On a Theorem of Jordan
J. P. Serre, 2003

<u>Main Point:</u> Results about permutation representations of groups translate into (usually more interesting) results about topology & arithmetic.

Example:

<u>Thm I</u>: Suppose $f: Y \to X$ is a deg d covering map of topological spaces and that Y is path connected. If $d \geq 2$, then there exists a continuous map $g: S^1 \to X$ which does not lift to Y.

<u>Thm A</u>: Suppose $f(x) \in \mathbb{Z}[x]$ is a monic, degree $d \geq 2$, irreducible poly. Then $\exists$ prime p s.t. $f(x)$ does not have any roots mod p. Furthermore, the natural density of the set of primes w/ this property exists and is $\geq 1/d$.

These results may not seem related at first blush, but are really two manifestations of the same fact about groups acting on finite sets.
↳ The connection is made through Galois / covering space theory!
I'll come back to that. First let's talk about permutation representations.

<u>Thm</u> (Jordan 1872) If a group G acts transitively on a set X with at least 2 elements, then $\exists g \in G$ which acts on X w/o fixed points.

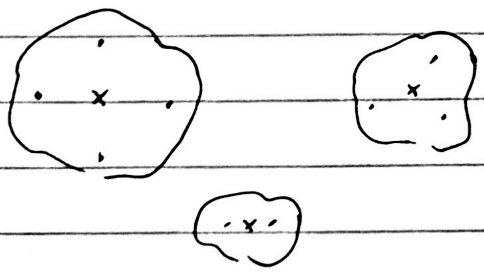
<u>Thm</u> (Cameron, Cohen 1992) If X has $d \geq 2$ elements, then @ least $1/d$ of the elements in G act w/o fixed points.

Jordan's theorem is an easy corollary of Burnside's Lemma, as we will see. The Cameron, Cohen result has a clever proof and is sharp (Consider the affine group $\mathrm{Aff}_1(\mathbb{F}_q) = \{ax+b\}$ acting on $\mathbb{A}^1(\mathbb{F}_q)$, then the $q-1$ non trivial translations have no fixed pts and these comprise $\frac{q-1}{(q-1)q} = \frac{1}{q}$ of the group.)

<u>Burnside's Lemma:</u> If G is a finite group acting on a finite set X, then the number of orbits of G on X is equal to the average number of points fixed by an element of G.

<u>Pf:</u> Let χ be the perm. character of G acting on X. So $\chi(g) = \#$ fixed pts of g in X. Let 1 be the trivial character. Then $\langle \chi, 1 \rangle = \frac{1}{|G|} \sum_{g \in G} \chi(g)$ is the multiplicity of the trivial rep in χ, and also plainly the average number of fixed pts.

On the other hand, we can see all of the trivial reps in $\mathbb{Q}X$:



The center of mass of each orbit is a nonzero vector fixed by G. Subtracting off the center of mass from an orbit centers it, and the resulting rep has no trivial components; so the multiplicity of the trivial rep is the number of orbits. ■

<u>Pf of Jordan:</u> If G acts transitively, then there is one orbit. Hence by Burnside the average number of points fixed is 1. But the identity fixes $d \geq 2$, so the only way to balance out the average is for some $g \in G$ to fix no elements. ■

3

That was easy. Jordan's theorem is all we need to prove the topology result Thm T.

Recall:

$\left\{\begin{array}{l}\text{Degree } d \text{ covering spaces} \\ f: Y \to X\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Actions of } \pi_1(X, x_0) \text{ on} \\ \text{a set w/ } d \text{ elements}\end{array}\right\}$

Abstractly: $\left\{\begin{array}{l}= \text{Bundle of } d \text{ element sets on} \\ X\end{array}\right\}$

$\left(\text{maps } g: X \to BS_d\right) \longleftrightarrow \left(\begin{array}{l}\text{group hom} \\ \pi_1(X, x_0) \to S_d\end{array}\right)$

Concretely: $f: Y \to X$, pick $x_0 \in X$, then $f^{-1}(x_0)$ is a set w/ d elements. Loops in X based at x_0 lift under f to paths starting and ending in $f^{-1}(x_0)$, hence induce permutations. This action only depends on the homotopy class of the loop hence induces a perm rep of $\pi_1(X, x_0)$. And given any such perm rep of $\pi_1(X, x_0)$, a cover can be reconstructed.

