7. Del

Characters

Version $-\infty$ — last update: 11/27/14 9:47:29 AM
Preliminar verison prone to errors and subjected to changes.
The version number says all!

Characters of finite abelian groups

Let A be a finite abelian group. Abelian groups can be both additively and multiplicatively written, but in our theoretical deliberations they will always be a multiplicative groups if the contrary is not explicitly stated.

Recall the group $\mu_n \subseteq \mathbb{C}^*$ of n-th roots of unity; that is $\mu_n = \{\, z \in \mathbb{C}^* \mid z^n = 1 \,\}$. It is cyclic of order n, a generator being $\exp 2\pi i/n$. This is not the only generator; indeed any power $\exp 2\pi i m/n$ where $(n, m) = 1$ will generate. A generator is called *a primitive root of unity*. The groups $\mathbb{Z}/n\mathbb{Z}$ and μ_n are isomorphic. Choosing a generator η of μ_n we can define an isomorphism $\mathbb{Z}/n\mathbb{Z} \to \mu_n$ by sending the residue class of a to the power η^a. This isomorphism depends on a choice of the primitive root η so $\mathbb{Z}/n\mathbb{Z}$ and μ_n are not canonically isomorphism, and we shall distinguish between them.

By a *character* of A we mean a group homomorphism $\chi\colon A \to \mathbb{C}^*$. As every element in a in A is of finite order, the character χ takes values in the subgroup of $\mathbb{C}^*$ of roots of unity. That is, if $a^n = e$, then $\chi(a)^n = \chi(a^n) = \chi(e) = 1$, so the values of χ belong to μ_n if $n = |A|$.

The set of characters of A is denoted $\hat{A}$. It is an abelian group; indeed, if χ_1 and χ_2 are two characters, the product $\chi_1\chi_2$ is defined as usual by $a \mapsto \chi_1(a)\chi_2(a)$, and one trivially sees that this is a group homomorphism ($\mathbb{C}^*$ is abelian). The neutral element in the character group is the *trivial character* given as $a \mapsto 1$. It is usual written as 1_A or sometimes as χ_0.

The two following examples are fundamental:

EXAMPLE 7.1. One has $\widehat{\mathbb{Z}/n\mathbb{Z}} \simeq \mu_n$. Since every character on $\mathbb{Z}/n\mathbb{Z}$ takes values in μ_n, there is the obvious map $\widehat{\mathbb{Z}/n\mathbb{Z}} \to \mu_n$ sending $\chi \to \chi(1)$. This is a group homomorphism by the definition of the group structure of the character group $\widehat{\mathbb{Z}/n\mathbb{Z}}$, and it is obviously injective since 1 generates $\mathbb{Z}/n\mathbb{Z}$. To see it is surjective, pick any n-th root of unity $\eta \in \mu_n$ and take a look at the homomorphism $\mathbb{Z} \to \mu_n$ sending a to η^a. It vanishes on $n\mathbb{Z}$, and thus furnishes us with a homomorphism from $\mathbb{Z}/n\mathbb{Z}$ to μ_n taking the value η at 1. ❄

EXAMPLE 7.2. One has $\hat{\mu}_n \simeq \mathbb{Z}/n\mathbb{Z}$. There is a natural map $\mathbb{Z}/n\mathbb{Z} \to \hat{\mu}_n$ sending a residue class $[a]$ to the a-th power map $\eta \mapsto \eta^a$. The power map is a group homomorphism $\mu_n \to \mu_n \subseteq \mathbb{C}^*$ that only depends on the residue class of a modulo n (if $a' = a + bn$ one has $\eta^{a'} = \eta^a\eta^{bn} = \eta^a$). Hence the a map $\mathbb{Z}/n\mathbb{Z} \to \hat{\mu}_n$ is well defined, and it is easily checked to be a group homomorphism.

It is injective since if $\eta^a = 1$ holds for all $\eta \in \mu_n$, it holds in particular for a primitive n-th root, and it follows thta $n|a$. To see that the map is surjective let η_0 be a primitive n-th root. It generates μ_n, so $\chi(\eta_0) = \eta_0^a$ for some integer a. Now any other $\eta \in \mu_n$ is of the shape $\eta = \eta_0^b$ with $b \in \mathbb{Z}$, and one has $\chi(\eta) = \chi(\eta_0^b) = \chi(\eta_0)^b = \eta_0^{ab} = \eta^a$. ❄

Functoriallity

Assume that A_1 and A_2 are two finite abelian groups and that $\psi\colon A_1 \to A_2$ is a group homomorphism. If χ is a character of A_2, the composition $\chi \circ \psi$ will be a character of A_1. This gives a map $\hat{A}_2 \to \hat{A}_1$, obviously a group homomorphism, which is denoted by $\hat{\psi}$, and by common usage it is called the *dual map*. The following lemma is usual expressed by saying that the hat construction is *functorial*[1]:

Lemma 7.1 *One has $\widehat{\mathrm{id}_A} = \mathrm{id}_{\hat{A}}$. Assume that ϕ and ψ are composable group homomorphisms. Then*

$$\hat{\psi} \circ \hat{\phi} = \widehat{\phi \circ \psi}.$$

PROOF: Obvious, but here are the details:

$$\hat{\psi}(\hat{\phi}(\chi)) = \hat{\psi}(\chi \circ \phi) = (\chi \circ \phi) \circ \psi = \chi \circ (\phi \circ \psi) = \widehat{\phi \circ \psi}(\chi).$$

❑

EXAMPLE 7.3. If $B \subseteq A$ and i denotes the inclusion map, then $\hat{\psi}(\chi) = \chi \circ i$ is nothing but the restriction $\chi|_B$ of χ to B. ❄

[1] For the cognoscenti: The map $A \mapsto \hat{A}$ is a contravariant functor from the category of finite abelian group to itself. It is a very special case of a general duality functor called *Matlis duality. It can also be generalized in another direction to what is callet Pontrjagin duality,*

Problem 7.1.

a) Let $a \in \mathbb{Z}$ and let $\psi\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the multiplication-by-a map. Show that the dual map $\hat{\psi}\colon \mu_n \to \mu_n$ is the a-th-power map $\eta \mapsto \eta^a$.

b) Let $a \in \mathbb{Z}$ and let $\phi\colon \mu_n \to \mu_n$ be the map $\eta \to \eta^a$. Show that $\hat{\phi}$ is multiplication by a.

