Finite abelian groups

Week of March 23, 2020

GU4041

Columbia University

March 26, 2020

The main theorem

Theorem

Let A be a finite abelian group. There is a sequence of prime numbers

$$p_1 \leq p_2 \leq \cdots \leq p_n$$

(not necessarily all distinct) and a sequence of positive integers

$$a_1, a_2, \ldots, a_n$$

(in no particular order) such that A is isomorphic to the direct product

$$A \xrightarrow{\sim} \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}.$$

In particular

$$|A| = \prod_{i=n}^{n} p_i^{a_i}.$$

The main theorem

Theorem

Let A be a finite abelian group. There is a sequence of prime numbers

$$p_1 \leq p_2 \leq \cdots \leq p_n$$

(not necessarily all distinct) and a sequence of positive integers

$$a_1, a_2, \ldots, a_n$$

(in no particular order) such that A is isomorphic to the direct product

$$A \xrightarrow{\sim} \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}.$$

In particular

$$|A| = \prod_{i=n}^{n} p_i^{a_i}.$$

The main theorem

Theorem

Let A be a finite abelian group. There is a sequence of prime numbers

$$p_1 \leq p_2 \leq \cdots \leq p_n$$

(not necessarily all distinct) and a sequence of positive integers

$$a_1, a_2, \ldots, a_n$$

(in no particular order) such that A is isomorphic to the direct product

$$A \xrightarrow{\sim} \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}.$$

In particular

$$|A| = \prod_{i=n}^{n} p_i^{a_i}.$$

The main theorem

Theorem

Let A be a finite abelian group. There is a sequence of prime numbers

$$p_1 \leq p_2 \leq \cdots \leq p_n$$

(not necessarily all distinct) and a sequence of positive integers

$$a_1, a_2, \ldots, a_n$$

(in no particular order) such that A is isomorphic to the direct product

$$A \xrightarrow{\sim} \mathbb{Z}_{p_1^{a_1}} \times \mathbb{Z}_{p_2^{a_2}} \times \cdots \times \mathbb{Z}_{p_n^{a_n}}.$$

In particular

$$|A| = \prod_{i=n}^{n} p_i^{a_i}.$$

Prime factors

This can be broken down into two theorems.

Theorem (Theorem 1)

Let A be a finite abelian group. Let $q_1, \ldots, q_r$ be the distinct *primes dividing $|A|$, and say*

$$|A| = \prod_j q_j^{b_j}.$$

Then there are subgroups $A_j \subseteq A$, $j = 1, \ldots, r$, with $|A_j| = q_j^{b_j}$, and an isomorphism

$$A \xrightarrow{\sim} A_1 \times A_2 \times \cdots \times A_r.$$

Prime factors

This can be broken down into two theorems.

Theorem (Theorem 1)

Let A be a finite abelian group. Let $q_1, \dots, q_r$ be the distinct *primes dividing $|A|$, and say*

$$|A| = \prod_j q_j^{b_j}.$$

Then there are subgroups $A_j \subseteq A$, $j = 1, \dots, r$, with $|A_j| = q_j^{b_j}$, and an isomorphism

$$A \xrightarrow{\sim} A_1 \times A_2 \times \cdots \times A_r.$$

Abelian groups of prime power order

Theorem (Theorem 2)

Let p be a prime and let A be a finite abelian group of order p^N for some $N > 1$. Then there is a sequence of positive integers $c_1 \leq c_2 \cdots \leq c_s$ and an isomorphism

$$A \xrightarrow{\sim} \mathbb{Z}_{p^{c_1}} \times \mathbb{Z}_{p^{c_2}} \times \cdots \times \mathbb{Z}_{p^{c_s}}.$$

Theorem 1 is essentially a series of applications of the Chinese Remainder Theorem, and is not very hard.

Theorem 2 is a more complicated induction argument.

Abelian groups of prime power order

Theorem (Theorem 2)

Let p be a prime and let A be a finite abelian group of order p^N for some $N > 1$. Then there is a sequence of positive integers $c_1 \leq c_2 \cdots \leq c_s$ and an isomorphism

$$A \xrightarrow{\sim} \mathbb{Z}_{p^{c_1}} \times \mathbb{Z}_{p^{c_2}} \times \cdots \times \mathbb{Z}_{p^{c_s}}.$$

Theorem 1 is essentially a series of applications of the Chinese Remainder Theorem, and is not very hard.

Theorem 2 is a more complicated induction argument.

