MATH 410: NOTES

JUAN SERRATOS

CONTENTS

1. Groups

1.1. Group Actions and Orbit-Stablizer Theorem.

Definition 1.1. Let G be a group and A be a set. Then a (left) **group action** is a map $\alpha\colon G \times A \to A$ such that the following two axioms are satisfied for all $g, h \in G$ and $a \in A$:

- $\alpha(e, x) = x$, and
- $\alpha(g, \alpha(h, x)) = \alpha(gh, x)$.

The usual convention for the notation of a group action is that we will denote it simply using a dot when the context is clear, that is, if we let G act on a set A, then $e \cdot x = x$ and $g \cdot (h \cdot x)) = (gh) \cdot x$ is the way we denote the two needed axioms above.

Example 1.1. The standard example is that if we have $G = S_n$ (or a G be a subgroup of S_n such as A_n) and $A = \{1, 2, \dots, n\}$. Then G acts on A by the formula $g \cdot x = g(x)$; that is, we're taking a bijective map $g\colon G \to G$ and $\alpha(g, x) = g(x) \in X$. The first axiom is $e \cdot x = e(x) = x$ is clear as $e\colon G \to G$ is the trivial mapping, and the second axiom is simple: given two bijective maps $g, h\colon G \to G$, then $g \cdot (h \cdot x)) = g \cdot (h(x)) = g(h(x)) = (g \circ h)(x) = (gh) \cdot x$. Furthermore, to make things clear, let $A = \{1, 2, 3\}$. Then if we have the cycle $(1\ 2\ 3)$, then $(1\ 2\ 3) \cdot x = (1\ 2\ 3)(x)$ and so checking all values in $A = \{1, 2, 3\}$, then $(1\ 2\ 3)(1) = 2$, $(1\ 2\ 3)(2) = 3$, $(1\ 2\ 3)(3) = 1$. For great measure consider the composition of two cycles $(1\ 2\ 3)(1\ 3\ 2)$ in S_3. Then we look towards checking the second axiom: $(1\ 2\ 3) \cdot (1\ 3\ 2) \cdot x = (1\ 2\ 3) \cdot (1\ 3\ 2)(x)$, and checking all values of $x \in A$, then $(1\ 3\ 2)(1) = 3$, $(1\ 3\ 2)(2) = 1$, and $(1\ 3\ 2)(3) = 2$, and so $(1\ 2\ 3)((1\ 3\ 2)(1)) = (1\ 2\ 3)(3) = 1$, $(1\ 2\ 3)((1\ 3\ 2)(2)) = (1\ 2\ 3)(1) = 2$, and $(1\ 2\ 3)((1\ 3\ 2)(3)) = (1\ 2\ 3)(2) = 3$. Now that we've checked this, we should have that this condides with the other side of this axiom: composing $(1\ 2\ 3)(1\ 3\ 2)$ gives us $(1)(2)(3) = e$ the identity permutation. Thus $(1)(2)(3) \cdot x = (1)(2)(3)(x)$ gives us $(1)(2)(3)(1) = 1$, $(1)(2)(3)(2) = 2$, and $(1)(2)(3)(3) = 3$. Thus the permutations agree on all values of $x \in A$. The second axiom is sastified for the these two cycles, but we've already done the general case in the first few sentences.

Definition 1.2. Let G be a group acting on a set X.

- A **fixed point** of an element $g \in G$ is an element $x \in X$ such that $g \cdot x = x$.
- The **stablizer** G_x of a point $x \in X$ is the set of elements $g \in G$ such that x is a fixed point of g, i.e. $G_x = \{g \in G\colon g \cdot x = x\}$.
- The **orbit** of an element $x \in X$ is the set of elements $y \in X$ such that $g \cdot x = y$ for some $g \in G$, and the of orbit of x is denoted by $G \cdot x = \{g \cdot x\colon g \in G\}$.

Remark 1.1. We say that a group action is *transitive* if and only it has exactly one orbit, that is, if there exists $x \in X$ with $G \cdot x = X$. This is true if and only if $G \cdot x = X$ for all $x \in X$. Or, rather, a group action is transitive if for any two $x, y \in X$ there exits a $g \in G$ such that $g \cdot x = y$. The set of all orbits of X under the group action of G is written as X/G, and is called the *quotient* of the action. A G-*invariant* element is an element $x \in X$ such that $g \cdot x = x$ for all $g \in G$. The set of all such x is denoted X_G and is called the G-invariants of X. When X is a G-module, i.e. X is an additive abelian group and G is acting on it with the additional action axiom that $g \cdot (a + b) = g \cdot a + g \cdot b$ with $a, b \in X$, then X^G is the zeroth cohomology group of G with coefficients in X, that is, $H^0(G; X) = X^G$.

For each $x \in X$, the **stabilzer** of x by G is defined as the set $G_x = \{g \in G\colon g \cdot x = x\}$, and another common notation for this set is $\mathrm{stab}(x)$. Sometimes this set defined as being the "stabilizer subgroup" of G. The reason should be clear: Clearly $G_x \subseteq G$ and $G_x \neq \varnothing$ as $e \in G$ and $e \cdot x = x$ by the action axioms, and so $e \in G_x$. Now take $a, b \in G_x$, then we need to show $ab^{-1} \in G_x$ (recall this is the subgroup test). So, as $a \cdot x = x$ and $b \cdot x = x$, and as $e \cdot x = x$, then $e \cdot x = bb^{-1} \cdot x = b^{-1}b \cdot x = b^{-1} \cdot x = x$; thus $b^{-1} \in G_x$. Then $ab^{-1} \cdot x = a \cdot (b^{-1} \cdot x) = a \cdot x = x$. Therefore $G_x \leq G$. This is typically not a normal subgroup, however.

