1 Required Proofs

1. **For any subgroup $H \leq G$, the following hold:**
   (a) $|Hg| = |H|$
   (b) $Hg = H \Leftrightarrow g \in H$
   (c) **Any two right cosets of H are equal or disjoint.**
   (d) $Hx = Hy \Leftrightarrow xy^{-1} \in H$

   Proof Recall that $Hg = \{hg : h \in H\}$. We thus have

   (a) Let's see that the map $\phi : H \to Hg$ given by $h \mapsto hg$ is a bijection. It is injective: if $h_1 g = h_2 g$, then multiplying on the right by g^{-1} implies that $h_1 = h_2$. It is surjective: if $x \in Hg$, then $x = h_1 g$ for some $h_1 \in H$. But then $x = \phi(h_1)$.
   (b) If $Hg = H$, clearly $g \in Hg$ so $g \in H$. Conversely, if $g \in H$, then since H is closed under multiplication (it is a subgroup), $Hg = H$.
   (c) If Hg_1 and Hg_2 are not disjoint, let $x \in Hg_1$ and Hg_2. Then $x = h_1 g_1 = h_2 g_2$ so $h_1^{-1} h_2 g_2 = g_1$. Now for any $hg_1 \in Hg_1$, we have $hg_1 = hh_1^{-1} h_2 g_2 \in Hg_2$ so $Hg_1 \subseteq Hg_2$. Since $|Hg_1| = |Hg_2|$ by (1), equality must hold.
   (d) First suppose $Hx = Hy$. Then to each $h \in H$, there exists h' so $hx = h'y$; that is, $xy^{-1} = h^{-1} h' \in H$. Conversely, if $xy^{-1} \in H$, then $x = xy^{-1} y \in Hy$ so $x \in Hx$ and $x \in Hy$ and by (3), $Hx = Hy$. ■

2. **The conjugacy relation is an equivalence relation on G, and for any $g \in G$, $|C_g| \cdot |G_G(g)| = |G|$.**

   Proof Recall that $x \sim y$ if and only if there exists $g \in G$ so $g^{-1} x g = y$.

   (a) *Reflexive:* $x \sim x$ since $1^{-1} x 1 = x$.
   (b) *Symmetric:* If $x \sim y$, then $g^{-1} x g = y$ and $(g^{-1})^{-1} y g^{-1} = x$ so $y \sim x$.
   (c) *Transitive:* If $x \sim y$ and $y \sim z$, then $g^{-1} x g = y$ and $h^{-1} y = z$, so $(gh)^{-1} xgh = z$ and $x \sim z$.

   Recall that $C_G(g) \leq G$. It suffices to show $[G : C_G(g)] = |C_g|$: in particular, I claim that the map from right cosets of $C_G(g)$ to conjugate elements of g given by $C_G(g)h \mapsto h^{-1} g h$ is a bijection. Let's first see that it is well-defined and injective. We have

$$\begin{aligned} C_G(g)h_1 = C_G(g)h_2 &\Longleftrightarrow h_1 h_2^{-1} \in C_G(g) \\ &\Longleftrightarrow h_1 h_2^{-1} g = g h_1 h_2^{-1} \\ &\Longleftrightarrow h_2^{-1} g h_2 = h_1^{-1} g h_1 \end{aligned}$$

   It is also surjective: if $hg^{-1}h$ is an arbitrary conjugate element, then it is the image of $C_G(g)h$. Thus the map is bijective, so

$$[G : C_G(g)] = |C_g| \Longrightarrow \frac{|G|}{|C_G(g)|} = |C_g|$$

   and the desired result holds. ■

3. **Subgroups of cyclic groups are also cyclic.**

Proof Let $G = \langle g \rangle$ be cyclic, and let $H \leq G$. If $H = \{1\}$ it is certainly cyclic; otherwise, let $n \neq 0$ be minimal so that $g^n \in H$. I claim that $H = \langle g^n \rangle$. Certainly $\langle g^n \rangle \subseteq H$ by closure under multiplication. If $h \in H$ is arbitrary, write $h = g^{kn+r}$ for some $k, r \in \mathbb{N}$ with $r < n$. But then $g^r = h(g^k)^{-n} \in H$, so by minimality of n, we must have $r = 0$. Thus $h = (g^n)^k \in \langle g^n \rangle$ so $H \subseteq \langle g^n \rangle$ and equality holds, as desired. ■

