ARITHMETIC STATISTICS COURSE NOTES

ROBERT J. LEMKE OLIVER

1. Integer polynomials and Hilbert irreducibility

We begin with a very loose statement of Hilbert's irreducibility theorem[1]. Unpacking how to turn this loose statement into a rigorous one will motivate some of the key themes of this course. And of course, its proof is good too!

Theorem 1.1 (Hilbert irreducibility; loose version)**.** *Asymptotically,* 100% *of integer polynomials of degree n are irreducible and have Galois group S_n.*

It turns out this theorem is true in a very robust sense (meaning it's applicable in many settings and variations, with respect to many notions of complexity; that's why it's a template for an entire class of theorem), but let's consider what this is saying relative to the notion of complexity we considered in the previous section, the largest absolute value of the coefficients. What this theorem is considering, in words, is the following:

- First, count the number of integer polynomials with complexity at most X, i.e. the size of the set

  $$\mathcal{P}_n(X) := \{f \in \mathbb{Z}[x] : f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, |a_i| \leq X \text{ for } 1 \leq i \leq n\}.$$

- Second, count the subset of those that are irreducible and have Galois group S_n, i.e. the size of the set

  $$\mathcal{P}_n(X; S_n) := \{f \in \mathcal{P}_n(X) : f \text{ is irreducible, and } \mathrm{Gal}(f) \simeq S_n\}.$$

- Then, compute the proportion of those polynomials that are irreducible with Galois group S_n, and take the limit as $X \to \infty$, i.e.

$$\lim_{X \to \infty} \frac{\#\mathcal{P}_n(X; S_n)}{\#\mathcal{P}_n(X)}. \tag{1.1}$$

The Hilbert irreducibility theorem, in its rigorous form, asserts that this limit in (1.1) is equal to 1:

Theorem 1.2 (Hilbert irreducbility; rigorous version)**.** *With notation as above, for any integer $n \geq 2$,*

$$\lim_{X \to \infty} \frac{\#\mathcal{P}_n(X; S_n)}{\#\mathcal{P}_n(X)} = 1.$$

Date: January 24, 2022.

[1]The Hilbert irreducibility theorem is now regarded as a template for a much broader class of theorem, some of which look almost nothing like this one. This one is, I believe, close to Hilbert's original version.

1.1. **The counting problem.** We will take a look at actual data in some small cases in just a second to get a better feel of what this theorem is asserting, but before we do that, it's convenient to first consider the counting problem. In this case, we're just trying to estimate $\#\mathcal{P}_n(X)$. If X is a positive integer, then there are exactly $2X+1$ integers in the interval $[-X, X]$, and hence exactly $(2X+1)^n$ choices for the n different coefficients of a polynomial $f \in \mathcal{P}_n(X)$. It's not a problem to assume that X is an integer, but it's convenient for the proof to come (and as a means of introducing some useful notation) to consider what happens when X is not an integer. We could still get an exact formula by replacing X by its floor – the number of integers in $[-X, X]$ is exactly $2\lfloor X \rfloor + 1$ – but instead, it's more motivating to consider how wrong our "simple" estimate $(2X+1)^n$ can be. In particular, most counting problems in arithmetic statistics don't admit an exact formula (for example, we're not going to get an exact answer for $\#\mathcal{P}_n(X; S_n)$) and so it's useful to understand how to write rigorous but inexact formulas.

In the case of counting integers in the interval $[-X, X]$, the formula $2X+1$ is always at least as large as the right answer, $2\lfloor X \rfloor + 1$, and it can only off by just less than 2 at the worst, coming from when X is just below an integer (e.g., $X = 99.999$). That means the number of integers in $[-X, X]$ is always between $2X-1$ and $2X+1$, so we can write it as $2X+\theta$ for some $\theta \in [-1, 1]$. Implicitly, θ is a function of X, but the content of this statement is that it's a *bounded* function. Back to polynomials, again by considering the choices for the n different coefficients, this means $\#\mathcal{P}_n(X) = (2X+\theta)^n$. Using the binomial theorem, we rewrite this in the temporarily cumbersome form,

$$\#\mathcal{P}_n(X) = (2X)^n + \binom{n}{1}(2X)^{n-1}\theta + \binom{n}{2}(2X)^{n-2}\theta^2 + \cdots + \theta^n.$$

What's important to absorb here is not the exact form – again, we're ultimately not shooting for an exact formula – so much as the order of magnitude of the various terms, remembering that we'll ultimately be taking the limit as $X \to \infty$. In particular, every subsequent term on the right-hand side is of a smaller order of magnitude than the first term, with the second term being the largest of these subsequent terms. Thus, we expect the contribution of all subsequent terms to have order of magnitude X^{n-1}, which we make rigorous by noting that the function

$$\frac{\binom{n}{1}(2X)^{n-1}\theta + \binom{n}{2}(2X)^{n-2}\theta^2 + \cdots + \theta^n}{X^{n-1}} \tag{1.2}$$

is bounded as $X \to \infty$. We thus introduce some notation that will enable us to write $\#\mathcal{P}_n(X) = (2X)^n + O(X^{n-1})$, where the big-oh term $O(X^{n-1})$ is keeping track of the order of magnitude of the hidden parts of this formula.