Abelian groups of prime power order

Theorem (Theorem 2)

Let p be a prime and let A be a finite abelian group of order p^N for some $N > 1$. Then there is a sequence of positive integers $c_1 \leq c_2 \cdots \leq c_s$ and an isomorphism

$$A \xrightarrow{\sim} \mathbb{Z}_{p^{c_1}} \times \mathbb{Z}_{p^{c_2}} \times \cdots \times \mathbb{Z}_{p^{c_s}}.$$

Theorem 1 is essentially a series of applications of the Chinese Remainder Theorem, and is not very hard.
Theorem 2 is a more complicated induction argument.

Additive notation

We will use *additive notation* for the abelian group A. So instead of writing $a \cdot b$ we write $a + b$, and instead of writing a^m we write ma, where m is any integer. We also write $-a$ instead of a^{-1} and 0 instead of e. Because A is abelian, we know $a + b = b + a$ for any $a, b \in A$.

Lemma

Let A be an abelian group. Then for any $m \in \mathbb{Z}$, the function $a \mapsto ma$ is a homomorphism.

Additive notation

We will use *additive notation* for the abelian group A. So instead of writing $a \cdot b$ we write $a + b$, and instead of writing a^m we write ma, where m is any integer. We also write $-a$ instead of a^{-1} and 0 instead of e. Because A is abelian, we know $a + b = b + a$ for any $a, b \in A$.

Lemma

Let A be an abelian group. Then for any $m \in \mathbb{Z}$, the function $a \mapsto ma$ is a homomorphism.

Additive notation

We will use *additive notation* for the abelian group A. So instead of writing $a \cdot b$ we write $a + b$, and instead of writing a^m we write ma, where m is any integer. We also write $-a$ instead of a^{-1} and 0 instead of e. Because A is abelian, we know $a + b = b + a$ for any $a, b \in A$.

Lemma

Let A be an abelian group. Then for any $m \in \mathbb{Z}$, the function $a \mapsto ma$ is a homomorphism.

Proof of the Lemma

Proof.

We need to show that, for all $a, b \in A$,

$$m(a+b) = ma + mb.$$

We prove this for $m > 0$ by induction; the case of $m < 0$ is similar. For $m = 1$ there is nothing to prove. Suppose we know the equality for m. Then

$$(m+1)(a+b) = m(a+b) + (a+b) = (ma+mb) + (a+b)$$

by the induction hypothesis. But now by associativity

$$(ma+mb) + (a+b) = ma + (mb+a) + b = ma + (a+mb) + b$$

where the last equality is allowed because A is abelian. □

Proof of the Lemma

Proof.

We need to show that, for all $a, b \in A$,

$$m(a+b) = ma + mb.$$

We prove this for $m > 0$ by induction; the case of $m < 0$ is similar. For $m = 1$ there is nothing to prove. Suppose we know the equality for m. Then

$$(m+1)(a+b) = m(a+b) + (a+b) = (ma+mb) + (a+b)$$

by the induction hypothesis. But now by associativity

$$(ma+mb) + (a+b) = ma + (mb+a) + b = ma + (a+mb) + b$$

where the last equality is allowed because A is abelian. □

Proof of the Lemma

Proof.

We need to show that, for all $a, b \in A$,

$$m(a+b) = ma + mb.$$

We prove this for $m > 0$ by induction; the case of $m < 0$ is similar. For $m = 1$ there is nothing to prove. Suppose we know the equality for m. Then

$$(m+1)(a+b) = m(a+b) + (a+b) = (ma+mb) + (a+b)$$

by the induction hypothesis. But now by associativity

$$(ma+mb) + (a+b) = ma + (mb+a) + b = ma + (a+mb) + b$$

where the last equality is allowed because A is abelian. □

Proof of the Lemma, concluded

Proof.

So far we have

$$(m+1)(a+b) = ma + (a + mb) + b.$$

Continuing by associativity

$$ma + (a + mb) + b = (ma + a) + (mb + b) = (m+1)a + (m+1)b$$

and we are done by induction.

Proof of the Lemma, concluded

Proof.

So far we have

$$(m+1)(a+b) = ma + (a+mb) + b.$$

Continuing by associativity

$$ma + (a+mb) + b = (ma+a) + (mb+b) = (m+1)a + (m+1)b$$

and we are done by induction.

□

A Proposition

Proposition

Suppose A is an abelian group of order mn, where $(m,n)=1$. Then there are subgroups $A_m, A_n \subseteq A$ such that $|A_m| = m$, $|A_n| = n$, such that the inclusion defines an isomorphism

$$A_n \times A_m \xrightarrow{\sim} A.$$

Proof.