4. **Groups of order p^2 (with p any prime) are commutative.**

Proof First recall that G is a disjoint union of its conjugacy classes. Let's first see that $Z(G) = \{g \in G : |C_g| = 1\}$. If $|C_g| = 1$, then $C_g = \{g\}$ so $x^{-1}gx = g$ and $gx = xg$ for any $x \in G$. Similarly, if $g \in Z(G)$, then $gx = xg$ for any $x \in G$ so $x^{-1}gx = g$ and $C_g = \{g\}$. Thus G is a disjoint union of its center along with its non-trivial conjugacy classes (this is commonly referred to as the *class equation*). Recall as well that $|C_g|$ divides $|G|$ for all $g \in G$.

Let $|G| = p^2$ and write $|G| = |Z(G)| + \sum_{i=1}^{k} |C_{g_i}|$ where the C_{g_i} are disjoint non-trivial conjugacy classes. Since $|C_{g_i}| > 1$, we must have $|C_{g_i}| \equiv 0 \pmod{p}$. Thus $|Z(G)| \equiv 0 \pmod{p}$, and since $|Z(G)| \geq 1$, we have $|Z(G)| = p$ or $|Z(G)| = p^2$.

If $|Z(G)| = p^2$, it is clear that G is commutative, so suppose $|Z(G)| = p$. Let $x \in G \setminus Z(G)$, so $Z(G) \lneq C_G(x)$. Thus p divides $|C_G(x)|$ and $|C_G(x)| \geq p+1$, so $|C_G(x)| = p^2$. Thus $C_G(x) = G$ and $x \in Z(G)$, a contradiction. ■

5. **First Isomorphism Theorem: for any homomorphism $\phi : G \to H$ of groups, $G/\ker(\phi) \cong \operatorname{im}(\phi)$.**

Proof Consider the map α from right cosets of $\ker(\phi)$ to $\operatorname{im}(\phi)$ given by $\ker(\phi)h = \phi(h)$. First, let's check that α is well-defined and injective. By properties of homomorphisms,

$$\begin{aligned}
\ker(\phi)h_1 = \ker(\phi)h_2 &\iff h_1 h_2^{-1} \in \ker(\phi) \\
&\iff \phi(h_1 h_2^{-1}) = 1 \\
&\iff \phi(h_1)\phi(h_2)^{-1} = 1 \\
&\iff \phi(h_1) = \phi(h_2)
\end{aligned}$$

and to see surjectivity, if $y \in \operatorname{im}(\phi)$, then $y = \phi(h)$ and $y = \alpha(\ker(\phi)h)$.

It remains to check that α is a homomorphism. Indeed,

$$\begin{aligned}
\alpha(\ker(\phi)h_1 \ker(\phi)h_2) &= \alpha(\ker(\phi)(h_1 h_2)) \\
&= \phi(h_1 h_2) \\
&= \phi(h_1)\phi(h_2) \\
&= \alpha(\ker(\phi)h_1)\alpha(\ker(\phi)h_2)
\end{aligned}$$

as required. ■

6. **If M, N are normal subgroups in a group G with $M \cap N = \{1\}$, then $mn = nm$ for all $m \in M$ and $N \in N$. If we assume additionally that $MN = G$, then $G \cong M \times N$.**

Proof To show that $mn = nm$, it suffices to show that $m^{-1}n^{-1}mn \in M \cap N = \{1\}$. Since M is normal and $m \in M$, $n^{-1}mn \in M$ so $m^{-1}n^{-1}mn \in M$. Similarly, $m^{-1}n^{-1}m \in N$ since N is normal, so $m^{-1}n^{-1}mn \in N$ as well.

