Simple proof of Chebotarëv’s theorem on roots of
unity∗†

P. E. Frenkel

Abstract

We give a simple proof of Chebotarëv’s theorem: Let $p$ be a prime
and $\omega$ a primitive $p$th root of unity. Then all minors of the matrix
$(\omega^{ij})_{i,j=0}^{p-1}$ are non-zero.

Let $p$ be a prime and $\omega$ a primitive $p$th root of unity. We write $\mathbf{F}_p$ for
the field with $p$ elements. In 1926, Chebotarëv proved the following theorem
(see [5]):

Theorem. For any sets $I, J \subseteq \mathbf{F}_p$ with equal cardinality, the matrix
$(\omega^{ij})_{i \in I, j \in J}$ has non-zero determinant.

Several independent proofs have been given, including ones by Dieudonné
[1], Evans and Isaacs [2], and Terence Tao [3]. Tao points out that the
theorem is equivalent to the inequality $|\text{supp} f| + |\text{supp} \hat{f}| \geq p + 1$ holding
for any function $0 \not\equiv f : \mathbf{F}_p \rightarrow \mathbb{C}$ and its Fourier transform $\hat{f}$, a fact also
discovered independently by András Biró. Biró posed this as Problem 3
of the 1998 Schweitzer Competition. The proof I gave in the competition
(the one in the present article) is published in Hungarian in [4, pp. 53–54.].
It was also discovered (as part of a more general investigation) by Daniel
Goldstein, Robert M. Guralnick and I. M. Isaacs [3, Section 6].

The proof is based on the following two lemmas. Lemma [1] is covered by
[7, Chapter 1], but we include a proof for the sake of completeness.

Lemma 1 $\mathbb{Z}[\omega]/(1 - \omega) = \mathbf{F}_p$.

∗Keywords and phrases: roots of unity, non-zero minors
†2000 Mathematics Subject classification: 11T22 (primary), 42A99, 11C20 (secondary)
Proof. Let Ω be an indeterminate and let Φp(Ω) = 1 + Ω + \cdots + Ωp−1 be the minimal polynomial of the algebraic integer ω. Consider the surjective ring homomorphisms
\[ \mathbb{Z}[Ω] \to \mathbb{Z}[Ω]/(Φ_p(Ω)) = \mathbb{Z}[ω], \quad Ω \mapsto ω \]
and
\[ \mathbb{Z}[Ω] \to \mathbb{Z}[Ω]/(1 − Ω, p) = \mathbb{F}_p, \quad Ω \mapsto 1. \]
The latter kernel contains the former one since Φp(Ω) ≡ p mod (1 − Ω). Therefore, the latter homomorphism factors through the former one via a surjective homomorphism \[ \mathbb{Z}[ω] \to \mathbb{F}_p \]
whose kernel is the ideal \((1 − ω, p)/(Φ_p(Ω)) = (1 − ω),\)
the last equality following from \(p ≡ Φ_p(ω) = 0 \mod (1 − ω). \)

Lemma 2 Let \(0 \not≡ g(x) ∈ \mathbb{F}_p[x]\) be a polynomial of degree \(< p\). Then the multiplicity of any element \(0 \not≡ a ∈ \mathbb{F}_p\) as a root of \(g(x)\) is strictly less than the number of non-zero coefficients of \(g(x)\).

Proof. For \(g(x)\) constant, the lemma is obviously true. Assume that it is true for any \(g(x)\) of degree \(< k\), with some fixed \(1 ≤ k < p\), and take \(g(x)\) of degree \(k\). If \(g(0) = 0\), then \(g(x)\) has the same number of non-zero coefficients and the same multiplicity of vanishing at \(a\) as \(g(x)/x\) does, so the lemma is true for \(g(x)\). If \(g(0) \not≡ 0\), then the number of non-zero coefficients exceeds the corresponding number for the derivative \(g’(x)\) by \(1\), and the multiplicity of vanishing at \(a\) exceeds that of \(g’(x)\) by at most \(1\). Now \(g’(x) \not≡ 0\) since \(g(x)\) is of positive degree \(k < p\), so the inequality of the lemma holds for \(g’(x)\) and therefore also for \(g(x)\).

Proof of the theorem. The theorem is equivalent to saying that if numbers \(a_j ∈ \mathbb{Q}(ω) (j ∈ J)\) satisfy \(\sum_{j ∈ J} a_jω^j = 0\) for all \(i ∈ I\), then all \(a_j\) must be zero. In fact, we may clearly assume that \(a_j ∈ \mathbb{Z}[ω]\). The above equalities mean that the polynomial
\[ g(x) = \sum_{j ∈ J} a_jx^j ∈ \mathbb{Z}[ω][x] \]
vanishes at \(ω^i\) for all \(i ∈ I\). So \(g(x)\) is divisible by \(\prod_{i ∈ I}(x − ω^i)\). Applying the homomorphism \(\mathbb{Z}[ω] \to \mathbb{Z}[ω]/(1 − ω) = \mathbb{F}_p\) to the coefficients of \(g(x)\) we get a polynomial \(\bar{g}(x) ∈ \mathbb{F}_p[x]\) that is divisible by \((x − 1)^{|I|}\). On the other
hand, $\bar{g}(x)$ has at most $|J|$ non-zero coefficients. As $|I| = |J|$, we deduce from Lemma 2 that $\bar{g}(x) \equiv 0$. This means that all $a_j$ are divisible by $1 - \omega$. We may divide all of them by $1 - \omega$ and iterate the argument. This leads to *descente infinie* unless all $a_j$ are zero.

□

Acknowledgements

The author is partially supported by OTKA grants T 042769 and T 046365. The author wishes to thank András Biró for calling his attention to the subject and for useful discussions.

References

[1] J Dieudonné, Une propriété des racines de l’unité, Collection of articles dedicated to Alberto González Domínguez on his sixty-fifth birthday. Rev. Un. Mat. Argentina 25 (1970/71), 1–3.

[2] R J Evans and I M Isaacs, Generalized Vandermonde determinants and roots of unity of prime order, Proc. Amer. Math. Soc 58 (1976), 51–54.

[3] D Goldstein, R M Guralnick, I M Isaacs, Inequalities for finite group permutation modules, ArXiv preprint math.GR/0310169

[4] V Prokaj, Jelentés az 1998. évi Schweitzer Miklós matematikai emlékversenyről (in Hungarian), Matematikai lapok 7./1–2. (1997) (published in 2002), 47–67.

[5] P Stevenhagen and H W Lenstra Jr, Chebotarév and his density theorem, Math. Intelligencer 18 (1996), no. 2, 26–37.

[6] Terence Tao, An uncertainty principle for cyclic groups of prime order, submitted to Math. Research Letters, arXiv:math.CA/0308286

[7] L C Washington, Introduction to Cyclotomic Fields, Springer, GTM series 83, 1982

Address. Mathematics Institute, Budapest University of Technology and Economics, Egry J. u. 1., Budapest, 1111 Hungary. E-mail: frenkelp@renyi.hu