Define

$$mA = \{ma, a \in A\}; nA = \{na, a \in A\}.$$

These are subgroups because they are the images of homomorphisms. Claim $mA \cap nA = \{0\}$. Suppose $x \in mA \cap nA$. Then there are $a, b \in A$ such that

$$x = ma = nb.$$

□

A Proposition

Proposition

Suppose A is an abelian group of order mn, where $(m,n) = 1$. Then there are subgroups $A_m, A_n \subseteq A$ such that $|A_m| = m$, $|A_n| = n$, such that the inclusion defines an isomorphism

$$A_n \times A_m \xrightarrow{\sim} A.$$

Proof.

Define

$$mA = \{ma, a \in A\}; nA = \{na, a \in A\}.$$

These are subgroups because they are the images of homomorphisms. Claim $mA \cap nA = \{0\}$. Suppose $x \in mA \cap nA$. Then there are $a, b \in A$ such that

$$x = ma = nb.$$

□

A Proposition

Proposition

Suppose A is an abelian group of order mn, where $(m,n)=1$. Then there are subgroups $A_m, A_n \subseteq A$ such that $|A_m|=m$, $|A_n|=n$, such that the inclusion defines an isomorphism

$$A_n \times A_m \xrightarrow{\sim} A.$$

Proof.

Define

$$mA = \{ma, a \in A\}; nA = \{na, a \in A\}.$$

These are subgroups because they are the images of homomorphisms.
Claim $mA \cap nA = \{0\}$. Suppose $x \in mA \cap nA$. Then there are $a, b \in A$ such that

$$x = ma = nb.$$

□

A Proposition

Proposition

Suppose A is an abelian group of order mn, where $(m,n) = 1$. Then there are subgroups $A_m, A_n \subseteq A$ such that $|A_m| = m$, $|A_n| = n$, such that the inclusion defines an isomorphism

$$A_n \times A_m \xrightarrow{\sim} A.$$

Proof.

Define

$$mA = \{ma, a \in A\}; nA = \{na, a \in A\}.$$

These are subgroups because they are the images of homomorphisms. Claim $mA \cap nA = \{0\}$. Suppose $x \in mA \cap nA$. Then there are $a, b \in A$ such that

$$x = ma = nb.$$

A Proposition

Proposition

Suppose A is an abelian group of order mn, where $(m,n) = 1$. Then there are subgroups $A_m, A_n \subseteq A$ such that $|A_m| = m$, $|A_n| = n$, such that the inclusion defines an isomorphism

$$A_n \times A_m \xrightarrow{\sim} A.$$

Proof.

Define

$$mA = \{ma, a \in A\}; nA = \{na, a \in A\}.$$

These are subgroups because they are the images of homomorphisms. Claim $mA \cap nA = \{0\}$. Suppose $x \in mA \cap nA$. Then there are $a, b \in A$ such that

$$x = ma = nb.$$

□

Proof of Proposition, continued

Proof.

Since $x = ma = nb$, we have

$$mx = m^2 a = mnb = 0.$$

Similarly $nx = 0$.

But there are constants $\alpha, \beta \in \mathbb{Z}$ such that $\alpha m + \beta n = 1$. Thus

$$x = (\alpha m + \beta n)x = \alpha \cdot mx + \beta \cdot nx = 0.$$

So $mA \cap nA = \{0\}$ as claimed.

Proof of Proposition, continued

Proof.

Since $x = ma = nb$, we have

$$mx = m^2a = mnb = 0.$$

Similarly $nx = 0$.
But there are constants $\alpha, \beta \in \mathbb{Z}$ such that $\alpha m + \beta n = 1$. Thus

$$x = (\alpha m + \beta n)x = \alpha \cdot mx + \beta \cdot nx = 0.$$

So $mA \cap nA = \{0\}$ as claimed.

Proof of Proposition, continued

Proof.

Since $x = ma = nb$, we have

$$mx = m^2a = mnb = 0.$$

Similarly $nx = 0$.
But there are constants $\alpha, \beta \in \mathbb{Z}$ such that $\alpha m + \beta n = 1$. Thus

$$x = (\alpha m + \beta n)x = \alpha \cdot mx + \beta \cdot nx = 0.$$

So $mA \cap nA = \{0\}$ as claimed. □

Proof of Proposition, continued

Proof.

Now define $A_n = mA$, $A_m = nA$ (careful!) Inclusion defines a homomorphism

$$f : A_n \times A_m \to A; \ \ f((u, v)) = u - v.$$

Suppose $(u, v) \in \ker f$. Then $u - v = 0$, so $u = v \in A_n \cap A_m = \{0\}$. Thus f is injective.

