Let $F$ be a field. Then all nonzero elements of $F$ are invertible:

$$F^\times = F - \{0\}.$$ 

An important part of the description of fields is that finite multiplicative subgroups of $F^\times$ are cyclic. In this note we give a detailed proof, see Serre [1, p. 4], of a slightly more general result and provide examples. We first prove a couple of straightforward lemmas.

Let $\mathbb{Z}_n$ be the cyclic group of order $n \geq 1$, defined as

$$\mathbb{Z}_n := \langle x \mid x^n = 1 \rangle.$$ 

Recall the Euler $\phi$ function: $\phi(n)$ counts the number of positive integers up to $n$ that are prime to $n$.

**Lemma 1.1.** The number of elements of $\mathbb{Z}_n$ with order $m \geq 1$ is $\phi(m)$ if $m|n$ and 0 otherwise.

**Proof.** For $x$ a generator of $\mathbb{Z}_n$, we claim that the order of $x^a$ in $\mathbb{Z}_n$ is $n/(a,n)$ for all $a \in \mathbb{Z}_{\geq 0}$. The claim is true for $a = 0$. Fix $a > 0$ and denote the order of $x^a$ by $k$. Check that

$$(x^a)^{n/(a,n)} = 1$$

since $n \mid an/(a,n)$ so that

$$k \mid n/(a,n).$$

We must also have $n|ak$ if the order of $x^a$ is $k$. Hence

$$n/(a,n) \mid a/(a,n) \cdot k.$$ 

But $n/(a,n)$ and $a/(a,n)$ are relatively prime implies

$$n/(a,n) \mid k.$$ 

Then (1.1) and (1.2) prove the claim that $k = n/(a,n)$.

Now we just need to count the solutions to $m = n/(a,n)$ for $0 \leq a \leq n - 1$. Since $n/(a,n)$ divides $n$ there are no solutions for $m$ not dividing $n$. For $m$ dividing $n$ we require

$$(a,n) = n/m.$$ 

Hence $a$ must be of the form $n/m \cdot b$ with $(b,m) = 1$ and $1 \leq b < m$. There are $\phi(m)$ such $b$s.

**Lemma 1.2.** We have

$$\sum_{d|n} \phi(d) = n$$

**Proof.** This follows from Lemma 1.1: since each element in $\mathbb{Z}_n$ has order $d$ dividing $n$, both sides of (1.3) count the number of elements in $\mathbb{Z}_n$.

**Theorem 1.3.** Let $G$ be a finite group of order $n$. For every divisor $d$ of $n$ suppose that the number of $g \in G$ satisfying $g^d = 1$ is at most $d$. Then $G$ is cyclic.

**Proof.** Denote by $\psi(m)$ the number of elements in $G$ of order $m$. Since every element of $G$ has order dividing $n$, we see

$$\sum_{d|n} \psi(d) = n.$$ 

Let $d$ be a divisor of $n$ and suppose $\psi(d) \neq 0$, with $x \in G$ of order $d$. Then

$$\langle x \rangle = \{1, x, x^2, \ldots, x^{d-1}\}.$$ 

---

*Date: Dec 1, 2012.*
For \( y \in \langle x \rangle \) we have \( y^d = (x^i)^d = (x^d)^i = 1 \), so by our hypothesis \( \langle x \rangle \) contains all the solutions \( g \in G \) to \( g^d = 1 \). In particular \( \langle x \rangle \) contains all the elements in \( G \) of order \( d \). By Lemma 1.1, \( \langle x \rangle \) contains exactly \( \phi(d) \) such elements. Hence we have proved that \( \psi(d) \) is 0 or \( \phi(d) \). Therefore, with (1.3) and (1.4),
\[
\psi(n) = \sum_{d|n} \phi(d) = \sum_{d|n} \phi(d) = n \tag{1.5}
\]
and we must have equality in (1.5) with \( \psi(d) = \phi(d) \) for all \( d|n \). In particular, \( \psi(n) = \phi(n) \geq 1 \) so that there is an element of \( G \) of order \( n \), proving that \( G \) is cyclic.

