ALGEBRA HANDOUT 2.5: MORE ON COMMUTATIVE GROUPS

PETE L. CLARK

1. Reminder on quotient groups

Let G be a group and H a subgroup of G. We have seen that the left cosets xH of H in G give a partition of G. Motivated by the case of quotients of rings by ideals, it is natural to consider the product operation on cosets. Recall that for any subsets S, T of G, by ST we mean $\{st \mid s \in S, t \in T\}$.

If G is commutative, the product of two left cosets is another left coset:

$$(xH)(yH) = xyHH = xyH.$$

In fact, what we really used was that for all $y \in G$, $yH = Hy$. For an arbitrary group G, this is a property of the subgroup H, called **normality**. But it is clear – and will be good enough for us – that if G is commutative, all subgroups are normal.

If G is a group and H is a normal subgroup, then the set of left cosets, denoted G/H, itself forms a group under the above product operation, called the **quotient group** of G by H. The map which assigns $x \in G$ to its coset $xH \in G/H$ is in fact a surjective group homomorphism $q : G \to G/H$, called the **quotient map** (or in common jargon, the "natural map"), and its kernel is precisely the subgroup H.

Theorem 1. *(Isomorphism theorem) Let $f : G \to G'$ be a surjective homomorphism of groups, with kernel K. Then G/K is isomorphic to G'.*

Proof. We define the isomorphism $q(f) : G/K \to G'$ in terms of f: map the coset xK to $f(x) \in G'$. This is well-defined, because if $xK = x'K$, then $x' = xk$ for some $k \in K$, and then

$$f(x') = f(x)f(k) = f(x) \cdot e = f(x),$$

since k is in the kernel of f. It is immediate to check that $q(f)$ is a homomorphism of groups. Because f is surjective, for $y \in G'$ there exists $x \in G$ such that $f(x) = y$ and then $q(f)(xK) = y$, so $q(f)$ is surjective. Finally, if $q(f)(xK) = e$, then $f(x) = e$ and $x \in K$, so $xK = K$ is the identity element of G/K. □

In other words, a group G' is (isomorphic to) a quotient of a group G iff there exists a surjective group homomorphism from G to G'.

Corollary 2. *If G and G' are finite groups such that there exists a surjective group homomorphism $f : G \to G'$, then $\#G' \mid \#G$.*

Proof. $G' \cong G/\ker f$, so $\#G' \cdot \#(\ker f) = \#G$. □

Remark: Suitably interepreted, this remains true for infinite groups.

Corollary 3. *("transitivity of quotients") If G' is isomorphic to a quotient group of G and G'' is isomorphic to a quotient group of G', then G'' is isomorphic to a quotient group of G.*

Proof. We have surjective group homomorphisms $q_1 : G \to G'$ and $q_2 : G' \to G''$, so the composition $q_2 \circ q_1$ is a surjective group homomorphism from G to G''. □

2. Cyclic groups

Recall that a group G is cyclic if there exists some element g in G such that every x in g is of the form g^n for some integer n. (Here we are using the conventions that $g^0 = e$ is the identity element of G and that $g^{-n} = (g^{-1})^n$.) Such an element g is called a generator. In general, a cyclic group will have more than one generator, and it is a number-theoretic problem to determine how many generators there are.

Example 1: The integers $\mathbb{Z}$ under addition are a cyclic group, because 1 is a generator. The only other generator is -1.

Example 2: We denote by Z_n the additive group of the ring $(\mathbb{Z}/n\mathbb{Z})$. It is also a cyclic group, because it is generated by the class of $1 \pmod{n}$.

We claim that these are the only cyclic groups, up to isomorphism. One (comparatively sophisticated) way to see this is as follows: let G be a cyclic group, with generator g. Then there is a unique homomorphism f from the additive group of the integers to G which maps 1 to g. The map f is surjective because, by assumption, every y in G is of the form g^n for some $n \in \mathbb{Z}$, i.e., $y = g^n = f(n)$. Let K be the kernel of this homomorphism. Then it is a subgroup of $(\mathbb{Z}, +)$, and since every additive subgroup of $(\mathbb{Z}, +)$ is an ideal, we have $K = n\mathbb{Z}$ for some $n \in \mathbb{N}$. Therefore by the isomorphism theorem, we have that G is isomorphic to the additive group of the quotient ring $\mathbb{Z}/n\mathbb{Z}$, i.e., to Z_n.

Corollary 4. *Every quotient group of a cyclic group is cyclic.*

Proof. We saw that a group is cyclic iff it is isomorphic to a quotient of $(\mathbb{Z}, +)$. Therefore a quotient G' of a cyclic group is a group that is isomorphic to a quotient of a quotient of $(\mathbb{Z}, +)$, and by Corollary 3 this simply means that G' is isomorphic to a quotient of $(\mathbb{Z}, +)$ and hence is itself cyclic. □

Proposition 5. *Let $n \in \mathbb{Z}^+$. For every positive divisor k of n, there is a unique subgroup of Z_n of order k, and these are the only subgroups of Z_n.*

Proof. For any divisor k of n, the subgroup generated by $k \pmod{n}$ of $(\mathbb{Z}/n\mathbb{Z}, +)$ has order $\frac{n}{k}$, and as k runs through the positive divisors of n so does $\frac{n}{k}$. So there is at least one cyclic subgroup of Z_n of order any divisor of n. Conversely, let H be a subgroup of $(\mathbb{Z}/n\mathbb{Z}, +)$ and let k be the least positive integer such that the class of k mod n lies in H. (Since the class of n lies in H, there is such a least integer.) I leave it to you to show that H is the subgroup generated by $k \pmod{n}$. □

Remark: Slicker is to observe that the subgroups of Z_n correspond to the ideals in $\mathbb{Z}/n\mathbb{Z}$ which – by a general principle on ideals in quotient rings – correspond to the ideals of $\mathbb{Z}$ containing $(n\mathbb{Z})$, which correspond to the positive divisors of n.

Corollary 6. *Subgroups of cyclic groups are cyclic.*

Proposition 7. *For $a \in \mathbb{Z}^+$, the order of the class of $a \in (\mathbb{Z}/n\mathbb{Z}, +)$ is $\frac{n}{\gcd(a,n)}$.*

Proof. Let $d = \gcd(a, n)$ and write $a = da'$. The (additive) order of $a \pmod n$ is the least positive integer k such that $n \mid ka$. We have $n \mid ka = kda' \iff \frac{n}{d} \mid ka'$, and since $\gcd(\frac{n}{d}, a) = 1$, the least such k is $\frac{n}{d}$. □

Corollary 8. *Let $a \in \mathbb{Z}$, $n \in \mathbb{Z}^+$.*
a) The class of $a \in Z_n$ is a generator if and only if $\gcd(a, n) = 1$. In particular there are $\varphi(n)$ generators.
b) For any $d \mid n$, there are precisely $\varphi(d)$ elements of Z_n of order d.
c) It follows that $\sum_{d \mid n} \varphi(d) = n$.