The action of G on X is *free* if and only if all stablizers are trivial; that is, for all $k \in X$, we have that $G_k = \{e_G\}$. An actions is called *faithful* if we have that the intersection of all stablizers is trivial $\{e_G\}$. Thus, if we let $E = \{G_x\}_{x \in X}$ denote the set of stabilizers for all $x \in X$, then the action on of G on X is free if and only if $\cup E = \{e_G\}$; the action of G on X is called faithful if $\cap E = \{e_G\}$. Furthermore, we can reformulate this as saying an action is faithful if for two distinct elements $g \neq h$ in G there exists an $x \in X$ such that $g \cdot x \neq h \cdot x$; contrapostivitly, if for all $x \in X$, we have $g \cdot x = h \cdot x$, then $g = h$. Moreover, an action is called free if for any two distinct elemenets $g \neq h$ in G and all $x \in X$ we have $g \cdot x \neq h \cdot x$; contrapositivtly, if we have $g \cdot x = h \cdot x$ for some $x \in X$, then $g = h$ in G. We can see how related these two notions are to one another. In fact, as you should've seen, a free action is faithful.

Proposition 1.1. A group G acts faithfully on X if and only if the homomorphism $G \to S_X$ has a trivial kernel.

Proof. Let G be a group acting on X and let the action be faithfull. For all $g \in G$, define $\sigma_g\colon X \to X$ where $\sigma_g\colon x \mapsto g \cdot x$; this map is a bijection from $X \to X$. Now define the map $\varphi\colon G \to S_X$ by $\varphi\colon g \mapsto \sigma_g$. Take $g, h \in G$. Then $\varphi(gh) = \sigma_{gh}$, and so take some $x \in X$. So $\sigma_{gh}(x) = gh \cdot x = g \cdot (h \cdot x) = \sigma_g(\sigma_h(x)) = (\sigma_g\sigma_h)(x)$; thus $\varphi(gh) = \sigma_g\sigma_h = \varphi(g)\varphi(h)$ and φ is a homomorphism. Now consider the kernel of this maps, i.e.
$\ker(\varphi) = \{z \in G\colon \varphi(z) = \sigma_z = \mathrm{id}_X\}$. If we take the trivial $e \in G$ then $\varphi(e) = \sigma_e$, and so on every element $x \in X$,

$\sigma_e(x) = e \cdot x = x$ by the first action axiom, and we see that $\sigma_e = \mathrm{id}_X$; therefore $e_G \in \ker(\varphi)$. Suppose that we have some other element $q \in \ker(\varphi)$ distinct from e_G. Then we have that $\sigma_q = \sigma_e$, i.e. for all $x \in X$, $\sigma_q(x) = q \cdot x = e \cdot x = \sigma_e(x)$, but as the action is faithfull then $q \cdot x = e \cdot x$ implies that $q = e$. Therefore the kernel is trivial.

For the opposite direction, suppose that the homomorphism we define in the first part of the proof has trivial kernel. As the homomorphism has trivial kernel, then we have that $\varphi\colon G \to S_X$ is injective. Suppose that we have $\varphi(g) = \varphi(h)$ for some $g, h \in G$. Then $\sigma_g = \sigma_h$, for all $x \in X$, $\sigma_g(x) = \sigma_h(x)$ so $g \cdot x = h \cdot x$ and as φ is injective, we have $g = h$. Therefore the action is faithfull. □

Theorem 1.1 (Orbit-Stabilizer)**.** Let G be a group which acts on a finite set X and fix $x \in X$. Then $|G \cdot x| = [G\colon G_x]$.

1.2. **Centralizers and Normalizers.** Let G be a group and let $A \subseteq G$.

Definition 1.3. Define $C_G(A) = \{g \in G\colon gag^{-1} = a \text{ for all } a \in A\}$. This subset of G is called the **centralizer** of A in G. Since $gag^{-1} = a$ if and only if $ga = ag$, $C_G(A)$ is the set of elements of G which commute with every element of A.

We can clearly see that $C_G(A) \subseteq G$ and $C_G(A) \neq \varnothing$ as $eae^{-1} = ea = a$ so $e \in C_G(A)$. Now take $x, y \in C_G(A)$. Then $x, y \in G$ and $xax^{-1} = a = yay^{-1}$. Lastly lets consider xy^{-1}:$(xy)a(xy)^{-1} = (xy)a(y^{-1}x^{-1}) = x(yay^{-1})x^{-1} = xax^{-1} = a$, and so $xy^{-1} \in C_G(A)$. Therefore the centralizer of A in G is a subgroup of G, i.e. $G_G(A) \leq G$.

Now if G is abelian, then we clearly see that $ga = ag$ for all $g \in G$ and $a \in A$, so $C_G(A) = G$.

Definition 1.4. Define $Z(G) = \{g \in G\colon gx = xg \text{ for all } x \in G\}$, the set of elments commuting with all the elements of G. This subset of G is called the **center** of G.