✷

Problem 7.2.

a) Show that if $\psi\colon A_1 \to A_2$ is a surjective map, then $\hat{\psi}$ is injective.

b) Let η_0 be a primitive n-t root of unity. Assume that $d|n$. Show that η_0^d is a primitive n/d-th root of unity. Use this to show that if $i\colon \mu_d \to \mu_n$ is the inclusion, then $\hat{i}\colon \hat{\mu_n} \to \hat{\mu_d}$ is surjective.

✷

Problem 7.3. Let $B \subseteq A$ be two finite abelian groups. Show that any character χ on B extends to a character on A. Hint: Use induction on the index $[A : B]$, and that $\mathbb{C}^*$ is divisible. ✷

Character groups and direct products

A natural question to ask is how the character group behaves in relation to direct products. And, as we soon shall see, the behavior is immaculate: The character group of a direct product is the direct product of the character groups of the factors—to be precise one should say that it is canonically isomorphic to the direct product of the character groups. Combining this with the fundamental theorem for finite abelian groups—that says a finite abelian group is isomorphic to a direct product of cyclic groups—and the examples 7.1 and 7.2 above, we can conclude that A and $\hat{A}$ are isomorphic. The isomorphism is not canonical so care must be taken, but it tells us what the group structure of $\hat{A}$ is. For example, the order is the same as the order of A.

Let A be an abelian group and let $A_i \subseteq A$ be two subgroups such that A is the direct product of A_1 and A_2. This amounts to the intersection $A_1 \cap A_2$ being trivial and $|A| = |A_1||A_2|$. Every element $a \in A$ may be written as a product $a = a_1 a_2$ with $a_i \in A_i$ in a unique way.

The inclusions $A_i \subseteq A$ induce maps $\hat{A} \to \hat{A}_i$ sending χ to the restriction $\chi|_{A_i}$ (which is just the same as $\hat{\iota}_i(\chi) = \chi \circ \iota_i$ if $\iota_i\colon A_i \to A$ denote the inclusion maps). These are group homomorphisms, and together they define a map $\hat{A} \to \hat{A}_1 \times \hat{A}_2$.

Proposition 7.1 *Given two finite abelian groups A_1 and A_2. The map $\hat{A} \to \hat{A}_1 \times \hat{A}_2$ given by $\chi \mapsto (\chi|_{A_1}, \chi|_{A_2})$ is an isomorphism of groups.*

Proof: First we check that it is injective. Assume that both maps $\chi|_{A_i}$ are trivial. As any $a \in A$ may be written as a product $a = a_1 a_2$ with $a_i \in A_i$, we find $\chi(a) = \chi(a_1)\chi(a_2) = 1 \cdot 1 = 1$.

We proceed by checking that the map is surjective. So let $\chi_i \in \hat{A}_i$ for $i = 1, 2$ be two given characters. Any $a \in A$ can be expressed as a product $a = a_1 a_2$ with unique elements $a_i \in A_i$. Hence we may form $\chi(a) = \chi(a_1)\chi(a_2)$. One checks without trouble that χ in this way is well defined (because the factorization $a = a_1 a_2$ is unique), and that it is a character of A. ❏

Corollary 7.1 *If $\{A_i\}_{i\in I}$ is a finite collection of finite abelian groups, then $\widehat{\prod_{i\in I} A_i} = \prod_{i\in I} \hat{A}_i$.*

Proof: Induction on the number of elements in I. ❏

Corollary 7.2 *Let A be a finite abelian group, then A and the character group $\hat{A}$ have the same number of elements; that is, $|\hat{A}\,| = |A|$.*

Proof: If $A \simeq \prod_{i\in I} \mathbb{Z}/n_i\mathbb{Z}$, then $\hat{A} \simeq \prod_{i\in I} \mu_{n_i}$ by proposition 7.1 on page 3 and example 7.1 on 2; and of course, $|\mu_n| = |\mathbb{Z}/n\mathbb{Z}| = n$. ❏

The characters of the characters

As already hinted at, the formation of characters is a kind of duality. In this it lies, among other things, that performing the hat operation twice brings us back to the group we started with.

For every group element $a \in A$ there is the character on the character group $\hat{A}$ best described as "the evaluation at a": It is the map $\hat{A} \to \mathbb{C}^*$ sending the character χ to the value $\chi(a)$ at a. In this way we arrive at a map $A \to \hat{\hat{A}}$ sending $a \in A$ to the "evaluation at a"; and of course this is a group homomorphism (check it!). The construction is natural, or functorial as one says, in the sense that every group homomorphism $\phi\colon A_1 \to A_2$ between finite abelian groups fits in the following commutative diagram:

$$\begin{tikzcd}
A_1 \arrow[r] \arrow[d, "\phi"'] & \hat{\hat{A}}_1 \arrow[d, "\hat{\hat{\phi}}"] \\
A_2 \arrow[r] & \hat{\hat{A}}_2
\end{tikzcd}$$

Problem 7.4. Check that the diagram is commutative. ✷

Proposition 7.2 *The map $A \to \hat{\hat{A}}$ is an isomorhism.*

Proof: Since the groups on both sides have the same number of elements, it suffices to show that the map is injective. If $a \in A$ is not the neutral element, we have to provide a character χ not vanishing[2] at a.

We first examine the case $A = \mathbb{Z}/n\mathbb{Z}$. Let $a \in \mathbb{Z}/n\mathbb{Z}$ be a non-zero element. If η is a primitive n-the root, one has $\eta^a \neq 1$, and by example 7.1, there is a character with $\chi(1) = \eta$. Hence $\chi(a) = \eta^a \neq 1$.

In the case of a general A, there is for some n a surjection $\pi \colon A \to \mathbb{Z}/n\mathbb{Z}$ mapping a to a non zero element, say a'. This follows from the fundamental theorem for finite abelian groups. By what we just did, there is a character χ on $\mathbb{Z}/n\mathbb{Z}$ not vanishing on a', and hence $\pi \circ \chi$ is a character on A not vanishing at a. ❏

The orthogonality relations

There are some important relations between the different characters of an abelian group A called the *orthogonality relations*. These relations come in pairs and the formulations are dual to each other; that is to say, the one interpreted for the dual group $\hat{A}$ gives the other for the group A. The orthogonality relations are not very mysterious, and finally they boil down to the equation

$$1 + \eta + \eta^2 + \cdots + \eta^{n-1} = 0,$$

satisfied by any non-trivial n-th-root of unity; one sees this by factoring the polynomial $x^n - 1$. As an illustration, assume that A is cyclic of order n with a generator g. A character χ on A is given by the value $\chi(g) = \eta$. Now $\chi(g^i) = \eta^i$, so if $\eta \neq 1$ the above relation becomes

$$\sum_{0 \leq i < n} \chi(g^i) = \sum_{a \in A} \chi(a) = 0,$$

and of course, if $\eta = 1$, we get

$$\sum_{a \in A} \chi(a) = |A|.$$

These two relations correspond to the ones below with respectively $\chi_1 = \chi$ and $\chi_2 = 1$. Recall that if $\eta \in \mathbb{C}^*$ and $|\eta| = 1$ one has $\eta^{-1} = \overline{\eta}$.

