10. 2/27

10.1. *Subgroups* Let $(G, \star)$ be a group. A *subgroup* of $(G, \star)$ is a group of the form $(H, \star)$, where H is a subset of G and the operation $\star$ remains the same. Explicitly, this means:

(1) H is *closed* under $\star$. That is, $x, y \in H$ implies $x \star y \in H$.
(2) H contains the identity element.
(3) H is closed under inversion. That is, $x \in H$ implies $x^{-1} \in H$.

Note that if (1) holds, then $\star$ is automatically associative as a binary operation on H. Also note that if H is nonempty, then (1) and (3) together imply (2), because $x \star x^{-1}$ is always the identity.

We will often abuse notation by omitting the operation $\star$ when we refer to the subgroup.

Example 10.1. What are the subgroups of $(\mathbf{Z}, +)$? They all take the form $(m\mathbf{Z}, +)$, where $m\mathbf{Z} = \{mk \mid k \in \mathbf{Z}\}$. In particular, note that $0\mathbf{Z} = \{0\}$.

Example 10.2. What are the subgroups of $(\mathbf{Z}/m\mathbf{Z}, +)$? They all take the form $d\mathbf{Z}/m\mathbf{Z}$. It turns out that we can always pick d so that it divides m.

Example 10.3. Endow $\mathbf{R}^2 = \mathbf{R} \times \mathbf{R}$ with coordinate-wise addition. Then it has many different kinds of subgroups. For instance, the axes $\{(x, 0\} \mid x \in \mathbf{R}\}$ and $\{(0, y) \mid y \in \mathbf{R}\}$ give us subgroups, but so does the line $\{(x, x) \mid x \in \mathbf{R}\}$. There are also subgroups like $(\mathbf{Z}^2, +)$.

10.2. What are the subgroups of $((\mathbf{Z}/m\mathbf{Z})^\times, \times)$?

Example 10.4. We saw earlier that $((\mathbf{Z}/5\mathbf{Z})^\times, \times)$ is isomorphic to $(\mathbf{Z}/4\mathbf{Z}, +)$. A choice of isomorphism $f : \mathbf{Z}/4\mathbf{Z} \to (\mathbf{Z}/5\mathbf{Z})^\times$ gives an explicit bijection from the set of subgroups of $\mathbf{Z}/4\mathbf{Z}$ to the set of subgroups of $(\mathbf{Z}/5\mathbf{Z})^\times$: namely, $(H, +) \mapsto (f(H), \times)$.

Example 10.5. The elements of $(\mathbf{Z}/8\mathbf{Z})^\times$ are the congruence classes of $1, 3, 5, 7$. We saw earlier that $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \pmod 8$. So, with the usual abuse of notation, $\{1, 3\}$ and $\{1, 5\}$ and $\{1, 7\}$ all define subgroups of $(\mathbf{Z}/8\mathbf{Z})^\times$. Note that each of these subgroups is isomorphic to $(\mathbf{Z}/2\mathbf{Z}, +)$. We can view them as the images of three different homomorphisms $\mathbf{Z}/2\mathbf{Z} \to (\mathbf{Z}/8\mathbf{Z})^\times$.

10.3. In general, if $f : (G', \star') \to (G, \star)$ is any homomorphism, then the image $f(G')$ always forms a subgroup of G.

Note that f restricts to a surjective map $G' \to f(G')$. If f happens to be <u>injective</u>, then the restricted map is both injective and surjective, so it is an isomorphism from G' onto the subgroup $f(G')$.

Conversely, every subgroup of G is the image of an injective homomorphism: namely, its inclusion into G.

Intuitively, this means subgroups of G carry the same information as injective homomorphisms into G.

10.4. Last time, we proved that if $a \in G$ satisfies

$$a^{\star k} = e,$$

then there is a well-defined homomorphism:

$$\begin{array}{rcl} (\mathbf{Z}/k\mathbf{Z}, +) & \to & (G, \star) \\ n + k\mathbf{Z} & \mapsto & a^{\star n} \end{array} \tag{10.1}$$

When is it injective?