We can make the clear observation that $C_G(G) = Z(G)$ and so we also have that $Z(G) \leq G$. If we do this directly, however, in good spirit, $Z(G)$ is trivially nonempty and obviously a subset of G. If we take $x, y \in Z(G)$. Then $yt = ty$ and $xs = sx$ for all s, t. Now $et = te$, that is, $y^{-1}yt = y^{-1}ty = tyy^{-1}$, multiplying by y we get $y^{-1}ty^2 = ty$ so $y^{-1}ty = t$ which gives $y^{-1}t = t^{-1}$; thus $y^{-1} \in Z(G)$. Lastly, take some $l \in G$, then $xy^{-1}l = xly^{-1} = lxy^{-1}$. Therefore $Z(G)$ is a subgroup of G.

Definition 1.5. Define $gAg^{-1} = \{gag^{-1}\colon a \in A\}$. Define the **normalizer** of A in G to be the set
$N_G(A) = \{g \in G\colon gAg^{-1} = A\}$.

The reason for defining the normalizer in this manner is possibly the main cannon of confusion for this defintion: for the set's needed condition $gAg^{-1} = A$, we're saying that $gag^{-1} = a'$ for some $a, a' \in A$ and we don't necessarily have that $a = a'$. Note that in the case where they are equivalent however, then we would have this element $g \in G$ that makes $gag^{-1} = a$ a true statement so $g \in C_G(A)$. Thus we see can predict, with good vision, that $C_G(A) \leq N_G(A)$. Furthermore, we have that $N_G(A) \leq G$.

1.3. **The Symmetric Group.** Let X be any set. Then we define the **symmetric group** to be the set
$\mathfrak{S}_X = \{\varphi\colon X \to X\colon \varphi \text{ is a bijection}\}$. You can easily verify that this in fact a group with the group operation being the usual composition of functions. Typically, we deal simply with the set $X = \{1, 2, 3, \ldots, n\}$.We assume familiarity with cycle notation.

Proposition 1.2. If the pair of cycles $\alpha = (a_1\ a_2\ \cdots\ a_m)$ and $\beta = (b_1\ b_2\ \cdots\ b_n)$ have no common entries, i.e. they're disjoint, then $\alpha\beta = \beta\alpha$.

Proof. Let a_i be in $\{a_1, a_2, \ldots a_m\}$. Then $\alpha\beta(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1}$, and $\beta\alpha(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}$. Similarily, let b_i be in $\{b_1, b_2, \ldots, b_n\}$. Then $\alpha\beta(b_i) = \alpha(\beta(b_i)) = \alpha(b_{i+1}) = b_{i+1}$, and $\beta(\alpha(b_i)) = \beta(b_i) = b_{i+1}$. □

1.3.1. *Transpositions and the Alternating Group.* First we need to recall that any elment of $\mathfrak{S}_n$ can be written as a product of disjoint cycles in a *unique* way. However, if we don't write the cycle as a product of disjoint cycles, then the representation of the cycle can take many forms: for example, $\sigma = (1\ 2\ 3)$ in $\mathfrak{S}_3$ may be written as $(1\ 3)(1\ 2)$, $(1\ 2)(1\ 3)(1\ 2)(1\ 3)$, and there are more representations (in fact, infinitely many ways!). And so, if we allow for the cycle to not be disjoint, then we're destroying the uniqueness of a representation of a permutation as a product of cycles.

Remark 1.2. Once again, recall that a 2-cycle is called a transposition, and for any $\mathfrak{S}_n$, we may write any $\sigma \in \mathfrak{S}_n$ as a product of two cycles (however not in a unique way). For example, we have $(1\ 2\ 3) = (1\ 3)(1\ 2)$ for $\mathfrak{S}_3$. In general, if $\sigma = (a_1\ a_2\ \ldots\ a_m) \in \mathfrak{S}_n$, then we can write this as a product of transpositions: $\sigma = (a_1\ a_m)(a_1\ a_{m-1})(a_1\ a_{m-2})\ \ldots\ (a_1 a_2)$. And so, we can say that $\mathfrak{S}_n$ is finitely generated if $n < \infty$ by the given set $\langle T\rangle = \langle\{(i\ j)\colon 1 \leq i < j \leq n\}\rangle = \mathfrak{S}_n$.

1.4. **Dihedral Group.** In general, the **dihedral group** is the group of symmetries of a regular polygon, where the elements in the groups are represenative of rotations and reflections. The group is defined as $D_{2n} = \langle r, s \colon r^n = s^2 = 1,\ rs = sr^{-1} \rangle$. We use the convention of denoting the dihedral group as D_{2n} rather than D_n as $|D_{2n}| = 2n$, as opposed to using D_n to denote the n-gon (e.g. for the group of symmetries of a triangle, $D_{2(3)} = D_6$ rather than D_3). We can note that, taking the geometric point of view, that $s \neq r^i$ for any i, as if we have a regular polygon (e.g. take a square) then if we rotate it as many times as we please, then it wouldn't make any sense for it to be equivalent to a roation along any axis (label and work it with a square to help visual aid). Furthermore, we also have that $sr^i \neq sr^j$, for all $0 \leq i, j \leq n-1$ with $i \neq j$, so a presentation of D_{2n} in terms of looking at its elements,

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}.$$

Remark 1.3. As we've seen in the definition of D_{2n} we have that $rs = sr^{-1}$ for all s, r, but we in fact have $r^i s = sr^{-i}$ for all $i \geq 1$. We proceed by induction: the base case is trivial, as we have it by definition. Let $r^k s = sr^{-k}$ for all $k \geq 1$. Then $r(r^k s) = (rr^k s) = r^{k+1} s = r(sr^{-k}) = (rs)r^{-k} = (sr^{-1})(r^{-k}) = s(r^{-1}r^{-k}) = s^{-1(k+1)}$, and we're done.