Proposition 7.3 (The first orthogonality relation) *Let A be a finite abelian group. Then for any pair of characters χ_1 and χ_2 on A the following relation holds*

$$\sum_{a \in A} \chi_1(a)\overline{\chi}_2(a) = \begin{cases} 0 & \text{if } \chi_1 \neq \chi_2 \ , \\ |A| & \text{if } \chi_1 = \chi_2 \ . \end{cases}$$

[2] In this setting vanishing means that $\chi(a) = 1$. That abelian groups can both be additive and multiplicative sometimes creates inextricable linguistical knots.

Proof: If $\chi_1 = \chi_2$ then $\overline{\chi}_2(a) = \chi_1(a)^{-1}$ and the sum is obviously equal to $|A|$.

Assume that $\chi_1 \neq \chi_2$. Then there is at least one element $b \in A$ such that $\chi_1(b) \neq \chi_2(b)$. Let $F = \sum_{a\in A} \chi_1(a)\overline{\chi}_2(a)$. Now, the product ab runs through A when a does, and therefore one has

$$F = \sum_{a\in A} \chi_1(ab)\overline{\chi}_2(ab) = \chi_1(b)\overline{\chi}_2(b) \sum_{a\in A} \chi_1(a)\overline{\chi}_2(a) = \chi_1(b)\overline{\chi}_2(b)F,$$

from which one infers that $F = 0$, since $\chi_1(b)\overline{\chi}_2(b) = \chi_1(b)\chi_2(b)^{-1} \neq 1$. ❏

In a dual version, that is reformulated for the character group, these relations become:

Proposition 7.4 (The second orthogonality relations)

$$\sum_{\chi\in\hat{A}} \chi(a_1)\overline{\chi}(a_2) = \begin{cases} 0 & \textit{if } a_1 \neq a_2 \\ |A| & \textit{if } a_1 = a_2 \end{cases}$$

Proof: By 7.2 A is the character group of $\hat{A}$, an element $a \in A$ corresponding to the character $\chi \mapsto \chi(a)$. The relation in the proposition is then just the orthogonality relation in proposition 7.3 translated to the dual setting. ❏

Dirichlet characters

Johann Peter Gustav Lejeune Dirichlet was a german mathematician living from 1805 to 1859. He was born in the small town Düren which to day has about 90 000 inhabitants. Düren lies in the western part of Germany not far from Aachen. At the time of Dirichlet's birth Düren was part of France, but after the Napoleon wars it was ceded to Prussia. Dirichlet studied in Paris, held positions in Breslau, Berlin and finally he became Gauss' successor in Göttingen.

When in 1837 Dirichlet proved his celebrated theorem of primes in arithmetic progressions, he introduced what is now called Dirichlet characters. They still play an irreplaceable role in the proof, and in general they are priceless tools in number theory.

Lejeune Dirichlet

Let $m \in \mathbb{N}$ be a natural number greater than one. The ring $\mathbb{Z}/m\mathbb{Z}$ of residue classes modulo m has a unit group $\mathbb{Z}/m\mathbb{Z}^*$ whose elements are the residue classes of integers relatively prime to m. By definition of Euler's ϕ-function the order of $\mathbb{Z}/m\mathbb{Z}^*$ is $\phi(m)$.

For $m = p$ a prime $\mathbb{Z}/p\mathbb{Z}$ is the field with p elements which usually is denoted by $\mathbb{F}_p$. The unit group $\mathbb{F}_p^*$ of non-zero elements is a cyclic group of order $p - 1$. In the case

m is a composite number, say $m = ab$ with a and b relatively prime, the ring $\mathbb{Z}/m\mathbb{Z}$ decomposes as the direct product $\mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ (this is the Chinese residue theorem or the Sun-Tze theorem that some like to call it), and consequently the unit group decomposes as well: $\mathbb{Z}/m\mathbb{Z}^* = \mathbb{Z}/a\mathbb{Z}^* \times \mathbb{Z}/b\mathbb{Z}^*$.

The Dirichlet characters are intimately related to the characters of the unit groups $\mathbb{Z}/m\mathbb{Z}^*$, but there are subtle differences. We prefer to define a *Dirichlet character modulo m* as a function $\chi\colon \mathbb{Z} \to \mathbb{C}$ satisfying the following three properties:

□ Periodicity: $\chi(n+m) = \chi(n)$ for all $n \in \mathbb{Z}$,

□ Multiplicativity: $\chi(nn') = \chi(n)\chi(n')$ for all $n, n' \in \mathbb{Z}$,

□ Vanishing: $\chi(n) = 0$ if and only if $(m,n) \neq 1$.

The last property specifies the value of χ on the integers having a common factor with m, and this is compatible with the periodicity since $(n+m,m) = (n,m)$. The last property implies that $\chi(1) \neq 0$, and from the multiplicativity we infer that $\chi(1) = 1$.

There is a special character called *the principal character modulo m*. It is mostly denoted by χ_0, but 1_m would be a better notation since it depends on m. It takes the value 1 at n when $(n,m) = 1$ and, as imposed by the third condition, $1_m(n) = 0$ whenever $(n,m) \neq 1$; *i.e.,* one has

$$\chi_0(n) = 1_m(n) = \begin{cases} 1 & \text{in case } (n,m) = 1 \ , \\ 0 & \text{in case } n \text{ and } m \text{ have a common factor} \ . \end{cases}$$

The first of the three requirements above says that χ has m as a period, however m is not necessarily the smallest period. The set of periods of χ is closed under addition. It is thus a subgroup of the integers $\mathbb{Z}$, and as such it has a unique positive generator. This is the *smallest* positive period of χ, and it is called *the conductor*[3] *of χ*. The Dirichlet character χ modulo m is said to be *a primitive character modulo m* if the conductor is equal to m; that is, if m is the *smallest* period for χ. If this is not case, one says that χ is *imprimitive*. For a prime modulus p, every character is primitive.