Pf of Thm T: The assumption that Y is path connected is equivalent to the action of $\pi_1(X, x_0)$ being transitive on $f^{-1}(x_0)$, and degree $d \geq 2$ means $|f^{-1}(x_0)| \geq 2$. ~~So Jordan's theorem implies that $\exists\, g \in \pi_1(X, x_0)$ which acts on $f^{-1}(x_0)$ w/o fixed points. Let $\tilde{g}: S^1 \to X$ be a map representing the loop class g. No fixed points of g means all lifts of $\tilde{g}$ are~~ If $g: S^1 \to X$ lifts to $\tilde{g}: S^1 \to Y$ (so $g = f \circ \tilde{g}$) and $y_0 \in \tilde{g}(S^1)$ ~~maps~~ is in $f^{-1}(x_0)$, then that means that the element of $\pi_1(X, x_0)$ rep'd by g fixes y_0. Jordan's thm says $\exists\, h \in \pi_1(X, x_0)$ w/o fixed pts in $f^{-1}(x_0)$, hence the map $S^1 \to X$ rep'ing h does not lift. ∎

In order to prove the arithmetic result Thm A we will need the Cameron, Cohen result and some review of algebraic number theory.

Pf of CC:

Let χ be the perm character of G acting on X. Since G acts transitively, $\chi = 1 + \psi$ for some character ψ s.t. $\langle \psi, 1 \rangle = 0$. (Burnside)

Note that $\chi^2 = 1 + 2\psi + \psi^2$ is the perm character for G acting on $X \times X$. Since G has @ least 2 orbits on $X \times X$ (diagonal and off)

we have $\langle \chi^2, 1 \rangle = 1 + \langle \psi^2, 1 \rangle \geq 2$. So $\langle \psi^2, 1 \rangle \geq 1$

Let $G_0 \subseteq G$ be the subset of elems w/ no fixed pts.

Then $(\chi(g)-1)(\chi(g)-d) \leq 0$ for $g \notin G_0$; and $= d$ for $g \in G_0$.

Since $(\chi-1)(\chi-d) = \psi \cdot (\psi - (d-1)) = \psi^2 - (d-1)\psi$ we have

i) $\langle (\chi-1)(\chi-d), 1 \rangle = \langle \psi^2, 1 \rangle - (d-1)\langle \psi, 1 \rangle \geq 1$

ii) $$\langle (\chi-1)(\chi-d), 1 \rangle = \frac{1}{|G|} \sum_{g \in G} (\chi(g)-1)(\chi(g)-d)$$

$$\leq \frac{1}{|G|} \sum_{g \in G_0} (\chi(g)-1)(\chi(g)-d) = d\frac{|G_0|}{|G|}.$$

Thus $|G_0|/|G| \geq 1/d$. ∎

Algebraic Number theory from a topological point of view:

Let $f(x) \in \mathbb{Z}[x]$ be a monic, irreducible, degree d polynomial and let $\mathcal{O} := \mathbb{Z}[x]/(f(x))$.

One of first goals in alg. num. theory is to understand how primes $p \in \mathbb{Z}$ decompose in $\mathcal{O}$. I'm going to use algebro-geometric duality ~~to interpret this geometrically~~, and an analogy w/ branched covers of 3-manifolds to interpret this geometrically, and explain what it has to do w/ roots mod p.

~~If p is not a critical value (ie, doesn't ramify in $\mathcal{O}$)~~

How $f(x)$ factors mod p is determined by how the Frobenius automorphism $\mathrm{Frob}_p : \overline{\mathbb{F}}_p \circlearrowleft$ acts on the roots of $f(x)$ mod p. ~~There are only finitely many primes p s.t. f(x) has a multiple root mod p (namely the primes dividing Δ(f).) Avoiding these,~~ Frob_p induces a permutation of the roots, the number of cycles in this permutation is the number of irred factors and the length of a cycle is the degree of the corresponding irred factor.

If $p \nmid \Delta(f)$, then Frob_p lifts to an element of $\mathrm{Gal}(\mathbb{Q}^f/\mathbb{Q})$ (the Galois gp of the Galois closure) well-defined up to conj; this lift acts on the roots of $f(x)$ the same as Frob_p acts on the roots mod p.

<u>Thm</u> (Chebotarev Density) If $G = \mathrm{Gal}(f)$ and $C \subseteq G$ is a subset stable under conjugation, then $\{p \in \mathbb{Z} : \mathrm{Frob}_p \in C\}$ has a natural density equal to $|C|/|G|$.

<u>Pf of Thm A</u>: Let $C_0 \subseteq G = \mathrm{Gal}(f)$ be the set of elements which don't fix any roots of $f(x)$. Since f is irred, G acts transitively on the roots. Hence $|C_0|/|G| \geq 1/d$.
Chebotarev implies that $\{p \in \mathbb{Z} : \mathrm{Frob}_p \in C_0\}$ has density $|C_0|/|G| \geq \frac{1}{d}$.
~~Hence~~ Note that $\mathrm{Frob}_p \in C_0$ iff $f(x)$ has no roots mod p. ∎
In particular, such primes exist and in fact ∞ly many.

Note: A random polynomial $f(x)$ of deg d is likely to have Galois group S_d. The density of elems in S_d which don't fix any points is $\approx 1/e \approx 37\%$. So this is what you expect to see for randomly chosen polys. Note the independence of d!