SPLITTING OF PRIMES IN $\mathbb{Q}(\sqrt[5]{2})$

GIEDRIUS ALKAUSKAS

Let us work the example of splitting of primes in a non normal field extension $k = \mathbb{Q}(\sqrt[5]{2})$. The five conjugates of $2^{1/5}$ are

$$a = 2^{1/5}, \quad b = \rho 2^{1/5}, \quad c = \rho^2 2^{1/5}, \quad d = \rho^3 2^{1/5}, \quad e = \rho^4 2^{1/5},$$

where ρ is a primitive $5-$th root of unity; that is, the root of the polynomial $X^4 + X^3 + X^2 + X + 1$. Let $K = k(\rho)$. Then K is a normal extension of rational numbers:

$$\mathbb{Q} \subset k \subset K.$$

There are at least 4 different automorphisms of K/k. These are $\rho \to \rho^i$ for $i = 1, 2, 3, 4$. Therefore, $[K : k] = 4$ and thus $[K : \mathbb{Q}]$=20. The discriminant of the polynomial $P(x) = X^5 - 2$ is $5^5 2^4$. Thus, only primes 2 and 5 (possibly) ramify in k. We have $(2) = (2^{1/5})^5$. We can factor (5) into prime ideals as well. In fact, the norm of number $2^{1/5} - 2$ is equal to -30. Therefore $(2^{1/5} - 2) = (2^{1/5})\mathfrak{q}\mathfrak{r}$, where $\mathfrak{q}$ and $\mathfrak{r}$ are ideals of first degree, dividind correspondingly 5 and 3. Taking the fifth power, we obtain:

$$(30 - 80 \cdot 2^{1/5} + 80 \cdot 2^{2/5} - 40 \cdot 2^{3/5} + 10 \cdot 2^{4/5}) = (2)\mathfrak{q}^5\mathfrak{r}^5.\mathcal{P}$$

Since (2) and $\mathfrak{r}$ are relatively prime with 5, this equation implies $5|\mathfrak{q}^5$. Since $\mathfrak{q}$ is a prime first degree ideal, this yields $(5) = \mathfrak{q}^5 = (5, 2^{1/5} - 2)^5$. We see that (2) ramifies with ramification index 5, which is not divisible by 2 (tame ramification case), and so there is a factor of exactly 2^4 if the discriminant D_k of $k/\mathbb{Q}$. Likewise, 5 ramifies with ramification index 5, which is divisible by 5 (wild ramification case), and so there is a factor at least 5^5 in D_k. Since the discriminant of this integer monic polynomial is the discriminant of the field times some integer square (more precisely, $\mathrm{Disc}(P) = D_k \cdot \left(\mathcal{O}_k : \mathbb{Z}[2^{1/5}]\right)^2$), we see that $D_k = 5^5 2^4$ and that the ring of integers of k is really $\mathbb{Z}[2^{1/5}]$.

We will now construct a Galois group of $K/\mathbb{Q}$. If we know what the automorphism does to a and b, we know then what it does to ρ. Hence we can present $G = \mathrm{Gal}(K/\mathbb{Q})$ as a permutation group on the five letters a, b, c, d, e. First we will find G by finding some subgroups of it, using Galois theory. Consider $K = \mathbb{Q}(\rho)(2^{1/5})$ as an extension of $\mathbb{Q}(\rho)$ of degree five. The five conjugates of $2^{1/5}$ over $\mathbb{Q}(\rho)$ are a, b, c, d, e and any element of Galois group $\mathrm{Gal}(K/\mathbb{Q}(\rho))$ is completely determined by knowing where it sends a. In particular, there is an element σ in $\mathrm{Gal}(K/\mathbb{Q}(\rho))$, which sends $2^{1/5}$ to $\rho 2^{1/5}$. That is, $a^\sigma = b$. The other numbers are permuted cyclically. In fact, since σ fixes ρ, we have $b^\sigma = (\rho a)^\sigma = \rho(a)^\sigma = c$. Similarly, $c^\sigma = d$, $d^\sigma = e$, $e^\sigma = a$. Therefore σ is represented by the five cycle (a, b, c, d, e), and

$$\mathrm{Gal}(K/\mathbb{Q}(\rho)) = \{1, \sigma, \sigma^2, \sigma^3, \sigma^4\}.$$