In general, all the elements of D_{2n} have a (unique) representation in the form $s^k r^i$, $k = 0$ or 1 and $0 \leq i \leq n-1$. If we take $x, y \in D_{2n}$, then $x = s^k r^i$ and $y = s^l r^j$ and for now we make no assumptions about the exponents on s. Then $xy = (s^k r^i)(s^l r^j) = s^k (r^i s^l) r^j = s^k (s^l r^{-i}) r^j = s^{k+l} r^{j-i}$. Thus this works, and it is clear that any assumptions upon the exponents l and k would've not changed the outcome.

We ca note here that D_2 is ismorphic to Z_2, which makes D_2 abelian, and that D_4 is isomorphic to K_4, the klein four-group. However, D_2 and D_4 are the exception as no other dihedral group is abelian beyond these two examples. Moreover, we have that D_{2n} is a subgroup of the symmetric group $\mathfrak{S}_n$ for $n \geq 3$.

2. Cosets

Let G be a group and let $H \leq G$. Then we define a (left) *coset* to be the set $gH = \{gh \colon h \in H\}$ for each $g \in G$. The element g of the coset gH is said to be a *representative* of the coset. Moreoever, the collection of left cosets is denoted G/H. That is to say, $G/H = \{gH \colon g \in G\}$. The common short-hand notation is to denote a represenative in G/H by $\overline{g}$, however, we will omit that largely here as it is perhaps clearer to not use it. To provide some interest, we should also note here that we can say, equivalently, that a left coset is an equivalence class of $G/\sim$ where $g_1 \sim g_2$ if and only if $g_1 = g_2 h$ for some $h \in H$. So, two cosets equivalent if $g_1 H = g_2 H$ as $g_1 h = g_2 l$ for some $h, l \in H$, so $g_1 = g_2 (l h^{-1}) = g_2 h_2$ where $h_2 = l h^{-1} \in H$.

Proposition 2.1. Let G be a group and let $H \leq G$. The left cosets of H in G form a partition of G.

Proof. Let $g \in G$. Since $1 \in H$, it follows that $g \cdot 1 = g \in gH$, so every element of G is in some coset of H and so the union of all cosets is all of G. By contrapositive, assume that we have $g_1 H$ and $g_2 H$ and $g_1 H \cap g_2 H \neq \varnothing$. Then we have at least one element in both cosets, so let $x \in g_1 H \cap g_2 H$. Then we may write x as $x = g_1 h_1$ and $x = g_2 h_2$, which means that $g_1 h_1 = g_2 h_2$, and so $g_1 = g_2 h_2 h_1^{-1}$; each element of $g_1 H$ has the form $g_1 h$ for some $h \in H$, and $g_1 h = (g_2 h_2 h_2^{-1}) h = g_2 (h_2 h_2^{-1}) \in g_2 H$. Thus we see that $g_1 H \subseteq g_2 H$, and the other inclusion follows by a similar argument. Therefore $g_1 H = g_2 H$. □

Proposition 2.2. Let $H \leq G$. Then any two cosets have the same order.

Proof. Take $g, k \in G$. Then let $\varphi \colon gH \to kH$ by $\varphi \colon gh \mapsto kh$. This map is well defined as if we let $gh = gh'$, then $g^{-1} gh = h' = h$. We can also define the map $\psi \colon kH \to gH$ by $\psi \colon kh \mapsto gh$, and this map is indeed well defined. Now take $gh \in gH$, then $(\psi\varphi)(gh) = \psi(\varphi(gh)) = \psi(kh) = (gh) = \mathrm{id}(gh)$, and similarily, if we take $kh \in kH$ then $\varphi(\psi(kh)) = \varphi(gh) = kh = \mathrm{id}(kh)$. Therefore we have a bijection between the two cosets and thus their cardinalities are the same. □

Corollary 2.1. Any left coset has the same order as H.

Definition 2.1. If $H \leq G$ then the **index** of H in G, written $[G \colon H]$, is the number of left (or right) cosets of H in G. That is, $[G \colon H] = |\{gH \colon g \in G\}|$

Remark 2.1. If G is finite, then $[G \colon H] = |G|/|H|$. Moreover, if $K \leq H \leq G$ then $[G \colon K] = [G \colon H][H \colon K]$ as we have

$$[G \colon H][H \colon K] = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = \frac{|G|}{|K|} = [G \colon K].$$

We will note here, without proof, that this is also true when considering infinite groups.

2.1. **Normal Subgroups.**

Definition 2.2. If G is a group and $H \leq G$, and for all $g \in G$ we have $gH = Hg$, then we say that H is a **normal subgroup** of G, and write $H \lhd G$.

Lemma 2.1. (i) Every subgroup of an abelian group G is normal.
(ii) A subgroup H is normal in G if and only if for all $g \in G$ and $h \in H$, then $ghg^{-1} \in H$

Proof. Suppose that G is an abelian group and $H \leq G$. Then if we take $g \in G$ and $gh \in gH$, then $gh = hg \in Hg$. So the equality of sets is obvious. Now for (ii): If we have a normal subgroup H of G, then $gH = Hg$, so if we take some $gh \in gH$, then $gh = h'g \in Hg$, so $ghg^{-1} = h' \in H$. For the opposite direction, take $g \in G$ and $h \in H$ and suppose $ghg^{-1} = h' \in H$. Then if $gh = h'g$, so $gh \in Hg$ and $h'g \in gH$, so we can see a containment of sets, i.e. $gH = Hg$ as we chose everything arbitrarily. □

Proposition 2.3. Let $\varphi\colon G \to H$ be a group homomorphism.
(i) $\ker \varphi \lhd G$.
(ii) If $K \lhd H$, then $\varphi^{-1}(K) \lhd G$.

