This next one is basic, but the portions highlighted in yellow indicate decent understanding of algebraic number theory on my part, and the earlier portions introduced me to the relation between the picard group and Jacobians which definitely show up again in a different incarnation in the theory of modular forms.

(Note: I was happy to find that there is utility in thinking about things in terms of the Picard group when dealing with finite fields for instance of any other field where the theory of integration (or more aptly put the use of appropriate differential forms I suppose) falls apart. I am still very, very new to this field but from what I understand, that is the general idea that motivates utility of thinking in terms of divisors).

Summary of "Realization of Groups with Pairing as Jacobians of Finite Graphs" by Gaudet, Jensen, Ranganathan, Wawrykow, Weisman

Caitlin Beecham

September 16, 2020

https://arxiv.org/pdf/1410.5144.pdf

The goal of this paper is to prove that any odd order finite abelian group H occurs as the Jacobian of some graph G. Namely, for all finite abelian groups H of odd order, we wish to construct a graph G such that

$$Jac(G) = H.$$

One first notes that any finite abelian group H is isomorphic to

$$H \cong \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z},$$

for some finite list of primes $\{p_i\}$. Thus, we would like to do the following. For any odd prime p_i and positive integer r_i, we would like to construct a graph G_i with Jacobian group

$$Jac(G_i) = \mathbb{Z}/p_i^{r_i}\mathbb{Z}.$$

Then, if $H \cong \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}$, we let the graph $G = \bigvee_i G_i$ be the wedge sum of these graphs, we get

$$\begin{aligned} Jac(G) &= Jac(\bigvee_i G_i) \\ &= \bigoplus_i Jac(G_i) \\ &= \bigoplus_i \mathbb{Z}/p_i^{r_i}\mathbb{Z} = H \end{aligned}$$

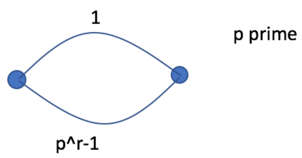
which gives the desired Jacobian group.

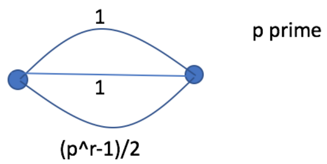
However, there is a slight problem. Namely, many lemmas cited or proven by the authors only work for "sufficiently large" p. Still, one can say that there exists a finite set of primes $\mathcal{P} \subseteq \mathbb{Z}$ such that for any abelian group H whose order is not divisible by any prime $p \in \mathcal{P}$, we can construct a graph G with

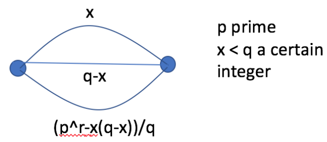
$$Jac(G) \cong H.$$

Furthermore, if the Generalized Riemann Hypothesis holds, then we can say that this list of forbidden primes is just $\mathcal{P} = \{2\}$. Namely, this improvement comes from the fact that assuming the Riemann Hypothesis improves bounds on sufficiently large primes p in relevant claims to bounds such as for primes $p > 10^9$. Then, these bounds are small enough that the cases unhandled by these claims can be handled brute force by computer.

In order to construct graphs G such that $Jac(G) = \mathbb{Z}/p^r\mathbb{Z}$ (we drop the indices i here for clarity, though we do repeat this process for all $i \in [n]$), we define a certain type of graph called a Banana Graph on a tuple $s = (s_1, \ldots, s_m)$ where if the s_i satisfy certain properties, we indeed get that $Jac(G) = Jac(B_s) = \mathbb{Z}/p^r\mathbb{Z}$.





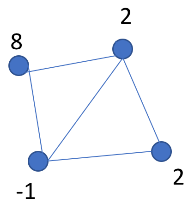


Many tedious number theoretic arguments follow for the purpose of constructing the tuple $s = (s_1, s_2, \ldots, s_m)$ with the desired properties for the given p, r (really p_i, r_i). One later concludes that the desired banana graphs (depending on certain conditions on p, r) are one of the following three graphs.

Definition: A pairing of a group K is a bilinear map $\langle \cdot, \cdot \rangle : K \times K \to \mathbb{Q}$ such that

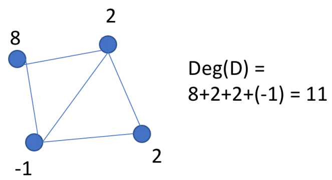
- for any fixed $k \in K$, the unary map $\langle k, \cdot \rangle$ is a group homomorphism
- and also $\langle \cdot, k \rangle$ is a group homomorphism.

Definition: A "divisor" or "vertex numbering" is a map $D : V(G) \to \mathbb{Z}$.



Definition: The "degree" of a vertex numbering D is

$$\sum_{v \in V} D(v).$$



Definition: A principal vertex numbering is one which lies in the image of the output of the following algorithm. Call the below algorithm T which takes in input f a vertex numbering and outputs D_f a vertex numbering. Namely, the algorithm T operates as follows.

1. Take input $f : V(G) \to \mathbb{Z}$.
2. Define $B_f : \overrightarrow{E}(G) \to \mathbb{Z}$ by $B_f(xy) := f(y) - f(x)$ where $\overrightarrow{E}(G) = \{\overrightarrow{xy} : xy \in E(G) \text{ or } yx \in E(G)\}$. (Note that $B_f(yx) = -B_f(xy)$).
3. Define a new numbering $D_f : V(G) \to \mathbb{Z}$ by $D_f(v) = \sum_{\overrightarrow{vw} \in \delta^+(v)} B_f(\overrightarrow{vw})$.
4. Output D_f.

Then, the set of principal vertex numberings is exactly the set $T(S)$ where S is the set of all vertex numberings (functions from $V(G) \to \mathbb{Z}$).

Note that one can add and subtract numberings simply using component-wise addition and subtraction.

$$D_1 + D_2 := \bigoplus_{v \in V} D_1(v) + D_2(v),$$
$$D_1 - D_2 = \bigoplus_{v \in V} D_1(v) - D_2(v).$$

The above gives rise to a natural equivalence relation on the set of numberings, denoted $\sim$, defined by $D_1 \sim D_2$ if and only if

$$D_1 - D_2 \text{ is a principal numbering.}$$

Now, the Jacobian group $Jac(G)$ is

$$Jac(G) \cong D_0 / \sim,$$

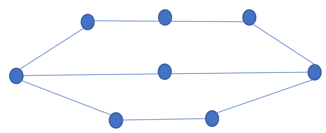
where $D_0 := \{(D : V(G) \to \mathbb{Z}) : deg(D) = 0\}$ is the set of degree 0 numberings.