This gives us 5 elements of the group of order 20. Now consider the normal extension $K/k = k(\rho)/k$ of degree four. Similarly, there is a unique automorphism, which fixes k and sends ρ

to ρ^2. Denote it by τ. Then $\rho^\tau = \rho^2$. Then $(\rho^2)^\tau = \rho^4$, $(\rho^3)^\tau = \rho$, $(\rho^4)^\tau = \rho^3$. Since τ fixes $2^{1/5}$, we thus can represent τ as a cycle $\tau = (b, c, e, d)$. Therefore

$$\mathrm{Gal}(K/k) = \{1, \tau, \tau^2, \tau^3\}.$$

None of last three are in the group generated by σ. In fact, it is easy to check using permutation representations or, alternatively, τ, τ^2 and τ^3 fix $\mathbb{Q}(2^{1/5})$, while from the group generated by σ only identity automorphism fixes k. Thus we get the whole group of 20 elements by multiplying these two elementwise. Thus,

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma^i\tau^j; \quad 0 \leq \sigma \leq 4, 0 \leq \tau \leq 3\}.$$

Adittionally, we have a relation $\tau\sigma = \sigma^3\tau$, which can be checked, using permutation representations we have given.

The splitting of the prime p from $\mathbb{Q}$ to K and of the prime ideal $\mathfrak{p}$ from k to K are governed by the Frobenius automorphisms. Thus, we combine this information to get the desired description of how the primes split from $\mathbb{Q}$ to k. First we need to divide the elements of G into conjugacy classes. Here is the complete list:

- i) $\{1\}$- the identity automorphism;
- ii) $\{\sigma, \sigma^2, \sigma^3, \sigma^4\}$- consisting of five-cycles;
- iii) $\{\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau, \sigma^4\tau\}$- consisting of four-cycles;
- iv) $\{\tau^2, \sigma\tau^2, \sigma^2\tau^2, \sigma^3\tau^2, \sigma^4\tau^2\}$ - consisting of permutations with two two-cycles;
- v) $\{\tau^3, \sigma\tau^3, \sigma^2\tau^3, \sigma^3\tau^3, \sigma^4\tau^3\}$ -consisting of four-cycles.
  (Note that conjugaton in the symmetric group, and hence in all its subgroups preserves the cycle structure).

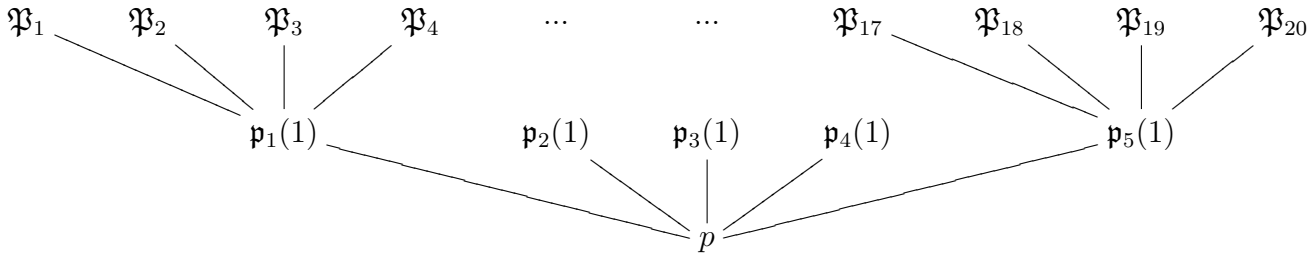
Let now $\mathfrak{P}$ be unramified prime in K which lies above a prime $\mathfrak{p}$, which in his turn lies above the prime p in $\mathbb{Q}$. Note that the fields k and $l = \mathbb{Q}(\rho)$ are disjoint (their common subfield will have a degree which would divide 4 and 5). Since l is a cyclotomic field with discriminant $D_l = 125$, and K is a composite field kl, the well known formula states that