Proof. Part a) is immediate from Proposition 7. For any $d \mid n$, each element of order d generates a cyclic subgroup of order d, and we know that there is exactly one such subgroup of Z_n, so the elements of order d are precisely the $\varphi(d)$ generators of this cyclic group. Part c) follows: the left hand side gives the number of elements of order d for each $d \mid n$ and the right hand side is $\#Z_n$. □

This leads to a very useful result:

Theorem 9. *(Cyclicity criterion) Let G be a finite group, not assumed to be commutative. Suppose that for each $n \in \mathbb{Z}^+$, there are at most n elements x in G with $x^n = e$. Then G is cyclic.*

Proof. Suppose G has order N, and for all $1 \leq d \leq N$, let $f(d)$ be the number of elements of G of order d. By Lagrange's Theorem, $f(d) = 0$ unless $d \mid N$, so $N = \#G = \sum_{d \mid N} f(d)$. Now, if $f(d) \neq 0$ then there exists at least one element of order d, which therefore generates a cyclic group of order d, whose elements give d solutions to the equation $x^d = e$. By our assumption there cannot be any more solutions to this equation, hence all the elements of order d are precisely the $\varphi(d)$ generators of this cyclic group. In other words, for all $d \mid n$ we have either $f(d) = 0$ or $f(d) = \varphi(d)$, so in any case we have

$$N = \sum_{d \mid N} f(d) \leq \sum_{d \mid N} \varphi(d) = N.$$

Therefore we must have $f(d) = \varphi(d)$ for all $d \mid N$, including $d = N$, i.e., there exists an element of G whose order is the order of G: G is cyclic. □

Corollary 10. *Let F be a field, and let $G \subset F^\times$ be a finite subgroup of the group of nonzero elements of F under multiplication. Then G is cyclic.*

Proof. Indeed, by basic field theory, for any $d \in \mathbb{Z}^+$ the degree d polynomial $t^d - 1$ can have at most d solutions, so the hypotheses of Theorem 9 apply to G. □

3. Products of elements of finite order in a commutative group

Let G be a commutative group, and let $x, y \in G$ be two elements of finite order, say of orders m and n respectively. There is a unique smallest subgroup $H = H(x, y)$ of G containing both x and y, called the **subgroup generated by** x and y. $H(x, y)$ is the set of all elements of the form $x^a y^b$ for $a, b \in \mathbb{Z}$. Moreover, since x has order m and y has order n, we may write every element of H as $x^a y^b$ with $0 \leq a < m$, $0 \leq b < n$, so that $\#H \leq mn$. In particular the subgroup of an abelian group generated by two elements of finite order is itself finite.

It is very useful to have some information about both the size of $H(x, y)$ and the order of the element xy in terms of m and n alone. However we cannot expect a complete answer:

Example 3: Suppose that $m = n = N$. We could take G to be the additive group of $\mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$, $x = (1, 0)$, $y = (0, 1)$. Then the subgroup generated by x and y is all of G, so has order N^2, and the order of $x + y$ is N. On the other hand, we could take $G = Z_N$ and $x = y = g$ some generator. Then $H(x, y) = G$ has order N and $\#xy$ is N if N is odd and $\frac{N}{2}$ is N is even. Or we could have taken $y = x^{-1}$ so that the $xy = e$ and has order 1. And there are yet other possibilities.

Example 4: Suppose that $\gcd(m, n) = 1$. We can show that xy has order mn, and hence is a generator for $H(x, y)$. Indeed, let $a \in \mathbb{Z}^+$ be such that $(xy)^a = e$, i.e., $x^a = y^{-a}$. But the order of x^a divides m and the order of y^{-a} divides n; since $\gcd(m, n) = 1$, $x^a = y^{-a} = 1$, so that $a \mid m$, $a \mid n$. Since, again, $\gcd(m, n) = 1$, this implies $a \mid mn$.

The general case is as follows:

Theorem 11. *Let x and y be elements of finite order m and n in a commutative group G. Denote by $H(x, y)$ the subgroup generated by x and y.*
a) $\operatorname{lcm}(m, n) \mid \#H(x, y) \mid mn$.
b) $\frac{\operatorname{lcm}(m,n)}{\gcd(m,n)} \mid \#(xy) \mid \operatorname{lcm}(m, n)$.

Proof. Step 1: We can define a surjective homomorphism of groups $\Psi : Z_m \times Z_n \to H(x, y)$ by $(c, d) \mapsto x^c y^{-d}$, so by $\#H(x, y) \mid \#(Z_m \times Z_n)$ by Corollary 2.

Step 2: Let K be the kernel of Ψ. By the Isomorphism theorem, $\#H(x, y) = \#(Z_m \times Z_n)/\#K = \frac{mn}{\#K}$, so $\#H(x, y) \mid mn$. Moreover, the kernel K consists of pairs (c, d) such that $x^c = y^d$. Let $f = \gcd(m, n)$. Let o be the order of $x^c = y^d$. Since the order of x^c divides m and the order of y^d divides n, $o \mid \gcd(m, n) = f$. There are f values of $c \pmod m$ for which x^c has order dividing f, and for each of these values, there is at most one value of $d \pmod n$ such that $x^c = y^d$ (because the elements y^i for $0 \leq i < n$ are distinct elements of G). This shows that the kernel can be viewed as a subset of Z_f, and it is easily checked to be a subgroup. So $\#K \mid f$ and hence

$$\operatorname{lcm}(m, n) = \frac{mn}{f} \mid \frac{mn}{\#K} = \#H(x, y).$$

Step 3: $(xy)^{\operatorname{lcm}(m,n)} = x^{\operatorname{lcm}(m,n)} y^{\operatorname{lcm}(m,n)} = 1$, so the order of xy divides $\operatorname{lcm}(m, n)$.

Step 4: Finally, suppose that $a \in \mathbb{Z}^+$ is such that $(xy)^a = x^a y^a = 1$, so $x^a = y^{-a}$. So the order of x^a, which is $\frac{m}{\gcd(a,m)}$ is equal to the order of y^{-a}, which is $\frac{n}{\gcd(a,n)}$. In other words, we have

$$m \gcd(a, n) = n \gcd(a, m).$$

Since $\gcd(\frac{m}{f}, n) = 1$, $\frac{m}{f} \mid \gcd(a, m)$, or

$$m \mid f \gcd(a, m) \mid fa.$$

Similarly

$$n \mid f\gcd(a,n) \mid fa.$$

Therefore $\operatorname{lcm}(m,n) \mid fa$, or $\frac{\operatorname{lcm}(m,n)}{\gcd(m,n)} \mid a$, completing the proof of the theorem. □

Remark: The divisibilities in Theorem 11 are best possible: if h and o are positive integers such that $\operatorname{lcm}(m,n) \mid h \mid mn$ and $\frac{\operatorname{lcm}(m,n)}{\gcd(m,n)} \mid o \mid \operatorname{lcm}(m,n)$, then there exist elements $x, y \in Z_m \times Z_n$ such that $\#H(x,y) = h$, $\#xy = o$.

