}}(b_i b_j) = \sum_k \sigma_k(b_i)\sigma_k(b_j)$ which is the same as the (i,j) entry of $M^t M$. Therefore

$$\det(T_B) = \det(M^t M) = \det(M)^2.$$

□

Lemma 2.7. *Let K be a number field and $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ for some $\alpha \in K$. Then*

$$\Delta(B) = \prod_{i<j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2$$

where σ_i are the embeddings of K into $\mathbb{C}$. Here $\Delta(B)$ denotes the discriminant.

Proof. First we recall a classical linear algebra result relating to the Vandermonde matrix, which states that

$$\det \begin{pmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ \vdots & & & \vdots & \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} \end{pmatrix} = \prod_{i<j} (x_i - x_j).$$

Combining this with Lemma 2.6 gives the result. □

Lemma 2.8. *Let f be a monic irreducible polynomial over a number field K and let α be one of its roots in $\mathbb{C}$. Then*

$$f'(\alpha) = \prod_{\beta \neq \alpha} (\alpha - \beta),$$

where the product is over the roots of f different from α.

Proof. We first write $f(x) = (x-\alpha)g(x)$ which we can do (over $\mathbb{C}$) as α is a root of f, where now $g(x) = \prod_{\beta \neq \alpha}(x - \beta)$. Differentiating we get

$$f'(x) = g(x) + (x - \alpha)g'(x).$$

If we now evaluate at α we get the result. □

Lemma 2.9. *Let $K = \mathbb{Q}(\alpha)$ be a number field with $n = [K : \mathbb{Q}]$ and let $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Then*

$$\Delta(B) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(m'_\alpha(\alpha))$$

where m'_α is the derivative of $m_\alpha(x)$ (which we recall denotes the minimal polynomial of α).

Proof. By Lemma 2.7 we have $\Delta(B) = \prod_{i<j}(\alpha_i - \alpha_j)^2$ where $\alpha_k := \sigma_k(\alpha)$. Next, we note that the number of terms in this product is $1+2+\cdots+(n-1) = \frac{n(n-1)}{2}$. So if we write each term as $(\alpha_i - \alpha_j)^2 = -(\alpha_i - \alpha_j)(\alpha_j - \alpha_i)$ we get

$$\Delta(B) = (-1)^{\frac{n(n-1)}{2}} \prod_{i=1}^{n} \prod_{i \neq j} (\alpha_i - \alpha_j).$$

Now, by lemmas 2.8 and 2.1 we see that

$$N_{K/\mathbb{Q}}(m'_\alpha(\alpha)) = \prod_{i=1}^{n} m'_\alpha(\alpha_i) = \prod_{i=1}^{n} \prod_{i \neq j} (\alpha_i - \alpha_j),$$

which gives the result. □

Lemma 2.10. *If K is a number field and $\alpha \in \mathcal{O}_K$ then $N_{K/\mathbb{Q}}(\alpha)$ is in $\mathbb{Z}$.*

Proof. The proof is standard. □

Lemma 2.11. *If K is a number field and $\alpha \in \mathcal{O}_K$ then $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ is in $\mathbb{Z}$.*

Proof. The proof is standard. □

Lemma 2.12. *Let K be a number field and $B = \{b_1, \ldots, b_n\}$ be elements in $\mathcal{O}_K$, then $\Delta(B) \in \mathbb{Z}$.*

Proof. Immediate by 2.11. □

Lemma 2.13. *Let $K = \mathbb{Q}(\alpha)$ be a number field, where α is an algebraic integer. Let $B = \{1, \alpha, \ldots, \alpha^{[K:\mathbb{Q}]-1}\}$ be the basis given by α and let $x \in \mathcal{O}_K$. Then $\Delta(B)x \in \mathbb{Z}[\alpha]$.*

Proof. See the Lean proof. □

Lemma 2.14. *Let $K = \mathbb{Q}(\alpha)$ be a number field, where α is an algebraic integer with minimal polynomial that is Eisenstein at p. Let $x \in \mathcal{O}_K$ such that $p^n x \in \mathbb{Z}[\alpha]$ for some n. Then $x \in \mathbb{Z}[\alpha]$.*

Proof. See the Lean proof. □

3. Cyclotomic fields

Lemma 3.1. *For n any integer, Φ_n (the n-th cyclotomic polynomial) is a polynomial of degree $\varphi(n)$ (where φ is Euler's Totient function).*

Proof. The proof is classical. □

Lemma 3.2. *For n any integer, Φ_n (the n-th cyclotomic polynomial) is an irreducible polynomial .*

Proof. The proof is classical. □

Lemma 3.3. *Let ζ_p be a p-th root of unity for p an odd prime, let $\lambda_p = 1-\zeta_p$ and $K = \mathbb{Q}(\zeta_p)$. Then*

$$\Delta(\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}) = \Delta(\{1, \lambda_p, \ldots, \lambda_p^{p-2}\}) = (-1)^{\frac{(p-1)}{2}} p^{p-2}.$$

Proof. First note $[K : \mathbb{Q}] = p - 1$.