Proof. For (i): $\ker \varphi$ is trivially nonempty, and so take $x, y \in \ker \varphi$. So $\varphi(1) = 1 = \varphi(yy^{-1}) = \varphi(y)\varphi(y^{-1}) = \varphi(y^{-1})$; thus $y^{-1} \in \ker \varphi$. Now $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) = 1$; thus $xy^{-1} \in \ker \varphi$ and $\ker \varphi \leq G$. Take $g \in G$ and and $h \in \ker \varphi$. Then $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = 1$. Therefore $ghg^{-1} \ker \varphi$ and $\ker \varphi \lhd G$. For (ii): Let $K \lhd H$. Then recall that the preimage is defined as $\varphi^{-1}(K) = \{g \in G\colon \varphi(x) \in K\}$. This set is nonempty as $\varphi(1) = 1 \in K$. Take $x, y \in \varphi^{-1}(K)$. Now $\varphi(1) = 1 = \varphi(yy^{-1}) = \varphi(y)\varphi(y^{-1}) \in K$. Clearly we will have that $xy^{-1} \in K$, so $K \leq G$. Now take $h \in \varphi^{-1}(K)$ and $g \in G$. Then $\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g^{-1}) \in \varphi(g)K\varphi(g^{-1}) \subseteq K$, as K is normal. Thus $ghg^{-1} \in \varphi^{-1}(K)$ and $\varphi^{-1}(K) \lhd G$. □

Proposition 2.4. If $H \leq G$ and $[G\colon H] = p$ for some prime p, then $H \lhd G$.

3. Conjugacy Classes

In a group G, two elements h and ℓ are called *conjugate* when $h = g\ell g^{-1}$ for some $g \in G$. Recall that for $H \leq G$, the *conjugate* subgroup of H by a fixed $g \in G$ is

$$gHg^{-1} = \{ghg^{-1}\colon h \in H\}.$$

If we fix some element $\ell \in G$, we may seek to know which, and how many, elements in G can be written as $g\ell g^{-1}$ for some $g \in G$. A trivial observation is that we may write the ℓ itself as a conjugate of ℓ, that is, $\ell(\ell)\ell^{-1} = \ell(1) = \ell$. We wish to prescribe a name to all these elements that can be written in terms of conjugacy by a fixed element (in our case, ℓ): we denote the set of all such elements in G by $\mathrm{cl}_G(\ell)$ and it is called the *conjugacy* class of ℓ. Formally, for an element $q \in G$, its *conjugacy class* is the set of all elements to it, i.e. $\mathrm{cl}_G(x) = \{gxg^{-1}\colon g \in G\}$.

Remark 3.1. In any group, $\mathrm{cl}_G(1) = \{1\}$, as $g1g^{-1} = gg^{-1} = 1$ for all $g \in G$. Moreover, if $x \in Z(G)$, then $gxg^{-1} = x$ for all $g \in G$, so $\mathrm{cl}_G(x) = \{x\}$. The converse is true here as well: if a conjugacy class has size 1, then it is in the center of the group. Moreover, if G is abelian then every elment is it own conjugacy class.

Proposition 3.1. Conjugacy is an equivalence relation.

Proof. In this instance, two elements $x \sim y$ if and only if there is a $g \in G$ such that $x = gyg^{-1}$. Now $x = 1x1^{-1} = x$, so $x \sim x$. Now let $x \sim y$ such that $x = gyg^{-1}$, so then $xg = gy$ and $g^{-1}xg = y$; thus $y \sim x$. Lastly, let $x \sim y$ and $y \sim z$ with $x = gyg^{-1}$ and $y = hzh^{-1}$. Then $x = g(hzh^{-1})g^{-1} = (gh)z(gh)^{-1}$, and so $x \sim z$. □

Remark 3.2. As conjugacy is an equivalence relation, then it forms a partition of G. Thus the size of G is the sum of all conjugacy classes, that is, $|G| = \sum_{\ell \in G} |\mathrm{cl}_G(\ell)|$.

Definition 3.1. For a group G and $g \in G$, its **centralizer** $Z(g)$ is the set of elements of G commuting with G; that is,

$$Z(g) = \{x \in G\colon xg = gx\}$$

A clear observation that follows from this definition is that if we intersect all centralizers of fixed elements in G, then we get the whole centralizer of the group, i.e. $\bigcap_{g \in G} Z(g) = Z(G)$.

Theorem 3.1. For each $g \in G$, its conjugacy class has the same size as the index of its centralizer:

$$|\mathrm{cl}_G(g)| = [G\colon Z(g)].$$

Corollary 3.1. For any finite group G,

$$|G| = |Z(G)| + \sum |\mathrm{cl}_G(x_i)|,$$

where the sum is taken over distinct conjugacy classes of size greater than 1.

