This documents assumes that you are familiar with the definitions involved. Please do notify me if there's any logical mistakes or unclear portions.

Theorem 1. *For $o(g) < \infty$, $o(g)$ is the smallest positive integer k with $g^k = 1$. Furthermore,*

$$g^m = 1 \iff o(g)|m \tag{1}$$
$$g^m = g^n \iff m \equiv n \pmod{o(g)} \tag{2}$$
$$o(g^d) = \frac{o(g)}{\gcd(o(g)), d)} \tag{3}$$

We note that $o(g) = \left|\{g^n \mid n \in \mathbb{Z}\}\right|$ is our definition.

Proof. Consider the list of powers $S = \{g, g^2, g^3, \dots\}$ there must be repetitions, otherwise $o(g) = \infty$. This means that $\exists a, b \in \mathbb{Z}^+, a < b$ s.t. $g^a = g^b$ implying $1 = g^{b-a}$ so $\exists m$ with $g^m = 1$. Let k be the smallest such integer now that we know it exists.

We first my show inclusion. Consider $T = \{1, g, \dots, g^{k-1}\}$, it is trivial that $T \in S$. For the other direction, let g^d be any element in S. We apply the division algorithm to see that $d = t \cdot k + r$ with $0 \leq r < k$.

$$g^d = g^{tk+r} = (g^k)^t g^r = g^r \in T$$

Thus we have equality of sets.

Now we have $o(g) \leq k$. To tie it all up, we need to show that the set $\{1, g, \dots, g^{k-1}\}$ are all distinct. This is trivial as if not then $g^a = g^b$ will indicate that our choice of k is contradicted.

Finally, for the three corollaries, we have the following

1. Suppose $k|m, m = tk$. Then $g^m = g^{tk} = 1$.

   Now for the other direction, let $g^m = 1, m = tk + r$ with the division algorithm. Then $g^{tk+r} = (1)g^r = 1$ implies that $r = 0$ and we have divisibility.

2. Trivial from the above techniques.

3. Say $o(g) = k, \gcd(k, d) = t \implies \exists k_1, d_1$ s.t. $k = tk_1, d = td_1, \gcd(k_1, d_1) = 1$. We know that by definition that $o(g^d)$ is the smallest positive integer, say l, such that $(g^d)^l = 1$.

$$(g^d)^l = 1 \iff g^{dl} = 1 \iff o(g)|dl \iff k|dl \tag{4}$$
$$\iff tk_1|td_1l \tag{5}$$
$$\iff k_1|d_1l \tag{6}$$
$$\iff k_1|l \tag{7}$$

   where the last step comes from $(k_1, d_1) = 1$. Hence the smallest number l is k_1, which is exactly what we want if we sub it all back in.

□

Theorem 2. *Subgroups of cyclic group are cyclic.*

Proof. Assume $G = \langle g \rangle$, and $H \leq G$. There are two cases:

1. $H = \{1\}$, trivial.

2. $|H| > 1$, so $\exists g^m \in H, m \in \mathbb{Z}^+$. Let k be the smallest positive integer with $g^k \in H$, and claim $H = \langle g^k \rangle$.

   For $\langle g^k \rangle \subset H$, we have this almost trivially by definition of g^k and properties of subgroups. On the other hand to show the other inclusion, we know $\forall x \in H, x \in G \implies x = g^d$. Now perform division with remainder,

   $$d = tk + r$$

   Notice that $g^r = g^{d-tk} = g^d(g^k)^{-t} = x(g^k)^{-t}$, with both terms in H, so $g^r \in H$. But since r is a remainder, we know $0 \leq r \leq k-1\ldots$ but we know k is the minimal $g^k \in H$! Hence $r = 0$.

   Finally,

   $$x = (g^k)^t \in \langle g^k \rangle \implies H \leq \langle g^k \rangle \tag{8}$$

   and we are done.