Remark: The situation is profoundly different for noncommutative groups: for every $m, n \geq 2$ and $2 \leq r \leq \infty$ there exists a group G containing elements x of order m, y of order n whose product xy has order r. Moreover, if $r < \infty$ then one can find a finite group G with these properties, whereas one can find an infinite group with these properties iff $\frac{1}{m} + \frac{1}{n} + \frac{1}{r} \leq 1$.

The following is a consequence of Theorem 11 (but is much simpler to prove):

Corollary 12. *Let $m, n \in \mathbb{Z}^+$. The group $Z_m \times Z_n$ is cyclic iff $\gcd(m,n) = 1$.*

Proof. The order of any element (c,d) divides $\operatorname{lcm}(m,n)$, and the order of $(1,1)$ is $\operatorname{lcm}(m,n)$. Therefore the group is cyclic iff $mn = \operatorname{lcm}(m,n)$ iff $\gcd(m,n) = 1$. □

4. Character theory of finite abelian groups

4.1. Introduction.

In this section our goal is to present the theory of characters of finite abelian groups. Although this is an "easy" theory in that we can present it in its entirety here, it nevertheless of the highest impotance, being the jumping off point for at least two entire disciplines of mathematics: the general theory of linear representations of groups, and Fourier analysis. The special case of characters of the unit groups $U(N) = (\mathbb{Z}/N\mathbb{Z})^\times$ will be used as one of the essential ingredients in the proof of Dirichlet's theorem on primes in arithmetic progessions.

Let G be a finite commutative group. A **character** $\chi : G \to \mathbb{C}^\times$ of G is a homomorphism from G to the group $\mathbb{C}^\times$ of nonzero complex numbers under multiplication.

Suppose $N = \#G$. By Lagrange's theorem we have, for any $g \in G$, that $g^N = e$ (the identity element), and thus for any character χ on G we have

$$\chi(g)^N = \chi(g^N) = \chi(e) = 1.$$

Thus $\chi(g)$ is itself a complex Nth root of unity. Recall that the set of all complex Nth roots of unity forms a cyclic group of order N, say μ_N. In other words, every character on a group G of order N is really just a homomorphism from G to μ_N, or equally well, from G into any fixed order N cyclic group.

We write $X(G)$ for the set of all characters of G. We can endow $X(G)$ with the structure of a group: given $\chi_1,\ \chi_2 \in X(G)$, we define their product "pointwise":

$$\forall g \in G,\ (\chi_1\chi_2)(g) := \chi_1(g)\chi_2(g).$$

The identity element is the **trivial character** $g \mapsto 1$ for all g, and the inverse of χ is the function $\chi^{-1} : g \mapsto \frac{1}{\chi(g)}$. Because for any $z \in \mathbb{C}$ we have $z\overline{z} = |z|^2$, if if z is a root of unity, then the inverse of z is given by its complex conjugate $\overline{z}$. It follows that the inverse of a character χ is also given by taking complex conjugates:

$$\overline{\chi}(g) = \overline{\chi(g)} = \frac{1}{\chi(g)} = \chi^{-1}(g).$$

4.2. **The Character Extension Lemma.**

Most of the content of the entire theory resides in the following result.

Lemma 13. *(Character Extension Lemma) Let H be a subgroup of a finite commutative group G. For any character $\psi : H \to \mathbb{C}^\times$, there are $[G : H]$ characters $\Psi : G \to \mathbb{C}^\times$ such that $\Psi|_H = \psi$.*

Proof. The result is clear if $H = G$, so we may assume that there exists $g \in G \setminus H$. Let $G_g = \langle g, H \rangle$ be the subgroup generated by H and g. Now we may or may not have $G_g = G$, but suppose that we can establish the result for the group G_g and its subgroup H. Then the general case follows by induction, since for any $H \subset G$ choose $g_1, \ldots, g_n$ such that $G = \langle H, g_1, \ldots, g_n \rangle$. Then we can define $G_0 = H$ and for $1 \leq i \leq n$, $G_i = \langle G_{i-1}, g_i \rangle$. Applying the Lemma in turn to G_{i-1} as a subgroup of G_i gives that in all the number of ways to extend the character ψ of $H = G_0$ is

$$[G_1 : G_0][G_2 : G_1] \cdots [G_n : G_{n-1}] = [G : G_0] = [G : H].$$

So let us now prove that the number of ways to extend ψ from H to $G_g = \langle H, g \rangle$ is $[G_g : H]$. For this, let d be the order of g in G, and consider $\tilde{G} := H \times \langle g \rangle$. The number of ways to extend a character ψ of H to a character of $\tilde{G}$ is equal to $\#\langle g \rangle = d$: such a homomorphism is uniquely specified by the image of $(1, g)$ in $\mu_d \subset \mathbb{C}^\times$, and all d such choices give rise to homomorphisms.

Moreover, there is a surjective homomorphism $\varphi : H \times \langle g \rangle$ to G_g: we just take $(h, g^i) \mapsto hg^{-i}$. The kernel of φ is the set of all pairs (h, g^i) such that $g^i = h$. In other words it is precisely the intersection $H \cap \langle g \rangle$, which has cardinality, say e, some divisor of d. It follows that

$$\#H_g = \frac{\#H \times \langle g \rangle}{\#H \cap \langle g \rangle} = \frac{d}{e} \cdot \#H,$$

so

$$[H_g : H] = \frac{d}{e}.$$

But a homomorphism $f : H \times \langle g \rangle \to \mathbb{C}^\times$ descends to a homomorhpism on the quotient H_g iff it is trivial on the kernel of the quotient map, i.e., is trivial on $H \cap \langle g \rangle$. In other words, the extensions of ψ to a character of H_g correspond precisely to the number of ways to map the order d element g into $\mathbb{C}^\times$ such that $g^{\frac{d}{e}}$ gets mapped to 1. Thus we must map g to a $\frac{d}{e}$th root of unity, and conversely all such mappings induce extensions of ψ. Thus the number of extensions is $\frac{d}{e} = [H_g : H]$. □

Corollary 14. *For any finite commutative group G, $X(G)$ is finite and*

$$\#X(G) = \#G.$$

Proof. Apply Lemma 13 with $H = 1$. □

Corollary 15. *For G a finite commmutative group and $g \in G$, TFAE:*
(i) For every $\chi \in X(G)$, $\chi(g) = 1$.
(ii) g is the identity element e of G.