Since $\zeta_p = 1 - \lambda_p$ we at once get $\mathbb{Z}[\zeta_p] = \mathbb{Z}[\lambda_p]$ (just do double inclusion). Next, let $\alpha_i = \sigma_i(\zeta_p)$ denote the conjugates of ζ_p, which is the same as the image of ζ_p under one of the embeddings $\sigma_i : \mathbb{Q}(\zeta_p) \to \mathbb{C}$. Now by Proposition 2.7 we have

$$\Delta(\{1, \zeta_p, \ldots, \zeta_p^{p-2}\}) = \prod_{i<j}(\alpha_i - \alpha_j)^2 = \prod_{i<j}((1-\alpha_i) - (1-\alpha_j))^2$$
$$= \Delta(\{1, \lambda_p, \ldots, \lambda_p^{p-2}\})$$

Now, by Proposition 2.9, we have

$$\Delta(\{1, \zeta_p, \cdots, \zeta_p^{p-2}\}) = (-1)^{\frac{(p-1)(p-2)}{2}} N_{K/\mathbb{Q}}(\Phi_p'(\zeta_p))$$

Since p is odd $(-1)^{\frac{(p-1)(p-2)}{2}} = (-1)^{\frac{(p-1)}{2}}$. Next, we see that

$$\Phi_p'(x) = \frac{px^{p-1}(x-1) - (x^p - 1)}{(x-1)^2}$$

therefore

$$\Phi_p'(\zeta_p) = -\frac{p\zeta_p^{p-1}}{\lambda_p}.$$

Lastly, note that $N_{K/\mathbb{Q}}(\zeta_p) = 1$, since this is the constant term in its minimal polynomial. Similarly, we see $N_{K/\mathbb{Q}}(\lambda_p) = p$. Putting this all together, we get

$$N_{K/\mathbb{Q}}(\Phi_p'(\zeta_p)) = \frac{N_{K/\mathbb{Q}}(p) N_{K\mathbb{Q}}(\zeta_p)^{p-1}}{N_{K/\mathbb{Q}}(-\lambda_p)} = (-1)^{p-1} p^{p-2} = p^{p-2}$$

□

Theorem 3.4. *Let ζ_p be a p-th root of unity for p an odd prime, let $\lambda_p = 1 - \zeta_p$ and $K = \mathbb{Q}(\zeta_p)$. Then $\mathcal{O}_K = \mathbb{Z}[\zeta_p] = \mathbb{Z}[\lambda_p]$.*

Proof. We need to prove is that $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. The inclusion $\mathbb{Z}[\zeta_p] \subseteq \mathcal{O}_K$ is obvious. Let now $x \in \mathcal{O}_K$. By Lemma 2.13 and Proposition 3.3, there is $k \in \mathbb{N}$ such that $p^k x \in \mathbb{Z}[\zeta_p]$. We conclude by Lemma 2.14. □

Lemma 3.5. *Let α be an algebraic integer all of whose conjugates have absolute value one. Then α is a root of unity.*

Proof. Lemma 1.6 of [Was82]. □

Lemma 3.6. *Let p be a prime, $K = \mathbb{Q}(\zeta_p)$ $\alpha \in K$ such that there exists $n \in \mathbb{N}$ such that $\alpha^n = 1$, then $\alpha = \pm\zeta_p^k$ for some k.*

Proof. If n is different to p then K contains a $2pn$-th root of unity. Therefore $\mathbb{Q}(\zeta_{2pn}) \subset K$, but this cannot happen as $[K : \mathbb{Q}] = p - 1$ and $[\mathbb{Q}(\zeta_{2pn}) : \mathbb{Q}] = \varphi(2np)$. □

Lemma 3.7. *Any unit u in $\mathbb{Z}[\zeta_p]$ can be written in the form $\beta\zeta_p^k$ with k an integer and $\beta \in \mathbb{R}$.*