$$\mathrm{disc}(D_K) = D_k^{[l:\mathbb{Q}]} \cdot D_l^{[k:\mathbb{Q}]}.$$

This implies that in K only the same primes (2 and 5) ramify. Let $\sigma(\mathfrak{P})$ be the Frobenius automorphism of $\mathfrak{P}$ relative to $\mathbb{Q}$, and $\sigma(\mathfrak{P}/\mathfrak{p})$ be the corresponding Frobenius automorphis of $\mathfrak{P}$ relative to k. Let $f(\mathfrak{P})$ be the order of $\sigma(\mathfrak{P})$ and suppose $f(\mathfrak{P}/\mathfrak{p})$ is the order of $\sigma(\mathfrak{P}/\mathfrak{p})$. Then we know that $\sigma(\mathfrak{P}/\mathfrak{p}) = \sigma(\mathfrak{P})^{f(\mathfrak{p})}$, where $f(\mathfrak{p})$ is the order of the prime ideal $\mathfrak{p}$. We have also that $f(\mathfrak{P}) = f(\mathfrak{p})f(\mathfrak{P}/\mathfrak{p})$. After reminding these basic facts, we will turn to our field and look into five conjugacy classes, where the Frobenius automorphism may lie. (Remember that the Galois group $H = \mathrm{Gal}(K/k)$ is generated by τ and consists of four elements).

i) $\sigma(\mathfrak{P}) = 1$. Then this Frobenius automorpism has order one, and since $n = fr$, where f is the order of prime ideal and r is a number of different conjugates, we have that all $\mathfrak{P}^g$ are different for $g \in G$, hence there are 20 ideals lying above such p in K. In this case $\sigma(\mathfrak{P})$

belongs to H, and so $\sigma(\mathfrak{P}/\mathfrak{p}) = \sigma(\mathfrak{P})$, and there are four distinct primes lying above $\mathfrak{p}$. Thus, all twenty conjugate prime ideals $\mathfrak{P}^g$ splitt into groups of four, thus giving five first degree ideals, lying in k and conjugate to $\mathfrak{p}$. It looks like this (we write the degrees of prime ideals in k in brackets).

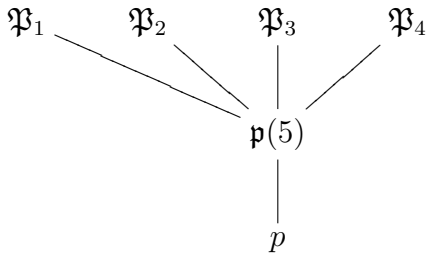


An example of such a prime is $p = 151$. Since $x^5 - 2 \equiv (x + 102)(x + 129)(x + 61)(x + 35)(x + 126) (\mathrm{mod}\ 151)$, then for $\alpha = 2^{1/5}$ we have:

$$(151) = (151, \alpha + 102)(151, \alpha + 129)(151, \alpha + 61)(151, \alpha + 35)(151, \alpha + 126).$$

Here from the definition of the Frobenius automorphism we have that $\theta^{\sigma(\mathfrak{P})} \equiv \theta^p (\mathrm{mod}\ \mathfrak{P})$. For $\theta = \rho$ this reads as $\rho \equiv \rho^p (\mathrm{mod}\ \mathfrak{P})$. Since ρ is a unit in the field K, the norm of the element $\mathcal{N}_{K/\mathbb{Q}}(\rho^{p-1} - 1)$ is divisible by $\mathfrak{P}$. Since this norm is $\left(\mathcal{N}_{\mathbb{Q}(\rho)/\mathbb{Q}}(\rho^{p-1} - 1)\right)^5 = 5^5$ unless $p \equiv 1 (\mathrm{mod}\ 5)$, the last case is the only one possible.

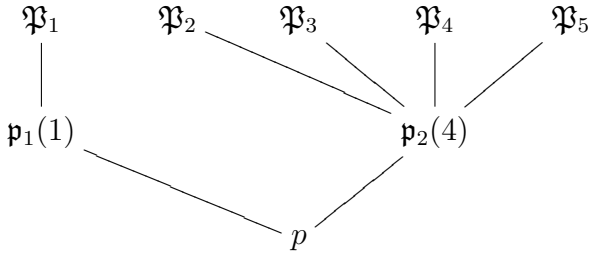
ii) $\sigma(\mathfrak{P})$ is in the conjugacy class $\{\sigma, \sigma^2, \sigma^3, \sigma^4\}$. Then $f(\mathfrak{P}) = 5$ and there are four fifth degree primes above p: $\mathfrak{P} = \mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{P}_3$ and $\mathfrak{P}_4$. The smallest s for which $\sigma(\mathfrak{P})^s \in H$ is in all cases equal to 5. So, $\sigma(\mathfrak{P}/\mathfrak{p}) = \sigma(\mathfrak{P})^5 = 1$. Thus, a prime ideal $\mathfrak{p}$ of k splits completely in K into four ideals $\mathfrak{P}_i$, $1 \leq i \leq 4$. Here $f(\mathfrak{p}) = 5$. Therefore in this case we have a unique prime ideal $\mathfrak{p}$ of degree 5 above p. It looks like this.