Proof. Certainly (ii) $\implies$ (i). Conversely, if $g \neq e$, then $H := \langle g \rangle$ is a nontrivial cyclic group. By Corollary 14, there exists a nontrivial character ψ of H. Since g generates H, this implies $\psi(g) \neq 1$. Now apply Lemma 13 to extend ψ to a character of G. □

From these results one can deduce that the character group construction behaves nicely under homomorphisms: suppose $f : G \to H$ is a homomorphism of finite commutative groups. Then we can define a map $X(f) : X(H) \to X(G)$ – note well: in the opposite direction! – just by taking a character $\chi : H \to \mathbb{C}^\times$ and precomposing it with f to get a character $\chi \circ f : G \to \mathbb{C}^\times$.

Proposition 16. *Let $f : G \to H$ be a homomorphism of finite commutative groups.*
a) The above map $X(f) : X(H) \to X(G)$ is a group homomorphism.
b) The homomorphism f is injective $\iff$ the homomorphism $X(f)$ is surjective.
c) The homomorphism f is surjective $\iff$ the homomorphism $X(f)$ is injective.

Proof. Part a) is a straightforward verification which we leave to the reader.

b) Assume first that f is injective. We may as well assume then that G is a subgroup of H and $f = \iota$ is the inclusion map. Then the induced homomorphism $X(\iota) : X(H) \to X(G)$ is nothing else than the map which restricts a character of H to a character of the subgroup G; that this restriction map is surjective is an immediate consequence of Lemma 13. Inversely, assume that f is not injective, so that there exists $e \neq g \in G$ such that $f(g) = e \in H$. By Corollary 15, there exists a character $\chi : G \to \mathbb{C}^\times$ such that $\chi(g) \neq 1$. But then for any character $\psi : H \to \mathbb{C}^\times$, we have

$$(\psi \circ f)(g) = \psi(e) = 1,$$

which shows that $\psi \circ f \neq \chi$, i.e., χ is not in the image of $X(f)$.

c) By the Extension Lemma, the number of characters on H which are trivial on $f(G)$ is $[H : f(G)]$. Therefore this quantity is equal to 1 – i.e., f is surjective – iff a character ψ on H for which $\psi \circ f$ is trivial is necessarily itself trivial. □

4.3. **Orthogonality relations.**

Theorem 17. *Let G be a finite abelian group, with character group G.*
a) For any nontrivial character $\chi \in X(G)$, we have $\sum_{g \in G} \chi(g) = 0$.
b) For any nontrivial element g of G, we have $\sum_{\chi \in X(G)} \chi(g) = 0$.

Proof. a) Put

$$S = \sum_{g \in G} \chi(g). \tag{1}$$

Since χ is nontrivial, there exists $g_0 \in G$ such that $\chi(g_0) \neq 1$. Multiplying both sides of (1) by $\chi(g_0)$, we get

$$\chi(g_0)S = \sum_{g \in G} \chi(g)\chi(g_0) = \sum_{g \in G} \chi(gg_0) = \sum_{g \in G} \chi(g) = S;$$

the penultimate equality holds because, as g runs through all elements of G, so does g_0. Therefore we have

$$(\chi(g_0) - 1)\, S = 0.$$

Since $\chi(g_0) \neq 1$, the inexorable conclusion is that $S = 0$. As for part b), if $g \neq e$, then by Corollary 15 there exists a character χ such that $\chi(g) \neq 1$, and then the argument is identical to part a).[1] □

Let us briefly explain why these are called orthogonality relations. Consider the set $\mathbb{C}^G$ of all functions $f : G \to \mathbb{C}$. Under pointwise addition and scalar multiplication, $\mathbb{C}^G$ is a complex vector space, of dimension equal to $\#G$. We can define a Hermitian inner product on $\mathbb{C}^G$ as follows:

$$\langle f, g \rangle := \frac{1}{\#G} \sum_{x \in G} f(x)\overline{g(x)}.$$

Now let χ_1 and χ_2 be characters of G. If $\chi_1 = \chi_2$, then we have

$$\langle \chi_1, \chi_1 \rangle = \frac{1}{\#G} \sum_{x \in G} |\chi_1(x)|^2 = 1,$$

whereas if $\chi_1 \neq \chi_2$, then $\chi_1 \chi_2^{-1}$ is nontrivial, and then Theorem 17 gives

$$\langle \chi_1, \chi_2 \rangle = \frac{1}{\#G} \sum_{x \in G} (\chi_1 \chi_2^{-1})(x) = 0.$$

In other words, the set $X(G)$ of characters of G is orthonormal with respect to the given inner product. In particular, the subset $X(G)$ of $\mathbb{C}^G$ is linearly independent. Since its cardinality, $\#G$, is equal to the dimension of $\mathbb{C}^G$, we conclude:

Corollary 18. *Let G be a finite commutative group, and let $\mathbb{C}^G$ be the $\mathbb{C}$-vector space of all functions from G to $\mathbb{C}$, endowed with the inner product*

$$\langle f, g \rangle = \frac{1}{\#G} \sum_{x \in G} f(x)\overline{g(x)}.$$

Then the set of characters of G forms an orthonormal basis with respect to $\langle \ , \ \rangle$. Therefore, any function $f : G \to \mathbb{C}$ can be expressed as a unique linear combination of characters. Explicitly:

$$f = \sum_{\chi \in X(G)} \langle f, \chi \rangle \chi.$$

This can be viewed as the simplest possible case of a **Fourier inversion formula**.

4.4. The canonical and illicit isomorphism theorems; Pontrjagin duality.

In the course of study of finite commutative groups, one sees that subgroups and quotient groups have many similar properties. For instance, subgroups of cyclic groups are cyclic, and also quotients of cyclic groups are cyclic. Moreover, a cyclic group of order n has a unique subgroup of every order dividing n and no other subgroups, and the same is true for its quotients. If one plays around for a bit with finite commutative groups, one eventually suspects the following result:

Theorem 19. *Let G and H be finite commutative groups. Then TFAE:*
(i) H can be realized as a subgroup of G: $\exists$ an injective homomorphism $H \to G$.
(ii) H can be realized as a quotient of G: $\exists$ a surjective homomorphism $G \to H$.

[1] Alternately, using the canonical isomorphism $G \cong X(X(G))$ described in the next section, one can literally deduce part b) from part a).