**Corollary 1.4.** For \( F \) a field, every finite multiplicative subgroup of \( F^\times \) is cyclic.

**Proof.** As we showed in class, \( x^d - 1 \in F[x] \) has at most \( d \) roots in \( F \). Therefore Theorem 1.3 applies.

**Corollary 1.5.** For \( F \) a field and \( G \) a finite multiplicative subgroup, the number of elements of \( G \) of order \( d \) is \( \phi(d) \) if \( d \) divides \( |G| \) and 0 otherwise.

**Corollary 1.6.** Let \( \mathbb{F}_q \) be a finite field. Then \( \mathbb{F}_q^\times \) must be a cyclic group of order \( q - 1 \).

**Example 1.7.** Corollary 1.6 implies that \( (\mathbb{Z}/p\mathbb{Z})^\times \) is cyclic. No formula is known for any of the \( \phi(p-1) \) generators of \( (\mathbb{Z}/p\mathbb{Z})^\times \). The smallest generators, for \( p \) running over the first 100 primes, are:
\[
1, 2, 2, 3, 2, 2, 3, 5, 2, 3, 2, 6, 3, 5, 2, 2, 2, 2, 7, 5, 3, 2, 3, 5, 2, 5, 2, 6, 3, 3, 2, 3,
2, 2, 6, 5, 2, 5, 2, 2, 2, 19, 5, 2, 3, 2, 3, 2, 6, 3, 7, 7, 6, 3, 5, 2, 6, 5, 3, 3, 2, 5, 17, 10, 2,
3, 10, 2, 2, 3, 7, 6, 2, 2, 5, 2, 5, 3, 21, 2, 2, 7, 5, 15, 2, 3, 13, 2, 3, 2, 13, 3, 3, 2, 7, 5, 2, 3, 2, 2.
\]
Tables like these were studied by Gauss. *Artin’s conjecture for primitive roots* (1927) states that each squarefree integer \( a \neq -1 \) is a generator for infinitely many primes \( p \). Despite much progress, the conjecture is still open.

We also note that, even though \( \mathbb{Z}/p^n\mathbb{Z} \) is not a field for \( n > 1 \), we do have that \( (\mathbb{Z}/p^n\mathbb{Z})^\times \) is cyclic for \( p \) an odd prime. In the following two examples we confirm Corollary 1.4 for the fields \( \mathbb{C} \) and \( \mathbb{Q}_p \).

**Example 1.8.** The elements of any finite subgroup of \( \mathbb{C}^\times \) must be of finite order. Therefore they must be roots of unity: complex numbers of the form
\[
\exp(2\pi i h/k) \quad \text{for} \quad h/k \in \mathbb{Q} \cap [0, 1).
\]
Hence any finite subgroup \( G \) of \( \mathbb{C}^\times \) is isomorphic to a finite subgroup of \( \mathbb{Q}/\mathbb{Z} \) and necessarily cyclic, generated by \( \exp(2\pi i h/k) \in G \) with minimal \( h/k > 0 \).

**Example 1.9.** Let \( \mathbb{Q}_p \) be the field of \( p \)-adic numbers for \( p \) an odd prime. The only roots of unity in \( \mathbb{Q}_p \) are the Teichmüller representatives
\[
\omega(1), \omega(2), \ldots, \omega(p-1).
\]
These are distinct solutions of \( x^{p-1} = 1 \) with \( \omega(i) \equiv i \mod p \). It may be shown that they form a cyclic group of order \( p - 1 \). Thus any finite subgroup of \( \mathbb{Q}_p^\times \) is a subgroup of this cyclic group. (The roots of unity in \( \mathbb{Q}_2 \) are just \( \pm 1 \).)

See [1, Chapter 2] for properties of the \( p \)-adic numbers. Available as a pdf here:


REFERENCES