Definition: A Banana Graph B_s on the tuple $s = (s_1, \ldots, s_m)$ is the graph constructed as follows.

- Take two vertices.
- Add m edges between them.
- Subdivide the ith edge $s_i - 1$ times.

Example: $B_{(4,2,3)}$.

B(4,3,2)



Now, it is a known fact that the size of the Jacobian Group of a connected graph G is equal to the number of spanning trees of G. Then, a natural question to ask is how to count the number of spanning trees in a Banana Graph. Note that one obtains a spanning tree by removing an edge from every path except one between the endpoints v, w of the banana. Thus, the number of spanning trees of B_s is

$$|Jac(G)| = \Bigg(\underbrace{\sum_{i=1}^{m}}_{\text{choose path } p_i \text{ to keep}} \Bigg(\underbrace{\prod_{j \in [m] \setminus \{i\}}}_{\text{choose edge from } p_j \text{ to remove}} s_j \Bigg)\Bigg)$$

Proposition 14: Fix a prime p, positive integer r. If we have positive integers $(s_1, \ldots, s_m)$ each coprime to p such that

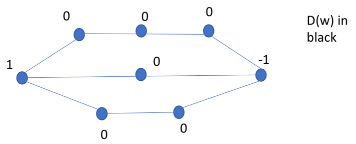
$$\underbrace{\sum_{j \in [m]} \prod_{i \in [m] \setminus \{j\}} s_i}_{\# \text{ of spanning trees } = |Jac(G)|} = p^r,$$

then

$$Jac(B_s) \cong (\mathbb{Z}/p^r\mathbb{Z}, \langle \cdot, \cdot \rangle).$$

Note: The meat of this result is that $Jac(G)$ is **cyclic**. (We already knew the rest (e.g. abelian, finite of order p^r)).

Proof: We will show it's cyclic by finding a generator. Namely, we consider the equivalence class $[D]$ of the numbering $D = v - w = 1v + (-1)w + 0 + 0 + \cdots + 0$. We will show that $[D]$ generates $Jac(G) = D_0/\sim$.



We aim to show that $[D]$ has order $o([D])$ equal to the size of the group $|Jac(G)| = p^r$.
By Lagrange's Theorem we know that

$$o([D]) = p^t$$

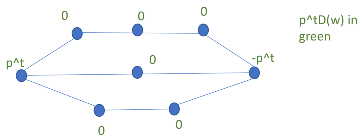
where $t \in \{0, 1, \ldots, r\}$.

We will eventually show $t = r$. For contradiction, assume that $t < r$.

Now, $o([D]) = p^t$ implies that $p^t[D] = e_{Jac(G)} = \{\text{class of principal numberings}\}$, which means $p^t D$ is a principal labeling. So, it arises from some labeling $f : V(G) \to \mathbb{Z}$ and corresponding edge map $B : \overrightarrow{E}(G) \to \mathbb{Z}$ as before.

Before any analysis, let's compute $p^t D(v)$. We just multiply each vertex number by p^t to get

$$\begin{aligned} p^t D &= p^t(1v + -1w + 0) \\ &= p^t v + -p^t w + 0. \end{aligned}$$



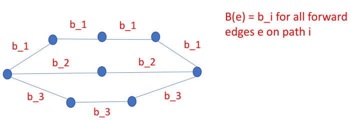
Now, $p^t D$ principal means there exists $f : V(G) \to \mathbb{Z}$ such that using corresponding $B : \overrightarrow{E}(G) \to \mathbb{Z}$ defined by $B(xy) = f(x) - f(y)$ and then defining D' by

$$D'(u) = \sum_{\text{edges } \overrightarrow{uy} \in \delta^+(u)} B(\overrightarrow{uy})$$

one actually obtains $D' = p^t D$.

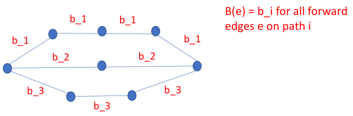
Lemma: For any two edges $e, r \in p_i$ (both directed from v to w), one has $B(e) = B(r)$.

So, on any path p_i from v to w, B is the constant function equal to b_i on all forward edges.



Notation: The vertices in p_i are called $v, p_i^1, p_i^2, p_i^3 \ldots, p_i^{s_i-1}, w$. Call $b_i := B(p_i^1)$.

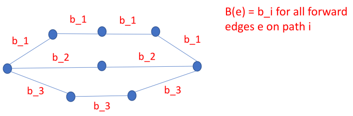
Proof of Lemma (by induction): (Base case trivial–Here's the inductive step). We know $B(p_i^{k-1}p_i^k) = b_i$ and we wish to show $B(p_i^k p_i^{k+1}) = b_i$.
Well, recall by definition of B, we have $B(xy) = f(x) - f(y)$. So, $b_i = B(p_i^{k-1}p_i^k) = f(p_i^{k-1}) - f(p_i^k)$ and $B(p_i^k p_i^{k+1}) = f(p_i^k) - f(p_i^{k+1})$.



Now, by definition of principality,

$$\begin{aligned}
p^t D(p_i^k) &= \sum_{\text{edges } \overrightarrow{e} \in \delta^+(u)} B(e) \\
&= B(p_i^k p_i^{k-1}) + B(p_i^k p_i^{k+1}) \\
&= -B(p_i^{k-1} p_i^k) + B(p_i^k p_i^{k+1}) \\
&= -b_i + B(p_i^k p_i^{k+1}) \\
0 &= -b_i + B(p_i^k p_i^{k+1}),
\end{aligned}$$

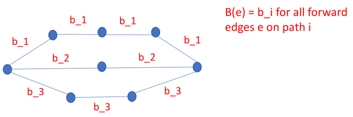
which gives $B(p_i^k p_i^{k+1}) = b_i$, proving the lemma. $\square$



Now, we continue to prove the theorem that $[D]$ is a generator of $Jac(G)$.
Observe: For all $i \in [m]$, one has $f(v) - f(w) = b_i s_i$. Why?
We have a telescoping sum

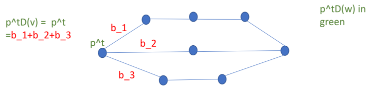
$$\begin{aligned}
f(v) - f(w) &= (f(v) - f(p_i^1)) + (f(p_i^1) - f(p_i^2)) \\
&\quad + (f(p_i^2) - f(p_i^3)) + \cdots + (f(p_i^{s_i-1}) - f(v)) \\
&= b_i + b_i + b_i + \cdots + b_i \\
&= b_i s_i.
\end{aligned}$$

So, we can isolate $b_i = \frac{f(v)-f(w)}{s_i}$.