□

Theorem 3. *Cosets properties:*

$$|Hg| = |H| \tag{9}$$
$$Hg = H \iff g \in H \tag{10}$$
$$Hx = Hy \text{ or } Hx \cap Hy = \varnothing \tag{11}$$
$$Hx = Hy \implies xy^{-1} \in H \tag{12}$$

Proof.
1. By construction as the map is $H \to Hg$ with elements $h \mapsto hg$ which is bijective.

2. See proof of 4, with $x = g, y = 1$.

3. Assume $Hx \cap Hy \neq \varnothing$, then $\exists z$ in the intersection. We know $z = h_1 x = h_2 y$ for some $h_1, h_2 \in H$. Then there exists an element h such that

   $$hx = hh_1^{-1}h_1x = hh_1^{-1}z = hh_1^{-1}h_2y \in Hy \tag{13}$$

   so $Hx \subseteq Hy$. Similar proof for other direction, then they are equal.

4. Suppose $Hx = Hy$, meaning that $x \in Hx$ by definition so $x \in Hy \implies x = hy, h \in H$ also by number 3. Then $xy^{-1} = h \in H$.

   For the other direction, suppose $xy^{-1} \in H$, then $xy^{-1}y \in Hy$ meaning that $x \in Hy$. Similarly we have $x \in Hx$ so that Hx and Hy are not disjoint. Now use point 3.

□

Theorem 4. *Show that conjugacy relation is an equivalence relation and* $|C_G(g)||\mathscr{C}_g| = |G|$

Proof. First, for the equivalence relation on G:

- Reflexive: $i^{-1}gi = g$
- Symmetric: if $x^{-1}gx = f$, then $\left(x^{-1}\right)^{-1} fx^{-1} = g$.
- Transitive: if $x^{-1}gx = f, y^{-1}fy = h$, then $(xy)^{-1}g(xy) = h$ as $(xy)^{-1} = y^{-1}x^{-1}$.

Next, we want to show the relationship on conjugacy classes and centralizers. From Lagrange, we know that $|G : H||H| = |G|$, so we can sort of match it up such that $C_G(g)$ is the subgroup and the conjugacy classes are like the cosets. Hence, if we show that $|G : C_G(g) = |\mathscr{C}_g|$, we are done.

Consider $\alpha(x) : C_G(g) \to \mathscr{C}_g$ with $C_G(g) \cdot x \mapsto x^{-1}gx$. Then α is well defined if:

$$C_G(g)x = C_G(g)y \tag{14}$$

$$xy^{-1} \in C_G(g) \tag{15}$$

$$xy^{-1}g = g(xy^{-1}) \tag{16}$$

$$y^{-1}gy = x^{-1}gx \tag{17}$$

$$\alpha(x) = \alpha(y) \tag{18}$$

Since each of those lines are iff implications, the reverse will show 1 to 1. Also, α is onto by construction, hence α is bijection and we are done. □

Theorem 5. *Cauchy's theorem: let p prime, and if $p \mid |G|$, then $\exists g \in G$ with $o(g) = p$.*

Proof. Consider the set $T = \{(g_1, g_2, \dots, g_p) \mid g_1g_2 \dots g_p = 1\}$ by choosing arbitrary $p - 1$ elements then fixing the g_p. Hence we have $|T| = |G|^{p-1}$.

Let $\alpha : T \to T, (g_1, \dots, g_p) \mapsto (g_2, g_3, \dots, g_p, g_1)$. We note that $(g_2g_3 \dots g_p)g_1 = g_1^{-1}g_1 = 1$, hence it's a valid mapping and one can also verify it's bijective.