Now, let's define $\phi : M \times N \to G$ by $\phi(m,n) = m \cdot n$. Since $M \cdot N = G$, ϕ is surjective, so let's check injectivity. We have using the identity proved earlier

$$\begin{aligned}\phi(m_1,n_1) = \phi(m_2,n_2) &\implies m_1 n_1 = m_2 n_2 \\ &\implies m_2^{-1} m_1 = n_2 n_1^{-1} \\ &\implies m_1 m_2^{-1}, n_1 n_2^{-1} \in M \cap N \\ &\implies m_1 m_2^{-1} = 1, n_1 n_2^{-1} \\ &\implies (m_1,n_1) = (m_2,n_2)\end{aligned}$$

so it remains to show that ϕ is a homomorphism. Indeed,

$$\begin{aligned}\phi((m_1,n_1)\cdot(m_2,n_2)) &= \phi(m_1 m_2, n_1 n_2) \\ &= m_1 m_2 n_1 n_2 \\ &= m_1 n_1 m_2 n_2 \\ &= \phi(m_1,n_1)\phi(m_2,n_2)\end{aligned}$$

by the claim proven earlier, as required. ■

7. **A commutative simple ring is either a field or a zero-ring.**

Proof If $R = \{0\}$ then it is certainly a zero-ring, so suppose $R \neq \{0\}$. First suppose R has zero divisors and get $a, b \neq 0$ with $a \cdot b = 0$. Define $N(a) = \{x \in \mathbb{R} : a \cdot x = 0\}$. Note that $N(a)R$: if $x, y \in N(a)$ then $(x+y)a = xa + ya = 0$, and for any $r \in R$, $(rx)a = r(xa) = 0$. Since $b \neq 0$, $b \in N(a)$, so $N(a) = R$ since R is simple. Now define $N = \{x \in R : xR = 0\}$. Again, NR since $(x+y)R = xR + yR = 0$ and $(ax)R = a(xR) = 0$. Note that $a \in N$ and $a \neq 0$, so as before, $N = R$ and R is a zero-ring.

Otherwise, we assume R has no zero divisors. Let $a \neq 0$, so $\{0\} \neq RaR$ and $Ra = R$. Since $a \in R$, get $e \in R$ so that $ea = a$. Then if b is arbitrary, $ba = bea$ so $(b - be)a = 0$ and since $a \neq 0$, $b = be$. Since R is commutative, $be = eb = b$ so $e \in R$ is an identity element Now if $x \neq 0$ is arbitrary, $Rx = R$ so there exists $y \in R$ so $yx = e$, so every x has an inverse. Thus R is a field. ■

8. **In an integral domain, every prime element is irreducible. In a prinicipal ideal domain,** $\gcd(a,b)$ **always exists and can be expresed as** $xa + yb$ **with some** $x, y \in R$**. In a principal ideal domain, every irreducible element is prime.**

Proof Let $p \in R$ be prime and suppose $d|p$. Get x so that $dx = p$; then, since p is prime, $p|x$ or $p|d$. If $p|d$, then $p \sim d$; if $p|x$, get x so that $x = py$. Then $dpy = p$ so $(dy-1)p = 0$ and since R is integral, $dy = 1$ so d is a unit.

Fix elements $a, b \in R$ and consider the ideal $I = \{xa + yb : x, y \in R\}$. This is an ideal: $x_1 a + y_1 b + x_2 a + y_2 b = (x_1 + x_2)a + (y_1 + y_2)b \in I$ and $r(xa + yb) = (rx)a + (ry)b$. Since R is a PID, $I = (d)$; note that $d|a$ and $d|b$. Since $d \in I$, $d = xa + yb$ for some $x, y \in R$; thus, if $c|a$

and $c|b$, then $c|xa+yb=d$, so d is a greatest common divisor. If d' is any other greatest common divisor, then $d'=ud$ so $d'=(ux)a+(uy)b$.

