Euler Circle

Albert Ye

May 6, 2020

§1 Week 1

§1.1 Solutions

A few interesting problems I've done:

2) (needed for 20) We know that $gH(gh)^{-1} = e = geg^{-1} = ghh^{-1}g^{-1} = gh(h^{-1}g^{-1})$. So $(gh)^{-1} = h^{-1}g^{-1}$. ■

6) Let us start at a complex value z. $\rho\tau$ is adding x and taking the negative of the value $z + x$. $\tau\rho^{-1}$ is taking the negative of z and subtracting x. Both outcomes lead to $-z - x$. ■

8) By definition, μ_n is a root of unity. The rest follows trivially. ■

11) Translations and glide reflections cannot work because they move the point irreparably away from the origin. For rotations, any rotation across a center $\neq (0, 0)$ will bring the point out of the origin. The center must be $(0, 0)$ and the angle can be anything. For reflections, any line that does not intersect $(0, 0)$ will take the point out of the origin, so only lines going through $(0, 0)$ can work.

20) We can just let τ be τ because $\tau^2 = e$. For ρ, we note that any rotation is a composition of two non-parallel lines. Hence, ρ can be expressed as two reflections, each of which can be reversed in one step. ■

21) We know from (2) that $gh = (gh)^{-1} = h^{-1}g^{-1} = hg$. ■

22) Fix two elements a, b in G. Assume that $ab \neq ba$. Then there are at best 5 elements a, b, ab, ba, e. However, we are given that G is order 4, contradiction. ■

23) Every element must have an inverse by definition of group. Because G is a group, all of the elements not with order 2 have some other inverse in the group. Commutativity allows us to pair up each element with its inverse. Hence, all that remains are the ones who only have inverses as themselves because they were only counted once – the rest all turned into identity.

For Wilson's, substitute $\mathbb{Z}/p\mathbb{Z}$ as G with multiplication as the operation. $(p-1)!$ is the product of all numbers $1 \cdots p-1$. Everything cancels out except for the ones with inverse as themself, namely 1 and $p-1$. Hence, the residue is -1. ■

§2 Week 2

§2.1 Notes

§2.1.1 Subgroup

Definition 2.1. Let G be a group. A nonempty subset H of G is a **subgroup** of G if

- $h_1, h_2 \in H \implies h_1 h_2 \in H$

- $h \in H \implies h^{-1} \in H$

If H is a subgroup of G we denote $H \leq G$.

Here is another way to create groups from groups:

§2.1.2 Direct Product

Definition 2.2. Let G, H be groups. Let their direct product $G \times H$ whose set is $\{(g,h) \forall g \in G, h \in H\}$ and whose operation is $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

§2.1.3 Homomorphism

Definition 2.3. Let G, H be groups. A **homomorphism** is a function $f : G \to H$ s.t. $f(g_1 g_2) = f(g_1) f(g_2)$.

Homomorphisms must *always* exist. Just see $f(g) = e_H \forall g \in G$.

Proposition 2.4

Let $f : G \to H$ be a homomorphism between groups G, H.

- $f(e_G) = e_H$
- $f(g^{-1}) = f(g)^{-1}$.
- order of $g \in G$ is $n \implies$ order of $f(g) \in H$ is *at most* n.

Proof. 1) $f(e_G) = f(e_G e_G) = f(e_G) f(e_G) \implies e_H = f(e_G)$
2) $e_H = f(e_G) = f(g g^{-1}) = f(g) f(g^{-1})$. Multiply by $f(g^{-1})$ to get the desired.
3) Let $g^n = e$. Then $e_H = f(e_G) = f(g^n) = f(g)^n$. This only shows that $f(g)$ has order $\leq n$. Just see the trivial homomorphism. □

Definition 2.5. Let $f : G \to H$ be a homomorphism.

- The **kernel** of f is the set of elements in G s.t. $f(g) = e_H$.
- The **image** of f is the set of elements in H that take on a value of $f(g)$ for some $g \in G$.

Definition 2.6. We call $f : X \to Y$:

- *injective* if $a = b \implies f(a) = f(b) \forall a, b \in X$.
- *surjective* if Y is the image of f.

Proposition 2.7

We claim that

- Kernels and images are subgroups.
- f is injective iff the kernel of f is $\{e_G\}$.
- Something else true by definition.

§2.1.4 Isomorphisms

Definition 2.8. An **isomorphism** is a bijective homomorphism.