On the other hand, if $a \in A$, let $\alpha m + \beta n = 1$ as before. Write $u = \alpha \cdot ma \in A_n$, $v = -\beta \cdot na \in A_m$. Then

$$f((u, v)) = \alpha \cdot ma - (-\beta \cdot na) = (\alpha m + \beta n)a = a,$$

so f is surjective as well. Thus f is an isomorphism. □

Proof of Proposition, continued

Proof.

Now define $A_n = mA$, $A_m = nA$ (careful!) Inclusion defines a homomorphism

$$f : A_n \times A_m \to A;\ \ f((u,v)) = u - v.$$

Suppose $(u,v) \in \ker f$. Then $u - v = 0$, so $u = v \in A_n \cap A_m = \{0\}$. Thus f is injective.

On the other hand, if $a \in A$, let $\alpha m + \beta n = 1$ as before. Write $u = \alpha \cdot ma \in A_n$, $v = -\beta \cdot na \in A_m$. Then

$$f((u,v)) = \alpha \cdot ma - (-\beta \cdot na) = (\alpha m + \beta n)a = a,$$

so f is surjective as well. Thus f is an isomorphism. □

Proof of Proposition, continued

Proof.

Now define $A_n = mA$, $A_m = nA$ (careful!) Inclusion defines a homomorphism

$$f : A_n \times A_m \to A;\ \ f((u,v)) = u - v.$$

Suppose $(u,v) \in \ker f$. Then $u - v = 0$, so $u = v \in A_n \cap A_m = \{0\}$. Thus f is injective.

On the other hand, if $a \in A$, let $\alpha m + \beta n = 1$ as before. Write $u = \alpha \cdot ma \in A_n$, $v = -\beta \cdot na \in A_m$. Then

$$f((u,v)) = \alpha \cdot ma - (-\beta \cdot na) = (\alpha m + \beta n)a = a,$$

so f is surjective as well. Thus f is an isomorphism. □

Proof of Proposition, continued

Proof.

Now define $A_n = mA$, $A_m = nA$ (careful!) Inclusion defines a homomorphism

$$f : A_n \times A_m \to A;\ \ f((u,v)) = u - v.$$

Suppose $(u,v) \in \ker f$. Then $u - v = 0$, so $u = v \in A_n \cap A_m = \{0\}$.
Thus f is injective.
On the other hand, if $a \in A$, let $\alpha m + \beta n = 1$ as before. Write $u = \alpha \cdot ma \in A_n$, $v = -\beta \cdot na \in A_m$. Then

$$f((u,v)) = \alpha \cdot ma - (-\beta \cdot na) = (\alpha m + \beta n)a = a,$$

so f is surjective as well. Thus f is an isomorphism. □

Proof of Proposition, continued

Proof.

Now define $A_n = mA$, $A_m = nA$ (careful!) Inclusion defines a homomorphism

$$f : A_n \times A_m \to A;\ \ f((u,v)) = u - v.$$

Suppose $(u,v) \in \ker f$. Then $u - v = 0$, so $u = v \in A_n \cap A_m = \{0\}$. Thus f is injective.

On the other hand, if $a \in A$, let $\alpha m + \beta n = 1$ as before. Write $u = \alpha \cdot ma \in A_n$, $v = -\beta \cdot na \in A_m$. Then

$$f((u,v)) = \alpha \cdot ma - (-\beta \cdot na) = (\alpha m + \beta n)a = a,$$

so f is surjective as well. Thus f is an isomorphism. □

Proof of Proposition, continued

Proof.

We see that

$$nm = |A| = |A_n| \cdot |A_m|.$$

But we still need to show that $|A_n| = n$ and $|A_m| = m$. It suffices to show that $|A_m|$ and n are relatively prime, because then n divides $nm = |A_n| \cdot |A_m|$ implies n divides $|A_n|$ by Gauss's Lemma; similarly m divides $|A_m|$, so we must have $n = |A_n|$ and $m = |A_m|$.
Thus suppose $p|gcd(|A_m|, n)$. Now we claim that $v \mapsto nv$ is an automorphism of A_m. Indeed, for $v = nb \in A_m$, $mv = mnb = 0$, so

$$\beta nv = \beta n(nb) = \alpha mv + \beta nv = v$$

so that $v \mapsto \beta v$ is the inverse automorphism. Since $p|n$, it follows that for $v \in A_m$, $pv = 0$ only if $v = 0$. □

Proof of Proposition, continued

Proof.

