“How to use finite fields for problems concerning infinite fields” by Jean-Pierre Serre

Summarized by Nate Harman

May 7, 2020

First Theorem

Theorem

If G is a finite p-group acting algebraically on $\mathbb{C}^n$, then there exists a fixed point for the action.

First Theorem

Theorem

If G is a finite p-group acting algebraically on $\mathbb{C}^n$, then there exists a fixed point for the action.

Proof.

Without loss of generality assume $\mathbb{C} = \mathbb{F}_q$ with q relatively prime to p.

First Theorem

Theorem

If G is a finite p-group acting algebraically on $\mathbb{C}^n$, then there exists a fixed point for the action.

Proof.

Without loss of generality assume $\mathbb{C} = \mathbb{F}_q$ with q relatively prime to p. Orbits of G on $\mathbb{F}_q^n$ must have sizes which are powers of p as G is a p-group. Since p does not divide $|\mathbb{F}_q^n|$ there must exist an orbit of size 1 (i.e. a fixed point).

□

“Without loss of generality”

G acting algebraically explicitly means for each $g \in G$ there are polynomials $P_{g,i} \in \mathbb{C}[x_1, x_2, \ldots x_n]$ for $i = 1, 2, \ldots n$ such that

$$g \cdot (x_1, x_2, \ldots x_n) = (P_{g,1}(x_1, x_2, \ldots, x_n), \ldots, P_{g,n}(x_1, x_2, \ldots, x_n)).$$

“Without loss of generality”

G acting algebraically explicitly means for each $g \in G$ there are polynomials $P_{g,i} \in \mathbb{C}[x_1, x_2, \ldots x_n]$ for $i = 1, 2, \ldots n$ such that

$$g \cdot (x_1, x_2, \ldots x_n) = (P_{g,1}(x_1, x_2, \ldots, x_n), \ldots, P_{g,n}(x_1, x_2, \ldots, x_n)).$$

G having no fixed points implies that the system of $n|G|$ equations

$$x_i - P_{g,i}(x_1, x_2, \ldots x_n) = 0$$

has no solutions in $\mathbb{C}^n$.

"Without loss of generality"

G acting algebraically explicitly means for each $g \in G$ there are polynomials $P_{g,i} \in \mathbb{C}[x_1, x_2, \ldots x_n]$ for $i = 1, 2, \ldots n$ such that

$$g \cdot (x_1, x_2, \ldots x_n) = (P_{g,1}(x_1, x_2, \ldots, x_n), \ldots, P_{g,n}(x_1, x_2, \ldots, x_n)).$$

G having no fixed points implies that the system of $n|G|$ equations

$$x_i - P_{g,i}(x_1, x_2, \ldots x_n) = 0$$

has no solutions in $\mathbb{C}^n$. Therefore by the Nullstellensatz there exist polynomials $Q_{g,i} \in \mathbb{C}[x_1, x_2, \ldots x_n]$ such that

$$\sum_{g,i} (x_i - P_{g,i}(x_1, x_2, \ldots x_n)) Q_{g,i}(x_1, x_2, \ldots x_n)) = 1$$

"Without loss of generality" (cont.)

Let $\Lambda \subset \mathbb{C}$ be the subring generated by $\frac{1}{p}$, the coefficients of the $P_{g,i}$s, and the coefficients of the $Q_{g,i}s$. In particular note that Λ is finitely generated as an algebra over $\mathbb{Z}$.

“Without loss of generality” (cont.)

Let $\Lambda \subset \mathbb{C}$ be the subring generated by $\frac{1}{p}$, the coefficients of the $P_{g,i}$s, and the coefficients of the $Q_{g,i}s$. In particular note that Λ is finitely generated as an algebra over $\mathbb{Z}$.

If $\mathfrak{m} \subset \Lambda$ is a maximal ideal then $\Lambda/\mathfrak{m}$ is a finite field $\mathbb{F}_q$ of characteristic prime to p.

"Without loss of generality" (cont.)