There is a certain resemblance between Theorem 19 and Proposition 16, but they are not the same. Proposition 16 asserts that if there is an injection $H \to G$, there is a surjection $X(G) \to X(H)$ (and similarly with "injection" and "surjection" interchanged). To deduce Theorem 19 from Proposition 16, one needs the following:

Theorem 20. *(Illicit Isomorphism Theorem) Any finite commutative group G is isomorphic to its chracter group $X(G)$.*

Some cases of Theorem 20 are easy to establish. For instance, since G and $X(G)$ have the same order, they must be isomorphic whenever $\#G$ is prime. Further, to give a character on a cyclic group of order N it suffices to send a fixed generator to any Nth root of unity in $\mathbb{C}$. More precisely, choosing a generator of an abstract cyclic group G order N amounts to choosing an isomorphism of G with $\mathbb{Z}/N\mathbb{Z}$ (we send the generator to 1 (mod N)). And the characters on $\mathbb{Z}/N\mathbb{Z}$ are all obtained by exponentiation: for any $c \in \mathbb{Z}/N\mathbb{Z}$, there is a unique character χ_a such that

$$\chi_c(1) = e^{2\pi i c/N}$$

and therefore for any $b \in \mathbb{Z}/N\mathbb{Z}$

$$\chi_c(b) = e^{2\pi i c b/N}.$$

It is immediate to check that $\chi_c \cdot \chi_{c'} = \chi_{c+c'}$, where addition is taken mod N. Thus we get a canonical isomorphism $X(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\sim} \mathbb{Z}/N\mathbb{Z}$.

Moreover, if G_1 and G_2 are finite commutative groups, then in a natural way

$$X(G_1 \times G_2) = X(G_1) \times X(G_2);$$

again we leave the details to the interested reader. Of course the analogous identity for products of any finite number of groups follows by induction.

Combining these observations, it follows that $G \cong X(G)$ for any finite commutative group G of the form $Z_{n_1} \times \ldots \times Z_{n_k}$, i.e., for any direct product of cyclic groups. Is this enough to prove Theorem 20? Indeed it is, because of the following:

Theorem 21. *(Fundamental theorem on finite commutative groups) Let G be a finite commutative group.*
a) There exist prime powers $p_1^{a_1}, \ldots, p_r^{a_r}$ (we allow $p_i = p_j$ for $i \neq j$) such that

$$G \cong Z_{p_1^{a_1}} \times \ldots \times Z_{p_r^{a_r}},$$

i.e., G is a direct product of finite cyclic groups of prime power order.
b) Moreover, this decomposition is essentially unique in the following (familiar) sense: if also we have

$$G \cong Z_{q_1^{b_1}} \times \ldots \times Z_{q_s^{b_s}},$$

then $r = s$ and there exists a bijection $\sigma : \{1, \ldots, r\} \to \{1 \ldots s\}$ such that for all $1 \leq i \leq r$, $q_{\sigma(i)} = p_i$ and $b_{\sigma(i)} = a_i$.

Now please bear with me while I make a few possibly confusing remarks about why I have labelled Theorem 20 the "illicit" isomorphism theorem. In some sense it is "lucky" that $G \cong X(G)$, in that it is not part of the general meaning of "duality" that an object be isomorphic to its dual object. Rather, what one has in much more generality is a canonical injection from an object to its **double dual**. Here, this means the following: we can construct a canonical map $G \to X(X(G))$. In other words, given an element g in G, we want to define a character, say $g\bullet$, *on* the character group, i.e., a homomorphism $X(G) \to \mathbb{C}^\times$. This may sound complicated at first, but in fact there is a very easy way to do this: define $g \bullet \chi := \chi(g)$! It is no problem to check that the association $g \mapsto g\bullet$ is a homomorphism of finite abelian groups. Moreover, suppose that for any fixed $g \in G$ the map $g\bullet$ were trivial: that means that for all $\chi \in X(G)$, $\chi(g) = 1$. Applying Corollary 15, we get that $g = 1$. Therefore this map

$$\bullet : G \to X(X(G))$$

is an injective homomorphism between finite abelian groups. Moreover,

$$\#X(X(G)) = \#X(G) = \#G,$$

so it is an injective homomorphism between finite groups of the same order, and therefore it must be an isomorphism.

In order to write down the isomorphism $\bullet$, we did not have to make any choices. There is a precise sense in which the isomorphism to the double dual is "canonical" and any isomorphism between G and $X(G)$ is "noncanonical", but explanining this involves the use of category theory so is not appropriate here. More interesting is to remark that there is a vastly more general class of commutative groups G for which $X(G)$ is defined in such a way as to render true all of the results we have proved here *except* the illicit isomorphism theorem: we need not have $G \cong X(G)$. For this we take G to be a commutative group endowed with a topology which makes it locally compact Hausdorff. Any commutative group G can be endowed with the discrete topology, which gives many examples. For a finite group the discrete topology is the only Hausdorff topology, so this is certainly the right choice, but an infinite group may or may not carry other interesting locally compact topologies. Some examples:

Example 1: The integers $\mathbb{Z}$: here we do want the discrete topology.

Example 2: The additive group $(\mathbb{R}, +)$ with its usual Euclidean topology: this is a locally compact group which is neither discrete nor compact. More generally, one can take $(\mathbb{R}^n, +)$ (and in fact, if G_1 and G_2 are any two locally compact commutative groups, then so is $G_1 \times G_2$ when endowed with the product topology).

Example 3: The multiplicative group $\mathbb{C}^\times$ of the complex numbers is again locally compact but neither discrete nor compact, but it is "closer to being compact" then the additive group $\mathbb{C} \cong \mathbb{R}^2$. In fact, considering polar coordinates gives an isomorphism of topological groups $\mathbb{C}^\times \cong \mathbb{R}^{>0} \times S^1$, where S^1 is the unit circle. Moreover, the logarithm function shows that $\mathbb{R}^{>0}$ is isomorphic as a topological group to $(\mathbb{R}, +)$, so all in all $\mathbb{C}^\times \cong (\mathbb{R}, +) \times S^1$. Note that S^1, the circle group, is itself a very interesting example.

Now, given any locally compact commutative group G, one defines the **Pontrjagin dual group** $X(G)$, which is the group of all continuous group homomorphisms from G to the circle group S^1. Moreover, $X(G)$ can be endowed with a natural topology.[2] Again, one has a natural map $G \to X(X(G))$ which turns out to be an isomorphism in all cases.

If G is a finite, discrete commutative group, then as we saw, any homomorphism to $\mathbb{C}^\times$ lands in S^1 (and indeed, the countable subgroup of S^1 consisting of all roots of unity) anyway; moreover, by discreteness every homomorphism is continuous. Thus $X(G)$ in this new sense agrees with the character group we have defined. But for infinite groups Pontrjagin duality is much more interesting: it turns out that G is compact iff $X(G)$ is discrete.[3] Since a topological space is both compact and discrete iff it is finite, we conclude that a topological group G which is infinite and either discrete or compact cannot be isomorphic to its Pontrjagin dual.