Lemma 10.6. *If k is the order of a in G, then (10.1) is injective.*

Proof. We must show that if $a^{\star n} = a^{\star n'}$, then $n \equiv n' \pmod{k}$. By long division, $n' - n = kq + r$ for some $q, r \in \mathbf{Z}$ with $0 \leq r < k$. We see that

$$a^{\star r} = (a^{\star k})^{\star q} \star a^{\star r} = a^{\star(kq+r)} = a^{\star(n-n')} = a^{\star n} \star (a^{-1})^{\star n'} = e.$$

So k being the order of a forces $r = 0$. □

10.5. Below, we write $\mathrm{ord}_G(a)$ for the order of a in G.

Theorem 10.7. *Let G, H be groups. Let $a \in G$ and $b \in H$. Then*

$$\mathrm{ord}_{G \times H}(a, b) = \mathrm{lcm}(\mathrm{ord}_G(a), \mathrm{ord}_H(b)).$$

Proof. Let $k = \mathrm{ord}_G(a)$ and $\ell = \mathrm{ord}_H(b)$. By Lemma 10.6, there are injective homomorphisms $(\mathbf{Z}/k\mathbf{Z}, +) \to (G, \star)$ and $(\mathbf{Z}/\ell\mathbf{Z}, +) \to (H, *)$. Together, they define an injective homomorphism $\mathbf{Z}/k\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z} \to G \times H$, where the group laws on the domain and range are defined coordinate-wise.

By our earlier discussion, the image of this map is a subgroup of $G \times H$ isomorphic to $(\mathbf{Z}/k\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z}, +)$. As it sends $(1, 1) \mapsto (a, b)$, we deduce:

$$\mathrm{ord}_{G \times H}(a, b) = \mathrm{ord}_{\mathbf{Z}/k\mathbf{Z} \times \mathbf{Z}/\ell\mathbf{Z}}(1, 1).$$

The right-hand side is the smallest natural number n such that $n \equiv 0 \pmod{k}$ and $n \equiv 0 \pmod{\ell}$. This is the very definition of $\mathrm{lcm}(k, \ell)$. □

10.6. Let us calculate the multiplicative order of 23 mod 105, *i.e.*, its order in the group $((\mathbf{Z}/105\mathbf{Z})^\times, \times)$.

Note that $105 = 3(5)(7)$. Applying the Chinese Remainder Theorem twice,

$$(\mathbf{Z}/105\mathbf{Z})^\times \quad \text{is isomorphic to} \quad (\mathbf{Z}/3\mathbf{Z})^\times \times (\mathbf{Z}/5\mathbf{Z})^\times \times (\mathbf{Z}/7\mathbf{Z})^\times.$$

Applying Theorem 10.7 twice,

$$\mathrm{ord}_{105}(23) = \mathrm{lcm}(\mathrm{ord}_3(23), \mathrm{ord}_5(23), \mathrm{ord}_7(23)).$$

Finally, we calculate $\mathrm{ord}_3(23) = \mathrm{ord}_3(2) = 2$ and $\mathrm{ord}_5(23) = \mathrm{ord}_5(3) = 4$ and $\mathrm{ord}_7(23) = \mathrm{ord}_7(2) = 3$. So the answer is $\mathrm{ord}_{105}(23) = \mathrm{lcm}(2, 3, 4) = 12$.

11. 3/1

11.1. What are the subgroups of $(\mathbf{Z}/14\mathbf{Z}, +)$?

(1) $\{0\}$.
(2) $\{0, 7\}$.
(3) $\{0, 2, 4, 6, 8, 10, 12\}$.
(4) $\mathbf{Z}/14\mathbf{Z}$ itself.

(As usual, we are writing a to mean $a + 14\mathbf{Z}$.)

11.2. How about $((\mathbf{Z}/14\mathbf{Z})^\times, \times)$? Note that $(\mathbf{Z}/14\mathbf{Z})^\times = \{1, 3, 5, 9, 11, 13\}$.

(1) $\{1\}$.
(2) $\{1, 13\}$.
(3) $\{1, 9, 11\}$.
(4) $(\mathbf{Z}/14\mathbf{Z})^\times$ itself.

11.3. Note that $|\mathbf{Z}/14\mathbf{Z}| = 14$ and $|(\mathbf{Z}/14\mathbf{Z})^\times| = 6$. What do you notice about the sizes of their subgroups?

Theorem 11.1 (Lagrange)**.** *If $(G, \star)$ is a finite group and $H \subseteq G$ defines a subgroup, then $|H|$ divides $|G|$.*

The idea of the proof is to study the subsets of G that look like $g \star H = \{g \star x \mid x \in H\}$. These are called the (left) cosets of H.

Proof. For any $g, g' \in G$, we claim that $g \star H$ and $g' \star H$ are either identical or disjoint. This will imply that as we run over $g \in G$, the cosets $g \star H$ partition G into pairwise-disjoint subsets. As they all have the same size as H, this in turn will imply that $|H|$ divides $|G|$.