Let $\Lambda \subset \mathbb{C}$ be the subring generated by $\frac{1}{p}$, the coefficients of the $P_{g,i}$s, and the coefficients of the $Q_{g,i}s$. In particular note that Λ is finitely generated as an algebra over $\mathbb{Z}$.

If $\mathfrak{m} \subset \Lambda$ is a maximal ideal then $\Lambda/\mathfrak{m}$ is a finite field $\mathbb{F}_q$ of characteristic prime to p. Upon reduction modulo $\mathfrak{m}$, the $P_{g,i}s$ define an action G on $\mathbb{F}_q$, and the equation

$$\sum_{g,i}(x_i - P_{g,i}(x_1, x_2, \dots x_n))Q_{g,i}(x_1, x_2, \dots x_n)) = 1$$

ensures that the action does not have any fixed points. This is impossible by the previous argument.

Almost free actions

We say that an action of a finite group G on a complex algebraic variety X is *almost free* if X has finitely many points $p_1, p_2, \ldots, p_k$ which are fixed by G, and the action on $X - \{p_1, p_2, \ldots p_k\}$ is free.

Almost free actions

We say that an action of a finite group G on a complex algebraic variety X is *almost free* if X has finitely many points $p_1, p_2, \dots, p_k$ which are fixed by G, and the action on $X - \{p_1, p_2, \dots p_k\}$ is free.

Theorem

Suppose we have two almost free actions of G on X with k and k' fixed points respectively. Then $k \equiv k' \mod |G|$.

Almost free actions

We say that an action of a finite group G on a complex algebraic variety X is *almost free* if X has finitely many points $p_1, p_2, \ldots, p_k$ which are fixed by G, and the action on $X - \{p_1, p_2, \ldots p_k\}$ is free.

Theorem

Suppose we have two almost free actions of G on X with k and k' fixed points respectively. Then $k \equiv k' \mod |G|$.

Sketch of proof.

If the actions are defined over a finite field $\mathbb{F}_q$ this is clear: By assumption every orbit either has size $|G|$ or 1 therefore the number of fixed points has to be the same modulo $|G|$.

Almost free actions

We say that an action of a finite group G on a complex algebraic variety X is *almost free* if X has finitely many points $p_1, p_2, \ldots, p_k$ which are fixed by G, and the action on $X - \{p_1, p_2, \ldots p_k\}$ is free.

Theorem

Suppose we have two almost free actions of G on X with k and k' fixed points respectively. Then $k \equiv k' \mod |G|$.

Sketch of proof.

If the actions are defined over a finite field $\mathbb{F}_q$ this is clear: By assumption every orbit either has size $|G|$ or 1 therefore the number of fixed points has to be the same modulo $|G|$.

Similarly to before, for any two such actions defined over $\mathbb{C}$ we can find a finitely generated ring Λ over which they are both defined, as well as a maximal ideal $\mathfrak{m}$ such that the actions remain almost free for $\Lambda/\mathfrak{m}$. $\square$

Ax-Grothendieck

Theorem (Ax, Grothendieck)

If $f : \mathbb{C}^n \to \mathbb{C}^n$ is an injective algebraic map, then f is surjective.

Ax-Grothendieck

Theorem (Ax, Grothendieck)

If $f : \mathbb{C}^n \to \mathbb{C}^n$ is an injective algebraic map, then f is surjective.

Proof.

For $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ the statement is obvious.
Similarly to before we can show that any such f over the complex numbers is defined over a finitely generated ring, and we can find a maximal ideal such that the reduction remains injective. $\square$

Ax-Grothendieck

Theorem (Ax, Grothendieck)

If $f : \mathbb{C}^n \to \mathbb{C}^n$ is an injective algebraic map, then f is surjective.

Proof.

For $f : \mathbb{F}_q^n \to \mathbb{F}_q^n$ the statement is obvious.
Similarly to before we can show that any such f over the complex numbers is defined over a finitely generated ring, and we can find a maximal ideal such that the reduction remains injective. □

Something to think about: What goes wrong if we try to run this argument with injectivity and surjectivity flipped?

