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 $g^{-1}xg = y$.

   (a) *Reflexive:* $x \sim x$ since $1^{-1}x1 = x$.
   (b) *Symmetric:* If $x \sim y$, then $g^{-1}xg = y$ and $(g^{-1})^{-1}yg^{-1} = x$ so $y \sim x$.
   (c) *Transitive:* If $x \sim y$ and $y \sim z$, then $g^{-1}xg = y$ 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 $C_G(g)h \mapsto h^{-1}gh$ is a bijection. Let's first see that it is well-defined and injective. We have

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

   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

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

   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

$$\begin{aligned}\phi(m_1,n_1) = \phi(m_2,n_2) &\implies m_1n_1 = m_2n_2\\ &\implies m_2^{-1}m_1 = n_2n_1^{-1}\\ &\implies m_1m_2^{-1}, n_1n_2^{-1} \in M \cap N\\ &\implies m_1m_2^{-1} = 1, n_1n_2^{-1}\\ &\implies (m_1,n_1) = (m_2,n_2)\end{aligned}$$

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

$$\begin{aligned}\phi((m_1,n_1)\cdot(m_2,n_2)) &= \phi(m_1m_2, n_1n_2)\\ &= m_1m_2n_1n_2\\ &= m_1n_1m_2n_2\\ &= \phi(m_1,n_1)\phi(m_2,n_2)\end{aligned}$$

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: $x_1a + y_1b + x_2a + y_2b = (x_1 + x_2)a + (y_1 + y_2)b \in I$ 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