One distinguishes between even and odd Dirichlet characters according to the value they take at -1. The character χ is *even* if $\chi(-1) = 1$ and *odd* if $\chi(-1) = -1$.

By the first of the three properties above the value $\chi(n)$ depends only on the residue class of n modulo m, hence χ induces a map $\chi'\colon \mathbb{Z}/m\mathbb{Z}^* \to \mathbb{C}$. The map χ' is multiplicative since χ is, and hence it is a *character* of the multiplicative group $\mathbb{Z}/m\mathbb{Z}^*$. Conversely, given a character χ' on $\mathbb{Z}/m\mathbb{Z}^*$, one may define a Dirichlet character modulo m by

$$\chi(n) = \begin{cases} 0 & \text{if } (n,m) \neq 1 \\ \chi'([n]) & \text{if } (n,m) = 1 \end{cases}$$

[3] Before World War II the german terminology for the conductor was *der Führer*. For political reasons this was changed in 1945.

where, conform to the conventions, $[n]$ stands for the residue class of n modulo m. The only thing to check is that χ behaves in multiplicative way also for those n having a common factor with m. But in that case nn' and m have a common factor as well whatever the integer n' is, and hence both $\chi(nn')$ and $\chi(n')\chi(n)$ vanish.

In this way one establishes a one-to-one correspondence between the characters of the unit group $\mathbb{Z}/m\mathbb{Z}^*$ and the Dirichlet characters modulo m. It also follows that non-zero values of a Dirichlet character are roots of unity whose orders divide $\phi(m)$.

The Dirichlet characters modulo m form a group under multiplication; the product of two is obviously a Dirichlet character modulo m, and the principal character acts as a unit element. They are all invertible; the inverse of χ being the complex conjugate $\overline{\chi}$. Indeed, if $(n, m) \neq 1$, all character vanish at n, the principal one included, and if $(n, m) = 1$, the value $\chi(n)$ is a root of unity and therefore one has $\chi(n)^{-1} = \overline{\chi}(n)$. To sum up what we have said so far, we have:

Proposition 7.5 *Let $m > 1$ be a natural number. The Dirichlet characters modulo m form a group under multiplication of order $\phi(m)$ with the principal character as the neutral element and the complex conjugate as inversion. If $\pi\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is the natural map, the assignment $\chi' \to \chi' \circ \pi$ sets up a group isomorphism between the character group of $\mathbb{Z}/m\mathbb{Z}^*$ and the group of Dirichlet characters modulo m.*

EXAMPLE 7.4. It is high time to look at a few examples with small m, and we start with the simplest case $m = 2$. The field $\mathbb{F}_2$ has two elements and the unit group $\mathbb{F}_2^*$ is reduced the trivial group. The only Dirichlet character is the principal one. It vanishes on all even numbers and takes the value 1 at the odd ones. ❋

EXAMPLE 7.5. Assume that $m = 3$. The field $\mathbb{F}_3$ has the two units ± 1, hence $\mathbb{F}_3^* = \mu_2 = \{\pm 1\}$, and there are two Dirichlet characters modulo 3, the principal one χ_0 and another one given as $\chi(3n \pm 1) = \pm 1$. ❋

EXAMPLE 7.6. Assume that $m = 4$. The unit group $\mathbb{Z}/4\mathbb{Z}^*$ has two elements, the residue classes of ± 1. There are two Dirichlet characters, the one that is not principal satisfies $\chi(4n + 1) = 1$ and $\chi(4n - 1) = -1$, and of course it vanishes on the even numbers. Be aware of the subtle point that the groups of units $\mathbb{Z}/3\mathbb{Z}^*$ and $\mathbb{Z}/4\mathbb{Z}^*$ are isomorphic and have the same characters, but the Dirichlet characters are certainly different. ❋

EXAMPLE 7.7. Let us take a look at the case $m = 5$. The unit group $\mathbb{F}_5^*$ is of order 4 consisting of ± 1 and ± 2; it is cyclic generated by either the residue class of 2 or of -2. Therefore if χ' denotes the character on $\mathbb{F}_4^*$ corresponding to the Dirichlet character χ, one sees that $\chi'(2)$ can be one of $\pm i$ or ± 1. Using this it is easy to fill in the following table of the values the different characters take:

Class mod 5	χ_1	χ_2	χ_3	χ_0
$5n+2$	i	-i	-1	1
$5n-1$	-1	-1	1	1
$5n-2$	-i	i	-1	1
$5n+1$	1	1	1	1
$5n$	0	0	0	0

The character group is cyclic generated by either of the two odd characters χ_1 or χ_2. The even non-principal character χ_3 generates a subgroup of order 2. ❄

PROBLEM 7.5. This exercise is about the Dirichlet characters modulo 8. Show that $\mathbb{Z}/8\mathbb{Z}^*$ is isomorphic to $\mu_2 \times \mu_2$, and consists of the residue classes of ± 1 and ± 3. One has $(\pm 3)^2 = 1$ and 3 and -3 generate $\mathbb{Z}/8\mathbb{Z}^*$. And hence that any character is given as $\chi(8n+3) = \epsilon_1$ and $\chi(8n-3) = \epsilon_2$ where ϵ_1 and ϵ_2 are elements from $\{\pm 1\}$, and all combinations the two signs can occure. Show that $\chi(8n-1) = \epsilon_1\epsilon_2$, and that $\chi(2n) = 0$. Verify the table

Class mod 8	χ_{--}	χ_{-+}	χ_{+-}	χ_0
$8n+3$	-1	-1	1	1
$8n-3$	-1	1	-1	1
$8n-1$	1	-1	-1	1
$8n$	0	0	0	0

Show that χ_{--} is an imprimitive non-trivial character which in fact coincides with the non-trivial character modulo 4. Show that the two other non-trivial characters are primitive. ✱

PROBLEM 7.6. Constuct the table like in example 7.7 for the case $m = 7$. ✱

PROBLEM 7.7. Show that if p is an odd prime, then there is only one real non-trivial character modulo p. Can you indentify it? ✱

EXAMPLE 7.8. The concept of a primitive character is slightly subtle, so hopefully this example, treating the case $m = 15$, will be clarifying. One has $\mathbb{Z}/15\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, and the unit group $\mathbb{Z}/15\mathbb{Z}^*$ is the group $\mathbb{Z}/3\mathbb{Z}^* \times \mathbb{Z}/5\mathbb{Z}^*$. It is of order 8 and is isomorphic to $\mu_2 \times \mu_4$.