Notation (Big-oh)**.** Given two functions $f(X)$ and $g(X)$ with $g(X)$ strictly positive, we say that $f(x) = O(g(X))$ if the ratio $f(X)/g(X)$ is bounded as $X \to \infty$. If we write $f(X) = g(X) + O(h(X))$, then we mean that the difference $f(X) - g(X)$ is $O(h(X))$.

Remark. If the bound implicit in a big-oh statement depends on a parameter in the problem, we sometimes denote that with a subscript. For example, as noted earlier, the function in (1.2) is bounded as $X \to \infty$, but the bound depends on the parameter n. We therefore might more specifically say it's $O_n(X^{n-1})$ and write $\#\mathcal{P}_n(X) = (2X)^n + O_n(X^{n-1})$. By contrast, in the formula $2X+\theta$ for the number of integers in $[-X, X]$, the parameter θ is between -1 and 1, neither of which depends on n in any way. We'd therefore write this formula

as $2X + O(1)$, without any subscript. I'll usually include subscripts when necessary to be precise, but you may pretend they're not there without losing anything.

We summarize this lengthy discussion of the (fairly easy!) counting problem in the following:

Proposition 1.3. *For any $n \geq 1$ and $X \geq 1$, $\#\mathcal{P}_n(X) = 2^n X^n + O_n(X^{n-1})$. If X is an integer, then we have further $\#\mathcal{P}_n(X) = (2X+1)^n$.*

1.2. **Actual data.** Let's now actually look at some data for polynomials. For any specific values of n and X, we can compute all polynomials in $\mathcal{P}_n(X)$, see whether they factor, and (particularly with the aid of a computer) their Galois group, assuming that they're irreducible. I've done this only for some very small degrees and values of X, but this data is representative of the general picture.

1.2.1. *Cubic polynomials.* If $n = 3$, then any polynomial $f \in \mathcal{P}_3(X)$ has at most three distinct roots in $\mathbb{C}$. If f is irreducible, these three roots must be distinct, and the Galois group must rearrange or permute them in some way. In particular, if f is irreducible, then $\mathrm{Gal}(f)$ will be a subgroup of the symmetric group S_3 (the group of all permutations of $\{1,2,3\}$), and it turns out that it's either all of S_3 or the alternating subgroup A_3, which (for $n = 3$ only!) is the same as the cyclic subgroup $C_3 = \langle (1,2,3) \rangle$. [2]

For the values $X = 5$, 10, and 20, we now compute (by computer) how many polynomials in $\mathcal{P}_3(X)$ are irreducible vs. reducible, and of those that are irreducible, how many have Galois group S_3 vs. A_3. This is recoreded in Table 1.2.1.

X	$\#\mathcal{P}_3(X)$	# Irred.	# Red.	$\#\,\mathrm{Gal}(f) \simeq S_3$	$\#\,\mathrm{Gal}(f) \simeq A_3$
5	1,331	1,002	329	976	26
10	9,261	7,878	1,383	7,760	118
20	68,921	63,274	5,647	62,906	368

TABLE 1. Statistics of integer cubic polynomials in $\mathcal{P}_3(X)$, i.e. those $f(x) = x^3 + a_1x^2 + a_2x + a_3$ with each $|a_i| \leq X$.

Theorem 1.2 asserts that the S_3 column should make up a larger and larger proportion of $\mathcal{P}_3(X)$ as X tends to infinity, eventually making up essentially 100%. For the data points we have, the percentages are about 73%, 84%, and 91%, which, considering that we've only taken $X = 20$, is not shabby!

1.2.2. *Quartic polynomials.* We now consider the analogous computation if $n = 4$, though with fewer values of X owing to the increased size of the problem. It turns out that there are five choices for the Galois group of an irreducible quartic polynomial: the full symmetric group S_4, the alternating group A_4, the dihedral group D_4, the Klein four group V_4, and the cyclic group C_4. This data is recored in Table 1.2.2.

As before, we can compute the percentage of polynomials that are irreducible with Galois group S_4; we find them to be about 71% and 84%. This is exhibiting the same general trend as the degree 3 case.