Proof. See the Lean proof. □

Lemma 3.8. *Let p be an odd prime, ζ_p a primitive p-th root of unity and let $K = \mathbb{Q}(\zeta_p)$. Then for any $i, j \in 0, \ldots, p-1$ with $i \neq j$, there exists a unit $u \in \mathcal{O}_K^\times$ such that $\zeta_p^i - \zeta_p^j = u * (\zeta_p - 1)$.*

Proof. This is Ex 34 in chapter 2 of [Mar18]. □

Lemma 3.9. *Let R be a Dedekind domain, p a prime and $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ ideals such that*

$$\mathfrak{a}\mathfrak{b} = \mathfrak{c}^p$$

and suppose $\mathfrak{a}, \mathfrak{b}$ are coprime. Then there exist ideals $\mathfrak{e}, \mathfrak{d}$ such that

$$\mathfrak{a} = \mathfrak{e}^p \qquad \mathfrak{b} = \mathfrak{d}^p \qquad \mathfrak{e}\mathfrak{d} = \mathfrak{c}$$

Proof. It follows from the unique decomposition of ideals in a Dedekind domain. □

4. Fermat's Last Theorem for regular primes

Lemma 4.1. *Let $p \geq 5$ be an prime number, ζ_p a p-th root of unity and $x, y \in \mathbb{Z}$ coprime.*

For $i \neq j$ with $i, j \in 0, \ldots, p-1$ we can write

$$(\zeta_p^i - \zeta_p^j) = u(1 - \zeta_p)$$

with u a unit in $\mathbb{Z}[\zeta_p]$. From this it follows that the ideals

$$(x+y), (x+\zeta_p y), (x+\zeta_p^2 y), \ldots, (x+\zeta_p^{p-1} y)$$

are pairwise coprime.

Proof. Lemma 3.8 gives that u is a unit. So all that needs to be proved is that the ideals are coprime. Assume not, then for some $i \neq j$ we have some prime ideal $\mathfrak{p}$ dividing by $(x + y\zeta_p^i)$ and $(x + y\zeta_p^j)$. It must then also divide their sum and their difference, so we must have $\mathfrak{p}|(1-\zeta_p)$ or $\mathfrak{p}|y$. Similarly, $\mathfrak{p}$ divides $\zeta_p^j(x + y\zeta_p^i) - \zeta_p^i(x + y\zeta_p^j)$ so $\mathfrak{p}$ divides x or $(1-\zeta_p)$. We can't have $\mathfrak{p}$ dividing x, y since they are coprime, therefore $\mathfrak{p}|(1-\zeta_p)$. We know that since $(1-\zeta_p)$ has norm p it must be a prime ideal, so $\mathfrak{p} = (1-\zeta_p)$. Now, note that $x + y \equiv x + y\zeta_p^i \equiv 0 \mod \mathfrak{p}$. But since $x, y \in \mathbb{Z}$ this means we would have $x + y \equiv 0 \pmod p$, which implies $z^p \equiv 0 \pmod p$ which contradicts our assumptions. □

Lemma 4.2. *Let p be an prime number, ζ_p a p-th root of unity and $\alpha \in \mathbb{Z}[\zeta_p]$. Then α^p is congruent to an integer modulo p.*

Proof. Just use $(x+y)^p \equiv x^p + y^p \pmod p$ and that ζ_p is a p-th root of unity. □

Lemma 4.3. *Let p be an prime number, ζ_p a p-th root of unity and $\alpha \in \mathbb{Z}[\zeta_p]$ with $\alpha = \sum_i a_i \zeta_p^i$. Let us suppose that there is i such that $a_i = 0$. If n is an integer that divides α in $\mathbb{Z}[\zeta_p]$, then n divides each a_i.*

Proof. Looking at $\alpha = a_0 + a_1\zeta_p + \cdots + a_{p-1}\zeta_p^{p-1}$, if one of the a_i's is zero and $\alpha/n \in \mathbb{Z}[\zeta_p]$, then $\alpha/n = \sum_i a_i/n\zeta_p^i$. Now, as $\alpha/n \in \mathbb{Z}[\zeta_p]$, pick the basis of $\mathbb{Z}[\zeta_p]$ which does not contain ζ_p (which is possible as any subset of $\{1, \zeta_p, \ldots, \zeta_p^{p-1}\}$ with $p-1$ elements forms a basis of $\mathbb{Z}[\zeta_p]$.). Then $\alpha = \sum_i b_i \zeta_p^i$ where $b_i \in \mathbb{Z}$. Therefore comparing coefficients, we get the result. □