Sylow Subgroups in $GL_n(\mathbb{Q})$

Theorem (Minkowski)

Suppose $G \subset GL_n(\mathbb{Q})$ is a finite group of order p^a. Then

$$a \leq M(n,p) := \left\lfloor \frac{n}{p-1} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \dots$$

Sylow Subgroups in $GL_n(\mathbb{Q})$

Theorem (Minkowski)

Suppose $G \subset GL_n(\mathbb{Q})$ is a finite group of order p^a. Then

$$a \leq M(n,p) := \left\lfloor \frac{n}{p-1} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \dots$$

Proof for $p \neq 2$.

Since G is finite we have that $G \subset GL_n(\mathbb{Z}[1/N])$ for some N. Therefore if q does not divide $2N$ we can realize G as a subgroup of $GL_n(\mathbb{F}_q)$.

Sylow Subgroups in $GL_n(\mathbb{Q})$

Theorem (Minkowski)

Suppose $G \subset GL_n(\mathbb{Q})$ is a finite group of order p^a. Then

$$a \leq M(n,p) := \left\lfloor \frac{n}{p-1} \right\rfloor + \left\lfloor \frac{n}{p(p-1)} \right\rfloor + \left\lfloor \frac{n}{p^2(p-1)} \right\rfloor + \dots$$

Proof for $p \neq 2$.

Since G is finite we have that $G \subset GL_n(\mathbb{Z}[1/N])$ for some N. Therefore if q does not divide $2N$ we can realize G as a subgroup of $GL_n(\mathbb{F}_q)$.

So we can bound $|G|$ by the cardinality of a p-Sylow subgroup of $GL_n(\mathbb{F}_q)$ for any q not dividing $2N$. An easy calculation gives that if we take q such that it generates $(\mathbb{Z}/p^2\mathbb{Z})^*$ a p-Sylow subgroup has size $p^{M(n,p)}$.

□

Sylow Subgroups in $GL_n(\mathbb{Q})$ cont.

Theorem (Minkowski)

a) For all primes p there exists a subgroup $P \subset GL_n(\mathbb{Q})$ such that $|P| = p^{M(n,p)}$.

b) if P' is any other subgroup of $GL_n(\mathbb{Q})$ of order p^a then P' is conjugate to a subgroup of P.

Sylow Subgroups in $GL_n(\mathbb{Q})$ cont.

Theorem (Minkowski)

a) For all primes p there exists a subgroup $P \subset GL_n(\mathbb{Q})$ such that $|P| = p^{M(n,p)}$.

b) if P' is any other subgroup of $GL_n(\mathbb{Q})$ of order p^a then P' is conjugate to a subgroup of P.

Proof sketch of (b) for $p \neq 2$.

Choose q as in the proof of the previous theorem. The image of P is a Sylow subgroup of $GL_n(\mathbb{F}_q)$, and therefore we can conjugate the image of P' into it. In other words we have an embedding $i : P' \hookrightarrow P$ which is the restriction of an inner automorphism of $GL_n(\mathbb{F}_q)$.

Sylow Subgroups in $GL_n(\mathbb{Q})$ cont.

Theorem (Minkowski)

a) For all primes p there exists a subgroup $P \subset GL_n(\mathbb{Q})$ such that $|P| = p^{M(n,p)}$.

b) if P' is any other subgroup of $GL_n(\mathbb{Q})$ of order p^a then P' is conjugate to a subgroup of P.

Proof sketch of (b) for $p \neq 2$.

Choose q as in the proof of the previous theorem. The image of P is a Sylow subgroup of $GL_n(\mathbb{F}_q)$, and therefore we can conjugate the image of P' into it. In other words we have an embedding $i : P' \hookrightarrow P$ which is the restriction of an inner automorphism of $GL_n(\mathbb{F}_q)$.

We have two representations $P' \hookrightarrow GL_n(\mathbb{Q})$ and $P' \to_i P \hookrightarrow GL_n(\mathbb{Q})$ which are isomorphic upon reduction modulo q. A result from modular representation theory says that since q does not divide $|P'|$ this implies they are isomorphic rationally.

$\square$

Thanks