[2]The operative fact here is that the Galois group of an irreducible polynomial of degree n is a *transitive* subgroup G of S_n, which means that for every $i \leq n$, there is some element of G that sends 1 to i. For example, the cyclic subgroup $\langle (1,2) \rangle \subseteq S_3$ is *not* transitive, since it has no element that sends 1 to 3.

X	$\#\mathcal{P}_4(X)$	# Irred.	# Red.	$\#S_4$	$\#A_4$	$\#D_4$	$\#V_4$	$\#C_4$
5	14,641	11,246	3,395	10,382	16	774	46	28
10	194,481	169,214	25,267	163,588	182	5,118	218	108

TABLE 2. Statistics of integer quartic polynomials in $\mathcal{P}_4(X)$, i.e. those $f(x) = x^4 + a_1x^3 + a_2x^2 + a_3x + a_4$ with each $|a_i| \leq X$.

1.2.3. *Van der Waerden's conjecture.* Another observation we can make from this data is that it appears in the process of going from (all polynomials) to (irreducible polynomials) to (irreducible polynomials with Galois group S_n), it's the first step that removes the most. In other words, it appears that there are more reducible polynomials than there are irreducible polynomials with Galois group not equal to S_n. This was also noticed by van der Waerden in 1936, and he conjectured that this phenomenon should hold for any degree n. There are always at least $(2X-1)^{n-1}$ reducible polynomials – choose the constant term equal to 0 – and in fact, this is essentially the right order of magnitude: the number of reducible polynomials in $\mathcal{P}_n(X)$ turns out to be $O_n(X^{n-1})$. (We'll prove a slighly weaker version of this below.) Van der Waerden's conjecture is that this is also at most the order of magnitude of the non-S_n irreducible polynomials:

Conjecture 1.4 (Van der Waerden; 1936)**.** *For any n, the number of irreducible polynomials in $\mathcal{P}_n(X)$ with Galois group not equal to S_n is $O_n(X^{n-1})$. Equivalently, $\#\mathcal{P}_n(X; S_n) = 2^nX^n + O_n(X^{n-1})$.*[3]

After 85 years, van der Waerden's conjecture was just proven by Bhargava in Summer 2021:

Theorem 1.5 (Bhargava; 2021)**.** *Van der Waerden's conjecture is true.*

We won't discuss this theorem more today, but I am hoping to at least present the ideas behind its proof later in the semester.

1.3. **A soft proof of Hilbert irreducibility.** We now turn to providing a soft proof of Hilbert irreducibility. A "soft" proof of an asymptotic result is one without an explicit error term. By contrast, van der Waerden's conjecture above asserts that $\#\mathcal{P}_n(X; S_n) = 2^nX^n + O_n(X^{n-1})$; this is *not* soft since there is an error term, namely, the $O_n(X^{n-1})$ term. We'll instead prove Hilbert irreducibility in the form

$$\lim_{X\to\infty} \frac{\#\mathcal{P}_n(X; S_n)}{2^nX^n} = 1.$$

Notice that this is implied by van der Waerden's conjecture, but is a strictly weaker assertion.[4]

We begin by proving first that 100% of polynomials are irreducible.

Theorem 1.6. *Let $\mathcal{P}_n(X; \text{Irred.}) \subseteq \mathcal{P}_n(X)$ be the subset consisting of those polynomials that are irreducible over $\mathbb{Z}$ (or, equivalently, over $\mathbb{Q}$).*

In loose terms, our strategy may be broken down as follows:

[3]This equivalence comes from noting that any polynomial not in $\mathcal{P}_n(X; S_n)$ is either irreducible or has small Galois group, and using the above claimed bound on reducible polynomials.

[4]If this is not obvious to you, it is absolutely worth your time to unpack why this is true.

(1) If a polynomial $f \in \mathcal{P}_n(X)$ is irreducible when it is reduced $(\mathrm{mod}\, p)$ for some prime p, then it must also be irreducible over $\mathbb{Z}$. (Lemma 1.7)
(2) The "probability" that a polynomial $f \in \mathcal{P}_n(X)$ is irreducible when reduced $(\mathrm{mod}\, p)$ for a given prime p is about $1/n$. (Lemma 1.8 + Lemma 1.9)
(3) It follows that the probability that $f\,(\mathrm{mod}\, p))$ is *not* irreducible is about $1 - \frac{1}{n}$.
(4) If $p_1, \dots, p_k$ are k distinct primes, the probabilities that f is reducible modulo p_i are roughly independent from each other, and thus the probability that f is reducible modulo *every* p_i is $(1 - \frac{1}{n})^k$. (Above point + Lemma 1.9)
(5) Since a reducible polynomial in $\mathcal{P}_n(X)$ must be reducible modulo every prime, the probability a polynomial in $\mathcal{P}_n(X)$ is reducible may be bounded by $(1 - \frac{1}{n})^k$ for *every* $k \geq 1$. (Combine above points + there are infinitely many primes)
(6) This probability becomes arbitrarily small as $k \to \infty$, and thus the probability that a polynomial in $\mathcal{P}_n(X)$ is reducible must tend to 0 as $X \to \infty$.
(7) If a polynomial is reducible with probability 0, then it must be *irreducible* with probability 1. This is the statement of Theorem 1.6.