Lemma 4.4. *Let $p \geq 3$ be an prime number, ζ_p a p-th root of unity and $\alpha \in \mathbb{Z}[\zeta_p]$. Let x and y be integers such that $x + y\zeta_p^i = u\alpha^p$ with $u \in \mathbb{Z}[\zeta_p]^\times$ and $\alpha \in \mathbb{Z}[\zeta_p]$. Then there is an integer k such that*

$$x + y\zeta_p^i - \zeta_p^{2k} x - \zeta_p^{2k-i} y \equiv 0 \pmod p.$$

Proof. Using lemma 3.7 we have $(x + y\zeta_p^i) = \beta\zeta_p^k\alpha^p$ which is congruent modulo p to $\beta\zeta_p^k a \pmod p$ for some integer a by 4.2. Now, if we consider the complex conjugate we have $\overline{(x + y\zeta_p^i)} \equiv \beta\zeta_p^{-k} a \pmod p$. Looking at $(x + y\zeta_p^i) - \zeta_p^{2k}\overline{(x + y\zeta_p^i)}$ then gives the result. ☐

Lemma 4.5. *Let $p \geq 5$ be an prime number, ζ_p a p-th root of unity and $K = \mathbb{Q}(\zeta_p)$. Assume that we have $x, y, z \in \mathbb{Z}$ with $\gcd(xyz, p) = 1$ and such that*

$$x^p + y^p = z^p.$$

Then without loss of generality, we may assume x, y, z are pairwise coprime and

$$x \not\equiv y \mod p.$$

Proof. The first part is easy.

Reducing modulo p, using Fermat's little theorem, you get that if $x \equiv y \equiv -z \pmod p$ then $3z \equiv 0 \pmod p$. But since $p > 3$ this means $p|z$ but this contradicts $\gcd(xyz, p) = 1$. Now, if $x \equiv y \pmod p$ then $x \not\equiv -z \pmod p$ we can relabel y, z so that wlog $x \not\equiv y$ (this uses that p is odd). ☐

Definition 4.6. A prime number p is called regular if it does not divide the class number of $\mathbb{Q}(\zeta_p)$.

Theorem 4.7. *Let p be an odd regular prime. Then*

$$x^p + y^p = z^p$$

has no solutions with $x, y, z \in \mathbb{Z}$ and $\gcd(xyz, p) = 1$.

Proof. First thing is to note that if $x^p + y^p = z^p$ then

$$z^p = (x + y)(x + \zeta_p y) \cdots (x + y\zeta_p^{p-1})$$

as ideals. Then since by 4.1 we know the ideals are coprime, then by lemma 3.9 we have that each $(x + y\zeta_p^i) = \mathfrak{a}^p$, for $\mathfrak{a}$ some ideal. Note that, $[\mathfrak{a}^p] = 1$ in the class group. Now, since p does not divide the size of the class group we have that $[\mathfrak{a}] = 1$ in the class group, so its principal. So we have $x + y\zeta_p^i = u_i\alpha_i^p$ with u_i a unit. So by 4.4 we have some k such that $x + y\zeta_p - \zeta_p^{2k}x - \zeta_p^{2k-1} \equiv 0 \pmod p$. If $1, \zeta_p, \zeta_p^{2k}, \zeta_p^{2k-1}$ are distinct, then 4.3 says that p divides x, y, contrary to our assumption. So they cannot be distinct, but checking each case leads to a contradiction, therefore there cannot be any such solutions. ☐

Theorem 4.8. *Let p be a regular prime and let $u \in \mathbb{Z}[\zeta_p]^\times$. If $u^p \equiv a \mod p$ for some $a \in \mathbb{Z}$, then there exists $v \in \mathbb{Z}[\zeta_p]^\times$ such that $u = v^p$.*

Theorem 4.9. *Let p be an odd regular prime. Then*

$$x^p + y^p = z^p$$

has no solutions with $x, y, z \in \mathbb{Z}$ and $p|xyz$.

Theorem 4.10. *Let p be an odd regular prime. Then*

$$x^p + y^p = z^p$$

has no solutions with $x, y, z \in \mathbb{Z}$ and $xyz \neq 0$.

References

[Mar18] Daniel A. Marcus. *Number fields*. Universitext. Springer, Cham, 2018. Second edition of [MR0457396], With a foreword by Barry Mazur.

[Sam70] Pierre Samuel. *Algebraic theory of numbers*. Translated from the French by Allan J. Silberger. Houghton Mifflin Co., Boston, Mass., 1970.

[Was82] Lawrence C. Washington. *Introduction to cyclotomic fields*, volume 83 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1982.