Here the example is $p = 11$. Since $x^5 - 2$ is irreducible modulo 11, then (11) is a prime ideal in k. For all integers in K we have $\theta^{\sigma(\mathfrak{P})} \equiv \theta^p (\mathrm{mod}\ \mathfrak{P})$. Since ρ is invariant under all automorphisms in this class, we have $\rho \equiv \rho^p (\mathrm{mod}\ \mathfrak{P})$, which, as we have seen, can only occur when $p \equiv 1 (\mathrm{mod}\ 5)$.

iii) $\sigma(\mathfrak{P})$ belongs to the conjugacy class $\{\tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau, \sigma^4\tau\}$. We can choose $\mathfrak{P}$ correctly among its conjugates in such manner that $\sigma(\mathfrak{P}) = \tau$. All elements in this class are of order four, and this means $f(\mathfrak{P}) = 4$, and we have 5 prime ideals of K above p: $\mathfrak{P} = \mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{P}_3, \mathfrak{P}_4$ and $\mathfrak{P}_5$. But in this case the behaviour of these ideals with respect to k differ. Since $\sigma(\mathfrak{P}) \in H$, we see that $\sigma(\mathfrak{P}/\mathfrak{p}) = \sigma(\mathfrak{P})$. In this case $f(\mathfrak{P}/\mathfrak{p}) = 4$ and $f(\mathfrak{p}) = 1$. Therefore

the prime $\mathfrak{p}$ is a first degree prime ideal which is inert in K; there we have $\mathfrak{P} = \mathfrak{p}$. It is quite a different picture for other conjugate ideals of $\mathfrak{P}$ (say, $\mathfrak{P}_2$), which have as Frobenius automorphism other element in this conjugacy class than τ. Then the smallest s for which $\sigma(\mathfrak{P}_2)^s \in H$ is $s = 4$, and therefore $\sigma(\mathfrak{P}_2/\mathfrak{p}_2) = \sigma(\mathfrak{P}_2)^4 = 1$. Hence there are four primes above $\mathfrak{p}_2$, and these should be $\mathfrak{P}_2$, $\mathfrak{P}_3, \mathfrak{P}_4, \mathfrak{P}_5$. Since $f(\mathfrak{P}_2/\mathfrak{p}_2) = 1$, we obtain $f(\mathfrak{p}_2) = 4$. Gathering all information together we obtain two primes in k above p; these are $\mathfrak{p}_1$ of degree 1 and $\mathfrak{p}_2$ of degree 4. Here is the picture.

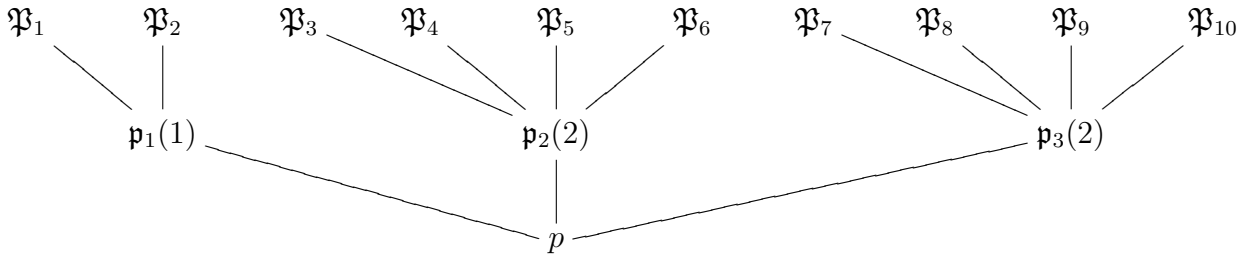


The prime splitting by this pattern is $p = 7$. Since $x^5 - 2 \equiv (x + 3)(x^4 + 4x^3 + 2x^2 + x + 4)(\text{mod } 7)$, then

$$(7) = (7, \alpha + 3)(7, \alpha^4 + 4\alpha^3 + 2\alpha^2 + \alpha + 4).$$

In this case from the definition of the Frobenius automorphism we have $\theta^{\sigma(\mathfrak{P})} \equiv \theta^p (\text{mod } \mathfrak{P})$ for all integers $\theta \in \mathcal{O}_K$. taking $\theta = \rho$, we see that all automorphisms in this class act like τ on ρ. Thus $\rho^2 \equiv \rho^p (\text{mod } \mathfrak{P})$. Thus the norm $\mathcal{N}_{K/\mathbb{Q}}(\rho^{p-2} - 1)$ is also divisible by $\mathfrak{P}$. Since this norm is 5^5 unless $p \equiv 2(\text{mod } 5)$, we see that this case occurs only when $p \equiv 2(\text{mod } 5)$.