We see that

$$nm = |A| = |A_n| \cdot |A_m|.$$

But we still need to show that $|A_n| = n$ and $|A_m| = m$. It suffices to show that $|A_m|$ and n are relatively prime, because then n divides $nm = |A_n| \cdot |A_m|$ implies n divides $|A_n|$ by Gauss's Lemma; similarly m divides $|A_m|$, so we must have $n = |A_n|$ and $m = |A_m|$.

Thus suppose $p | gcd(|A_m|, n)$. Now we claim that $v \mapsto nv$ is an automorphism of A_m. Indeed, for $v = nb \in A_m$, $mv = mnb = 0$, so

$$\beta nv = \beta n(nb) = \alpha mv + \beta nv = v$$

so that $v \mapsto \beta v$ is the inverse automorphism. Since $p|n$, it follows that for $v \in A_m$, $pv = 0$ only if $v = 0$. □

Proof of Proposition, continued

Proof.

We see that

$$nm = |A| = |A_n| \cdot |A_m|.$$

But we still need to show that $|A_n| = n$ and $|A_m| = m$. It suffices to show that $|A_m|$ and n are relatively prime, because then n divides $nm = |A_n| \cdot |A_m|$ implies n divides $|A_n|$ by Gauss's Lemma; similarly m divides $|A_m|$, so we must have $n = |A_n|$ and $m = |A_m|$.

Thus suppose $p|gcd(|A_m|, n)$. Now we claim that $v \mapsto nv$ is an automorphism of A_m. Indeed, for $v = nb \in A_m$, $mv = mnb = 0$, so

$$\beta nv = \beta n(nb) = \alpha mv + \beta nv = v$$

so that $v \mapsto \beta v$ is the inverse automorphism. Since $p|n$, it follows that for $v \in A_m$, $pv = 0$ only if $v = 0$. □

Proof of Proposition, continued

Proof.

We see that

$$nm = |A| = |A_n| \cdot |A_m|.$$

But we still need to show that $|A_n| = n$ and $|A_m| = m$. It suffices to show that $|A_m|$ and n are relatively prime, because then n divides $nm = |A_n| \cdot |A_m|$ implies n divides $|A_n|$ by Gauss's Lemma; similarly m divides $|A_m|$, so we must have $n = |A_n|$ and $m = |A_m|$.
Thus suppose $p|gcd(|A_m|, n)$. Now we claim that $v \mapsto nv$ is an automorphism of A_m. Indeed, for $v = nb \in A_m$, $mv = mnb = 0$, so

$$\beta nv = \beta n(nb) = \alpha mv + \beta nv = v$$

so that $v \mapsto \beta v$ is the inverse automorphism. Since $p|n$, it follows that for $v \in A_m$, $pv = 0$ only if $v = 0$. □

A key lemma

So p is an automorphism of $|A_m|$ but p divides the order of A_m. We pause for a key lemma:

Lemma

Let B be a finite abelian group of order divisible by p. Then B contains a non-zero element of order p.

This Lemma contradicts the earlier conclusion that $pv = 0 \Rightarrow v = 0$. So the Lemma completes the proof of the Proposition.

The Lemma is true even if B is not abelian, and will be proved later. So it can be skipped for now.

A key lemma

So p is an automorphism of $|A_m|$ but p divides the order of A_m. We pause for a key lemma:

Lemma

Let B be a finite abelian group of order divisible by p. Then B contains a non-zero element of order p.

This Lemma contradicts the earlier conclusion that $pv = 0 \Rightarrow v = 0$. So the Lemma completes the proof of the Proposition.

The Lemma is true even if B is not abelian, and will be proved later. So it can be skipped for now.

A key lemma

So p is an automorphism of $|A_m|$ but p divides the order of A_m. We pause for a key lemma:

Lemma

Let B be a finite abelian group of order divisible by p. Then B contains a non-zero element of order p.

This Lemma contradicts the earlier conclusion that $pv = 0 \Rightarrow v = 0$. So the Lemma completes the proof of the Proposition.

The Lemma is true even if B is not abelian, and will be proved later. So it can be skipped for now.

A key lemma

So p is an automorphism of $|A_m|$ but p divides the order of A_m. We pause for a key lemma:

Lemma

Let B be a finite abelian group of order divisible by p. Then B contains a non-zero element of order p.

This Lemma contradicts the earlier conclusion that $pv = 0 \Rightarrow v = 0$. So the Lemma completes the proof of the Proposition.