$p^t D$ principal means that $p^t D$ came from the corresponding f, B so we have

$$\begin{aligned}
p^t D(v) &= \sum_{e \in \delta^+(v)} B(e) \\
&= \sum_{i \in [m]} B(v p_i^1) \\
&= \sum_{i \in [m]} b_i \\
p^t &= \sum_{i \in [m]} b_i.
\end{aligned}$$



Continuing on we have

$$\begin{aligned}
p^t &= \sum_{i\in[m]} b_i \\
&= \sum_{i\in[m]} \frac{f(v)-f(w)}{s_i} \\
&= (f(v)-f(w)) \sum_{i\in[m]} \frac{1}{s_i} \\
&= (f(v)-f(w)) \sum_{i\in[m]} \frac{1}{s_i} \frac{\prod_{j\in[m]} s_j}{\prod_{j\in[m]} s_j} \\
&= \frac{(f(v)-f(w))}{\prod_{j\in[m]} s_j} \sum_{i\in[m]} \frac{\prod_{j\in[m]} s_j}{s_i}.
\end{aligned}$$

Continuing on we have

$$\begin{aligned}
p^t &= \left(\frac{(f(v)-f(w))}{\prod_{j\in[m]} s_j}\right)\left(\sum_{i\in[m]} \frac{\prod_{j\in[m]} s_j}{s_i}\right) \\
&= \left(\frac{(f(v)-f(w))}{\prod_{j\in[m]} s_j}\right)\left(\underbrace{\sum_{i\in[m]} \prod_{j\in[m]\setminus\{i\}} s_j}_{\#\text{ of spanning trees}=|Jac(G)|=p^r}\right) \\
&= \frac{(f(v)-f(w))}{\prod_{j\in[m]} s_j} p^r.
\end{aligned}$$

Now we have

$$\begin{aligned}
p^t &= \frac{(f(v)-f(w))}{\prod_{j\in[m]} s_j} p^r \\
p^t \prod_{j\in[m]} s_j &= (f(v)-f(w))p^r \\
\prod_{j\in[m]} s_j &= (f(v)-f(w))(p^{r-t}).
\end{aligned}$$

Now, by assumption $t < r$ which means $p \mid RHS$ which implies $p \mid LHS$. So, $p \mid \prod_{j\in[m]} s_j$. Since p is prime, this means $p \mid s_k$ for some $k \in [m]$. However, that is a contradiction, since $gcd(s_j, p) = 1$ for all s_j. Thus, we have shown $t = r$, which means we found a generator and $Jac(G)$ is cyclic.

Now, what is the associated pairing? The mondromy pairing is defined as $\langle D_1, D_2\rangle = \frac{1}{m}\sum_{u\in V(G)} D_2(u)f(u)$ where m is the order of $[D_1]$ in the Jacobian Group so that namely, mD_1 is a principal divisor (numbering). Then, mD_1 a principal divisor means that there exists a divisor (numbering) $f : V(G) \to \mathbb{Z}$ such that $div(f) = mD_1$. Now, take $D_1 := D$ and $D_2 := D$. Since $Jac(G) = \langle [D]\rangle$ is cyclic with $[D]$ as its generator we know that $m = p^r$ in this case. Also, since the Jacobian group is cyclic and pairings are bilinear, it suffices to compute the value of the pairing on D, D to determine the entire pairing. So, the mondromy pairing can be computed as

$$\begin{aligned}\langle D, D\rangle &= \frac{1}{p^r}\sum_{u\in V(G)} D(u)f(u)\\ &= \frac{1}{p^r}(D(v)f(v)+D(w)f(w))\end{aligned}$$

since $D(u)=0$ for all $u \neq v, w$. Now,

$$\begin{aligned}\langle D, D\rangle &= \frac{1}{p^r}(D(v)f(v)+D(w)f(w))\\ &= \frac{1}{p^r}(f(v)-f(w))\\ &= \frac{1}{p^r}(b_i s_i)\end{aligned}$$

for all $i \in [m]$. Now,

$$\begin{aligned}\langle D, D\rangle &= \frac{1}{p^r}(b_i s_i)\\ &= \frac{1}{p^r}(\frac{\prod_{j=1}^m s_j}{s_i})s_i\\ &= \frac{1}{p^r}\prod_{j=1} s_j,\end{aligned}$$

and we are done. We have shown that the mondromy pairing gives the above value on the generator which then by bilinearity shows that

$$\langle x, y\rangle = \frac{(\prod_{j=1}^m s_j)xy}{p^r}$$

is indeed the mondromy pairing on this group and associated graph. □

Quadratic Reciprocity:

Definition: The Legendre Symbol of an integer a with respect to a prime p is defined as

$$(\frac{a}{p}) = \begin{cases} 1 & \text{if } n^2 \equiv a (\text{mod } p) \text{ for some } n \in \mathbb{Z} \\ -1 & \text{otherwise }. \end{cases}$$

This is also sometimes referred to as the "quadratic character" mod p. Then, the Law of Quadratic Reciprocity says that if p, q distinct primes, then

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

which is useful because the RHS is easily computable, and if we know one of $(\frac{p}{q})$ or $(\frac{q}{p})$ (which recall are always ± 1) then we can easily can easily find the other without determining whether the number p is a square mod p.