Proof. As we showed earlier, conjugacy classes partition G, so $|G| = \sum_{\ell \in G} |\mathrm{cl}_G(\ell)|$, and by Theorem 4.1., we have $|G| = \sum_{\ell \in G} [G\colon Z(g)] = \sum_{l \in G} |G|/|Z(g)|$. If we take some $w \in G$, and $|\mathrm{cl}_G(w)| = 1$, then we must have that the element in $\mathrm{cl}_G(w)$ is w itself: as every conjugacy class itself is in it as $w = 1w1^{-1} = w$, so this is necessary. Moreover, if $\mathrm{cl}_G(w) = \{w\}$, then we have that $w = gwg^{-1}$, so $wg = gw$, i.e. $w \in Z(G)$. So we can collect all these conjugacy classes with size one (all those $w_i \in G$ such that $Z(w_i) = G$) into a single term, we get

$$|G| = |Z(G)| + \sum |\mathrm{cl}_G(x_i)|$$

where the te sum is carried out only over those those conjugacy classes with more than one element. □

Theorem 3.2. If G is a finite group then each conjugacy class in G has size dividing $|G|$.

Note here that this is not an immediate consequence of Langrange, as conjugacy classes are not subgroup. A simple way to see this is that the only conjugacy class containging the identity is the identity itself. As, if you had $1 \in \mathrm{cl}_G(x)$ for some $x \neq 1 \in G$, then $1 = gxg^{-1}$ for some $g \in G$, so $1g = g = xg$, so $x = 1$, which is a contradiction and we must have $1 \notin \mathrm{cl}_G(x)$.

4. Sylow Theorems

Definition 4.1. Let G be group and p be prime.

- A group of order p^α for some $\alpha \geq 1$ is called a p-group. Subgroups of G which are p groups are called p-subgroups.
- If G is a group of order $p^\alpha m$, where $p \nmid m$, then a subgroup of order p^α is called a **Sylow p-subgroup** of G.
- The set of Sylow p-subgroups of G will be denoted by $\mathrm{Syl}_p(G)$ and the number of Sylow p-subgroups of G will be denoted by $n_p(G)$ (or just n_p when clear).

Theorem 4.1 (Sylow's Theorem)**.** Let G be a group of order $p^\alpha m$, where p is a prime not dividing m

- Sylow p-subgroups of G exist, i.e. $\mathrm{Syl}_p(G) \neq \varnothing$.
- If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$, i.e. Q is contained in some conjugate of P. In particular, any two Sylow p-subgroups of G are conjugate in G.
- The number of Sylow p-subgroups of G is given by considering $n_p \equiv 1 \pmod p$ and the fact that $n_p \mid m$.

4.1. **Counting to Force Normalization of a Sylow p-subroup.** Let G be a group and $|G| = n$, let p be prime dividing n and let $P \in \mathrm{Syl}_p(G)$. If $|P| = p$, then every nonidentity element of P has order p (we use this a lot in semidirect products) and every element of G of order p is in some conjugate of P. By Lagrange, distinct conjugates of P interesect in the identity, and so in this case the number of elements of G of order p is $n_p(p-1)$.

If Sylow p-subgroups for different primes have different orders (cf. Exercise 6.1 that follows this section) and we assume none these is normal, we can sometimes show that the number of elements of prime order is $> |G|$. This contradiction forces one of the n_p to be 1 and thus giving us a normal Sylow p-subgroup in G.

Example 4.1. Let $|G| = 105 = 3 \cdot 5 \cdot 7$. Then use many choices for the n_3, n_5, and n_5, but if we assume $n_3 = 7$, $n_5 = 21$, and $n_7 = 15$ (for their respective max):

$$\begin{gathered}\text{the number of elments of order 3 is } 7 \cdot 2 = 14\\ \text{the number of elments of order 5 is } 21 \cdot 4 = 84\\ \text{the number of elments of order 7 is } 15 \cdot 6 = 90\end{gathered}$$

which implies that the number of elements of prime order is $90 + 84 + 14 = 188$, but this greater than 105, so we have a contradiction.

5. Semidirect Products

Exercise 5.1. Classify the structure of a group of order 20.

Proof. Let G be a group of order 20. Then $|G| = 20 = 2^2(5)$, and so by Sylow's Theorem, we have $n_5 \mid 4$ and $n_5 \equiv 1 \pmod 5$, which implies that $n_5 = 1$, however, $n_2 = 1$ or $n_2 = 5$. Let K be the unique, normal 5-Sylow and let H be a 2-Sylow. Then the orders of H and K are relatively prime as $\gcd(5,4) = 1$ and so their intersection must be trivial, i.e. $H \cap K = \{1\}$. Moreover, $HK \leq G$, and so $|HK| = (|H||K|)/(H \cap K) = 20/1 = 20$, and so by the Recognition Theorem, we have that $G \simeq K \rtimes_\varphi H$, where $\varphi\colon H \to \mathrm{Aut}(K)$. As $|K| = 5$, we have that $K \simeq Z_5$, and as $|H| = 4$, then $H \simeq Z_2 \times Z_2$ or $H \simeq Z_4$.