There are thus altogether four non-trivial imprimitive Dirichlet characters modulo 15. Three induced from the three non-trivial characters χ_1, χ_2 and χ_3 of $\mathbb{Z}/5\mathbb{Z}^*$ and one from the only non-trivial character ψ on $\mathbb{Z}/3\mathbb{Z}^*$.

Additionally, there are three non-trivial primitive characters. They are the three products $\psi\chi_i$ with $i = 1$, 2 and 3, and of course, there is the principal one.

We take a closer look at the three characters χ_i. These all have period 5, and they vanish on the set $5\mathbb{Z} \cup 3\mathbb{Z}$ of integers having 3 or 5 as a factor. Now, the same three characters on $\mathbb{Z}/5\mathbb{Z}^*$ induce Dirichlet characters modulo 5 as well, our friends from example 7.7. These all have period 5, but contrary to the previous case, they do not vanish on multiples of 3 unless they also are divisible by 5. So the point we want to illustrate, is that the same characters on the same unit group $\mathbb{Z}/5\mathbb{Z}^*$ induce different Dirichlet characters modulo 5 and modulo 15! ❄

Orthogonality relations

In view of the correspondence between Dirichlet characters modulo m and the characters on group $\mathbb{Z}/m\mathbb{Z}^*$, the orthogonality relations we proved for the characters of an abelian group in propositions 7.3 and 7.4 on page 5 migrate immediately to corresponding orthogonality relations for the Dirichlet characters modulo m:

Proposition 7.6 *Let $m > 1$ be a natural number and let a and b be two integers. Then*

$$\sum_{\chi} \chi(a)\overline{\chi}(b) = \begin{cases} \phi(m) & \textit{if } a \equiv b \mod m \textit{ and } (a,m) = (b,m) = 1 \\ 0 & \textit{otherwise }, \end{cases}$$

where the sum is taken over all Dirichlet characters modulo m.

PROOF: If either a or b has a common factor with m, all terms of the sum on the left vanish. If $(a,m) = (b,m) = 1$, the formulas are just the orthogonality relations for the characters on the unit group $\mathbb{Z}/m\mathbb{Z}^*$, *i.e.,* proposition 7.3 on page 5. ❑

When proving Dirichlet theorem about primes in arithmetic progressions, we shall apply the previous proposition in the following form

Proposition 7.7 *Let $m > 1$ be an natural number and let $a \in \mathbb{Z}$. Then*

$$\sum_{\chi} \chi(a) = \begin{cases} \phi(m) & \textit{if } a \equiv 1 \mod m \\ 0 & \textit{otherwise,} \end{cases}$$

where the sum is taken over all Dirichlet characters of modulus m.

PROOF: Just take $b = 1$ in the previous proposition. ❑

PROBLEM 7.8. Translate the second orthogonality relation in proposition 7.4 on page 6 to a statement about Dirichlet characters. ✸

PROBLEM 7.9. Describe all Dirichlet characters modulo 12 and modulo 24. ✸

The quadratic character

One of the famous functions in number theory is the Legendre symbol appearing in the formulation of quadratic reciprocity. For an odd prime p and $n \in \mathbb{Z}$ the *Legendre symbol* is defined as

$$\Big(\frac{n}{p}\Big) = \begin{cases} 1 & \text{if } n \text{ is a square modulo } p \\ -1 & \text{if } n \text{ is not a square modulo } p \\ 0 & \text{if } (n,p) \neq 1 \end{cases},$$

The Legendre symbol is as we shall see, a primitive Dirichlet character. It is called the *quadratic character modulo p*.

We state without proof, the famous law of *quadratic reciprocity* discovered by Euler and proven by Gauss:

Theorem 7.1 *Let p and q be two odd primes. Then*

$$\Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) = (-1)^{(p-1)/2\cdot(q-1)/2}.$$

The theorem says that if either p or q is of the form $4k+1$ then p a square mod q if and only if q is a square mod p, and if both are of the form $4k+3$, then one of them is a square modulo the other, while the other is not a square modulo the first.

Problem 7.10. Show that 17 is not a square modulo 107. ✷

Problem 7.11. Let p be an odd prime. Recall that the set $A = \{\pm k \mid 0 \leq k \leq (p-1)/2\}$ is called the set of *least representatives* for the residues classes modulo p. In this way the least representatives are divided into a negative part and a positive part. Among the $p-1$ numbers n, $2n$, $\ldots$,$(p-1)n$ a certain number, say μ has a least representative in the negative part of A. Show Gauss' lemma: $\big(\frac{n}{p}\big) = (-1)^{\mu}$. Hint: Show that the residue classes of $n, 2n, \ldots, (p-1)n$ is a full set of representatives for the non-zero residue classes mod p. Uses Wilson's theorem: $(p-1)! \equiv -1 \mod p$. ✷

Problem 7.12. Show that $\big(\frac{2}{p}\big) = (-1)^{(p^2-1)/8}$. ✷

The group of units $\mathbb{F}_p^*$ in the field $\mathbb{F}_p$ with p elements is a cyclic group of order $p-1$. Inside this group is sitting a copy of μ_2; indeed one has $\{\pm 1\} \subseteq \mathbb{F}_p$ since p is odd. From Fermats little theorem—saying that $a^{p-1} = 1$ when $a \in \mathbb{F}_p^*$—we infer that $a^{(p-1)/2} \in \mu_2$. Hence there is the character

$$\psi\colon \mathbb{F}_p \to \mu_2 \qquad \text{given by} \qquad a \mapsto a^{(p-1)/2}.$$

which we denote by ψ for short. Interpreted as a function on the integers it is described as

$$\psi(n) \equiv \begin{cases} 0 & \text{if } (n,p) \neq 1 \\ n^{(p-1)/2} & \text{if } (n,p) = 1 \end{cases}$$

Appealing to the little Fermat theorem once more, one has $(a^2)^{(p-1)/2} = 1$, and whith this, it is easily verified that wed have the following exact sequence:

$$\begin{tikzcd} 1 \arrow[r] & \mu_2 \arrow[r] & \mathbb{F}_p^* \arrow[r, "s"] & \mathbb{F}_p^* \arrow[r, "\psi"] & \mu_2 \arrow[r] & 1, \end{tikzcd}$$

where s denotes the squaring-map $s(a) = a^2$. An element $a \in \mathbb{F}_p^*$ is therefore a square if and only if $a^{(p-1)/2} = 1$. We have shown that the Dirichlet character associated to ψ coincides with the Legendre symbol.