We now make this strategy precise by first proving the promised sequence of lemmas.

Lemma 1.7. *If a monic polynomial $f \in \mathbb{Z}[x]$ is irreducible when reduced $(\mathrm{mod}\, p)$ for some prime p, then it is also irreducible in $\mathbb{Z}[x]$.*

Proof. Contrapositive: If f factors in $\mathbb{Z}[x]$, then it also factors $(\mathrm{mod}\, p)$. □

Lemma 1.8. *The number of monic, degree n polynomials $(\mathrm{mod}\, p)$ that are irreducible is exactly*

$$\frac{1}{n} \sum_{d|n} \mu(d) p^{n/d}.$$

Here, the sum is over the divisors d of n, and $\mu(d)$ is the Möbius function[5]*, defined by*

$$\mu(d) := \begin{cases} (-1)^r, & \text{if } d \text{ is squarefree and has } r \text{ distinct prime divisors} \\ 0, & \text{if } d \text{ is not squarefree.} \end{cases}$$

A number is *squarefree* if it is not divisible by a nontrivial square. For example, neither 4 nor $12 = 4 \cdot 3$ is squarefree, while $6 = 2 \cdot 3$ and $30 = 2 \cdot 3 \cdot 5$ both are squarefree. We thus have $\mu(4) = 0$, $\mu(12) = 0$, $\mu(6) = (-1)^2 = 1$, and $\mu(30) = (-1)^3 = -1$.

Example. The divisors of $n = 6$ are $d = 1, 2, 3, 6$. These have $\mu(d) = 1, -1, -1, 1$, respectively. What Lemma 1.8 is asserting, therefore, is that the number of irreducible, monic, degree 6 polynomials modulo any prime p is exactly

$$\frac{1}{6}\left(p^6 - p^3 - p^2 + p\right).$$

Let's see where this comes from in the context of the proof below. If we have any irreducible polynomial f of degree 6 over $\mathbb{F}_p$, we can obtain the field extension $\mathbb{F}_{p^6}/\mathbb{F}_p$ by adjoining to $\mathbb{F}_p$ any root of f. In fact, by properties of finite fields, $\mathbb{F}_{p^6}$ is the splitting field of f, so f has all six of its roots in $\mathbb{F}_{p^6}$. Thus, we get a "map" from the set of irreducible polynomials to their six roots in $\mathbb{F}_{p^6}$.[6]

[5] `https://en.wikipedia.org/wiki/Mobius_function`

[6] Strictly speaking, it's better to create an equivalence relation on $\mathbb{F}_{p^6}$, where $\alpha \sim \beta$ if α and β are roots of the same irreducible polynomial in $\mathbb{F}_p[x]$, and to have the codomain of this map be the set of equivalence classes.

What's the image of this map? The extension $\mathbb{F}_{p^6}/\mathbb{F}_p$ is algebraic, so every element in $\mathbb{F}_{p^6}$ is the root of some irreducible polynomial, but that irreducible polynomial doesn't have to have degree 6. The elements that don't have degree 6 will be contained in some proper subextension of $\mathbb{F}_{p^6}$. Proper subextensions of $\mathbb{F}_{p^n}$ are the fields $\mathbb{F}_{p^d}$ for d a nontrivial divisor of n – or, equivalently, the fields $\mathbb{F}_{p^{n/d}}$ for d a proper divisor – so the proper subextensions of $\mathbb{F}_{p^6}$ are $\mathbb{F}_{p^3}$, $\mathbb{F}_{p^2}$, and $\mathbb{F}_p$. Since $\mathbb{F}_p$ is contained in both $\mathbb{F}_{p^3}$ and $\mathbb{F}_{p^2}$, if we want to get rid of the elements of $\mathbb{F}_{p^6}$ that are in a proper subextension, we can get rid of the elements that are in either $\mathbb{F}_{p^3}$ or $\mathbb{F}_{p^2}$. There are p^3 and p^2 of these, respectively, and, accounting for the p elements in the intersection $\mathbb{F}_{p^3} \cap \mathbb{F}_{p^2} = \mathbb{F}_p$, we find by inclusion/exclusion that

$$\#\{\alpha \in \mathbb{F}_{p^6} : \alpha \text{ not in a proper subextension}\} = p^6 - p^3 - p^2 + p.$$

Since any irreducible polynomial is associated to six different α on the left-hand side, we conclude that the number of irreducible polynomials is exactly

$$\frac{1}{6}(p^6 - p^3 - p^2 + p).$$

In general, these signs will be dictated by inclusion/exclusion on divisibility, and that's something the Möbius function is built to handle.