Example: $f : \mathbb{R} \to (\mathbb{R}_{>0}, \times), f(x) = e^x$.

Definition 2.9. An **automorphism** is the isomorphism $f : G \to G$.

Isomorphisms and automorphisms are homomorphisms.

Proposition 2.10
For any $h \in G$, the map $\phi_h : G \to G$ given by $\phi_h(g) = hgh^{-1}$ is an automorphism. Such automorphisms are called **inner automorphisms**.

Definition 2.11. The **conjugate** of g by h is $hgh^{-1} \in G$. The **conjugacy class** is the set of all such conjugates.

§2.1.5 Group Actions

Groups should be looked at as movements.

Definition 2.12. Let X be a set, G a group. (X can be any set.) A **left action** of G on X is a function $f : G \times X \to X$ s.t.

- $ex = x \forall x \in X$
- $(g_1 g_2)x = g_1(g_2 x) \forall g_1, g_2 \in G, x \in X$

A **right action** is defined similarly, as $X \times G = X$.

Definition 2.13. Alternatively, each $g \in G$ gives a permutation of the elements of X, i.e. an element of S_X. A **group action** is a homomorphism $f : G \to S_X$.

Important:

- All groups act on themselves with left multiplication
- G acts on itself by conjugation on $G \times X : X$

Theorem 2.14 (Cayley's Theorem)
Any finite group is isomorphic to a subgroup of S_n for some positive integer n.

This looks nice, but is really inefficient. $|S_n|$ is literally factorial time!
To prevent collapsing elements into one x value, we define

Definition 2.15. A group action $G \to x$ is **faithful** if whenever $gx = x \forall x \in X$, then $g = e$.

Conjugation is not necessarily faithful, as if $g \in Z(G)$, then $gx = x$.

Definition 2.16. A group action G on X is **transitive** if $\forall x, y \in X$, there exists $g \in G$ s.t. $gx = y$.

§2.2 Homework

Problem 2.17 (1)**.** Show that if G and H are finite groups, and $G \cong H$, then $|G| = |H|$. Find an example to show that the converse is false.

Solution. We know that this is true by definition, as G and H are bijective. Each element of G must map to an element of H.

The two groups $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ do not fit. We cannot generate the element 3 from the elements of 1, because we can sum to at most 1. ■

Problem 2.18 (2)**.** Show that $G \times H \cong H \times G$

Solution. For $G \times H$, all of the elements of G and H are paired to each other with G as the first element. For $H \times G$, the same elements exist but with G as the second element instead. Thus, we can map each element of $G \times H$ to each element of $H \times G$ by flipping the order. ■

Problem 2.19 (3)**.** Show that if $H, K \leq G$, then

- $H \cap K \leq G$.
- $H \cup K$ is not necessarily a subgroup of G.

Solution. For part 1, all we need is proof of closure. If $H \cap K$ is not closed, then it implies that H or K is also not closed.
FOR part 2, some element in $H \cup K$ could not also be in $H \cup K$. There are many such subgroups of $G = S_3$. ■

Problem 2.20 (4)**.** When is the function $f : G \to G$ given by $f(g) = g^2$ a homomorphism?

Solution. $f(g_1g_2) = g_1g_2g_1g_2$. We want it of the form $f(g_1g_2) = g_1g_1g_2g_2$, which can be attained iff $g_1g_2 = g_2g_1$, implying G must be abelian. ■

Problem 2.21 (5)**.** We showed that if $f : G \to H$ is a homomorphism, and $g \in G$ has order n, then $f(g) \in H$ has order $\leq n$. Show that the order of $f(g)$ divides n.

Solution. We saw from our proof that the order of $f(g) \in H$ had order $\leq n$ that $f(g)^n = f(e_G) = e_H$. If $ord(f(g)) \nmid n$, then this cannot be true. ■

Problem 2.22 (6)**.** Is every subgroup of $G_1 \times G_2$ necessarily of the form $H_1 \times H_2$, where $H_1 \leq G_1$ and $H_2 \leq G_2$? Give a proof or find a counterexample.

Solution. We claim that this is **not** necessarily true. Note that $\{(0,0),(1,1)\}$ is a subgroup. All properties of a group but closure are inherited from $\mathbb{Z}/2\mathbb{Z}$. This is also closed. However, it is not a direct product of any other subgroups of $\mathbb{Z}/2\mathbb{Z}$ ■

Problem 2.23 (11)**.** Show that $\mathrm{Aut}(G)$ is a group. Show that $\mathrm{Inn}(G) \leq \mathrm{Aut}(G)$. (the operation is $\circ$).