The Lemma is true even if B is not abelian, and will be proved later. So it can be skipped for now.

A key lemma

So p is an automorphism of $|A_m|$ but p divides the order of A_m. We pause for a key lemma:

Lemma

Let B be a finite abelian group of order divisible by p. Then B contains a non-zero element of order p.

This Lemma contradicts the earlier conclusion that $pv = 0 \Rightarrow v = 0$. So the Lemma completes the proof of the Proposition.

The Lemma is true even if B is not abelian, and will be proved later. So it can be skipped for now.

Proof of the key lemma

Proof.

This is again an inductive proof. Say $|B| = pN$. If $N = 1$ then B is cyclic of order p and we know the result. Suppose we know the result for all $|B|$ of order pk with $k < N$. If B has no nontrivial proper subgroup, then B is cyclic of prime order; so B must have a proper subgroup $H \subsetneq B$, $|H| > 1$. If p divides $|H|$ then by induction H has a non-zero element of order p, and we are done. So assume p does not divide $r = |H|$. Since

$$p \,|\, |B| = |H||B/H| = r \cdot |B/H|$$

and p does not divide r, it follows that $p \,|\, |B/H|$. Since $|B/H| < |B|$, the induction step implies there is $g \in B/H$ of order p. □

Proof of the key lemma

Proof.

This is again an inductive proof. Say $|B| = pN$. If $N = 1$ then B is cyclic of order p and we know the result. Suppose we know the result for all $|B|$ of order pk with $k < N$. If B has no nontrivial proper subgroup, then B is cyclic of prime order; so B must have a proper subgroup $H \subsetneq B$, $|H| > 1$. If p divides $|H|$ then by induction H has a non-zero element of order p, and we are done. So assume p does not divide $r = |H|$. Since

$$p \mid |B| = |H||B/H| = r \cdot |B/H|$$

and p does not divide r, it follows that $p \mid |B/H|$. Since $|B/H| < |B|$, the induction step implies there is $g \in B/H$ of order p. □

Proof of the key lemma

Proof.

This is again an inductive proof. Say $|B| = pN$. If $N = 1$ then B is cyclic of order p and we know the result. Suppose we know the result for all $|B|$ of order pk with $k < N$. If B has no nontrivial proper subgroup, then B is cyclic of prime order; so B must have a proper subgroup $H \subsetneq B$, $|H| > 1$. If p divides $|H|$ then by induction H has a non-zero element of order p, and we are done. So assume p does not divide $r = |H|$. Since

$$p||B| = |H||B/H| = r \cdot |B/H|$$

and p does not divide r, it follows that $p||B/H|$. Since $|B/H| < |B|$, the induction step implies there is $g \in B/H$ of order p.

Proof of the key lemma

Proof.

This is again an inductive proof. Say $|B| = pN$. If $N = 1$ then B is cyclic of order p and we know the result. Suppose we know the result for all $|B|$ of order pk with $k < N$. If B has no nontrivial proper subgroup, then B is cyclic of prime order; so B must have a proper subgroup $H \subsetneq B$, $|H| > 1$. If p divides $|H|$ then by induction H has a non-zero element of order p, and we are done. So assume p does not divide $r = |H|$. Since

$$p \,|\, |B| = |H||B/H| = r \cdot |B/H|$$

and p does not divide r, it follows that $p \,|\, |B/H|$. Since $|B/H| < |B|$, the induction step implies there is $g \in B/H$ of order p. □

Proof of the key lemma

Proof.

Let $\pi : B \to B/H$ be the quotient map, $\pi(b) = g \in B/H$. Thus $b \notin H$ but $\pi(pb) = pg = 0$, so $pb \in H$, so $rpb = 0$. Let $a = rb$, so $pa = 0$. We suppose $a = 0$ and derive a contradiction. Use Bezout's relation yet again. Since $(p, r) = 1$ there are integers γ, δ such that

$$b = (\gamma p + \delta r)b = \gamma pb + \delta a = \gamma pb + 0 \in H,$$

contradiction. □

Proof of the key lemma

Proof.

Let $\pi : B \to B/H$ be the quotient map, $\pi(b) = g \in B/H$. Thus $b \notin H$ but $\pi(pb) = pg = 0$, so $pb \in H$, so $rpb = 0$. Let $a = rb$, so $pa = 0$. We suppose $a = 0$ and derive a contradiction. Use Bezout's relation yet again. Since $(p, r) = 1$ there are integers γ, δ such that

$$b = (\gamma p + \delta r)b = \gamma pb + \delta a = \gamma pb + 0 \in H,$$

contradiction. □

Proof of the key lemma

Proof.