The definition of the Legendre symbol is restricted to p being a prime, but it can be gerealised to any odd odd number, and it is then called the *Jacobi symbol*. Assume $m = p_1^{e_1} \cdot \dots \cdot p_r^{e_r}$ is an odd composite number. There is a surjection $\mathbb{Z}/m\mathbb{Z}^* \simeq \prod_i \mathbb{Z}/p_i^{e_i}\mathbb{Z}^* \to \prod_i \mathbb{Z}/p_i\mathbb{Z}^*$, and for each of the factors $\mathbb{Z}/p_i\mathbb{Z}^*$ we have the quadratic character $\psi_i \colon \mathbb{Z}/p_i\mathbb{Z} \to \mu_2$. Hence their product $\psi_1 \cdot \dots \cdot \psi_r$ is a character on $\mathbb{Z}/m\mathbb{Z}$ with values in μ_2, as well as is the combination $\psi_1^{e_1} \cdot \dots \psi_r^{e_r}$. This is called the *Jacobi symbol*, and is the quadratic character modulo m. It is denoted by $\left(\frac{n}{m}\right)$, and one has

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right)^{e_1} \cdot \dots \cdot \left(\frac{n}{p_r}\right)^{e_r}$$

PROBLEM 7.13. Show that $\left(\frac{n}{m}\right)$ is multiplicative in both n and m. ✷

PROBLEM 7.14. It is no longer true that $\left(\frac{n}{m}\right) = 1$ implies that n is a sqaure modulo m. Give an example that manifests this. However, if $\left(\frac{n}{m}\right) = -1$, then n cannot be a square modulo m. Show this. ✷

Addendum

For the benefit of those in the audience who are not completely comfortable with Euler's ϕ-function, we give a quick an dirty exposition of its main properties. And in view of their prominent role in the theory of Dirichlet characters we use the opportunity to describe the groups of units in the finite rings $\mathbb{Z}/n\mathbb{Z}$.

The Euler ϕ-function

There are two definitions of ϕ easily seen to be equivalent. On the one hand $\phi(m)$ is the number residue classes $\overline{n}$ such that n and m are relatively prime. This is equivalent to m being invertible in the ring $\mathbb{Z}/m\mathbb{Z}$; indeed $(n, m) = 1$ is equivalent to there being a relation $1 = an + bm$ with $a, b \in \mathbb{Z}$, and this in its turn, is equivalent to n being invertible mod m (then inverse is the class of a).

Hence $\phi(m)$ is the order of the unit group $\mathbb{Z}/m\mathbb{Z}^*$, *i.e.*, $\phi(m) = |\mathbb{Z}/m\mathbb{Z}^*|$. The computation of $\phi(m)$ hinges on the two following propositions.

Proposition 7.8 *The Euler ϕ-function is multiplicative, i.e., if n and n' are two relatively prime natural numbers, one has:*

$$\phi(nn') = \phi(n)\phi(n')$$

Proof: Since n and n' are relatively prime, the Chinese remainder theorem gives a ring isomorphism $\mathbb{Z}/nn'\mathbb{Z} \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}$ which induces an isomorphism between the unit groups: $\mathbb{Z}/nn'\mathbb{Z}^* \simeq \mathbb{Z}/n\mathbb{Z}^* \times \mathbb{Z}/n'\mathbb{Z}^*$. The proposition follows. ❏

In case $m = p$ is a prime, the ring $\mathbb{Z}/p\mathbb{Z}$ is a field, and of course $\mathbb{Z}/p\mathbb{Z}^*$ is of order $p - 1$. This proves the first case $\nu = 1$ of the following proposition.

Proposition 7.9 *Assume that p is a prime and ν a natural number. Then $\phi(p^\nu) = p^{\nu-1}(p-1)$.*

We would like to use the following very general lemma:

Lemma 7.2 *Let A and B be commutative rings with 1 an let $\phi\colon A \to B$ be a surjective ring homomorphism with kernel I. Assume that $I^2 = 0$. Then there is an exact sequence of unit groups:*

$$\begin{tikzcd} 0 \arrow[r] & 1+I \arrow[r] & A^* \arrow[r, "\phi^*"] & B^* \arrow[r] & 1 \end{tikzcd}$$

where ϕ^* denotes the restriction of ϕ to the units.

Proof: From $I^2 = 0$ it follows that $1 + a$ is a unit for all $a \in I$; indeed, $1 - a$ is an inverse to $1 + a$: $(1 + a)(1 - a) = 1 - a^2 = 1$. In the same vain $1 + I$ is closed under multiplication since $(1+a)(1+b) = 1+a+b+ab = 1+a+b$, and clearly $1+I = \operatorname{Ker}\phi^*$. Observe that the multiplicative group $1 + I$ is isomorphic to the additive group I.

What is left is to see that ϕ^* is surjective. So take any unit $b \in B^*$. Lift b to some a in A and b^{-1} to some a'. One has $aa' = 1 + \alpha$ with $\alpha \in I$, but this gives $aa'(1 - \alpha) = 1$ and a is invertible. ❏

Proof of Proposition 7.9: The proof goes by induction on the exponent ν. If $\nu = 1$, we are through as already remarked just before the proposition. If $\nu > 1$, there is the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & p^\nu\mathbb{Z}/p^{\nu+1}\mathbb{Z} \arrow[r] & \mathbb{Z}/p^{\nu+1}\mathbb{Z} \arrow[r, "\phi"] & \mathbb{Z}/p^\nu\mathbb{Z} \arrow[r] & 0 \end{tikzcd},$$

where ϕ is the natural reduction mod p^ν homomorphism. The kernel $p^\nu\mathbb{Z}/p^{\nu+1}\mathbb{Z}$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ (an isomorphism sends the class of a mod p to the class of $p^\nu a$ mod $p^{\nu+1}$), and by the general lemma above, there is an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & 1 + p^\nu\mathbb{Z}/p^{\nu+1}\mathbb{Z} \arrow[r] & \mathbb{Z}/p^{\nu+1}\mathbb{Z}^* \arrow[r] & \mathbb{Z}/p^\nu\mathbb{Z}^* \arrow[r] & 1 \end{tikzcd}.$$

Counting orders, we get

$$|\mathbb{Z}/p^{\nu+1}\mathbb{Z}^*| = |\mathbb{Z}/p^\nu\mathbb{Z}^*||p^\nu\mathbb{Z}/p\mathbb{Z}| = p^{\nu-1}(p-1)p = p^\nu(p-1),$$

and the proposition follows. ❏

We sum up the properties of the ϕ-function in the following proposition:

Proposition 7.10 *The following hold for the Euler ϕ-function:*

- □ $\phi(nn') = \phi(n)\phi(n')$ *when* $(n, n') = 1$,
- □ $\phi(p^\nu) = p^{\nu-1}(p-1)$ *when* p *is a prime,*
- □ $\phi(n)/n = \prod_{p|n}(1-p^{-1})$.