Solution. As all automorphisms are bijective functions, we only need to prove closure. However, even this is true, as the composition of two bijective functions is itself bijective.

Next, we prove that an inner automorphism is a group. We know that an inner automorphism is already a **subset** of the group of automorphisms. Again, everything except closure is inherited from the group of automorphisms. But for closure, we have that

$$(\phi_h \circ \phi_k)(g) = (\phi_h(\phi_k(g)) = \phi_h(kgk^{-1}) = h(kgk^{-1})h^{-1} = \phi_{hk}(g).$$

■

Definition 2.24. The **alternating group** A_n is the group of permutations with an even number of swaps.

Problem 2.25 (15)**.** Prove that A_n is a group.

Solution. The identity and invertibility axioms are trivial.

We claim A_n is associative. Let s_1, s_2, s_3 be permutations. Then

$$(s_1 \circ s_2)(s_3) = (s_1)(s_2 \circ s_3) \implies s_1(s_2(s_3(x))) = s_1(s_2(s_3(x))).$$

Finally, we claim A_n is closed. This is obvious, as the composition of two permutations with an even number of swaps cannot have an odd number of swaps. ■

Problem 2.26 (23)**.** Consider a pentagon together with all its diagonals. Show that, up to switching the colors, there are 6 ways of coloring the edges and diagonals of the pentagon red and blue, so that the red edges form a cycle of length 5, and the blue edges also form a cycle of length 5. Call these colorings the *mystic pentagons*.

Solution. We fix the first point P. We know that the number of red cycles is $4 \cdot 3 \cdot 2 \cdot 1 = 24$ if we fix P. However, this graph is undirected, and our count is directed as we cared about direction. Each cycle was traversed forward and backward, so we divide by 2.
It is well known that each such red cycle has a blue complementary cycle. However, we are again double counting because simply flipping the colors is given to be identical. Thus, we divide by 2 again to get 6. ■

Problem 2.27 (24)**.** Show that there is a homomorphism $\phi : S_5 \to S_6$, obtained by permuting the vertices of the mystic pentagons. Show that $\ker(\phi) = \{e\}$.

Solution. The group S_5 acts on the set of permutations described in the previous problem. Thus, we have $\phi : S_5 \to S_6$, each $\sigma \in S_5$ giving a different permutation of the vertices and a grouping of the edges. There are 6 edges to choose from, thus that is equivalent to permuting 6 things. Hence, we have S_6.
The second claim is equivalent to claiming ϕ is injective. Every element in S_5 gives a different permutation of the vertices. However, each cycle has 5 ways to configure it. We could partition the edges the same way and just cyclic shift the vertices. However, there are six cycles to choose from, ensuring that each different configuration has a match in a different cycle. Therefore, ϕ must be injective. ■

§3 Week 3

§3.1 Notes

§3.1.1 Cosets

Definition 3.1. Let G be a group, H a subgroup of G. Then the **left coset** is $gH = \{gh | h \in H\}$ and the **right coset** is $Hg = \{gh | h \in H\}$. The two are not equal.

Example: Let $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$. Then $H \leq G$ and there are three distinct cosets, namely $H, 1 + H, 2 + H$.

Example: Let G be a group acting on a set X and let $x \in X$. Let G_x be the stabilizer of x, i.e. $G_x = \{g \in G | gx = x\}$. The left cosets of G_x are in bijection with the orbit of x.

Proposition 3.2

Let G be a group and $H \leq G$. Let g_1H, g_2H be cosets. Then either $g_1H = g_2H$ or $g_1H \cap g_2H = \{\}$.

Proof. Suppose $g_1H \cap g_2H \neq \varnothing$, so there is some $x \in g_1H \cap g_2H$. Thus there exist $h_1, h_2 \in H$ such that $x = g_1h_1$ and $x = g_2h_2$. THus $g_1h_1 = g_2h_2$, so $g_1 = g_2h_2h_1^{-1}$. If $g_1h \in g_1H$, then $g_1h = g_2h_2h_1^{-1}h \in g_2H$. Thus $g_1H \subseteq g_2H$.

By symmetry $g_2H \subseteq g_1H$ as well, so $g_1H = g_2H$. □

Proposition 3.3

$g_1H = g_2H \iff g_1^{-1}g_2 = H$.