Definition: A Dirichlet Character χ mod q is a function $\chi : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ constructed from a group homomorphism (where both group operations are multiplication)

$$\phi : \mathbb{Z}/q\mathbb{Z}^\times \to \mathbb{C}^\times.$$

which we extend to take input in all of $\mathbb{Z}/q\mathbb{Z}$ by assigning $\chi(g) = 0$ for non-units $g \in \mathbb{Z}/q\mathbb{Z} \setminus (\mathbb{Z}/q\mathbb{Z})^\times$ (and just $\chi = \phi$ for the units).

Definition: The Principal Character mod n (n need not be prime) is the Dirichlet Character $\chi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}$ defined by

$$\chi(g) = \begin{cases} 1 & \text{if } gcd(g, n) = 1 \\ 0 & \text{otherwise }. \end{cases}$$

This is just one specific Dirichlet Character that exists for every natural number n. One also notes that the set of characters on $\mathbb{Z}/n\mathbb{Z}$ forms a group under pointwise multiplication

$$\chi_1\chi_2(g) := \chi_1(g)\chi_2(g),$$

and in this group the identity element is the Principal Character.

Definition: A Dirichlet Character on $\mathbb{Z}$ is a function $\chi : \mathbb{Z} \to \mathbb{C}$ which is the lift of a character $\chi_k : \mathbb{Z}/k\mathbb{Z} \to \mathbb{C}$ for some $k \in \mathbb{Z}$. (Lift means exactly what one would expect. It means that we extend χ_k to $\tilde{\chi_k}$ by assigning $\tilde{\chi_k}(x) = \chi_k(\bar{x})$ where $\bar{x}$ is the equivalence class of $x \mod k$).

Definition: A "Modulus" of two characters $\chi_1 \mod 4$ and $\chi_2 \mod p$ is a number N such that $4, p \mid N$ and $\tilde{\chi_1}(n) = \tilde{\chi_2}(n)$ for all n with $gcd(n, N) = 1$.

Definition: The Conductor of a Character $\chi_N \mod N$ is be the smallest positive divisor $c \mid N$ such that there exists a character $\chi_c \mod c$ with $\tilde{\chi_N}(a) = \tilde{\chi_c}(a)$ for all $a \in \mathbb{Z}$ coprime to N.

Definition: The Conductor of a group of Characters is the LCM of the Conductors of each element.

Proposition 17: For any sufficiently large prime p, there exists a prime q such that

- q is a non-square mod p,
- $q \equiv 3 \mod 4$ and
- $q < 2\sqrt{p}$.

Proof: Let χ_1 be the non-principal character mod 4. (One can show that there are only two valid characters mod 4 by recalling that the character must restrict to a group homomorphism over the units in $\mathbb{Z}/4\mathbb{Z}$, and we pick the non-principal one), which takes values

$$\begin{aligned}
\chi_1(0) &= 0 \\
\chi_1(1) &= 1 \\
\chi_1(2) &= 0 \\
\chi_1(3) &= -1.
\end{aligned}$$

Let χ_2 be the quadratic character mod p which is just the Legendre Symbol $\chi_2(g) = (\frac{g}{p})$ which indicates whether g is a square mod p.

Clearly, the Conductor $f \in \mathbb{Z}$ of the group generated by χ_1, χ_2 must be $f \geq LCM(4, p)$ and the exponent divides 2. Also, in fact that is an equality. Then, we define a form $\chi = 1 + \chi_1\chi_2 - \chi_1 - \chi_2$ and the above allows us to apply a Theorem 1.4 cited in `http://pollack.uga.edu/generalsplit6.pdf`.

Theorem 1.4 guarantees the existence of a number q_2 such that

$$q_2 << (4p)^{\frac{1}{4}+\epsilon f \epsilon} << 2p^{\frac{1}{4}+2\epsilon} < 2\sqrt{p}$$

such that $\chi(q_2) \neq 0$.

Then, by construction of $\chi = 1 + \chi_1\chi_2 - \chi_1 - \chi_2$, one knows that $\chi_2(q_2) \neq 0$ means that $\chi_1(q_2) = \chi_2(q_2) = -1$. So, $\chi_1(q_2) = -1$ which means that q_2 is not a square mod 4 which means $q_2 \equiv 3 \mod 4$ and $\chi_2(q_2) = (\frac{q_2}{p}) = -1 \mod p$ means that q_2 is not a square mod p. $\square$.

A field extension $K/\mathbb{Q}$ is Galois if it is the splitting field of a separable polynomial over $\mathbb{Q}$. Intuitively, a Galois Extension is one that is both normal and separable. Normal means that any polynomial with a root in K splits completely in K. So intuitively for any such polynomial K contains all the roots of the polynomial in question. Separable means that the minimal polynomial of any element in K is separable (means no repeated roots in the algebraic closure). In fact, one need only check the separability of the generators of the field $K/\mathbb{Q}$. To summarize, a Galois Extension is one with full automorphism group, meaning that
$|Aut(K/\mathbb{Q})| = [K : \mathbb{Q}] = dim_{\mathbb{Q}}(K)$.

Why do normal and separable guarantee a full automorphism group? Well, any automorphism of $K/\mathbb{Q}$ sends the roots of an irreducible polynomial to other roots of that polynomial. **Normal means we have all the roots available and separable means that none of them coincide.**

Non-Example: $K := \mathbb{Q}((2)^{\frac{1}{3}})$ is not a Galois field extension because it is not normal. Namely, it contains one root of $m(x) = x^3 - 2$ but not all of them. (One can see this by noting that $\mathbb{Q}((2)^{\frac{1}{3}}) \subseteq \mathbb{R}$, yet the roots are $(2)^{\frac{1}{3}} \in \mathbb{R}$ and $(2)^{\frac{1}{3}}\zeta_3, (2)^{\frac{1}{3}}\zeta_3^2 \in \mathbb{C} \setminus \mathbb{R}$). So, it does not have full automorphism group since any automorphism of $K/\mathbb{Q}$ must send roots to roots which means there is only one automorphism, namely the one that sends $(2)^{\frac{1}{3}}$ to itself.

