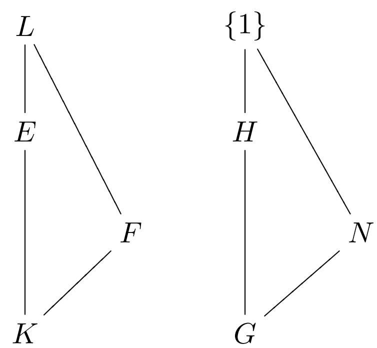
PRIMES OF DEGREE 1 AND CONGRUENCE CONDITIONS

KEITH CONRAD

For a number field K and a finite extension E/K, set

$$\mathrm{Spl}(E/K) = \{\mathfrak{p} \text{ in } K : \mathfrak{p} \text{ splits completely in } E\},$$
$$\mathrm{Spl}_1(E/K) = \{\mathfrak{p} \text{ in } K : \text{some } \mathfrak{P}|\mathfrak{p} \text{ in } E \text{ has } f(\mathfrak{P}|\mathfrak{p}) = 1\}.$$

Theorem 1. *Let E/K be a finite extension and F/K be a Galois extension. Let L/K be the Galois closure of E/K, $G = \mathrm{Gal}(L/K)$, $H = \mathrm{Gal}(L/E)$.*



Then $\mathrm{Spl}_1(E/K) = \mathrm{Spl}(F/K)$ up to a set of primes with density 0 if and only if $F \subset E$ and $\bigcup_{\sigma\in G} \sigma H \sigma^{-1} = N$, where $N = \mathrm{Gal}(L/F)$. In this case, $\mathrm{Spl}_1(E/K) = \mathrm{Spl}(F/K)$ up to only finitely many exceptions.

Of course, usually $\bigcup_{\sigma\in G} \sigma H \sigma^{-1}$ will not be a subgroup of G.

Proof. When $\mathfrak{p}$ is unramified in E, the condition that $\mathfrak{p} \in \mathrm{Spl}_1(E/K)$ is equivalent to some Frobenius element over $\mathfrak{p}$ in G fixing the field E. That is, the Frobenius conjugacy class of $\mathfrak{p}$ in G must lie in $\bigcup_{\sigma\in G} \sigma H \sigma^{-1}$.

By the Chebotarev density theorem, the sets $\mathrm{Spl}_1(E/K)$ and $\mathrm{Spl}(F/K)$ have densities

$$d(\mathrm{Spl}_1(E/K)) = \frac{\#(\bigcup_{\sigma\in G} \sigma H \sigma^{-1})}{\#G}, \quad d(\mathrm{Spl}(F/K)) = \frac{1}{[F:K]}.$$

Bauer's theorem (see, for instance, Neukirch's *Class Field Theory* p. 135) says $\mathrm{Spl}_1(E/K)$ lies in $\mathrm{Spl}(F/K)$ up to a set of primes with density 0 if and only if $F \subset E$. Therefore if $\mathrm{Spl}_1(E/K) = \mathrm{Spl}(F/K)$ up to a set with density 0, then $F \subset E$. In this case, set $N = \mathrm{Gal}(L/F)$, so $N \lhd G$. Then

$$d(\mathrm{Spl}(F/K)) = \frac{\#N}{\#G},$$

so $F \subset E \Longrightarrow H \subset N \Longrightarrow \bigcup_{\sigma\in G} \sigma H \sigma^{-1} \subset N$. Since $\mathrm{Spl}_1(E/K)$ and $\mathrm{Spl}(F/K)$ are equal up to a set of density 0, they have the same density, so we obtain

$$\bigcup_{\sigma\in G} \sigma H \sigma^{-1} = N.$$

This equality shows the sets $\mathrm{Spl}_1(E/K)$ and $\mathrm{Spl}(F/K)$ contain the same primes of K unramified in E, so the sets can differ only in ramified primes, which is a finite set.

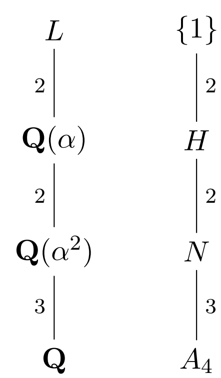
For the converse direction, we get $\mathrm{Spl}_1(E/K) \subset \mathrm{Spl}(F/K)$ since $F \subset E$. The two sets of primes have equal density by hypothesis, so they are equal up to a set of density 0. $\square$