Proof. Since $e \in H$, $g_2 \in g_2H$. THus $g_1H = g_2H \iff g_2 \in g_1H$ or $g_1^{-1}g_2 \in H$. Consider cosets $k + 3\mathbb{Z}$ and $l + 3\mathbb{Z}$. These are equal iff $-k + l \in 3\mathbb{Z}$. □

Proposition 3.4

Corollary: Let G be a finite group and $H \leq G$. Then any two cosets of H in G have the same size.

Proof. Let g_1H and g_2H be two cosets. We find a bijection $\phi : g_1H \to g_2H$. We define ϕ by $\phi(g_1h) = g_2h$. To see this is a bijection, we add the inverse $\psi : g_2H \to g_1H$ s.t. $\psi(g_2h) = g_1h$. It's easy to see that ϕ and ψ are inverses. □

§3.1.2 Lagrange's Thm.

Theorem 3.5 (Lagrange)

Let G be a finite group of order n, and let $H \leq G$ have order m. Then $m|n$.

Proof. WE partition G into several subsets, each of size m. The natural partition is simply the cosets of H. These each have size m and they are disjoint. Their union is G, which has size n. Thus $m|n$. □

Corollary 3.6

The order of any element of G divides the order of G.

Proof. Let $g \in G$ be any element, and let H be the subgroup generated by G. Then apply Lagrange on G, H. □

Theorem 3.7 (Fermat's Little Theorem)
Let p be a prime and let $p \nmid a, a \in \mathbb{Z}$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. The nonzero elements of $\mathbb{Z}/p\mathbb{Z}$ form a group $(\mathbb{Z}/p\mathbb{Z}^\times$ of order $p-1$. Since $p \nmid a$, it's represented by some elements of $\mathbb{Z}/p\mathbb{Z}^\times$, say b. Let m be the order of b in $\mathbb{Z}/p\mathbb{Z}^\times$. We know that $m|p-1$, so $b^{p-1} = e$ in $\mathbb{Z}/p\mathbb{Z}^\times$, which means that $a^{p-1} \equiv 1 \pmod{p}$. $\square$

§3.2 Homework

Problem 3.8 (1)**.** Show that for $n \geq 2$, $|A_n| = \frac{n!}{2}$.

Solution. As $S_n = n!$, we are motivated to show that there is some homomorphism $f : A_n \to B_n$, where B_n is the *set* containing all permutation with an odd number of transpositions. Let τ be some transposition. Then obviously $f(\sigma) = \tau\sigma \in B_n$. ■

Problem 3.9 (2)**.** Describe the groups $\mathbb{Q}/\mathbb{Z}$ and $\mathbb{R}/\mathbb{Q}$ as well as you can.

Solution. We know that both groups are quotient groups as $\mathbb{Q}$ and $\mathbb{R}$ are abelian and $\mathbb{Q}, \mathbb{R}, \mathbb{Z}$ are all groups.

The group $\mathbb{Q}/\mathbb{Z}$ consists of $\{\dots, -1+q, q, 1+q, 2+q, \dots\}$ for $q \in \mathbb{Q}$. The group $\mathbb{R}/\mathbb{Z}$ is similar, but for all rationals and reals as opposed to integers and rationals. ■

Problem 3.10 (3)**.** Suppose that $H, K \lhd G$, and that $H \cap K = \{e\}$. Show that if $h \in H$ and $k \in K$, then h and k commute.

Solution. We know that $g^{-1}hg \in H, g^{-1}kg \in K$ for $g \in G, h \in H, k \in K$. We take advantage of the fact that K, H are subgroups of G.

It must be true that $h \cdot (kh^{-1}k^{-1} \in H$, and it must be true that $(hkh^{-1}) \cdot k^{-1} \in K$. This implies that

$$\begin{aligned} & hkh^{-1}k^{-1} \in H \cap K \\ \implies & hkh^{-1}k^{-1} = e \\ \implies & hkh^{-1}k^{-1} = e = hh^{-1}kk^{-1}. \end{aligned}$$

So h, k commute. ■

Problem 3.11 (5)**.** Suppose $K \lhd H$ and $H \lhd G$. Then K is a subgroup of G. Is it necessarily normal? Prove or give a counterexample.

Solution. We claim this is not necessarily true. Consider subset $A = \{(12)(34), e\}$ and $B = \{(12)(34), (13)(42), (23)(41), e\}$. $A \lhd B$ and $B \lhd S$, but A is not normal to S. ■

Problem 3.12 (6)**.** The *commutator subgroup* $[G, G]$ of G is the subgroup generated by all elements of the form $[g, h] := ghg^{-1}h^{-1}$. (So, it contains all products of elements of the form $[g, h]$.) Show that $[G, G] \lhd G$, and that $G/[G, G]$ is abelian.