Let $\pi : B \to B/H$ be the quotient map, $\pi(b) = g \in B/H$. Thus $b \notin H$ but $\pi(pb) = pg = 0$, so $pb \in H$, so $rpb = 0$. Let $a = rb$, so $pa = 0$. We suppose $a = 0$ and derive a contradiction. Use Bezout's relation yet again. Since $(p, r) = 1$ there are integers γ, δ such that

$$b = (\gamma p + \delta r)b = \gamma pb + \delta a = \gamma pb + 0 \in H,$$

contradiction.

□

The general case

Corollary

Suppose A is an abelian group of order $\prod_{i=1}^{r} m_i$, where $(m_i, m_j) = 1$ whenever $i \neq j$. Then there are subgroups A_{m_i}, $i = 1, \ldots, r \subseteq A$ such that $|A_{m_i}| = m_i$, and such that the inclusion defines an isomorphism

$$A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r} \xrightarrow{\sim} A.$$

Proof.

We complete the proof by induction on n. Write $M = \prod_{i=1}^{n-1} m_i$, so that $|A| = M \cdot m_i$. By the Proposition we have an isomorphism

$$A_M \times A_{m_r} \xrightarrow{\sim} A.$$

Now apply the induction step to write $A_M \xrightarrow{\sim} \prod_{i=1}^{r-1} A_{m_i}$. So

$$A \xrightarrow{\sim} A_M \times A_{m_r} \xrightarrow{\sim} A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r}.$$

The general case

Corollary

Suppose A is an abelian group of order $\prod_{i=1}^{r} m_i$, where $(m_i, m_j) = 1$ whenever $i \neq j$. Then there are subgroups A_{m_i}, $i = 1, \ldots, r \subseteq A$ such that $|A_{m_i}| = m_i$, and such that the inclusion defines an isomorphism

$$A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r} \xrightarrow{\sim} A.$$

Proof.

We complete the proof by induction on n. Write $M = \prod_{i=1}^{n-1} m_i$, so that $|A| = M \cdot m_i$. By the Proposition we have an isomorphism

$$A_M \times A_{m_r} \xrightarrow{\sim} A.$$

Now apply the induction step to write $A_M \xrightarrow{\sim} \prod_{i=1}^{r-1} A_{m_i}$. So

$$A \xrightarrow{\sim} A_M \times A_{m_r} \xrightarrow{\sim} A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r}.$$

The general case

Corollary

Suppose A is an abelian group of order $\prod_{i=1}^{r} m_i$*, where* $(m_i, m_j) = 1$ *whenever* $i \neq j$*. Then there are subgroups* A_{m_i}*,* $i = 1, \dots, r \subseteq A$ *such that* $|A_{m_i}| = m_i$*, and such that the inclusion defines an isomorphism*

$$A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r} \xrightarrow{\sim} A.$$

Proof.

We complete the proof by induction on n. Write $M = \prod_{i=1}^{n-1} m_i$, so that $|A| = M \cdot m_i$. By the Proposition we have an isomorphism

$$A_M \times A_{m_r} \xrightarrow{\sim} A.$$

Now apply the induction step to write $A_M \xrightarrow{\sim} \prod_{i=1}^{r-1} A_{m_i}$. So

$$A \xrightarrow{\sim} A_M \times A_{m_r} \xrightarrow{\sim} A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r}.$$

The general case

Corollary

Suppose A is an abelian group of order $\prod_{i=1}^{r} m_i$, where $(m_i, m_j) = 1$ whenever $i \neq j$. Then there are subgroups A_{m_i}, $i = 1, \ldots, r \subseteq A$ such that $|A_{m_i}| = m_i$, and such that the inclusion defines an isomorphism

$$A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r} \xrightarrow{\sim} A.$$

Proof.

We complete the proof by induction on n. Write $M = \prod_{i=1}^{n-1} m_i$, so that $|A| = M \cdot m_i$. By the Proposition we have an isomorphism

$$A_M \times A_{m_r} \xrightarrow{\sim} A.$$

Now apply the induction step to write $A_M \xrightarrow{\sim} \prod_{i=1}^{r-1} A_{m_i}$. So

$$A \xrightarrow{\sim} A_M \times A_{m_r} \xrightarrow{\sim} A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r}.$$

The general case

Corollary

Suppose A is an abelian group of order $\prod_{i=1}^{r} m_i$, where $(m_i, m_j) = 1$ whenever $i \neq j$. Then there are subgroups A_{m_i}, $i = 1, \ldots, r \subseteq A$ such that $|A_{m_i}| = m_i$, and such that the inclusion defines an isomorphism

$$A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r} \xrightarrow{\sim} A.$$

Proof.