So it remains to show that if $g \star H$ and $g' \star H$ intersect, then they are identical. If they share an element a, then we can write $a = g \star h = g' \star h'$ for some $h, h' \in H$. Since H is closed under $\star$, we see that

$$g \star H = g \star (h \star H) = a \star H = g' \star (h' \star H) = g' \star H,$$

proving the claim. □

Corollary 11.2. *If G is finite and $a \in G$, then $\mathrm{ord}_G(a)$ divides $|G|$.*

Proof. The set of powers $a^{\star n}$, as we run over integers n, forms a subgroup of G. □

Corollary 11.3 (Euler)**.** *If $m \in \mathbf{N}$ and $a \in \mathbf{Z}$ is coprime to m, then $\mathrm{ord}_m(a)$ divides $\varphi(m)$. In particular, $a^{\varphi(m)} \equiv 1 \pmod{m}$.*

Proof. By definition, $\varphi(m) = (\mathbf{Z}/m\mathbf{Z})^\times$. So the first statement follows from the previous corollary by taking $G = (\mathbf{Z}/m\mathbf{Z})^\times$. To get the second statement, write $a^{\varphi(m)} = (a^{\mathrm{ord}_m(a)})^{\varphi(m)/\mathrm{ord}_m(a)}$. □

Corollary 11.4 (Fermat)**.** *If p is prime and does not divide $a \in \mathbf{Z}$, then $a^{p-1} \equiv 1 \pmod{p}$.*

Proof. Recall that $\varphi(p) = p - 1$. □

11.4. *Bonus material to the lecture* Below, we gather everything known about $((\mathbf{Z}/m\mathbf{Z})^\times, \times)$.

11.4.1. First, if $m = p_1^{e_1} \cdots p_r^{e_r}$, then by repeated application of the Chinese Remainder Theorem,

$$(\mathbf{Z}/m\mathbf{Z})^\times \quad \text{is isomorphic to} \quad (\mathbf{Z}/p_1^{e_1}\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/p_r^{e_r}\mathbf{Z})^\times$$

In particular, $\mathrm{ord}_m(a) = \mathrm{lcm}(\mathrm{ord}_{p_1^{e_1}}(a), \ldots, \mathrm{ord}_{p_r^{e_r}}(a))$.

11.4.2. By Legendre's Theorem, the size of any subgroup of $(\mathbf{Z}/p^e\mathbf{Z})^\times$ must divide $\varphi(p^e)$. The result below is exercise 3.6.3 in Stillwell, assigned on Problem Set 3.

Theorem 11.5. *For primes p and arbitrary $e \in \mathbf{N}$, we have*

$$\varphi(p^e) = p^{e-1}(p-1).$$

11.4.3. Recall that if a is a primitive root mod p^e, then

$$\begin{aligned} (\mathbf{Z}/\varphi(p^e)\mathbf{Z}, +) &\to ((\mathbf{Z}/p^e\mathbf{Z})^\times, \times) \\ n + \varphi(p^e)\mathbf{Z} &\mapsto a^n + p^e\mathbf{Z} \end{aligned}$$

is an isomorphism. It turns out:

Theorem 11.6. *For <u>odd</u> primes p and arbitrary $e \in \mathbf{N}$, there is always a primitive root mod p^e.*

Theorem 11.7. *There is no primitive root mod 2^e when $e \geq 3$.*

11.5. We sketch the $e = 1$ case of Theorem 11.6.

For any $d \in \mathbf{N}$, let $\psi(d)$ be the number of invertible congruence classes $a + p\mathbf{Z}$ such that $\mathrm{ord}_p(a) = d$. By Corollary 11.2, the order of any element of $(\mathbf{Z}/p\mathbf{Z})^\times$ must divide $\varphi(p) = p-1$, so by partitioning the elements of $(\mathbf{Z}/p\mathbf{Z})^\times$ according to their orders, we obtain

$$p - 1 = \sum_{d \text{ divides } p-1} \psi(d).$$

At the same time, by counting the number of fractions $\frac{a}{p-1}$ with $1 \leq a \leq p-1$ and denominator d in lowest terms, we see that

$$p - 1 = \sum_{d \text{ divides } p-1} \varphi(d).$$

So we are done if we can show that $\psi(d) \leq \varphi(d)$ for all d. This is what Stillwell does on page 62.