Proof of Lemma 1.8. If $f(x) \in \mathbb{F}_p[x]$ is monic and irreducible of degree n, we obtain the finite field $\mathbb{F}_{p^n}$ by adjoining one of the roots α of f, i.e. $\mathbb{F}_{p^n} = \mathbb{F}_p[\alpha]$.[7] In fact, since all finite fields of order p^n are isomorphic, $\mathbb{F}_{p^n}$ is the splitting field of f over $\mathbb{F}_p$, and each of its n roots is defined in $\mathbb{F}_{p^n}$. Consequently, we can associate to an irreducible polynomial its set of n roots in $\mathbb{F}_{p^n}$.

Conversely, given any element $\alpha \in \mathbb{F}_{p^n}$, we can find its minimal polynomial $m_\alpha(x)$ over $\mathbb{F}_p$. By the definition of a minimal polynomial (and the fact that $\mathbb{F}_p$ is a field), $m_\alpha(x)$ is guaranteed to be irreducible, but it is not guaranteed to have degree n; for example, if $\alpha \in \mathbb{F}_p \subseteq \mathbb{F}_{p^n}$, then $m_\alpha(x) = x - \alpha$. More generally, the proper subextensions of $\mathbb{F}_{p^n}$ are of the form $\mathbb{F}_{p^{n/d}}$ where $d > 1$ is a divisor of n, and if α is in any of these proper subextensions, then its minimal polynomial will not have degree n. For any d (including $d = 1$), there are $p^{n/d}$ elements of $\mathbb{F}_{p^{n/d}}$. By inclusion/exclusion, we then find that the number of elements in $\mathbb{F}_{p^n}$ *not* contained in any proper subextension of $\mathbb{F}_{p^n}$ is given by

$$p^n + \sum_{\substack{d|n \\ d>1}} \mu(d) p^{n/d} = \sum_{\substack{d|n \\ d\geq 1}} \mu(d) p^{n/d}.$$

(If this is the first time you've seen something like this, it is worth unpacking what it says, and why it's true, in the cases $n = 6$ (above example), $n = 30$, and $n = 12$.) Since the association is between irreducible polynomials of degree n and their n roots, we divide the abover number to obtain the number of irreducible polynomials:

$$\#\{f \in \mathbb{F}_p[x] : f \text{ monic, irreducible}, \deg f = n\} = \frac{1}{n} \sum_{\substack{d|n \\ d\geq 1}} \mu(d) p^{n/d}.$$

This is the claim of the lemma. □

[7] In number theory, we typically do this *formally*, i.e. by considering the quotient ring $\mathbb{F}_p[x]/(f(x))$, to avoid having to "pick" a root.

The next lemma considers how many polynomials in $\mathcal{P}_n(X)$ are congruent to a given polynomial $(\mathrm{mod}\, p)$. This will be used to justify our "probability" statements in the sketch proof of Theorem 1.6. In fact, we will use this for composite moduli m in addition to prime moduli, which luckily adds no difficulty to the proof.

Lemma 1.9. *Let $g \in \mathbb{Z}[x]$ be a monic polynomial of degree n, and let $m \geq 1$ be a positive integer. For any $X \geq m$, we have*

$$\#\{f \in \mathcal{P}_n(X) : f \equiv g \,(\mathrm{mod}\, m)\} = \frac{2^n X^n}{m^n} + O_n(X^{n-1}).$$