Solution. Let $g \in G, h \in [G, G]$. We know that $ghg^{-1} = (ghg^{-1})(h^{-1}h) = [g, h]h \in [G, G]$. Hence, $[G, G] \lhd G$.

For commutivity, we have

$$(a[G, G])(b[G, G]) = ab[G, G] = ab[b, a][G, G] = ba[G, G] = (b[G, G])(a[G, G]).$$

■

§4 Week 4

§4.1 Homework

Problem 4.1 (1)**.** Show that there is an injective homomorphism $f : S_m \times S_n \to S_{m+n}$.

Solution. Note that we have a pair containing some permutation of $1 \cdots m$ and some permutation of $1 \cdots n$. We can add $m-1$ to all elements on the right side (permutation of $1 \cdots n$) to get some unique permutation of $1 \cdots m+n$.
Now we know that f is an injective function. Now we claim it is a homomorphism. $f(ab) = f(a \circ b)$. Because a, b are permutations, we know that $f(a \circ b) = f(a) \circ f(b)$. ■

Problem 4.2 (4)**.** Prove $N_G(H) \leq G$, and that it is the largest subgroup K such that $H \lhd K$.

Solution. We only need to prove that $N_G(H)$ is a group.
Identity. $eHe^{-1} = H$ is obviously true, so the identity is in $N_G(H)$.
Associativity. This is inherited from G.
Invertability. Assume $g \in N_G(H)$. Then, $g^{-1}Hg = g^{-1}(gHg^{-1})g = eHe = H$.
Closure. Let $g, h \in N_G(H)$. We know that $H = gHg^{-1} = g(hHh^{-1})g^{-1} = (gh)H(h^{-1}g^{-1}) = (gh)H(gh)^{-1}$, so $N_G(H)$ is closed.
As $N_G(H)$ meets all the criteria of a group, it must be one. Now we claim it's the largest subgroup of G K such that $H \lhd K$. Assume there is some value of g such that $gHg^{-1} = H$, but g is not in $N_G(H)$. We have a contradiction, as by definition of $N_G(H)$ it must be in $N_G(H)$. ■

Problem 4.3 (7)**.** Show that a Sylow-2 subgroup of A_4 is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Solution. First note that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = H$ is composed of only elements e, a, b, ab, and that all non-identity elements have order 2. Also note that a $|A_4| = 12$, so a Sylow-2 subgroup of A_4 must have order 4.
We choose the subgroup $G = \{e, (12)(34), (13)(24), (14)(23)\}$. G must be associative and all elements are their own inverses. All that is left is closure. There are only 6 pairs to test out, and all lead to some other element. But more importantly, every two non-identity elements produces the third by composition. This can also be easily verified. Therefore, G is a group, and it is also of the form $\{e, a, b, ab\}$. Hence, we can make an isomorphism between the two. ■

§5 Week 5

Problem 5.1 (9)**.** The numbers in the sequence 101, 104, 109, 116,... are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \ldots$. For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.

Solution. This is essentially an exercise in the Euclidean algorithm.

$$\begin{aligned}\gcd(100+n^2, 100+(n+1)^2) &= \gcd(100+n^2, 100+n^2+2n+1)\\ &= \gcd(100+n^2, 2n+1)\\ &= \gcd(n^2+100-100(2n+1), 2n+1) \quad = \gcd(n^2-200n, 2n+1).\end{aligned}$$

As $\gcd(n, 2n+1) = 1$, we solely need $\gcd(n-200, 2n+1) = \gcd(n-200, 401)$. Therefore, we have that the maximal gcd is $\boxed{401}$. ■

Problem 5.2 (12)**.** Prove that for each positive integer n, there are pairwise relatively prime integers $k_0, k_1 \ldots, k_n$, all strictly greater than 1, such that $k_0 k_1 \cdots k_n - 1$ is the product of two consecutive integers.