For the case of $H \simeq Z_4$, we have that $\varphi\colon Z_4 \to \mathrm{Aut}(Z_5)$, but $\mathrm{Aut}(Z_5) \simeq Z_4$, so $\varphi\colon Z_4 \to Z_4$. Let x denote the generator of Z_4 and y denote the generator of the codomain Z_4. Now we need for the order of y to satisfy specific

properties, in particular, $|y^i| = 4/(\gcd(4,i))$ and we need for $|y^i|$ to divide 4. Testing for values of i up to 4, we have that $i \in [[1,4]]$ are all choices that work. Now we have four mappings:

$$\psi_1 \colon Z_4 \to Z_4, \psi_1 \colon x \mapsto y^4 = 1$$
$$\psi_2 \colon Z_4 \to Z_4, \psi_2 \colon x \mapsto y$$
$$\psi_3 \colon Z_4 \to Z_4, \psi_3 \colon x \mapsto y^2$$
$$\psi_4 \colon Z_4 \to Z_4, \psi_4 \colon x \mapsto y^3$$

The map ψ_1 produces the group $Z_5 \times Z_4$. We need to consider the other maps and whether or not they are isomorphic to one another. We do this by recognizing that ψ_2 and ψ_4 both have order 4, as when we map $\psi_2(x^4) = y^4 = 1$ and $\psi_3(x^4) = (y^3)^4 = y^{12} = 1$. This implies that $Z_5 \rtimes_{\psi_1} Z_4 \simeq Z_5 \rtimes_{\psi_3} Z_4$. Lastly, we have $Z_5 \rtimes_{\psi_3} Z_4$.

For the case of $H \simeq Z_2 \times Z_2$, we have $\varphi \colon Z_2 \times Z_2 \to Z_4$. We note here that $Z_2 \times Z_2 = \langle a, b \colon a^2 = b^2 = (ab)^2 = 1 \rangle$. Once again, let y denote the generator of Z_4. Now we, similarily, need φ to satisfy certain conditions: $|y^j| = 4/(\gcd(4,j)$ and $y^j \mid 2$. Thus the only satisfactory values of j for which this works for are $j = 2$ and 4. So we will mappings:

$$\alpha_1 \colon Z_2 \times Z_2 \to Z_4, \alpha_1 \colon a, b \mapsto y^2, 1$$
$$\alpha_2 \colon Z_2 \times Z_2 \to Z_4, \alpha_2 \colon a, b \mapsto 1, y^2$$
$$\alpha_3 \colon Z_2 \times Z_2 \to Z_4, \alpha_3 \colon a, b \mapsto y^2, y^2$$
$$\alpha_4 \colon Z_2 \times Z_2 \to Z_4, \alpha_1 \colon a, b \mapsto 1, 1$$

We can immediately notice that α_4 gives rise to $Z_4 \times Z_2 \times Z_2$. Moreover, we can see that we will have isomorphisms between α_1 and α_2, and so $Z_4 \rtimes_{\alpha_1} Z_2 \times Z_2 \simeq Z_4 \rtimes_{\alpha_2} Z_2 \times Z_2$. The nontrivial case that we actually hence have is $Z_4 \rtimes_{\alpha_3} Z_2 \times Z_2$. □

Example 5.1. Classify the structure of a group of order 28.

Proof. Let G be a group of order 28. Then $|G| = 28 = 14 \cdot 2 = 7 \cdot 2^2$, and so $n_7 \mid 4$ and $n_7 \equiv 1 \pmod 7$ which meas that $n_7 = 1$. However, $n_2 = 7$ or 1. Let K denote the unique, normal 7-Sylow and let H be a 2-Sylow. Then $|K| = 7$ so $K \simeq Z_6$ and $|H| = 4$ so either $H \simeq Z_4$ or $H \simeq Z_2 \times Z_2$. Furthermore, by the same reasoning as the last exercise, we have $G \simeq K \rtimes_\varphi H$, where $\varphi \colon H \to \mathrm{Aut}(K)$, or, rather, $\varphi \colon H \to Z_6$.

If $H \simeq Z_4$, then we will consider mappings $\psi \colon Z_4 \to Z_5$. Let $Z_4 = \langle x \rangle$ and $Z_6 = \langle y \rangle$. Then we need that $|y^i| = 6/(\gcd(6,i)$ to divide 4. So the only choices of i that satisfy this are $i = 3$ and 6. Thus we have the maps

$$\psi_1 \colon Z_4 \to Z_6, \psi_1 \colon x \mapsto y^6 = 1$$
$$\psi_2 \colon Z_4 \to Z_6, \psi_2 \colon x \mapsto y^3$$

The first mapping gives rise to $Z_6 \rtimes_{\psi_1} Z_4 \simeq Z_6 \times Z_4$, and the second mapping simply produces $Z_6 \rtimes_{\psi_2} Z_4$.

If $H \simeq Z_2 \times Z_2$, then we consider mappings $\alpha \colon Z_2 \times Z_2 \to Z_6$. Once again, we need to find satisfactory conditions for j respective to $|y^j| = 6/\gcd(6,j)$ such that this divides 2. In this instance, the only satisfactory choice are $j = 6$ and 3. Thus we have mappings

$$\alpha_1 \colon Z_2 \times 2 \to Z_6,\ \alpha_1 \colon a, b \mapsto 1, 1$$
$$\alpha_2 \colon Z_2 \times Z_2 \to Z_6,\ \alpha_2 \colon a, b \mapsto y^3, y^3$$
$$\alpha_3 \colon Z_2 \times Z_2 \to Z_6,\ \alpha_3 \colon a, b \mapsto 1, y^3$$
$$\alpha_4 \colon Z_2 \times Z_2 \to Z_6,\ \alpha_2 \colon a, b \mapsto 1, y^3$$

The last two mappings can be seen to induce the same group, i.e. $Z_6 \rtimes_{\alpha_3} Z_2 \times Z_2 \simeq Z_6 \rtimes_{\alpha_4} Z_2 \times Z_2$, and we of course have the trivial mapping given by α_1, so we also have $Z_6 \times Z_2 \times Z_2$. The other group we have is $K_6 \rtimes_{\alpha_2} Z_2 \times Z_2$. □