Proof. We adapt the argument we gave in determining the size of $\mathcal{P}_n(X)$. Suppose $g(x) = x^n + c_1 x^{n-1} + \cdots + c_n$. If we write $f \in \mathcal{P}_n(X)$ as $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, then for $f \equiv g \,(\mathrm{mod}\, m)$, we must have $a_1 \equiv c_1 \,(\mathrm{mod}\, m)$, $\ldots$, and $a_n \equiv c_n \,(\mathrm{mod}\, m)$. In particular, for each $i \leq n$, we wish to understand the number of integers $a_i \in [-X, X]$ that are congruent to $c_i \,(\mathrm{mod}\, m)$. If $a_i \equiv c_i \,(\mathrm{mod}\, m)$, then $\frac{a_i - c_i}{m}$ is an integer, so this number is the same as the number of integers in the modified interval $[\frac{-X-c_i}{m}, \frac{X-c_i}{m}]$. There will be $\frac{2X}{m} + O(1)$ integers in this interval regardless of the actual value of c_i, so there will be $\frac{2X}{m} + O(1)$ choices for each coefficient a_i. Consequently, the total number of polynomials congruent to $g \,(\mathrm{mod}\, m)$ is

$$\left(\frac{2X}{m} + O(1)\right)^n = \frac{2^n X^n}{m^n} + O_n(X^{n-1}),$$

as claimed. □

A useful way of interpreting Lemma 1.9 is as follows. Since there are $2^n X^n + O_n(X^{n-1})$ polynomials in $\mathcal{P}_n(X)$, the *proportion* of polynomials in $\mathcal{P}_n(X)$ that satisfy the congruence condition $f \equiv g \,(\mathrm{mod}\, m)$ is $\frac{1}{m^n} + O_n(\frac{1}{X})$. This is particularly useful in concert with things like Lemma 1.8. For example, these two lemmas together show that the proportion of polynomials in $\mathcal{P}_n(X)$ that are irreducible $(\mathrm{mod}\, p)$ is

$$\begin{aligned}\frac{\#\{g \,(\mathrm{mod}\, p) : g \text{ monic, irreducible}, \deg g = n\}}{p^n} + O_n\left(\frac{1}{X}\right) &= \frac{1}{n} + \frac{1}{n}\sum_{\substack{d|n \\ d>1}} \mu(d) p^{n/d-n} + O_n\left(\frac{1}{X}\right) \\ &\approx \frac{1}{n}.\end{aligned}$$

as we claimed. (As indicated in our sketch, we will often say things about "probabilities." This is a useful notion to have in mind, and will motivate many of our arguments, and will typically be made rigorous by considering instead proportions like we've done here.)

Before turning to the proof of Theorem 1.6, we add one technical lemma not indicated in our sketch. It's not a strict requirement, but it is convenient. It will be used to go from the "exact" probability that a polynomial is irreducible $(\mathrm{mod}\, p)$ to a more convenient, but approximate, proportion.

Lemma 1.10. *For every $n \geq 2$, there is a constant $c_n > 0$ such that*

$$\frac{\#\{g \,(\mathrm{mod}\, p) : g \text{ monic, irreducible}, \deg g = n\}}{p^n} \geq c_n$$

for every prime p.

Proof. The exact proportion

$$\frac{1}{n} + \frac{1}{n} \sum_{\substack{d|n \\ d>1}} \mu(d) p^{n/d-n}$$

tends to $1/n$ as $p \to \infty$, so for example is $\geq \frac{1}{2n}$ for sufficiently large primes (say, $p \geq N$). For the finitely many primes $p < N$, the proportion is positive – there's at least one irreducible polynomial, and the denominator is finite – so there is a minimum value of this proportion for these primes. Take c_n to be the smaller of this minimum and $\frac{1}{2n}$. □

We now have everything in place to prove Theorem 1.6.

Proof of Theorem 1.6. As indicated by our sketch, we will prove the equivalent statement that the proportion of polynomials in $\mathcal{P}_n(X)$ that are reducible tends to 0 as X tends to infinity. In other words, we wish to show

$$\limsup_{X \to \infty} \frac{\#\{f \in \mathcal{P}_n(X) : f \text{ reducible}\}}{2^n X^n} = 0.$$

(We could equivalently write this statement with a limit instead of a limsup, but it's not obvious that the limit exists. A limsup *always* exists, so it's easier to work with.) We'll do this by showing that the limsup can be made arbitrarily small.

If a polynomial in $\mathcal{P}_n(X)$ is reducible, then it must be reducible modulo every prime by Lemma 1.7. Let $p_1, \ldots, p_k$ be k distinct primes. Let R_1 be the number of reducible polynomials $(\mathrm{mod}\, p_1)$, R_2 the number $(\mathrm{mod}\, p_2)$, etc., and let $m = p_1 \ldots p_k$. By the Chinese remainder theorem, the number of polynomials $(\mathrm{mod}\, m)$ that are reducible $(\mathrm{mod}\, p_i)$ for each $i \leq k$, is exactly $R_1 \cdots R_k$. By Lemma 1.9, the proportion of polynomials in $\mathcal{P}_n(X)$ that are reducible $(\mathrm{mod}\, p_i)$ for each i is

$$\begin{aligned} \frac{R_1 \cdots R_k}{m^n} + O_n\left(\frac{1}{X}\right) &= \frac{R_1}{p_1^n} \cdots \frac{R_k}{p^k} + O_n\left(\frac{1}{X}\right) \\ &\leq (1 - c_n)^k + O_n\left(\frac{1}{X}\right), \end{aligned}$$

where c_n is the constant from Lemma 1.10. Consequently, we find for every k that

$$\limsup_{X \to \infty} \frac{\#\{f \in \mathcal{P}_n(X) : f \text{ reducible}\}}{2^n X^n} \leq (1 - c_n)^k.$$