iv) $\sigma(\mathfrak{P})$ belongs to the conjugacy class $\{\tau^2, \sigma\tau^2, \sigma^2\tau^2, \sigma^3\tau^2, \sigma^4\tau^2\}$. All elements have order 2, and so $f(\mathfrak{P}) = 2$. This means that there are 10 prime ideals $\mathfrak{P}_i$. $1 \leq i \leq 10$, of order 2 in K, lying above p. By choosing suitable conjugate of $\mathfrak{P}$, we may assume that $\sigma(\mathfrak{P}) = \tau^2$. Then $\sigma(\mathfrak{P}) \in H$ and we deduce, as always, that $\sigma(\mathfrak{P}/\mathfrak{p}) = \sigma(\mathfrak{P})$. Therefore $f(\mathfrak{P}/\mathfrak{p})$=2. Hence we have two prime ideals in K above $\mathfrak{p} = \mathfrak{p}_1$, say $\mathfrak{P} = \mathfrak{P}_1$ and $\mathfrak{P}_2$. They both have τ^2 as their Frobenius automorphism. Since $f(\mathfrak{p}_1) = 1$, $\mathfrak{p}_1$ is a prime ideal in k of degree 1. For the rest conjugates of $\mathfrak{P}$ (say, for $\mathfrak{P}_3$), the Frobenius automorphism $\sigma(\mathfrak{P}_3) = \sigma\tau^2$ or other element in the conjugacy class out or remaining three. Then $\sigma(\mathfrak{P}_3) \notin H$, but $\sigma(\mathfrak{P}_3)^2 = 1 \in H$, so $f(\mathfrak{P}_3/\mathfrak{p}_2) = 1$. Therefore, there are four prime ideals above $\mathfrak{p}_2$, and additionally $f(\mathfrak{p}_2) = 2$. In this case the eight primes $\mathfrak{P}_i$, $3 \leq i \leq 10$, split into groups of four, each group lying above one of two ideals $\mathfrak{p}_2$ or $\mathfrak{p}_3$. Summarising, in k we have one first degree ideal and two second degree ideals above p. The picture is the following:



The example here is $p = 19$. Since $x^5 - 2 \equiv (x+4)(x^2+18x+16)(x^2+16x+16) (\text{mod } 19)$, then

$$(19) = (19, \alpha + 4)(19, \alpha^2 + 18\alpha + 16)(19, \alpha^2 + 16\alpha + 16).$$

Likewise like in case iii) we deduce that $\rho^{\tau^2} \equiv \rho^p (\text{mod } \mathfrak{P})$. Hence $\rho^4 \equiv \rho^p (\text{mod } \mathfrak{P})$. Similarly, we deduce that this occurs only when $p \equiv 4 (\text{mod } 5)$.

v) $\sigma(\mathfrak{P})$ belongs to the conjugacy class $\{\tau^3, \sigma\tau^3, \sigma^2\tau^3, \sigma^3\tau^3, \sigma^4\tau^3\}$. Here we have the same situation as in case iii). This case occurs only when $p \equiv 3 (\text{mod } 5)$.

Summarising, we can certainly decide how the prime p splits in $\mathbb{Q}(\sqrt[5]{2})$ only by knowing what the residue of p modulo 5, with the exception that $p \equiv 1 (\text{mod } 5)$ can split completely or remain inert. This exemple fits well with the Chebotarev density theorem. This theorem states that (in our case) the analitic density of primes in i) is $1/20$, primes in ii) make $1/5$ part of all primes, and all cases iii), iv) and v) have $1/4$ primes, splitting by that pattern. Hence the major interest in this field is to describe $1/5-$th of the primes among $p \equiv 1 (\text{mod } 5)$, which split completely.

References

[1] H. M. Stark, *Galois Theory, Algebraic Numbers and zeta functions*, Springer-Verlag (1995)