So α is a permutation on T, and part of the symmetric group $\alpha \in S_p$. More importantly, $\alpha^p = I$, so $o(a)|p$ meaning that $o(a)$ can be either 1 or p. Then we can rewrite

$$T = \{\text{elements in a 1-cycle } \cup \text{ elements in a } p\text{-cycle}\} \tag{19}$$

Let's count this smartly in two ways,

$$|T| = |G|^{p-1} = r + sp$$

where r is the number of 1 cycle, and s be the number of orbits with p elements. Since we know $p \mid |G|$, we should be able to divide by p on both sides, meaning that r is a multiple of p. It cannot be zero, as the trivial 1 is in it, then that means there exists at least p elements (we only need 2 though!) of the 1 cycle. Since the one cycle looks like $g_1 = g_2 = \dots = g_p$, we are done as that means $g_1g_1 \dots g_1 = (g_1)^p = 1$. □

Theorem 6. *If $M, N \trianglelefteq G, M \cap N = \{1\}, M \cdot N = G$, then $G \cong M \times N$.*

We first need a lemma.

Lemma 1. *If $M, N \trianglelefteq G, M \cap N = \{1\}$, then $mn = nm$ for all elements.*

Proof. Consider $m^{-1}n^{-1}mn = 1$ where the first three and the 2nd three are considered in different ways. Recall that since they are normal subgroups, conjugation doesn't affect them, hence the first 3 can be considered in N while the 2nd three is in M. Hence we have $mn = nm$. □

Proof. Consider $\alpha : M \times N \to G, (m, n) \mapsto mn$. We wish to show it is a homomorphism.

It is onto by the $M \cdot N = G$ condition.

It is one-to-one as

$$\alpha(m_1, n_1) = \alpha(m_2, n_2) \tag{20}$$

$$m_1 n_1 = m_2 n_2 \tag{21}$$

$$m_2^{-1} m_1 = n_2 n_1^{-1} = \{1\} \tag{22}$$

The last line comes from the fact that the left side is in M, the right side is in N and their intersection is only 1. Hence $m_2 = m_1, n_2 = n_1$.

Finally,

$$\alpha\left((m_1, n_1)(m_2, n_2)\right) \stackrel{?}{=} \alpha(m_1.n_1)\alpha(m_2, n_2) \tag{23}$$

$$\alpha\left((m_1 m_2, n_1 n_2)\right) \stackrel{?}{=} \tag{24}$$

$$m_1 m_2 n_1 n_2 = m_1 n_1 m_2 n_2 \tag{25}$$

$$m_2 n_1 = n_1 m_2 \tag{26}$$

and the last line uses our lemma. Now α is an isomorphism and we are done. □

Theorem 7. *Given a mapping $\phi : R \to T$ that the image is a sub-ring of T, and the kernel is an ideal in R. Also show the 1st isomorphism theorem:*

$$R/\ker(\phi) \cong \Im(\phi) \tag{27}$$

Proof. We first show that image of homomorphism is a subring. It is easy to show that it's non-empty by construction, and the subtraction/multiplication condition comes naturally. For the kernel, the fact that it's a subring is also easy, and the ideal test is also fairly simple.

The non-trivial part is the isomorphism theorem. We consider the map $\alpha : R/\ker(\phi) \to \Im(\phi)$ with the following operation $\ker(\phi) + x \mapsto \phi(x)$. Our notation of $\ker(\phi) + x$ is the congruence classes modulo the kernel.

We show it is well defined, if $x \cong y$:

$$\begin{aligned} x \equiv y \pmod{\ker(\phi)} \\ y - x \in \ker(\phi) \\ \phi(y - x) = 0 \\ \phi(y) - \phi(x) = 0 \\ \phi(y) = \phi(x) \\ \alpha(y) = \alpha(x) \end{aligned}$$

Since it is iff statements, the backwards way shows one-to-one. Furthermore, α is onto by construction due to properties of image. We are now done after we prove the homomorphism properties, which is quite easy. □

Theorem 8. *Prove that if R is a simple commutative ring, then it is either a field or a zero ring.*

Proof. Assume that R is a commutative, simple ring. We have two cases based on the existence of zero divisors:

1. If $\exists a, b \neq 0$ with $ab = 0$. We consider the set $N(b) = \{x \in R \mid xb = 0\} \trianglelefteq R$. We know it is non-empty as $0 \in N(b)$, and one can easily prove that this is indeed an ideal.