PROOF: The two first formulas are already shown. For the last, write $n = p_1^{\nu_1} \cdot \dots \cdot p^{\nu_r}$ with the p_i's different primes. Using the two first properties we find the expression

$$\phi(n) = \prod_i p_i^{\nu_i - 1}(p_i - 1).$$

Divide throughout by n to arrive at the third formula in the proposition. ❏

The behavior of the Euler ϕ-function is rather erratic. For example, A. Schinzel has shown that the fractions of two consecutive values of $\phi(n)$ form a dense subset of the set of all positive real numbers; that is, the fraction $\phi(n+1)/\phi(n)$ can be as close as you want to any number in $\mathbb{R}^+$. However the quotient $\phi(n)/n$ behaves somehow more regularly. Obviously $\phi(n)/n < 1$, and if p is a prime one has $\phi(p)/p = 1 - 1/p$, which is close to one. There being infinity many prime we infer that

$$\limsup_{n\to\infty} \phi(n)/n = 1.$$

This is illustrated in the figure below, where the values $\phi(n)$ is plotted against n for n up to 800. The cloud of plotted points is clearly bounded above by the line $y = x$. On the other hand, if n has a lot of prime factors the quotient $\phi(n)/n$ tends to be small.

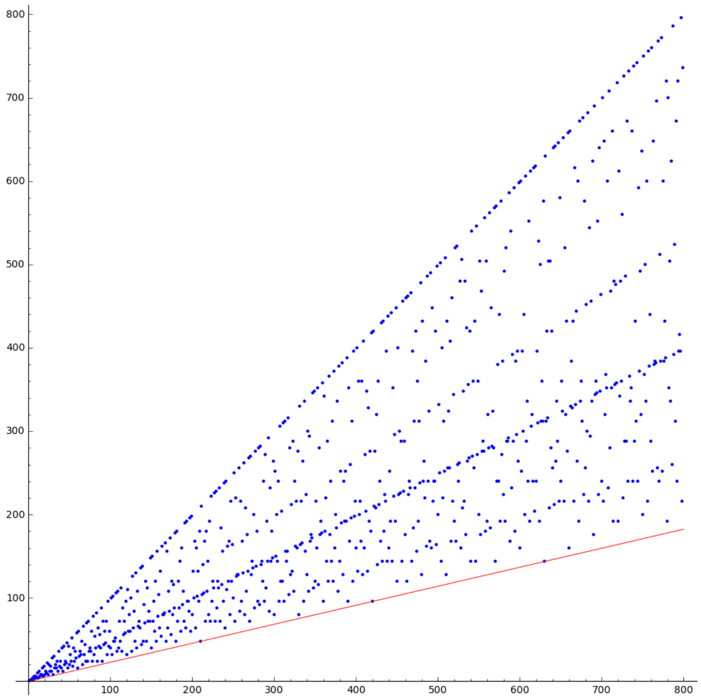
In lemma 6.1 on page 5 in chapter 6 we established the inequality

$$\prod_{p\leq x}(1-p^{-1}) < 1/\log x,$$

and taking $n = \prod_{p\leq n} p$, a number with an awful lot of prime factors, we obtain a number with $\phi(n)/n < 1/\log x$. This shows that

$$\liminf_{n\to\infty} \phi(n)/n = 0.$$

This behavior is not apparent in the figure, the reason being that n has to be a very large number for $\phi(n)/n$ to be very small, certainly much larger than 800. Of the numbers of the form $\prod_{p\leq n} p$ considered above, only $2\cdot 3\cdot 5\cdot 7$ is less than 800!



$\phi(n)$ against n for $n \leq 800$

Problem 7.15. On the figure the line $y = 8/35 \cdot x$ is printed in red. Can you explain why (the line is printed, not why it is red)? There are three blue dots on it; explain that. Can you predict the coordinates of those points? And what is the next blue dot on the line? ✷

Problem 7.16. There seems to be a lot of blue dots on the line $y = 1/2 \cdot x$. Why? ✷

The groups of units $\mathbb{Z}/n\mathbb{Z}^*$

Let $n = \prod_{p|n} p^{\nu_p}$ be the prime factorization of the natural number n. By our friends the chineses the ring $\mathbb{Z}/n\mathbb{Z}$ decomposes as the direct product of rings $\mathbb{Z}/n\mathbb{Z} \simeq \prod_{p|n} \mathbb{Z}/p^{\nu_p}\mathbb{Z}$, and hence there is a corresponding decomposition of the group of units $\mathbb{Z}/n\mathbb{Z}^* = \prod_{p|n} \mathbb{Z}/p^{\nu_p}\mathbb{Z}^*$. Thus, knowing the group structure of each of the factor groups we know the structure of the group $\mathbb{Z}/n\mathbb{Z}^*$. In what follows we determine the group structure of $\mathbb{Z}/p^{\nu}\mathbb{Z}^*$ for p a prime.

The cases p odd and $p = 2$ are slightly different, although the underlying structure is the same. In both cases there is an obvious reduction map $\mathbb{Z}/p^{\nu}\mathbb{Z}^*$ to a cyclic group, respectively $\mathbb{Z}/p\mathbb{Z}^*$ and $\mathbb{Z}/4\mathbb{Z}^*$. In case $p = 2$ the group $\mathbb{Z}/4\mathbb{Z}^*$ is the simplest factor group that gives something, $\mathbb{Z}/2\mathbb{Z}^*$ being trivial.We shall see that these sequences are split, and in both cases the kernel will be cyclic.