Taking k arbitrarily large, the right-hand side tends to 0 since $c_n > 0$, and thus the limsup must actually equal 0. □

This proves that 100% of polynomials in $\mathcal{P}_n(X)$ are irreducible. To prove the stronger statement about Galois groups, we will use the same underlying strategy. However, we will need one additional definition plus one key lemma (treated as a black box for right now, unfortunately).

1.4. **Getting to Galois groups via factorization types.**

Definition. Suppose a polynomial f factors as $f = f_1^{e_1} \ldots f_r^{e_r}$, where the f_i are distinct irreducible polynomials and the e_i are positive integers. The *factorization type* of f is the list of pairs $(\deg f_1, e_1), \ldots, (\deg f_r, e_r)$. We often instead write this list in the form $(\deg f_1)^{e_1} \ldots (\deg f_r)^{e_r}$. We say a factorization type is *unramified* if it has no repeated factors, i.e. each $e_i = 1$.

Example. An irreducible polynomial of degree n has factorization type $(n, 1)$, which we typically write as simply n. Analogously, the polynomial $(x^3 - 2)(x^2 + 1)$ has factorization type 32, the polynomial $(x^3 - 2)(x^2 + 1)(x + 1)(x + 2)$ has type 3211, and the polynomial $(x^3 - 2)(x^2 + 1)(x + 1)^2(x + 2)$ has factorization type 321^21. All but the last are unramified.

We will sometimes refer to a factorization type as "admissible $(\mathrm{mod}\, p)$," which is a factorization type that can occur $(\mathrm{mod}\, p)$. For example, the factorization type 111 is *not* admissible for polynomials $(\mathrm{mod}\, 2)$, since it's not possible to write down a monic polynomial with three distinct linear factors $(\mathrm{mod}\, 2)$. (There are only two monic linear polynomials $(\mathrm{mod}\, 2)$.) Every factorization type is admissible modulo sufficiently large primes p.

The connection between Galois groups and factorization types is the following.

Lemma 1.11. *Let $f \in \mathcal{P}_n(X)$. Then $\mathrm{Gal}(f) \simeq S_n$ if and only if, for each unramified factorization type, there is a prime p for which $f \,(\mathrm{mod}\, p)$ has that factorization type.*

Proof. Discussed later in the semester. For right now, we'll note the key idea is the Frobenius element of the Galois group, and give a loose, unjustified explanation. If $f \,(\mathrm{mod}\, p)$ has a given unramified factorization type, then there is an element in $\mathrm{Gal}(f)$ – namely, Frobenius at p – whose cycle type (though of as a permutation in S_n) is the same as its factorization type. A subgroup of S_n containing all possible cycle types is necessarily equal to all of S_n. □

Next, we consider the probability a polynomial $(\mathrm{mod}\, p)$ has a given factorization type. We do so in analogy with Lemma 1.10, providing only a relatively imprecise (but sufficient!) result. It could be made more precise without too much trouble, however.

Lemma 1.12. *Let $n \geq 2$. There is a constant $c_n' > 0$ such that for any unramified factorization type of degree n and any prime p for which it's admissible, the proportion of monic polynomials $(\mathrm{mod}\, p)$ of degree n that have that factorization type, is at least c_n'.*

Proof. Suppose the unramified factorization type is $d_1 \dots d_r$, where $d_1 + \cdots + d_r = n$. For each $i \leq n$, let t_i be the number of d_j with $d_j = i$ (possibly allowing $t_i = 0$). In other words, each t_i keeps track of the number of irreducible factors of degree i. The condition that $d_1 + \dots d_r = n$ is equivalent to $t_1 + 2t_2 + \cdots + nt_n = n$.