Finally, suppose $q \in R$ is irreducible and $q|ab$. Note that $\gcd(q,a)|q$ so either $q \sim \gcd(q,a)$ or $1 \sim \gcd(q,a)$. In the first case, $q|a$. In the second case, there exists x,y so that $1 = xq+ya$. Then $b = xqb+yab$ and $q|xqb$ and $q|yab$, so $q|b$. ■

9. **Every Euclidean domain is a principal ideal domain.**

   Proof Let J be an arbitrary ideal and let $d \in J$ be such that $N(d)$ is minimal. Clearly $(d) \subseteq J$; it suffices to show that $J \subseteq (d)$. If $x \in J$ is arbitrary, write $x = qd+r$ with $N(r) < N(d)$. Noce that $r = x-qd \in J$, so by minimality of d, $r=0$. Thus $x = qd \in (d)$. ■

2 All Definitions

2.1 Groups

1. A **group** is a pair $(G,*)$ with $*: G \times G \to G$ such that
   (a) $(a*b)*c = a*(b*c)$
   (b) There exists $e \in G$ with $e*a = a*e = a$
   (c) For each $a \in G$, there exists $b \in G$ so $ab = ba = e$.
   We say that G is **commutative** if $a*b = b*a$ for all $a,b \in G$.
2. We say that H is a **subgroup** of G and write $H \leq G$ if $(H,*)$ is a group. Given an element h, the **subgroup generated by** h denoted by $\langle g\rangle$ is the set $H = \{h^n : n \in \mathbb{N}\}$.
3. The **order of a group** G is $|G|$. The **order of an element** g is $|\langle g\rangle|$.
4. A group is **cyclic** if it is generated by a single element.
5. The **center** of a group is the set $Z(G) := \{x \in G : xg = gx \forall g \in G\}$. The **centralizer** of an element is the set $C_G(g) := \{x \in G : xg = gx\}$.
6. We say that a and b are **conjugate elements**, and write $a \sim b$, if there exists $x \in G$ so $x^{-1}ax = b$. We say that K and H are **conjugate subgroups** if there exists x so that $x^{-1}Hx = K$.
7. The **centralizer of a subgroup** is $C_G(H) = \{x \in G : xh = hx \forall h \in H\}$. The **normalizer of a subgroup** is $N_G(H) = \{x \in G : x^{-1}Hx = H\}$.
8. A **right coset** of a subgroup H is a set Hx for some $x \in G$.
9. The **index** of a subgroup H in G, denoted $[G:H]$, is the number of distinct right cosets of H.
10. Given a normal subgroup HG, the **factor group** H/G is the group of right cosets of H with multiplication $(Hx)(Hy) = H(xy)$.
11. A **simple group** is a group whose only normal subgroups are itself and the trivial group.
12. A **homomorphism** of groups is a map $\phi: G \to H$ so that $\phi(g*h) = \phi(g) \times \phi(h)$. It is an **isomorphism** if ϕ is also bijective, and an **automorphism** if the map is from G to itself. Given a homomorphism ϕ, we define the **kernel** $\ker(\phi) = \{x \in G : \phi(x) = 1\}G$ and **image** $\mathrm{im}(\phi) = \{\phi(x) : x \in G\} \leq H$.
13. The **symmetric group** S_n is the group of permutations on $[n]$, with composition operation. The **parity** of a permutation is the parity of the number of 2-cycles needed to represent the permutation. Given a permutation σ, we define the **signature** of σ by $\mathrm{sgn}(\sigma) = 1$ if σ is even, and -1 if it is odd.