In our examples, it is easy to see that $\mathrm{Hom}(\mathbb{Z}, S^1) = S^1$, which according to the general theory implies $\mathrm{Hom}(S^1, S^1) = \mathbb{Z}$: that is, the discrete group $\mathbb{Z}$ and the compact circle group S^1 are mutually dual groups. This is the theoretical underpinning of Fourier series.

However, if G is neither discrete nor compact, then the same holds for $X(G)$, so there is at least a fighting chance for G to be isomorphic to $X(G)$. Indeed this happens for $\mathbb{R}$: $\mathrm{Hom}(\mathbb{R}, S^1) = \mathbb{R}$, where we send $x \in \mathbb{R}$ to the character $t \mapsto e^{2\pi itx}$.[4] This is the theoretical underpinning of the Fourier tranform.

Another sense in which the isomorphism between G and $X(G)$ for a finite commutative group G is "illicit" is that turns out not to be necessary in the standard number-theoretic applications. A perusal of elementary number theory texts reveals that careful authors take it as a sort of badge of honor to avoid using the illicit isomorphism, even if it makes the proofs a bit longer. For example, the most natural analysis of the group structure of $(\mathbb{Z}/2^a\mathbb{Z})^\times$ for $a \geq 3$ would consist in showing: (i) the group has order 2^{a-1}; (ii) it has a cyclic subgroup of order 2^{a-2}; (iii) it has a noncyclic quotient so is itself not cyclic. Applying Theorem 21 one can immediately conclude that it must be isomorphic to $Z_{2^{a-2}} \times Z_2$. In our work in Handout 9.5, however, we show the isomorphism by direct means.

This was first drawn to my attention by a close reading of J.-P. Serre's text [Se73][5] in which the illicit isomorphism is never used. Indeed, the careful reader will see that, following Serre, our main application of character groups – namely the proof of Dirichlet's theorem on primes in arihtmetic progressions – uses only $\#X(G) = \#G$, but not $X(G) \cong G$.

[2] If you happen to know something about topologies on spaces of functions, then you know that there is one particular topology that always has nice properties, namely the **compact-open** topology. That is indeed the correct topology here.

[3] Similarly, G is discrete iff $X(G)$ is compact; this follows from the previous statement together with $G \cong X(X(G))$.

[4] Similarly $\mathbb{R}^n$ is self-dual for any n.

[5] This is a wonderful book, but don't be fooled by the name: it is a graduate level text in number theory!

However, to my mind, avoiding the proof of Theorem 21 gives a misleading impression of the difficulty of the result.[6] On the other hand, Theorem 21 evidently has some commonalities with the fundamental theorem of arithmetic, which makes it somewhat desirable to see the proof. In the next section we provide such a proof, which is not in any sense required reading.

5. Proof of the Fundamental theorem on finite commutative groups

First some terminology: Let G be a commutative group, written multiplicatively.

If $\#G = p^a$ is a prime power, we say G is a **p-group**.

For $n \in \mathbb{Z}^+$, we put $G[n] = \{x \in G \mid x^n = 1\}$. This is a subgroup of G.

We say that two H_1, H_2 subgroups of G are **complementary** if $H_1 \cap H_2 = \{1\}$, $H_1H_2 = G$. In other words, every element g of G can be uniquely expressed in the form h_1h_2, with $h_i \in H_i$. In yet *other* (equivalent) words, this means precisely that the homomorphism $H_1 \times H_2 \to G$, $(h_1, h_2) \mapsto h_1h_2$ is an isomorphism. We say that a subgroup H is a **direct factor** of G if there exists H' such that H, H' are complementary subgroups. Thus, in order to prove part a) it suffices to show that every finite commutative group has a nontrivial direct factor which is cyclic of prime power order; and in order to prove part b) it suffices (but is much harder!) to show that if $G \cong H \times H' \cong H \times H''$ then $H' \cong H''$.

More generally if we have a finite set $\{H_1, \ldots, H_r\}$ of subgroups of G such that $H_i \cap H_j = \{1\}$ for all $i \neq j$ and $G = H_1 \cdots H_r$, we say that the H_i's form a set of complementary subgroups and that each H_i is a direct factor. In such a circumstance we have $G \cong H_1 \times \ldots \times H_r$.

We now begin the proof of Theorem 21.

Step 1 (primary decomposition): For any commutative group G, let G_p be the set of elements of G whose order is a power of p. Also let $G^{p'}$ be the set of elements of G whose order is prime to p. It follows from Theorem 11b) that G_p and $G^{p'}$ are both subgroups of G. We claim that G_p and $G^{p'}$ are complementary subgroups. Certainly $G_p \cap G^{p'} = \{e\}$, since any element of the intersection would have both order a power of p and relatively prime to p and thus have order 1 and be the identity. On the other hand, let x be any element of G, and write its order as $p^k \cdot b$ with $\gcd(p, b) = 1$. Thus we can choose i and j such that $ip^k + jb = 1$, and then $x = x^1 = x^{ip^k+jb} = (x^{p^k})^i \cdot (x^b)^j$, and by Proposition 7 the order of $(x^{p^k})^i$ divides b (so is prime to p) and the order of $(x^b)^j$ divides p^k. This proves the claim. Now a simple induction argument gives the following:

Proposition 22. *Let G be a finite abelian group, of order $n = p_1^{a_1} \cdots p_r^{a_r}$. Then the subgroups $\{G_{p_i}\}_{i=1}^r$ form a set of complementary subgroups, and the canonical map $H_1 \times \ldots \times H_r \to G$, $(h_1, \ldots, h_r) \mapsto h_1 \cdots h_r$ is an isomorphism of groups.*

[6] The real reason it is often omitted in such treatments is that the authors know that they will be giving a more general treatment of the structure theory finitely generated modules over a principal ideal domain, of which the theory of finite commutative groups is a very special case.

Thus any finite commutative group can be decomposed, in a unique way, into a direct product of finite commutative groups of prime power order. We may therefore assume that G is a commutative p-group from now on.

Step 2: We prove the following refinement of Theorem 9 for commutative p-groups:

Proposition 23. *Let p be a prime and G be a finite commutative group of order p^a for some $a \in \mathbb{Z}^+$. TFAE:*
(i) G has exactly p elements of order p.
(ii) G is cyclic.