Non-Example: $K := \mathbb{F}_p(t^{\frac{1}{p}}) \cong \mathbb{F}_p(t)[x]/(x^p - t)$ is not a Galois field extension because it is not separable. Namely, the minimal polynomial $(x^p - t)$ of the element $t^{\frac{1}{p}} \in K$ is not separable. Namely, it factors as $(x - t^{\frac{1}{p}})^p$. This means that $K/\mathbb{Q}$ does not have full automorphism group, though now for a different reason. It contains all the roots of $(x^p - t)$ but they all coincide which means that once again the the automorphism group $(\mathbb{F}_p(t^{\frac{1}{p}}))/(\mathbb{F}_p(t)) = \{id\}$ is trivial.

Fun fact: In most fields, a polynomial being irreducible implies that it is separable. (Fields in which this holds are called "Perfect fields"). Some examples of perfect fields are:

- Fields of infinite characteristic and
- Finite fields.

However, as shown above, in infinite fields of finite characteristic it is possible for an irreducible polynomial to have repeated roots.

Example: $K := \mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2 - 2)$ is a Galois Extension over $\mathbb{Q}$ since it is normal and separable. (For both of these properties it suffices to check just the generators of this field extension, namely $\{\sqrt{2}\}$). Its minimal polynomial is $x^2 - \sqrt{2} = (x + \sqrt{2})(x - \sqrt{2})$ which is separable. Also, note that K is normal since $-\sqrt{2} \in K$. The extension $K/\mathbb{Q}$ has full automorphism group $Aut(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. Note that $|Aut(K/\mathbb{Q})| = 2 = [K : \mathbb{Q}]$.

Example: $K = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha})$ is a Galois Extension with Galois group

$$Gal(K/\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

where any $\sigma_i \in Gal(K/\mathbb{Q})$ is completely determined by where it sends $\sqrt{-1}$ and $\sqrt{\alpha}$.

Namely, note that the requirement

$$\sigma : \sqrt{-1} \mapsto \pm\sqrt{-1} \text{ and}$$
$$\sigma : \sqrt{\alpha} \mapsto \pm\sqrt{\alpha}.$$

gives a natural intuitive connection between the Galois Group and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, which is why I chose to define it this way.

However, note that a more cannonical way is to define it as a "simple extension" $K = Q(\theta)$ (one formed by adjoining one element θ which we call "primitive"). How do we find such a primitive element θ?
Note that by the Galois Correspondence, every intermediate field K' (where $\mathbb{Q} \subseteq K' \subseteq K$) is the fixed field of some subgroup of the Galois Group $Aut(K/\mathbb{Q})$. Now, since there are only finitely many subgroups, there are only finitely many intermediate fields. Any element not in one of these intermediate fields will be a primitive element.

In our case, the intermediate fields are $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{\alpha})$, and $\mathbb{Q}(\sqrt{i}\sqrt{\alpha})$. These are fixed fields of the subgroups of $Aut(K/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$ which correspond to the subgroups $\langle(0,1)\rangle$,$\langle(1,0)\rangle$,$\langle(1,1)\rangle$ in $\mathbb{Z}/2\mathbb{Z}$).
Then, $\theta = \sqrt{-1} + \sqrt{\alpha}$ is a primitive element. Now, that we have a primitive element θ a basis for K as a $\mathbb{Q}-$vector space is $\{1, \theta, \theta^2, \theta^3\}$. (In general it is $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ where $n = [K : \mathbb{Q}]$ is the degree of the extension).

Definition: The Discriminant of a Galois Field Extension $K/\mathbb{Q}$ (of degree $[K : \mathbb{Q}] =: n$) is

$$\Delta_{K/\mathbb{Q}} = (det(\sigma_i(\theta^j)))^2 \quad \text{where } i, j \in [n]$$

where θ is a primitive element of this extension (namely a number $\theta \in K$ such that $\mathbb{Q}(\theta) = K$) which means that $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is a basis as a vector space for K over $\mathbb{Q}$, and $\{\sigma_i : i \in [n]\} = Gal(K/\mathbb{Q})$ is the set of field automorphisms of K which fix $\mathbb{Q}$ pointwise.

Note: One can even define the Discriminant for fields that are not Galois by looking at a Galois closure $L \supsetneq K \supsetneq \mathbb{Q}$. Then, one defines $G := Aut(L/\mathbb{Q})$ and $H := Aut(L/K)$. One can then look at coset representatives $\sigma \in gH$ for all cosets in G/H (although those cosets do not form a group in this case). One then uses these σ to calculate the discriminant.

Example: For the field $K = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha}) = \mathbb{Q}(\sqrt{-1} + \sqrt{\alpha})$, the field discriminant is $\Delta_{K/Q} = (det(\sigma_i((\sqrt{-1} + \sqrt{\alpha})^j)))^2$ where $\theta = i + \sqrt{\alpha}$ is our primitive element.

Proposition 18: For sufficiently large prime p and integer $r > 1$, there exist non-squares (modulo p) $q_1 = 1 \mod 4$ and $q_2 = 3 \mod 4$, with $q_1, q_2 < 2\sqrt{p^r}$.

Proof: As before let χ_1 be the nontrivial character mod 4 and let χ_2 be the quadratic character (Legendre symbol $(\frac{\cdot}{p})$) mod p. We want $q_2 = 3$ mod 4 and q_2 not square mod p, which translate to $\chi_1(q_2) = -1$ and $\chi_2(q_2) = -1$.

To find such q_2, consider the field extension $K = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha})$ where $\alpha = (-1)^{\frac{p-1}{2}} p$.

This extension is degree 4 (and recall that it's Galois since its the splitting field of a separable polynomial, namely the product of the minimal polynomials of i and $\sqrt{\alpha}$ respectively). Its discriminant is $(4p)^2$, with field conductor $4p$. (The discriminant and field conductor are related:

`https://en.wikipedia.org/wiki/Conductor-discriminant_formula`).

Now, the above properties, namely $K/\mathbb{Q}$ Galois, $[K : \mathbb{Q}] = 4$ and conductor of $K/\mathbb{Q}$ equal to $4p$, along with the fact that χ_1, χ_2 are quadratic characters (meaning they have order two in their respective character groups), one can apply Theorem 1.7 in `http://pollack.uga.edu/generalsplit6.pdf`.

