

Solution to Sheet 3.

Facts from multiplicative number theory.

Given some $n = p_1^{e_1} \cdots p_r^{e_r} \in \mathbb{N}$, we want to investigate the structure of the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$. By the chinese remainder theorem we find

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \left(\prod_{i=1}^n (\mathbb{Z}/p_i^{e_i}\mathbb{Z}) \right)^\times \cong \prod_{i=1}^n (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times,$$

so we really only care about the structure of $(\mathbb{Z}/p^e\mathbb{Z})^\times$. There, the structure is given by

$$(\mathbb{Z}/p^e\mathbb{Z})^\times \cong \begin{cases} \text{a cyclic subgroup of order } \varphi(p^e) & \text{if } p \text{ is odd} \\ \langle 3 \rangle & \text{if } p = 2 \text{ and } e \leq 2 \\ \pm\langle 5 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{e-2}\mathbb{Z} & \text{if } p = 2 \text{ and } e \geq 3. \end{cases}$$

A generator of \mathbb{F}_p^\times , or more generally, a generator of $(\mathbb{Z}/p^e\mathbb{Z})^\times$ is called a *root of unity*. We have the *Legendre symbol*, which for $a \in \mathbb{Z}$ and an odd prime p is given by

$$\left(\frac{a}{p} \right) = \begin{cases} 0 & \text{if } p \mid a \\ (-1) & \text{if there is no solution mod } p \text{ to } x^2 = a \\ 1 & \text{otherwise.} \end{cases}$$

It is multiplicative in a , hence it yields a character $(\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$. The subgroup of *quadratic residues mod p* is given by $\text{Ker} \left(\left(\frac{\cdot}{p} \right) \right) = \langle \varpi^2 \rangle$ for ϖ a root of unity. *Quadratic reciprocity* states that for two odd primes p, q , we have

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

and there are the *supplementary laws*

$$\left(\frac{-1}{p} \right) = (-1)^{\frac{p-1}{2}} \quad \text{and} \quad \left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}.$$

Given a finite abelian group G , we define the group of *characters* of G as

$$\widehat{G} = \text{Hom}_{\mathbf{Ab}}(G, \mathbb{C}^\times) = \text{Hom}_{\mathbf{Ab}}(G, S^1).$$

Given a cyclic group $G \cong \mathbb{Z}/n\mathbb{Z}$, there is an isomorphism $G \cong \widehat{G}$ given by $a \mapsto (1 \mapsto \zeta_n^a)$, where ζ_n is an n -th root of unity. As we also have $\widehat{G} \oplus \widehat{H} = \widehat{G \oplus H}$, this shows that there are isomorphisms $G \cong \widehat{G}$ for *all* finite abelian groups¹.

¹The first isomorphism is the universal property of the direct sum: We have

$$\text{Hom}_{\mathbf{Ab}}(G \oplus H, \mathbb{C}^\times) \cong \text{Hom}_{\mathbf{Ab}}(G, \mathbb{C}^\times) \oplus \text{Hom}_{\mathbf{Ab}}(H, \mathbb{C}^\times).$$

Remember that every finite group is a finite product (equivalently, finite direct sum) of cyclic groups.

Exercise 1 & 2.

1. Note that the real characters are exactly those $\chi : (\mathbb{Z}/p\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ with $\chi^2 = 1$. As p is odd, there are exactly two solutions to $x^2 = 1$, hence there are exactly 2 real characters mod p , one of which is the trivial one (induced by the principle character mod 1), and the other is given by the legendre symbol. The same reasoning goes through mod p^e for $e \geq 2$ (the multiplicative group is cyclic of even order), but now the characters are induced from characters mod p .

2. For $n = 2^r$, we find again that the real Dirichlet characters are in bijection with the set $\{x \in \mathbb{Z}/n\mathbb{Z} \mid x^2 - 1 = 0\}$. By the structure of the multiplicative group given above, this set has 1 element if $r = 1$, it has 2 elements if $r = 2$ and 4 elements if $r \geq 3$. We find:

- The multiplicative group of $\mathbb{Z}/2\mathbb{Z}$ is trivial, so there is only the character given by $1 \mapsto 1$, which is induced by the principle character.
- On $\mathbb{Z}/4\mathbb{Z}$ we have again the principle character and the primitive character χ_{-4} uniquely defined via $\chi_{-4}(-1) = -1$.
- On $\mathbb{Z}/8\mathbb{Z}$ we have the principle character, the one induced by χ_{-4} and the two characters $\chi_{\pm 8}$, where $\chi_{\pm 8}(3) = \mp 1$, $\chi_{\pm 8}(5) = -1$ and $\chi_{\pm 8}(7) = \pm 1$.