   Furthermore, we actually know that $a \in N(b)$ also, and since R is simple, $N(b) = R$ by definition. Hence, $xb = 0, \forall x \in F \implies R \cdot b = 0$.

   Next consider $N = \{y \in R \mid Ry = 0\} \trianglelefteq R$. It is again non-empty as 0 is in it, and again ideal is left as an trivial exercise. From the characterization of b above, we know that $b \in N$ also, proving again that $N = R$ by definition of simple.

   Hence this means that R is a zero ring.

   As an aside, since the multiplication operation is without information, we know the addition subgroup is an ideal (doesn't contradictions simplicity as it's all the elements). Hence there's a prime number of elements in R, or simply $R = \{0\}$.

2. Assume R has no zero divisors, and is non-empty. Consider $R_a = \{ra \mid r \in R\} \trianglelefteq R$. It's non-empty by construction, and ideal properties comes almost trivially. Once again, we then know that $R_a = R$ by simple property.

   Now as we know that $R_a = R, a \in R$, hence there must be an element e such that $a = ea$! For any other element b, we have

$$\begin{aligned} ba &= bea \\ ba - bea &= 0 \\ (b - be)\, a &= 0 \implies b - be = 0 \end{aligned}$$

   so e is our fixed identity as R is commutative.

Finally, for any $x \neq 0$, we can have the same ideal as described above of $\{0\} \neq R_x = R$. And now with $e \in R$ identity in our pocket, we can conclude there exists an element y such that $e = yx$, and again we can use commutative property to have $xy = yx = e$.

Now R is a field.

□

Theorem 9. *Prime implies irreducibility. Furthermore, in a PID irreducibility implies prime.*

Proof. This is in an integral domain. Assume that p is prime, and let $d|p$ so $\exists x, dx = p$.

Now, we know $p|dx$ and p is prime, hence either $p|d$ or $p|x$. The latter condition signifies that $\exists y$ s.t.

$$py = x \tag{28}$$

$$dx = dpy = p \implies p(dy - 1) = 0 \tag{29}$$

hence by non-zero definition, $dy = 1 \implies d \sim 1$.

Now, for the PID statement. Assume that R is a PID, with $q \in R$ irreducible and $q|ab$. We need tho show that $q|a$ or $q|b$.

Consider $\gcd(q, a)$, by lemma on existence of gcd in PIDs, we know $\exists d, \gcd(q, a) = d \implies d \sim \gcd(q, a)$. Now $d|q, d|a$, and q is irreducible so either d is unit or $d \sim q$.

If $d \sim q$, then $q|d$ and $d|a$ and we are done by transitivity.

If $d \sim 1$ (unit), we consider $d = sq + ta$ for some s, t (exists due to gcd operator). Furthermore, we note that there is a $f, fd = 1$. Hence

$$1 = fd = fsq + fta \tag{30}$$

$$b = fsqb + ftab \tag{31}$$

by commutative property. Note that q divides both terms as q appears in the first one and $q|ab$ is one of our assumptions, so it divides b, $q|b$. □

Theorem 10. *ED $\implies$ PID*

Proof. Let R be an ED, and $J \trianglelefteq R$. If $J = \{0\}$, then $J = (0)$ is principal, so assume $J \neq \{0\}$. We choose $0 \neq d \in J$ with the smallest possible $N(d)$.

Claim that $J = (d)$. Since $d \in J \implies rd \in J, \forall r \in R$ so $(d) \subseteq J$.

Conversely, $\forall x \in J, \exists q, r \in R$ such that $x = qd + r$. Either $r = 0$ or $N(r) < N(d)$ by ED's properties.

Notice that r is in J as $r = x - qd \in J$, so $N(r) < N(d)$ cannot happen as we chose d as the minimum. Hence $r = 0$, and $x = q(d) \in (d)$. So $J \subseteq (d) \implies J = (d)$ with above. □