Theorem 1.7 gives us an upper bound on the desired prime

$$q_2 << 2p^{\frac{1}{2}+\epsilon} < 2\sqrt{p^r}.$$

To get the desired prime q_1 we apply Theorem 1.7 again, however now requiring that $q_1 = 1 \mod 4$ and q_1 not square mod p, which translate to $\chi_1(q_1) = 1$ and $\chi_2(q_1) = -1$, and we have found the desired q_1, q_2 and we are done. $\square$.

Generalized Riemann Hypothesis:
Say $\chi : \mathbb{Z} \to \mathbb{C}$ is a Dirichlet character. One then defines the Dirichlet L-function as

$$L(\chi, s) := \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

which takes in input in $\{s \in \mathbb{C} : Re(s) > 1\}$. By analytic continuity, this function can then be extended to take input in all of $\mathbb{C}$.

Generalized Riemann Hypothesis: For every Dirichlet Character χ and every complex number $s \in \mathbb{C}$ such that $L(\chi, s) = 0$ and $s \notin \mathbb{R}^-$ (we call such s "non-trivial" zeros of $L(\chi, s)$), one has $Re(s) = \frac{1}{2}$.

Note: Plugging in $\chi(n) = 1$ gives $L(\chi, s)$ equal to the Riemann-Zeta function. This then gives the Standard Riemann Hypothesis (which is usually stated as "The real part of every non-trivial zero of the Riemann-Zeta function is $\frac{1}{2}$").

Proposition 19 (conditional on the Generalized Riemann Hypothesis): For any prime $p > 10^9$, there exists a prime number q such that

- $q = 3$ mod 4,
- q a non-square mod p and

- $q < 2\sqrt{p}$.

Note that this is identical to an earlier proposition except now we have replaced "for sufficiently large p" with "for all $p > 10^9$". The bound given here 10^9 is sufficiently small that we can handle all cases not handled by this theorem (namely primes $< 10^9$) by brute force computer search.

Proof: Let $\alpha = (-1)^{\frac{p-1}{2}} p$.
Consider $K = \mathbb{Q}(\sqrt{-1}, \sqrt{\alpha})$ an extension of degree 4.

Definition: The ring of integers O_k of a field extension $K/\mathbb{Q}$ is the set of $\{\beta \in K : m_{\beta/\mathbb{Q}}(x) \in \mathbb{Z}[x]\}$ whose minimal polynomials have only integer coefficients. They are meant to be a ring $O_K \subseteq K$ analogous to $\mathbb{Z} \subseteq \mathbb{Q}$.

Properties of the Ring of Integers O_k: Any ideal $I \subseteq O_K$ factors uniquely as a product of prime ideals

$$I = \prod_i P_i^{e_i}.$$

Note that this is essentially saying that O_K may not be a UFD because elements may not factor uniquely, it is still something close to a UFD in that ideals factor uniquely.

By the way, the size of the class group, which is the group of fractional ideals of O_k modulo the group of principal ideals of O_k, measures the extent to which O_k fails to be an actual unique factorization domain. Intuitively, a small class group means that O_k is "close" to being a unique factorization domain, while a large class group means that O_k is "far" from being a unique factorization domain. I should also add, if it was not tacitly clear, that the class group *of a ring of integers*, O_k, is always finite. The proof is non-trivial and takes more than a couple lines.

Example: Take $K := \mathbb{Q}(\sqrt{-5})$. Then, one can check $O_K = \mathbb{Z}\sqrt{-5}$.

(Computing O_K is actually a very non-trivial task. One first takes a $\mathbb{Q}$-basis $\mathcal{B}$ of K and scales the elements until they belong to O_K, which really involves clearing denominators to modify their minimal polynomials to get related ones with integer coefficients. Then, one knows that this new set $\mathcal{B}' \subseteq O_K$. It may not be a $\mathbb{Z}$-basis though as it may not span all of O_K. However, the span $span(\mathcal{B}')$ has rank equal to O_K, which means its index in O_K is finite. So we sandwich O_K as $span(\mathcal{B}') \subseteq O_K \subseteq \frac{1}{\Delta_{K/\mathbb{Q}}} span(\mathcal{B}')$ and looks at subgroups of $(\frac{1}{\Delta_{K/\mathbb{Q}}} span(\mathcal{B}'))/O_K$ which contain $span(\mathcal{B}')$ to find an actual $\mathbb{Z}$-basis).

Example: Take $K := \mathbb{Q}(\sqrt{-5})$. Then, one can check $O_K = \mathbb{Z}\sqrt{-5}$. As noted, O_K may not be a UFD and here it is not since $6 = (1+\sqrt{-5})(1-\sqrt{-5}) = 2*3$ and the two factorizations do not differ by units, so they really are "distinct" so to speak. However, ideals factor uniquely into products of prime ideals in O_K. (Even more generally, this holds true in any "Dedekind Domain" which is an Integral Domain that is Noetherian, Integrally Closed and Height 1).

For the purposes of this paper, we will rely heavily on the fact that ideals in O_K factor uniquely into prime ideals in order to guarantee the existence of a prime number with certain properties later. (Namely, it will turn out that this prime number is the norm of a prime ideal in O_K).

Definition: If $(\frac{P}{K/\mathbb{Q}})$ is a Galois field extension $K/\mathbb{Q}$, $P \subseteq O_K \subseteq L$ is a prime ideal which is unramified over p(meaning that if we have $pO_K = P^{e_0} \prod_i Q_i^{e_i}$ where P, Q_i are distinct prime ideal factors of O_k, then $e_0 = 1$), and $(p) \subseteq \mathbb{Z}$ a prime ideal, then define the Artin Symbol of the prime ideal P as

$$\sigma = (\frac{P}{K/Q})$$

to be the unique element $\sigma \in Gal(K/Q)$ such that for every element $\beta \in K$,

$$\sigma(\beta) \equiv \beta^p \bmod P$$

or equivalently stated

$$\sigma(\beta) - \beta^p \in P.$$

Once again, for our specific purposes, we will use the existence of such a σ in order to apply a cited theorem which guarantees the existence of a prime number with certain properties.

Now, in our particular case $[K : \mathbb{Q}] = 4$ and $\Delta = (4p)^2$. Then, Theorem 5.1 in `https://www.jstor.org/stable/2153734?seq=13#metadata_info_tab_contents` states

Theorem 5.1 (Conditional on the Generalized Riemann Hypothesis): Let $K/\mathbb{Q}$ be a Galois extension with $K \neq \mathbb{Q}$. Let $\Delta = |\Delta_{K/Q}|$ and $n = [K : Q]$. Let $\sigma \in Gal(K/Q)$.

