Math 250a hw5

8. Let p be a prime number, and let $A = \mathbb{Z}/p^4\mathbb{Z}$ ($r \in \mathbb{Z}_{\geq 1}$). Let $G = A^\times$. Show that G is cyclic, except in the case when

$$p = 2, r \geq 3$$

in which case it is of type $(2, 2^{r-2})$. [Hint: In the general case, show that $\langle 1+p \rangle \cong \mathbb{Z}/p^{r-1}\mathbb{Z}$ and $G \cong \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$. In the exceptional case, show that $\langle 5 \rangle \cong \mathbb{Z}/2^{r-2}\mathbb{Z}$ and $G \cong \langle 5 \rangle \times \{\pm 1\}$.]

The idea is provided in the hint. Here are some handy observations.

About binomial coefficients, $\nu_p(\binom{p^m}{i}) = m - \nu_p(i)$ where $\nu_p(n)$ denotes the exponent of the largest power of p which divides n.

In the general case, to show that the order or $1+p$ is not p^m for any $m < r-1$, observe that $\forall a \in \mathbb{Z}, \forall m < r$,

$$a \equiv 1 \mod p^r \implies a \equiv 1 \mod p^m.$$

Since $\nu_p(i) < i$ for all prime p and positive integers i, we have

$$(1+p)^{p^m} = \sum_{i=0}^{p^m} \binom{p^m}{i} p^i \equiv 1 + p^{m+1} \mod p^{m+2}.$$

Then $\forall m < r-1$, $(1+p)^{p^m} \not\equiv 1 \mod p^{m+2}$. By contrapositive, $(1+p)^{p^m} \not\equiv 1 \mod p^r$.

To show that $G \cong \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$, consider the homomorphism

$$f : G \to (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}, x \mapsto x \mod p.$$

Indeed, $\langle 1+p \rangle = \ker f$ since LHS is contained in RHS and orders match. Since f is a surjection, $G/\ker f \cong \mathbb{Z}/(p-1)\mathbb{Z}$. Since $p \neq 2, r \geq 1$, $p-1$ and p^{r-1} are coprime. By the classification of abelian groups, $G \cong \mathbb{Z}/p^{r-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$.

In the exceptional case, consider the homomorphism

$$f : G \to (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z}, x \mapsto x \mod 4.$$

Again, $\langle 5 \rangle = \ker f$ and -1 represents the preimage of $-1 \in (\mathbb{Z}/4\mathbb{Z})^\times$ under f.

11. Let R be the ring of trigonometric polynomials as defined in the text. Show that R consists of all functions f on $\mathbb{R}$ which have an expression of the form

$$f(x) = a_0 + \sum_{m=1}^{n} (a_m \cos mx + b_m \sin mx),$$

where $a_0, a_m, b_m \in \mathbb{R}$. Define the **trigonometric degree** $\deg_{tr}(f) := \max\{r \in \mathbb{Z} : a_r \neq 0 \text{ or } b_r \neq 0\}$. Prove that

$$\deg_{tr}(fg) = \deg_{tr}(f) + \deg_{tr}(g).$$

Deduce from this that R has no zerodivisors, and that the functions $\sin x$ and $1 - \cos x$ are irreducible elements in that ring.

Suppose $\deg_{tr}(f) = r, \deg_{tr}(g) = s$. Let the highest degree terms of f be $a\cos(rx) + b\sin(rx)$ and the highest degree terms of g be $c\cos(sx) + d\sin(sx)$. Then $a^2 + b^2 > 0$ and $c^2 + d^2 > 0$. The highest possible trigonometric degree of fg is $r + s$. The degree $r + s$ terms of fg are $\frac{ac-bd}{2}\cos((r+s)x)$ and $\frac{ad+bc}{2}\sin((r+s)x)$. Since $(ac-bd)^2 + (ad+bc)^2 = (a^2+b^2)(c^2+d^2) \neq 0$, we know that not both coefficients vanish, and $\deg_{tr}(fg) = r + s$.