3. We inspect the map

$$\mu : \widehat{(\mathbb{Z}/r\mathbb{Z})^\times} \times \widehat{(\mathbb{Z}/s\mathbb{Z})^\times} \rightarrow \widehat{(\mathbb{Z}/n\mathbb{Z})^\times} \quad (\chi_1, \chi_2) \mapsto \chi_1 \chi_2.$$

We claim that this map is injective. Indeed, assume that we are given two characters χ_1 mod r and χ_2 mod s such that for all $m \in \mathbb{N}$,

$$\chi(m) = \chi_1(m \bmod r) \chi_2(m \bmod s).$$

Then whenever we are given $m \in \mathbb{N}$ such that $m \equiv 1 \pmod{s}$, we find

$$\chi(m) = \chi_1(m),$$

and similarly for χ_2 . But the chinese remainder theorem asserts that these equalities already define χ_1 and χ_2 uniquely: For any $a \in (\mathbb{Z}/r\mathbb{Z})^\times$, there is some $m \in \mathbb{N}$ such that $m \equiv a \pmod{r}$ and $m \equiv 1 \pmod{s}$. Now μ is an injective map of sets with the same cardinality, hence bijective.

It remains to show that χ_1 and χ_2 are primitive iff χ is. Suppose first that χ_1 was not primitive, i.e., has conductor $d < r$. Then we can write $\chi_1 = \tilde{\chi} \chi_{0,r}$ where $\tilde{\chi}$ is a character mod d and $\chi_{0,r}$ is the principal character mod r . Now $\chi' = \tilde{\chi} \chi_2$ is a character modulo ds and induces χ , since

$$\chi = \chi \chi_{0,rs} = \chi_1 \chi_2 \chi_{0,rs} = \tilde{\chi} \chi_{0,r} \chi_2 \chi_{0,rs} = \chi' \chi_{0,r} \chi_{0,rs} = \chi' \chi_{0,rs}.$$

There is a neat way to now show the converse. Let $\varphi_2(n)$ denote the number of primitive characters mod n . For any $d \mid n$, the set of primitive characters mod d is in bijection with the characters mod n of conductor d , so we find

$$\varphi(n) = \widehat{\#}(\widehat{\mathbb{Z}/n\mathbb{Z}})^\times = \sum_{d \mid n} \varphi_2(n) = (1 \star \varphi_2)(n),$$

implying that $\varphi_2 = \mu \star \varphi$ by moebius-inversion. Hence φ_2 is multiplicative. We have shown already that the inverse of μ restricts to a (necessarily) injective map

$$\mu^{-1} : \{\text{primitive characters mod } n\} \rightarrow \{\text{pr. characters mod } r\} \times \{\text{pr. characters mod } s\}.$$

By multiplicity of φ_2 , this is a injective map of sets of the same cardinality, therefore μ^{-1} is a bijection, and we are done.

Alternatively we can calculate this directly. Assume that χ_1 and χ_2 are primitive. Choose a character $\tilde{\chi} \bmod d$ that induces χ , so we may write

$$\chi_1 \chi_2 = \tilde{\chi} \chi_{0,rs} = (\tilde{\chi}_1 \chi_{0,r})(\tilde{\chi}_2 \chi_{0,s}),$$

where $\tilde{\chi}_1$ is a character of conductor $d_1 \mid r$ and $\tilde{\chi}_2$ is a character of conductor $d_2 \mid s$. But by uniqueness of χ_1 and χ_2 , we find $\chi_1 = \tilde{\chi} \chi_{0,r}$ and $\chi_2 = \tilde{\chi} \chi_{0,s}$, implying $d = rs$ by primitivity of χ_1 and χ_2 .

4. Writing $n = 2^r q$ with q odd, we find that the number of primitive real characters mod n is given by

$$\begin{cases} 1 & \text{if } r = 0 \text{ and } q \text{ square-free,} \\ 0 & \text{if } r = 1 \text{ and } q \text{ square-free,} \\ 1 & \text{if } r = 2 \text{ and } q \text{ square-free,} \\ 2 & \text{if } r = 3 \text{ and } q \text{ square-free,} \\ 0 & \text{if } r \geq 4 \text{ or } q \text{ not square-free.} \end{cases}$$

5. Clearly the product of two fundamental discriminants (FDs) is again a FD, and we have $\chi_{D_1 D_2} = \chi_{D_1} \chi_{D_2}$. Also, given a fundamental discriminant D with $|D| = d_1 d_2$ and $(d_1, d_2) = 1$, there are fundamental discriminants D_1, D_2 with $d_i = \pm D_i$ and $D_1 D_2 = D$. So we can reduce to the case where $|D| = p^r$ is a prime power. As a first reality check, we find that if p is odd, the only fundamental discriminant of this type is $D = (-1)^{\frac{p-1}{2}} p$, in which case χ_D is given by the unique real primitive character, given by (using quadratic reciprocity)

$$\chi_D(q) = \left(\frac{(-1)^{(p-1)/2} p}{q} \right) = \left(\frac{q}{p} \right).$$

There are no FDs with $|D| = 2$ or $|D| = 2^r$ with $r \geq 4$. If $|D| = 4$ there is one ($D = -4$), and if $n = 8$ there are two ($D = \pm 8$). Using quadratic reciprocity and the supplementary laws, it is easily seen that these are exactly the characters described above.