In the odd case the result is simply that $\mathbb{Z}/p^{\nu}\mathbb{Z}^*$ is cyclic, while if $p = 2$, the unit groups are isomorphic to direct products $\mathbb{Z}/2^{\nu-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ if $\nu \geq 3$, and $\mathbb{Z}/4\mathbb{Z}^* = \mu_2$ and $\mathbb{Z}/2\mathbb{Z}^*$ is trivial. That is, one has:

Proposition 7.11 *Let p be a prime number.*

□ *If $p \neq 2$, then the group of units $\mathbb{Z}/p^\nu\mathbb{Z}^*$ is cyclic of order $p^{\nu-1}(p-1)$.*

□ *If $p = 2$ and $\nu \geq 3$, the group of units $\mathbb{Z}/2^\nu\mathbb{Z}^*$ is isomorphic to the direct product $\mathbb{Z}/2^{\nu-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

□ *$\mathbb{Z}/4\mathbb{Z}^*$ is cyclic of order 2, and $\mathbb{Z}/2\mathbb{Z}^*$ is trivial.*

The proof will be a series of lemmas, the first being:

Lemma 7.3 *For any natural number a one has*

$$(1+p)^{p^a} \equiv 1 + p^{a+1} \mod p^{a+2}.$$

PROOF: Induction on a, the start $a = 1$ is clear. So assume that

$$(1+p)^{p^a} \equiv 1 + p^{a+1} \mod p^{a+2}.$$

Now, since the binomial coefficients $\binom{p}{k}$ for $k \neq 1, p$ all are divisible by p, it holds that if $x \equiv y \mod p^s$, then $x^p \equiv y^p \mod p^{s+1}$. This gives

$$(1+p)^{p^{a+1}} \equiv (1+p^{a+1})^p = 1 + p \cdot p^{a+1} + \sum_{k \geq 2} \binom{p}{k} p^{k(a+1)} \equiv 1 + p^{a+2} \mod p^{a+3}$$

since $k(a+1) \geq a+3$ as $k \geq 2$. ❑

We start with treating the case of odd p, and start with the simplest case $\mathbb{Z}/p\mathbb{Z}$. This is a field, and there is the general esult

Proposition 7.12 *If k is a field and $G \subseteq k^*$ a finite subgroup, then G is cyclic.*

PROOF: Let d be the exponent of G; *i.e.,* the least common multiple of the orders of all the elements in G. A finite group G is cyclic if and only if $d = |G|$; indeed, if G is cyclic this is clear, and for the implication the other way use that there is always an element of order d in G. The elements in G satisfy the equation $x^d = 1$, which has at most d solutions. It follows that $d = |G|$, and G is cyclic. ❑

Lemma 7.4 *Assume that p is an odd prime. The the group of units $\mathbb{Z}/p^\nu\mathbb{Z}^*$ is cyclic of order $p^{\nu-1}(p-1)$.*

PROOF: We determined the order in previous paragraph.

The reduction modulo p map induces an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & K \arrow[r] & \mathbb{Z}/p^\nu\mathbb{Z}^* \arrow[r] & \mathbb{Z}/p\mathbb{Z}^* \arrow[r] & 1 \end{tikzcd}$$

where the kernel K is of order $p^{\nu-1}$. Lift a generator of $\mathbb{Z}/p\mathbb{Z}^*$ to an element $g \in \mathbb{Z}/p^\nu\mathbb{Z}^*$, then $g^{p-1} = a \in K$, and since $p-1$ is relatively prime to the order $p^{\nu-1}$ of K, there is an element $b \in K$ with $b^{p-1} = a$. Therefore $(ga)^{p-1} = 1$, and the sequence splits[4]; that is $\mathbb{Z}/p^\nu\mathbb{Z}^* \simeq K \times \mathbb{Z}/p\mathbb{Z}^*$. Since $\mathbb{Z}/p\mathbb{Z}^*$ is cyclic of order $p-1$, it suffices to show that K i cyclic (of order $p^{\nu-1}$). This we shall do by showing that $1+p$ is a generator. By lemma 7.3 above one has in $\mathbb{Z}/p^\nu\mathbb{Z}^*$ (that is modulo p^ν)

$$(1+p)^{p^{\nu-2}} = 1 + p^{\nu-1} \neq 1$$

since $p^{\nu-1}$ is non-zero in $\mathbb{Z}/p^\nu\mathbb{Z}$, and we conclude that the order of $1+p$ is equal to $p^{\nu-1}$. ❑

Lemma 7.5 *The group of units $(\mathbb{Z}/4\mathbb{Z})^*$ is a cyclic group of order 2, and $\mathbb{Z}/2\mathbb{Z}^*$ is trivial. If $v > 2$, it holds that $\mathbb{Z}/2^v\mathbb{Z}^*$ is isomorphic to a product of two cyclic groups respectively of orders 2 and $2^{\nu-2}$.*

PROOF: The residue classes in $\mathbb{Z}/4\mathbb{Z}$ are 0, ± 1 and 2 and ± 1 are the only units, hence $\mathbb{Z}/4\mathbb{Z}^*$ is isomorphic with μ_2. In the general, case the exact sequence

$$1 \longrightarrow K \longrightarrow \mathbb{Z}/2^\nu\mathbb{Z}^* \longrightarrow \mathbb{Z}/4\mathbb{Z}^* \longrightarrow 1$$

corresponding to the reduction modulo 4 map splits, indeed $\{\pm 1\} \subseteq \mathbb{Z}/2^\nu\mathbb{Z}^*$ gives a splitting. Just as in the case with $p > 2$, we show that the kernel K is cyclic. The first element you think of in kernel, is 5, and it turns out to be a generator:

$$5^{2^{\nu-2}} = (1+4)^{2^{\nu-2}} = 1 + 2^{2^{\nu-2}} \cdot 4 = 1,$$

and 5 is of order a power of 2. Furthermore on has

$$5^{2^{\nu-3}} = (1+4)^{2^{v-3}} = 1 + 2^{2^{\nu-2}} \cdot 4 = 1 + 2^{\nu-1} \neq 1.$$

This shows that the order of 5 is $2^{\nu-2}$, which is the same as the order of the kernel K. Hence the kernel is cyclic. ❑

[4] This is a general fact. If in an exact sequence of abelian groups, the two extreme groups are of relatively prime order, the sequence splits. (It is even true, but much deeper, for non abelian finite groups.)