Proof. We already know that (ii) $\implies$ (i), of course. Assume (i); the natural strategy is to appeal to our cyclicity criterion Theorem 9. In this case we wish to show that for any $0 < k \leq a$, there are at most p^k elements of G of order dividing p^k. We accomplish this by induction (!); the case of $k = 1$ is our hypothesis, so assume that for all $1 \leq \ell < k$ the number of elements of order dividing p^ℓ in G is at most p^ℓ and we wish to show that the number of element of order dividing p^k is at most p^k. For this, consider the endomorphism

$$\varphi : G[p^k] \to G[p^k], \ x \mapsto x^{p^{k-1}}.$$

Now the kernel of φ is precisely $G[p^{k-1}]$, which we have inductively assumed has order at most p^{k-1}. If the order of $G[p^k]$ exceeds p^k, then since

$$\varphi(G[p^k]) \cong G[p^k]/\operatorname{Ker}(\varphi),$$

we would have $\#\varphi(G[p^k]) > p$. But by Proposition 7 the image of φ consists entirely of elements of order dividing p, contradiction. □

Step 3:

Proposition 24. *Let G be a finite commutative p-group, and let p^a be the maximum order of an element of G. Then every cyclic subgroup C of order p^a is a direct factor of G: there exists a complementary subgroup H, giving an isomorphism $G \cong C \times H$.*

Proof. The result holds vacuously for commutative groups of order p. Assume that it holds for all commutative groups of order p^k for $k < a$, and suppose we have $G = p^a$, x an element of maximal order in G and $C = \langle x \rangle$ If the order of x is p^a, then $G = C$ is cyclic and the conclusion again holds trivially. Otherwise, by Proposition 23, there exists an order p subgroup K of G not contained in C, so $C \cap K = \{e\}$. Then the cyclic subgroup $(C + K)/K$ has maximal order in G/K; by induction there exists a complementary subgroup H of G/K, i.e., a subgroup H containing K such that $(C + K) \cap H = K$, $(C + K) \cdot H = G$. It follows that $H \cap C \subset K \cap C = \{e\}$ and $C \cdot H = G$, so C and H are complementary subgroups. □

We may now deduce Theorem 21a) from Proposition 24. Indeed, given any finite p-group G we choose an element x of maximum order p^a, which generates a cyclic subgroup C of maximum order, which according to Proposition 24 has a complementary subgroup H and thus $G \cong Z_{p^r} \cong H$. Applying the same procedure to H, eventually we will express G as a product of finite cyclic groups of p-power order.

Step 4: Finally we address the uniqueness of the decomposition of a commutative p-group into a direct product of cyclic groups.[7] Suppose we have

$$G \cong Z_{p^{a_1}} \times \ldots \times Z_{p^{a_r}} \cong Z_{p^{b_1}} \times \ldots \times Z_{p^{b_s}}.$$

We may assume that $a_1 \geq \ldots \geq a_r$ and $b_1 \geq \ldots \geq b_s$, and we wish to prove that $r = s$ and $a_i = b_i$ for all i. We may also inductively assume the uniqueness statement for commutative p-groups of smaller order than G. Now let $\varphi : G \rightarrow G$ be $x \mapsto x^p$. Then we have

$$\varphi(G) \cong Z_{p^{a_1-1}} \times \ldots \times Z_{p^{a_r-1}} \cong Z_{p^{b_1-1}} \times \ldots \times Z_{p^{b_s-1}}.$$

Since $\#\varphi(G) < \#G$, by induction the two decompositions are unique, the only proviso being that if an exponent c_i is equal to 1, then $Z_{p^{c_i-1}}$ is the trivial group, which we do not allow in a direct factor decomposition. Therefore suppose that k is such that $a_i = 1$ for all $i > k$ and l is such that $b_j = 1$ for all $j > l$. Then we get $k = l$ and $a_i = b_i$ for all $1 \leq i \leq k$. But now we have

$$p^{r-k} = \frac{\#G}{p^{a_1+\ldots+a_k}} = \frac{\#G}{p^{b_1+\ldots+b_k}} = p^{s-k},$$

so we conclude $r = s$ and thus $a_i = b_i$ for $1 \leq i \leq r$.

It is interesting to ask which of the steps go through for a group which is infinite, non-commutative or both.

Step 1 fails in a non-commutative group: the elements of p-power order need not form a subgroup. For instance, the symmetric group S_n is generated by transpositions. In any commutative group one can define the subgroups G_p for primes p, and they are always pairwise disjoint. The subgroup they generate is called the **torsion subgroup** of G and often denoted $G[\text{tors}]$: it consists of all elements of finite order.

Step 2 fails for noncommutative finite p-groups: The quaternion group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ is a noncyclic group of order $8 = 2^3 = p^3$ which has exactly $p = 2$ elements of order dividing p. It is false for all infinite abelian groups, since an infinite group can only be cyclic if its torsion subgroup is trivial.

Step 3 fails for finite noncommutative groups: again Q_8 is a counterexample.

As for Step 4, one may ask the following

Question 1. *Suppose we have three groups H, G_1, G_2 such that $H \times G_1 \cong H \times G_2$. Must it then be the case that $G_1 \cong G_2$?*

Without any restrictions the answer to this question is negative. For instance, one can take $H = G_1 = (\mathbb{R}, +)$, $G_2 = 0$, and note that $\mathbb{R} \times \mathbb{R} \cong \mathbb{R}$ as $\mathbb{Q}$-vector spaces, hence as commutative groups. On the other hand:

Theorem 25. *(Remak-Krull-Schmidt) If H, G_1 and G_2 are all finite groups, then indeed $H \times G_1 \cong H \times G_2$ implies $G_1 \cong G_2$.*

A group G is **indecomposable** if it is not isomorphic to $H_1 \times H_2$ with H_1 and H_2 both nonzero. By Theorem 21, a finite commutative group is indecomposable iff

[7] This part of the proof follows [Su95].

it is cyclic of prime power order. Any finite group can be written as a product of indecomposable groups. Using Theorem 25 it can be shown that if

$$G \cong H_1 \times \ldots \times H_r = K_1 \times \ldots \times K_s,$$

where each H_i and K_j are indecomposable (nontrivial) groups, then $r = s$ and there exists a bijection $\sigma : \{1, \ldots, r\} \to \{1, \ldots, r\}$ such that $K_i \cong H_{\sigma(i)}$ for $1 \leq i \leq r$.

6. Wilson's Theorem in a Finite Commutative Group

Here is one of the classic theorems of elementary number theory.

Theorem 26. *(Wilson's Theorem) For an odd prime p,* $(p-1)! \equiv -1 \pmod{p}$.

Remark: The *converse* of Wilson's Theorem also holds: if for some integer $n > 1$ we have $(n-1)! \equiv 1 \pmod{n}$, then n is prime. In fact it can be shown that for all composite $n > 4$, $n \mid (n-1)!$ (exercise).

Most of the standard proofs involve starting with an elementary group-theoretic fact and then recasting it to avoid group-theoretic language to a greater or lesser extent. Since this handout is meant to be a "comprehensive" guide to finite commutative groups, we may as well give the argument in its proper language.

For a finite group G, let $d_2(G)$ be the number of order 2 elements in G.