Then, there is a prime ideal $P \subseteq O_K$ with $(\frac{P}{K/Q}) = \sigma$ of residue degree 1 satisfying $N(P) = |O_K/P| \leq (4log\Delta + 2.5n + 5)^2$. (Here's where we needed to use the Artin Symbol!)

In our case, we have $\Delta = (4p)^2$ and $4 = [K : \mathbb{Q}]$. Let $\sigma \in Gal(K/\mathbb{Q})$. Then, Theorem 5.1 applied to our problem, says there exists a prime ideal $P \subseteq O_K$ with $(\frac{P}{K/Q}) = \sigma$ of residue degree 1 satisfying

$$\begin{aligned} q := N(P) = |O_K/P| &\leq (4log((4p)^2) + 2.5 * 4 + 5)^2 \\ &= (4log((4p)^2) + 15)^2. \end{aligned}$$

and $(4log((4p)^2) + 15)^2 < 2\sqrt{p}$ provided $p > 10^9$ proving the result. $\square$.

Note: Above we used the fact that the norm of a prime ideal $P \subseteq O_K$ is $q := N(P)$ is always a prime number.

Lemma 20: Let q be an odd prime and $k \in \mathbb{Z}$ such that

$$(\frac{k}{q}) = (\frac{-1}{q}).$$

Then, there exists $0 < c < q$ such that $c(q - c) \equiv k \bmod q$.

Proof: Consider the set

$$R_q = \{\ell \in \mathbb{F}_q : (\frac{\ell}{q}) = (\frac{-1}{q})\}.$$

Now, consider the map $\phi : \mathbb{F}_q \to \mathbb{F}_q$ defined by

$$\phi(x) = -x^2.$$

One knows that the image $\phi(\mathbb{F}_q) \subseteq R_q$. Why? That is equivalent to saying that

$$\{(\frac{-x^2}{q}) = (\frac{-1}{q})\} \text{ for all } x \in \mathbb{F}_q.$$

We now prove that

$$(\frac{-x^2}{q}) = (\frac{-1}{q}) \text{ for all } x \in \mathbb{F}_q.$$

Note that if ($-1 = a^2 \bmod q$) is a square mod p, then so is $-x^2 = (-1)x^2 = (ax)^2 \bmod q$. (Recall something being a square is the same as its Legendre Symbol taking the value 1). Also, if $-1 \neq x^2 \bmod q$ for all $x \in \mathbb{F}_q$ is a non-square mod p, then so is $-x^2$ since the Legendre Symbol is multiplicative which means $(\frac{-x^2}{q}) = (\frac{-1}{q})(\frac{x^2}{q}) = -1 * 1 = -1$. So, indeed $(\frac{-x^2}{q}) = (\frac{-1}{q})$ for all $x \in \mathbb{F}_q$. This means $\phi(\mathbb{F}_q) \subseteq R_q$.

Does ϕ surject onto R_q? That happens if for all $a \in R_q$ there exists $x \in \mathbb{F}_q$ such that $-x^2 = a$ which happens exactly when $x^2 + a$ has a root in $\mathbb{F}_q$.

Now, since $x^2 + a$ has at most 2 roots in $\mathbb{F}_q$, this map is at most 2-to-1 and since $|R_q| = \frac{q-1}{2} < |\mathbb{F}_q|$ and since x is the root of at most 1 polynomial $x^2 + b$ (varied over b) meaning that the map defined as the "inverse" of the pre-image map $a \mapsto \{x : x^2 + a = 0\}$ is in fact a function (meaning it is well defined since for every input x there is a unique a such that $x^2 + a = 0$). So, for all $k \in R_q$, there exists $c \in \mathbb{F}_q$ such that $\phi(c) = -c^2 = k$ and we have that $k = -c^2 = c(q - c) \bmod q$ as desired. $\square$.

Lemma 21: Let p be a sufficiently large prime p with $p \equiv 1 \bmod 4$ and let $r \in \mathbb{Z}^+$. Then, there exists a prime q with $(\frac{q}{p^r}) = -1$ (so q is not a square mod p^r) and a positive integer $c < q$ such that

$$\frac{p^r - c(q-c)}{q}$$

is a positive integer.

Proof: By Proposition 18, there exists a non-square q with $(\frac{-1}{q}) = (\frac{p^r}{q})(\in \{\pm 1\})$ and $\frac{q^2}{4} < p^r$. By Lemma 20, there exists $c \in \mathbb{Z}^+$ such that $p^r = -c^2 = c(q-c) \bmod q$. So, we have $q \mid (p^r - c(q-c))$ and also $(p^r - c(q-c))$ is positive since $c < q$. $\square$.

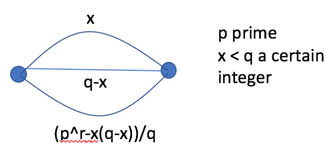
Proposition 22: For any sufficiently large prime p and integer $r \in \mathbb{Z}^+$, there exists $s = (s_1, \ldots, s_m)$ such that $gcd(s_i, p) = 1$ for all i, $\prod_{j=1}^m s_j$ is a non-residue (= not a square) mod p, and

$$\sum_{i=1}^m \frac{\prod_{j=1}^m s_j}{s_i} = p^r.$$

Proof: First case: $p \equiv 3 \bmod 4$. Choose $s = (s_1, s_2) = (1, p^r - 1)$ and right away we're done since s_1, s_2 coprime to p, their product is $s_1 s_2 = p^r - 1 \equiv -1 \bmod p$ which is not a square mod p. (Recall that $p = 1 \bmod 4$ if and only if -1 is a square mod p)!