Corollary 1. *Let $f(X) \in \mathbf{Z}[X]$ be a monic irreducible. Set $E = \mathbf{Q}(\alpha)$, where $f(\alpha) = 0$, and let $L/\mathbf{Q}$ be the Galois closure of $E/\mathbf{Q}$. Set $G = \mathrm{Gal}(L/\mathbf{Q})$ and $H = \mathrm{Gal}(E/\mathbf{Q})$. Then the set of primes p such that $f(X) \bmod p$ has a root in $\mathbf{Z}/p\mathbf{Z}$ is determined by a finite set of congruence conditions up to finitely many exceptions if and only if $\bigcup_{\sigma\in G} \sigma H \sigma^{-1}$ is a normal subgroup of G, say N, such that G/N is abelian.*

Proof. For primes p not dividing the discriminant of f (which excludes only finitely many primes), $f(X) \bmod p$ has a root in $\mathbf{Z}/p\mathbf{Z}$ if and only if p lies in $\mathrm{Spl}_1(E/\mathbf{Q})$. The number fields in which p splitting completely is determined by congruence conditions are the subfields of cyclotomic fields, which are the finite abelian extensions of $\mathbf{Q}$ by the Kronecker-Weber theorem. $\square$

To find examples of this phenomenon, we look for a finite group G with a (non-normal) subgroup H such that $\bigcup_{\sigma\in G} \sigma H \sigma^{-1}$ is a (necessarily normal) subgroup of G whose quotient is abelian. Then we try to realize G as a Galois group over $\mathbf{Q}$. To make sure H corresponds to a subfield whose Galois closure is the top field, we need $\bigcap_{\sigma\in G} \sigma H \sigma^{-1}$ to be trivial.

An example is $G = A_4$ with H any subgroup of size 2. Then $\bigcup_{\sigma\in G} \sigma H \sigma^{-1}$ is the (normal) subgroup N of size 4, so the quotient G/N has size 3 and thus is abelian. We want to realize A_4 as the Galois group of a polynomial of degree $[G : H] = 6$. A search with PARI yields the choice $X^6 - 3X^2 - 1$. Let α be a root. Then the subfield of $\mathbf{Q}(\alpha)$ corresponding to N will be a cubic subfield, and it is $\mathbf{Q}(\alpha^2)$. The minimal polynomial of α^2 over $\mathbf{Q}$ is $X^3 - 3X - 1$. The roots of this cubic polynomial are $\zeta + \zeta^{-1}$ as ζ runs over the primitive 9th roots of unity, so $\mathbf{Q}(\alpha^2)$ is the maximal real subfield of the 9-th cyclotomic field.



The polynomial $X^6 - 3X^2 - 1$ is non-normal and its Galois closure over $\mathbf{Q}$ is nonabelian, but for primes p,

$$X^6 - 3X^2 - 1 \bmod p \text{ has a root in } \mathbf{Z}/p\mathbf{Z} \iff p \equiv \pm 1 \bmod 9 \text{ or } p = 3.$$

Such primes up to 100 are 3, 17, 19, 37, 53, 71, 73, and 89.

Bob Griess noted there is an infinite family of finite G with non-normal subgroup H such that the union of the subgroups of G conjugate to H is a subgroup of G. Take $G = \mathrm{AGL}_n(\mathbf{F})$, which is the group of affine linear transformations $f_{A,\mathbf{b}} \colon \mathbf{v} \mapsto A\mathbf{v} + \mathbf{b}$ on $\mathbf{F}^n$, where $\mathbf{F}$ is a finite field. (Here $A \in \mathrm{GL}_n(\mathbf{F})$ and $\mathbf{b} \in \mathbf{F}^n$.) Inside G we have the subgroup T of all translations $t_{\mathbf{b}} \colon \mathbf{v} \mapsto \mathbf{v} + \mathbf{b}$. Check by a computation that

$$f_{A,\mathbf{c}} \circ t_{\mathbf{b}} \circ f_{A,\mathbf{c}}^{-1} = t_{A\mathbf{b}},$$

so T is a normal subgroup of G. In fact, G is the semidirect product $T \rtimes \mathrm{GL}_n(\mathbf{F})$, where $\mathrm{GL}_n(\mathbf{F})$ acts on T by standard matrix-vector multiplication.

Let $n \geq 2$ and choose a nonzero proper subspace W of $\mathbf{F}^n$. (To fix ideas, you could take W to be a one-dimensional subspace, but it doesn't really matter.) Let $H_W = \{t_{\mathbf{b}} : \mathbf{b} \in W\}$. This is a nonzero proper subgroup of T. For any one nonzero $\mathbf{b}$ in $\mathbf{F}^n$, $\{A\mathbf{b} : A \in \mathrm{GL}_n(\mathbf{F})\} = \mathbf{F}^n - \{\mathbf{0}\}$. Therefore the conjugation formula above shows H_W is not a normal subgroup of G and the union of the subgroups of G which are conjugate to H_W is T, a normal subgroup. The quotient group G/T is $\mathrm{GL}_n(\mathbf{F})$, which is non-abelian.