We complete the proof by induction on n. Write $M = \prod_{i=1}^{n-1} m_i$, so that $|A| = M \cdot m_i$. By the Proposition we have an isomorphism

$$A_M \times A_{m_r} \xrightarrow{\sim} A.$$

Now apply the induction step to write $A_M \xrightarrow{\sim} \prod_{i=1}^{r-1} A_{m_i}$. So

$$A \xrightarrow{\sim} A_M \times A_{m_r} \xrightarrow{\sim} A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r}.$$

Completion of the proof of Theorem 1

Recall the statement: Let A be a finite abelian group. Let $q_1, \ldots, q_r$ be the distinct primes dividing $|A|$, and say

$$|A| = \prod_j q_j^{b_j}.$$

Then there are subgroups $A_j \subseteq A, j = 1, \ldots, r$, with $|A_j| = q_j^{b_j}$, and an isomorphism

$$A \xrightarrow{\sim} A_1 \times A_2 \times \cdots \times A_r.$$

Write $m_j = q_j^{b_j}, j = 1, \ldots, r$. Then $(m_j, m_i) = 1$ whenever $i \neq j$. We apply the Corollary. Thus there are subgroups $A_{m_j}, j = 1, \ldots, r$, with $|A_{m_j}| = m_j = q_j^{b_j}$, such that

$$A \xrightarrow{\sim} A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r}.$$

Set $A_j = A_{m_j}$ and we are done.

Completion of the proof of Theorem 1

Recall the statement: Let A be a finite abelian group. Let $q_1, \ldots, q_r$ be the distinct primes dividing $|A|$, and say

$$|A| = \prod_j q_j^{b_j}.$$

Then there are subgroups $A_j \subseteq A$, $j = 1, \ldots, r$, with $|A_j| = q_j^{b_j}$, and an isomorphism

$$A \xrightarrow{\sim} A_1 \times A_2 \times \cdots \times A_r.$$

Write $m_j = q_j^{b_j}$, $j = 1, \ldots, r$. Then $(m_j, m_i) = 1$ whenever $i \neq j$. We apply the Corollary. Thus there are subgroups A_{m_j}, $j = 1, \ldots, r$, with $|A_{m_j}| = m_j = q_j^{b_j}$, such that

$$A \xrightarrow{\sim} A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r}.$$

Set $A_j = A_{m_j}$ and we are done.

Completion of the proof of Theorem 1

Recall the statement: Let A be a finite abelian group. Let $q_1, \ldots, q_r$ be the distinct primes dividing $|A|$, and say

$$|A| = \prod_j q_j^{b_j}.$$

Then there are subgroups $A_j \subseteq A$, $j = 1, \ldots, r$, with $|A_j| = q_j^{b_j}$, and an isomorphism

$$A \xrightarrow{\sim} A_1 \times A_2 \times \cdots \times A_r.$$

Write $m_j = q_j^{b_j}$, $j = 1, \ldots, r$. Then $(m_j, m_i) = 1$ whenever $i \neq j$. We apply the Corollary. Thus there are subgroups A_{m_j}, $j = 1, \ldots, r$, with $|A_{m_j}| = m_j = q_j^{b_j}$, such that

$$A \xrightarrow{\sim} A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r}.$$

Set $A_j = A_{m_j}$ and we are done.

Completion of the proof of Theorem 1

Recall the statement: Let A be a finite abelian group. Let $q_1, \ldots, q_r$ be the distinct primes dividing $|A|$, and say

$$|A| = \prod_j q_j^{b_j}.$$

Then there are subgroups $A_j \subseteq A$, $j = 1, \ldots, r$, with $|A_j| = q_j^{b_j}$, and an isomorphism

$$A \xrightarrow{\sim} A_1 \times A_2 \times \cdots \times A_r.$$

Write $m_j = q_j^{b_j}$, $j = 1, \ldots, r$. Then $(m_j, m_i) = 1$ whenever $i \neq j$. We apply the Corollary. Thus there are subgroups A_{m_j}, $j = 1, \ldots, r$, with $|A_{m_j}| = m_j = q_j^{b_j}$, such that

$$A \xrightarrow{\sim} A_{m_1} \times A_{m_2} \times \cdots \times A_{m_r}.$$

Set $A_j = A_{m_j}$ and we are done.