Second Case: $p \equiv 1 \bmod 4$. Say we have x and q chosen (as in Lemma 21) such that $\frac{p^r - x(q-x)}{q}$ is a positive integer. Now, let

$$s_1 = x$$
$$s_2 = q - x$$
$$s_3 = \frac{p^r - x(q-x)}{q}$$



Both x and $q - x$ are smaller than p, which means they are both coprime to p. So, also their product $x(q-x)$ is coprime to p, which means that $p^r - x(q-x)$ is coprime to p (since otherwise if not coprime and p prime would mean $p \mid p^r - x(q-x)$ which means $p \mid x(q-x)$ a contradiction). Then, if $p^r - x(q-x)$ is coprime to p meaning $p^r - x(q-x)$ and p share no common factors, then dividing by q to get $\frac{p^r - x(q-x)}{q}$ can only remove some factors of $p^r - x(q-x)$ so the coprime property is preserved.

Now, is $\prod s_i = s_1 s_2 s_3$ a non-square mod p as desired? Well,

$$s_1 s_2 s_3 = x(q-x)\frac{p^r - x(q-x)}{q}.$$

Now, recall that we chose x and q to be as in Lemma 21 and Lemma 18, namely so that $(\frac{-1}{q}) = (\frac{p^r}{q})$. Now, denote $c := x(q-x)$. Then, $s_1 s_2 s_3 = c\frac{(p^r - c)}{q}$ we know $c\frac{(p^r-c)}{q} = \frac{cp^r - c^2}{q}$ is a square mod p if and only if $\frac{(-1)c^2}{q}$ is a square mod p.

Is

$$\frac{(-1)(x(q-x))^2}{q}$$

a square mod p?

Since $p \equiv 1 \bmod 4$, we have that $-1 \equiv y^2 \bmod p$ is a square mod p^r (since as we proved in class that $p \equiv 1 \mod 4$ if and only if -1 is a square mod p). Now the whole numerator is a square mod p. So that means that $s_1 s_2 s_3$ is a non-square mod p^r, which by definition of the Legendre symbol means $(\frac{s_1 s_2 s_3}{p^r})(= (\frac{q}{p^r})) = -1$. $\square$

That concludes the proof of the Relaxed Version of Main Theorem that there exists a finite set of primes $\mathcal{P} \subseteq \mathbb{Z}$ such that for any Abelian Group H whose order is not divisible by any prime $p \in \mathcal{P}$, we can construct a graph G with

$$Jac(G) \cong H.$$

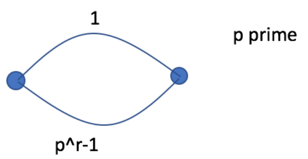
Namely, for any given prime $p \notin \mathcal{P}$ and $r \in \mathbb{Z}+$, we have constructed the desired set $s = (s_1, \ldots, s_m)$ and corresponding Banana Graph G such that $Jac(G) = \mathbb{Z}/p^r\mathbb{Z}$. To strengthen the result to get the proof of the Main Theorem, we need one more result.

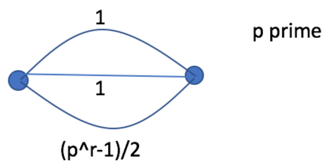
Proposition 23: Let p be an odd prime with $p \not\equiv 1 \mod 24$ and let $r > 1$ be an integer. Then, there exists $s = (s_1, \ldots, s_m)$ such that $\prod_i s_i$ is a non-square mod p and

$$\sum_{i=1}^{m} \frac{\prod_{j=1}^{m} s_j}{s_i} = p^r.$$

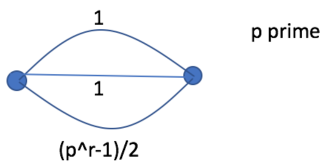
Proof: We consider three cases.

1. If $p = 3 \mod 4$, we use $s = (s_1, s_2) = (1, p^r - 1)$.
2. If $p = 5 \mod 8$, we use $s = (s_1, s_2, s_3) = (1, 1, \frac{p^r-1}{2})$. Now $p = 5 \mod 8$ means $p = 1 \mod 4$ which means that $-1 = p^r - 1 \mod p$ is a square mod p. Now, is $s_1 s_2 s_3$ a square? It is a square if and only if $\frac{1}{2} = 2^{-1}$ is a square mod p. Also, note 2^{-1} is a square mod p if and only if 2 is a square mod p. However, $p = 5 \mod 8$ means that 2 is not a square mod p.





3. $p = 2 \mod 3$. If $p = 3 \mod 4$ we are in the first case. Otherwise $p = 1 \mod 4$ and 2 is a non-square mod p. Once again we use $s = (s_1, s_2, s_3) = (1, 1, \frac{p^r-1}{2})$. So, as stated in the hypothesis the only remaining case not covered by the above is $p = 1 \mod 24$. $\square$



Now, note that as stated earlier, conditional on the GRH, for all primes $p > 10^9$ (this bound is better than the "sufficiently large p" bound which doesn't use GRH) we have constructed the desired graph. Now, by the above lemma if $p \neq 1 \mod 24$ is an odd prime, we also have the desired graph. Now, the only remaining cases to handle are odd primes $q < 10^9$ with $q = 1 \mod 24$. We note that $= 1 \mod 24$ is a fairly restrictive condition, and these remaining cases are handled brute force by a computer.

To summarize, the authors showed that there is some finite list of primes $\mathcal{P}$ such that any abelian group

H of order not divisible by these primes occurs as the Jacobian of some graph. Namely, they first showed that for any sufficiently large odd prime p_i and positive integer r_i, we can construct a graph G_i with Jacobian group

$$Jac(G_i) = \mathbb{Z}/p_i^{r_i}\mathbb{Z}.$$

Conditional on the GRH they have actually shown that the forbidden list of primes is now $\mathcal{P} = \{2\}$.

Then, if $H \cong \prod_i \mathbb{Z}/p_i^{r_i}\mathbb{Z}$, by letting the graph $G = \bigvee_i G_i$ be the wedge sum of these graphs, one obtains

$$\begin{aligned} Jac(G) &= Jac(\bigvee_i G_i) \\ &= \bigoplus_i Jac(G_i) \\ &= \bigoplus_i \mathbb{Z}/p_i^{r_i}\mathbb{Z} = H \end{aligned}$$

and we have constructed a graph whose Jacobian is the desired group H. Furthermore, if the GRH holds, one has that the list of forbidden primes is actually just $\mathcal{P} = \{2\}$, so in that case we can realize any odd order abelian group as the Jacobian of some graph.