Solution. We use induction. Note that for $n = 0$, setting $k_0 = 3$ leads to $k_0 - 1 = 1 \cdot 2$. For $n = 1$, setting $k_0 = 3, k_1 = 7$ leads to $k_0 k_1 - 1 = 4 \cdot 5$. And for $n = 2$, setting $k_0 = 3, k_1 = 7, k_2 = 31$ leads to $k_0 k_1 k_2 - 1 = 25 \cdot 26$.
For the induction, we claim that if $k_0 k_1 \ldots k_n = a^2 + a + 1$, then $k_{n+1}(a^2 + a + 1) = (a+1)^4 + (a+1)^2 + 1$, where k_{n+1} is some integer relatively prime to all $k_i \forall i \in \{0, 1, \cdots, n\}$.
First, we claim that $k_{n+1} = \dfrac{(a+1)^4 + (a+1)^2 + 1}{a^2 + a + 1}$ is always an integer. But dividing gives us $k_{n+1} = a^2 + 3a + 3$, which is always an integer as a is always an integer.
Next, we claim that $\gcd(k_0, k_1, \ldots, k_n, k_{n+1}) = 1$ – in other words, all k_i are relatively prime for $i \in \{0, 1, \ldots, n-1\}$. We just use the Euclidean Algorithm. This is equivalent to $\gcd(k_0 k_1 \cdots k_n, k_{n+1}) = 1$.

$$\begin{aligned} & \gcd(k_{n+1}, k_0 k_1 \cdots k_n) = 1 \\ \implies & \gcd(a^2 + 3a + 3, a^2 + a + 1) = 1 \\ \implies & \gcd(2a + 2, a^2 + a + 1) = 1 \\ \implies & \gcd(2(a+1), a(a+1) + 1) = 1, \end{aligned}$$

which must be true. Hence, k_{n+1} is relatively prime to all other k_i, and we are done. ■

Problem 5.3 (14)**.** Use Jordan-Hölder to prove the Fundamental Theorem of Arithmetic – each number has a unique prime factorization.

Solution. Let n be a positive integer and p_i be a prime such that $p_i \geq p_{i+1}$.
We can think of a number $k = p_1 p_{2n}$ as the finite abelian group $\mathbb{Z}/k\mathbb{Z}$. Let $G_i = (\mathbb{Z}/p_1\mathbb{Z}) \times (\mathbb{Z}/p_2\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_i\mathbb{Z})$ for all i, and let $G_0 = e$. Note that $G_n = \mathbb{Z}/k\mathbb{Z}$. Suppose we want to go from G_i to G_{i+1}. Then we would just take the direct product $G_i \times \mathbb{Z}/p_{i+1}\mathbb{Z}$.
First, we state a lemma.

Lemma 5.4
$(\mathbb{Z}/a\mathbb{Z}) \times (\mathbb{Z}/b\mathbb{Z}) \cong (\mathbb{Z}/ab\mathbb{Z})$ with addition.

Proof. We claim that the isomorphism in question is $\phi : \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ such that $\phi((i,j)) = aj + i$. We know that this is bijective because combining $(i,j) = aj + i$ is like choosing cell (i,j) of an $a \times b$ grid. Each (i,j) leads to a different cell, and each cell has a different (i,j) index.
We also claim that ϕ is a homomorphism. This is relatively easy to show.

$$\begin{aligned} \phi((i_1, j_1) \cdot (i_2, j_2)) &= \phi((i_1, j_1) + (i_2, j_2)) \\ &= \phi((i_1 + i_2, j_1 + j_2)) \\ &= a(j_1 + j_2) + (i_1 + i_2) \\ &= a(j_1) + i_1 + a(j_2) + i_2 \\ &= \phi((i_1, j_1)) + \phi((i_2, j_2)) \\ &= \phi((i_1, j_1)) \cdot \phi((i_2, j_2)). \end{aligned}$$

Thus, it must be a homomorphism. As it's also bijective, it must be an isomorphism. ■

Using ϕ, we can turn each $G_i = (\mathbb{Z}/p_1\mathbb{Z} \times \cdots \times \mathbb{Z}/p_i\mathbb{Z}$ into $G_i = \mathbb{Z}/p_1p_2 \cdots p_i\mathbb{Z}$. So now we want to show that G_i is the maximal normal subgroup of G_{i+1}. We know that $\mathbb{Z}/a\mathbb{Z} \lhd \mathbb{Z}/b\mathbb{Z} \iff a \mid b$. Therefore, we know that $G_i \lhd G_{i+1}$ by definition. We also know that $\frac{|G_{i+1}|}{|G_i|}$ is prime, so there's nothing between G_i and G_{i+1} that could be a normal subgroup. Hence, we have that G_i is a maximal normal subgroup of G_{i+1} for all i, and that G is a composition series. Thus, we are done by Jordan-Hölder. ■