14. If p^k divides $|G|$ for maximal k, then a Sylow $p-$subgroup H of G is a subgroup with $|H| = p^k$.

2.2 Rings

1. A **ring (with identity)** is the fusion of an abelian group and a monoid, compatible via distributive laws. A ring without identity takes a semigroup instead of a monoid. To be precise, $(R, \times, +)$ is a ring if
   (a) $(R, +)$ is an abelian group
   (b) $(R, \times)$ is a semigroup: $(a \times b) \times c = a \times (b \times c)$ for all $a, b, c \in R$. If R has an identity, then there exists e so that $e \times a = a \times e = a$ for all $a \in R$.
   (c) Distributive laws: $a \times (b + c) = a \times b + a \times c$ and $(a + b) \times c = a \times c + b \times c$.

2. A **division ring** is a ring in which every element has a multiplicative inverse. A commutative division ring is called a **field**. A **zero-ring** is a ring in which $ab = 0$ for all $a, b \in R$. The set $R^\times$ denotes the set of **units** in R; i.e. elements with a multiplicative inverse.

3. An **ideal** I in R is a subring (perhaps without identity) such that for all $a \in R$ and $b \in I$, $ab \in I$ and $ba \in I$. We say that $a \sim b \pmod I$ if $a - b \in I$. The equivalence classes induced by $\sim$ are called **congruence classes**. The **principal ideal generated by** a is the set (a) which is the intersection of all ideals of R containing a. When R is commutative, $(a) = aR = Ra$. We say that an ideal I is **principal** if $I = (a)$ for some $a \in R$. We say that a proper ideal I of R is **maximal** if the only ideal properly containing it is R. It is a fact that every proper ideal of R is contained in a maximal ideal of R (Zorn's lemma)! Ideals I and J are **comaximal** if $I + J = R$.

4. If R is a ring and I is an ideal in R, then I is a normal subgroup of $(R, +)$. Let R/I denote the congruence classes modulo I, with addition $(a + I) + (b + i) = (a + b) + I$ and multiplication $(a + I)(b + I) = (ab) + I$. Under these operations, R/I is a ring called the **factor ring** of R by I.

5. We say that $\phi : R \to S$ is a **ring homomorphism** if $\phi(x + y) = \phi(x) + \phi(y)$ and $\phi(xy) = \phi(x)\phi(y)$. Then we have the **kernel** $\ker(\phi) = \{a \in R : \phi(a) = 0\}$ and **image** $\mathrm{im}(\phi) = \{\phi(a) : a \in R\}$. Note that $\ker(\phi)$ is an ideal of R and $\mathrm{im}(\phi)$ is a subring of S.

6. A **zero-divisor** in a ring R is a non-zero element $a \in R$ such that there exists $b \neq 0$ so that $ab = 0$. An **integral domain** is a commutative ring with identity and no zero divisors. A **principal ideal domain** is an integral domain such that every ideal of R is principal.

7. In a commutative ring with identity R, we say that $a|b$ (a **divides** b) if there exists r so that $b = ar$. We say that a and b are **associates** and write $a \sim b$ if there exists a unit u so that $a = bu$. Let's summarize some basic facts:
   (a) u is a unit if and only if $u|1$ if and only if $(u) = (1)$.
   (b) u is a unit if and only if $(u) = (1)$.
   (c) In an integral domain R, $a \sim b$ if and only if $a|b$ and $b|a$. Equivalently, $(a) = (b)$.

8. Let R be an integral domain. A **non-trivial factorization** of a is an equation of the form $a = bc$ where b, c are not units and not associates of a. We say that a is **irreducible** if it does not have a non-trivial factorization. We say that a is **prime** if whenever $a|bc$, then $a|b$ or $a|c$. Note that in an integral domain, every prime is irreducible. Given elements a and b, we denote their **greatest common divisor** to be the set of elements d so that $d|a$ and $d|b$ and, whenever $c|a$ and $c|b$, then $c|d$.