Now, let p be a prime and let N_i be the number of irreducible polynomials $(\mathrm{mod}\, p)$ of degree i. For the factorization type to be admissible $(\mathrm{mod}\, p)$, we must have $N_i \geq t_i$ for each i.[8] It follows that the number of polynomials $(\mathrm{mod}\, p)$ with factorization type $d_1 \dots d_r$ is exactly

$$\binom{N_1}{t_1}\binom{N_2}{t_2}\cdots\binom{N_n}{t_n}.$$

This number is positive by the assumption that the factorization type is admissible, so, mimicking the proof of Lemma 1.10, it suffices to understand its behavior as $p \to \infty$. Paying attention to the order of magnitude in p, by Lemma 1.8, we have

$$N_i = \frac{p^i}{i} + O(p^{i-1}),$$

[8] In other words, there must be at least as many irreducible polynomials $(\mathrm{mod}\, p)$ as we're demanding our factorization type have.

and thus for each i for which $t_i \geq 1$,

$$\begin{aligned}\binom{N_i}{t_i} &= \frac{N_i!}{t_i!(N_i - t_i)!} \\ &= \frac{N_1(N_1-1)\dots(N_i - t_i + 1)}{t_i!} \\ &= \frac{N_i^{t_i}}{t_i!} + O(p^{i(t_i-1)}) \\ &= \frac{p^{it_i}}{i^{t_i}t_i!} + O(p^{it_i - 1}).\end{aligned}$$

It follows that

$$\binom{N_1}{t_1}\binom{N_2}{t_2}\cdots\binom{N_n}{t_n} = \frac{p^{t_1+2t_2+\dots+nt_n}}{t_1!\cdot 2^{t_2}t_2!\cdots n^{t_n}t_n!} + O(p^{n-1}) = \frac{p^n}{t_1!\cdot 2^{t_2}t_2!\cdots n^{t_n}t_n!} + O(p^{n-1}),$$

since $t_1 + 2t_2 + \dots nt_n = n$. This is a kind of horrible expression in the denominator, but the key thing to observe is that it's some constant depending only on the factorization type. Thus, as $p \to \infty$, the *proportion* of polynomials $(\mathrm{mod}\, p)$ that have factorization type $d_1 \dots d_r$ is

$$\lim_{p\to\infty} \frac{\binom{N_1}{t_1}\binom{N_2}{t_2}\cdots\binom{N_n}{t_n}}{p^n} = \frac{1}{t_1!\cdot 2^{t_2}t_2!\cdots n^{t_n}t_n!}.$$

This number is positive, and the lemma follows. □

We're now ready to prove the Galois group version of Hilbert irreducibility.

Proof of Theorem 1.2. We wish to show that

$$\lim_{X\to\infty} \frac{\#\mathcal{P}_n(X; S_n)}{2^n X^n} = 1.$$

As in the proof of Theorem 1.6, we will instead show that

$$\limsup_{X\to\infty} \frac{\#\mathcal{P}_n(X; \text{not } S_n)}{2^n X^n} = 0,$$

where $\mathcal{P}_n(X; \text{not } S_n)$ is the set of polynomials whose Galois group is not S_n, either because they're not irreducible or because their Galois group is smaller than S_n. By Lemma 1.11, if $f \in \mathcal{P}_n(X; \text{not } S_n)$, then f will "miss" some unramified factorization type $(\mathrm{mod}\, p)$ for *every* prime p. By Lemma 1.12 and Lemma 1.9, the proportion of polynomials that miss a particular unramified factorization type at k distinct primes is at most $(1 - c_n')^k$. Taking $k \to \infty$, this becomes arbitrarily small, and we conclude that asymptotically 0% of polynomials in $\mathcal{P}_n(X)$ miss that particular factorization type modulo every prime p, and thus also that 0% of polynomials miss *any* unramified factorization type. Thus, 100% have each factorization type modulo some prime, and thus 100% have Galois group S_n by Lemma 1.11. □

1.5. **Important points and discussion.** Though there are other proofs of Hilbert irreducibility, the idea of using primes to probe arithmetic objects is ubiquitous and important. We will see similar ideas throughout this course. Instead of constantly referring to polynomials, or number fields, or whatever, as satisfying congruence conditions $(\mathrm{mod}\, p)$ we will typically talk about objects satisfying "local conditions." For example, the condition that a polynomial $f(x) \in \mathbb{Z}[x]$ is irreducible $(\mathrm{mod}\, p)$ is a local condition. Similarly, the condition that a polynomial $f(x)$ have a given factorization type is also a local condition. It's useful

to have this terminology since some of the local conditions we look at in this course will end up being somewhat far from congruence conditions (as you have seen them in discrete math or elementary number theory). This will be important when we start talking about number fields. Number fields are defined through irreducible polynomials, but for example it doesn't really make sense to say that the fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-3})$ are congruent $(\mathrm{mod}\, 5)$ even though their defining polynomials $x^2 - 2$ and $x^2 + 3$ are congruent $(\mathrm{mod}\, 5)$. They do, however, satisfy the same local condition at 5.