Theorem 27. *(Wilson's Theorem in a Finite Commutative Group)*
Let $(G, +)$ be a finite commutative group, and let $S = \sum_{x \in G} x$. Then:
a) If $d_2(G) \neq 1$, then $S = 0$.
b) If $d_2(G) = 1$ – so that G has a unique element, say t, of order 2 – then $d_2(G) = t$.

Proof. We set

$$G[2] = \{x \in G \mid 2x = 0\}.$$

Every nonzero element of $G[2]$ has order 2, so by Theorem 21, we must have $G[2] \cong Z_2 \times \ldots \times Z_2 = Z_2^k$ is a direct product of copies of the cyclic group of order 2.[8]

Consider the *involution* $\iota : G \to G$ given by $x \mapsto -x$. The *fixed points* of ι – i.e., the elements $x \in G$ such that $\iota(x) = x$ – are precisely the elements of $G[2]$. Thus the elements of $G \setminus G[2]$ occur in pairs of distinct elements $x, -x$, so $\sum_{x \in G \setminus G[2]} x = 0$. In other words, $\sum_{x \in G} x = \sum_{x \in G[2]} x$, and we are reduced to the case $G[2] \cong Z_2^k$.
Case 1: $k = 0$, i.e., $G[2] = 0$. Then

$$\sum_{x \in G[2]} x = \sum_{x \in \{0\}} x = 0.$$

Moreover, in this case $d_2(G) = 0$, in agreement with the statement of the theorem.
Case 2: $k = 1$, i.e., $G[2] = Z_2$. Then

$$\sum_{x \in G[2]} x = \sum_{x \in Z_2} x = 0 + 1 = 1,$$

where 1 is the unique element of order 2 in $Z_2 \cong G[2]$ (and thus also the unique element of order 2 in G). Again, this agrees with the statement of the theorem.

[8] Actually invocation of Theorem 21 is overkill here: any 2-torsion commutative group admits the unique structure of a vector space over the field $\mathbb{F}_2$ with 2 elements. Being finite, $G[2]$ is certainly finite-dimensional over $\mathbb{F}_2$, so is isomorphic as a vector space – hence *a fortiori* as an additive group – to $\mathbb{F}_2^n$.

Case 3: $k \geq 2$. Then $d_2(G) \geq 3$, so we wish to show $S = \sum_{x \in Z_2^k} x = 0$. For each $1 \leq i \leq k$, half of the elements of Z_2^k have ith coordinate $0 \in Z_2$; the other half have ith coordinate $1 \in Z_2$. So the sum of the ith coordinates of the elements of Z_2^k is $2^k/2 = 2^{k-1} = 0 \in Z_2$, since $k \geq 2$: every coordinate of S equals 0, so $S = 0$. □

We now show that Theorem 27 implies Theorem 26. Let $\mathbb{F}$ be a finite field. We take $G = \mathbb{F}^\times$, the multiplicative group of nonzero elements of $\mathbb{F}$.[9] Now $x \in G[2] \iff x^2 = 1$, and the polynomial $t^2 - 1$ has exactly two roots in any field of characteristic different from 2 and exactly one root in any field of characteristic 2. So $d_2(\mathbb{F}^\times)$ is equal to 1 if $\#F$ is odd and equal to 0 if $\#F$ is even. Thus:

Corollary 28. *Let $\mathbb{F}$ be a finite field, put $P = \prod_{x \in \mathbb{F}^\times} x$. Then:*
a) If $\#\mathbb{F}$ is even, then $P = 1$.
b) If $\#\mathbb{F}$ is odd, then P is the unique element of order 2 in $\mathbb{F}^\times$, namely -1.
So for any odd prime p, the second case holds for the field $\mathbb{Z}/p\mathbb{Z}$: Wilson's Theorem.

As we mentioned above, Wilson's Theorem construed as a statement about the product of all residue classes from 1 up to $n - 1$ modulo n holds exactly when n is prime. On the other hand, for composite n we may still apply Theorem 27 to the finite commutative group $U(n) = (\mathbb{Z}/n\mathbb{Z})^\times$.

Theorem 29. *(Gauss) Let $n > 2$ be an integer, and let $U(n)$ be the multiplicative group of units of the finite ring $\mathbb{Z}/n\mathbb{Z}$. Put $P = \prod_{x \in U(n)} x$. Then:*
a) We always have $P = \pm 1 \pmod{n}$.
b) In fact $P = -1 \pmod{n}$ if and only if n is 4, an odd prime power p^a, or twice an odd prime power $2p^a$.

Let us prove part a). Applying Theorem 27 to $G = U(n)$, we see that $P = 1 \pmod{n}$ unless $d_2(G) = 1$, in which case it is the unique element of order 2 in G. But for all $n > 2$ there is certainly *at least* one element of order 2 in $U(n)$, namely $-1 \pmod{n}$. So if it happens that there is exactly one such element, it must be -1, and thus we must have $P = -1 \pmod{n}$.

To prove part b) we must determine for which n we have $d_2(U(n)) = 1$. Since $\#U(n) = \varphi(n)$ is even for all $n \geq 2$; thus, since $U(n) \setminus U(n)[2]$ has even order, we must have $d_2(U(n)) \geq 1$. Note further that $d_2(U(n)) = 1$ when $U(n)$ is cyclic, i.e., when there exists a primitive root modulo n. Elsewhere in these notes[10] we show that primitive roots modulo n exist precisely when n is 4, an odd prime power or twice an odd prime power: this proves half of Theorem 29b). For the other values of n $U(n)$ is not cyclic, but there are noncyclic groups G with $d_2(G) = 1$. So one has to look a bit more carefully at the structure of the groups $U(n)$ for general n. We leave the details to the interested reader.

Remark: After searching the literature for sources the material of this section, I found a paper of the early American group theorist George Abram Miller [Mi03]. The parallel between this paper and the material of the present section is nearly exact. In particular Miller proves Theorem 27 (his proof is remarkably close to the one given here) and applies it to prove Theorem 29. That this result was first stated

[9] Note well that we are now talking about multiplicative groups rather than additive groups. It makes no mathematical difference, of course, but the reader may wish to pause to reorient to the new notation.

[10] As of this writing, this takes place in a handout called *A Word on Primitive Roots.*

and proved by Gauss is not mentioned in Miller's paper, but its title suggests that he may have been aware of this.

References

[Mi03] G.A. Miller, *A new proof of the generalized Wilson's theorem.* Ann. of Math. (2) 4 (1903), 188–190.

[Se73] J.-P. Serre, *A course in arithmetic.* Translated from the French. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973.

[Su95] D.B. Surowski, *The Uniqueness Aspect of the Fundamental Theorem of Finite Abelian Groups.* Amer. Math. Monthly, 102 (1995), 162–163.