5.1. **Inner Direct Product.** Suppose that G is a group and $H \triangleright G$, $K \leq G$, and $H \cap K = \{1\}$. We seen in the past that $HK = \{hk \colon h \in H, k \in K\}$ does indeed form a subgroup of G, i.e. $HK \leq G$. Now, since $H \cap K = \{1\}$, then for every $x \in HK$, we have a unique pair (h,k) such that $x = hk$. For now, Now, if we take some $g_1, g_2 \in HK$ such that $g_1 = h_1k_1$ and $g_2 = h_2k_2$ for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$, then $g_1g_2 = (h_1k_1)(h_2k_2) = h_1k_1h_2k_2 = h_1k_1h_2k_1^{-1}k_1k_2 = h_1(k_1h_2k^{-1})k_1k_3 = h_1\varphi_{k_1}(h_2)k_3$, where $\varphi \colon K \longrightarrow \mathrm{Aut}(H)$ by $\varphi \colon k \longmapsto \varphi_k$ and φ takes some element $x \in H$ to kxk^{-1}, i.e. $\varphi_k \colon x \longmapsto kxk^{-1}$. Therefore we have that the maps coincide.

We can take note of that the fact that g_1g_2 is completely determined by the group homomorphism:

$$\varphi \colon K \longrightarrow \mathrm{Inn}(H) \leq \mathrm{Aut}(H)$$
$$k \longmapsto \varphi_k$$

Moreover, given two groups H and K, we want to define possible group structures on $H \times K = \{(h,k) \colon h \in H, k \in K\}$.

Theorem 5.1. Let H and K be two groups. Let $\psi\colon K \longrightarrow \mathrm{Inn}(H)$ be a group homomorphism. Equip the set $H \times K$ by the following group operation: for $(h_1, k_1), (h_2, k_2) \in H \times K$,

$$(h_1, k_1) \cdot (h_2, k_2) = (h_1\psi(k_1)(h_2), k_1k_2).$$

Then $(H \times K, \cdot)$ is a group, and is denoted by $H \rtimes_\psi K$, called the **semi-direct product** of H and K with respect to ψ.

Proof. As H and K are both groups and are both nonempty as needed, then $H \times K$ is nonempty. Now, suppose we have $(h_1, k_1), (h_2, k_2) \in H \rtimes_\psi K$. Then $(h_1, k_1) \cdot (h_2, k_2) = (h_1\psi(k_1)(h_2), k_1k_2)$, and since $\psi(k_1)(h_2)$ produces an element in H as ψ is itself an automorphism, we have that $(h_1, k_1) \cdot (h_2, k_2) = (h_2h, k_1k_2) \in H \times K$, where $h = \psi(k_1)(h_2)$. Thus we have closure. Now, the identity element of $H \rtimes_\psi K$ is simply $(1, 1)$. For inverses, we're going to define that for some $(h, k) \in H \rtimes_\psi K$, its inverse is $(h, k)^{-1} = (\psi(k^{-1})(h^{-1}), k^{-1})$; so, $(h, k) \cdot (h, k)^{-1} = (h\psi(k)(\psi(k^{-1})(h^{-1})), yy^{-1})$. The left side of this is a cluster fuck but its not so bad to actually compute: firstly $\psi(k^{-1})(h^{-1}) = k^{-1}h^{-1}k$, and so $\psi(k)(k^{-1}h^{-1}k) = k(k^{-1}h^{-1}k)k^{-1} = h^{-1}$; thus, $(h, k) \cdot (h, k)^{-1} = (h(h^{-1}), yy^{-1}) = (1, 1)$. Lastly we need to check associatvity:

$$\begin{aligned}
((h, k) \cdot (x, y)) \cdot (l, t) &= (h\psi(k)(x), ky)) \cdot (l, t) \\
&= (hkxk^{-1}, ky) \cdot (l, t) \\
&= (hkxk^{-1}\psi(ky)(l), kyt) \\
&= (hkxk^{-1}(ky)l(ky)^{-1}, k(yt)) \\
&= (hkxyly^{-1}k^{-1}, k(yt)) \\
&= (h\psi(k)(xyly^{-1}), k(yt)) \\
&= (h\psi(k)(x\psi(y)(l)), k(yt) \\
&= (h, k) \cdot (x\psi(y)(l), yt) \\
&= (h, k) \cdot ((x, y) \cdot (l, t));
\end{aligned}$$

we should note here that we were using the fact that H and K are groups to do a lot of the work in their respective slots. Therefore $H \rtimes_\psi K$ is a group. □

6. Rings

6.1. Euclidean Domains.

Definition 6.1. Any function $N\colon R \to \mathbf{Z}_{\geq 0}$ with $N(0) = 0$ is called a **norm** on the integral domain R. If $N(a) > 0$ for all $a \neq 0$ define N to be a positive norm.

Definition 6.2. The integral domain R is said to be a **Euclidean Domain** if there is a norm N on R such that for any two elements $a, b \in R$ with $b \neq 0$ there exists elements $q, r \in R$ with

$$a = qb + r \text{ with } r = 0 \text{ or } N(r) < N(b).$$

The element q is called the **quotient** and the element r is the **remainder** of the division.

Remark 6.1. Recall that if D is a square free integer, then we can produce the field $\mathbf{Q}(\sqrt{D}) = \{a + b\sqrt{D}\colon a, b \in \mathbf{Q}\}$. We may observe that $\mathbf{Q}(\sqrt{D}) \subseteq \mathbf{C}$, and so we can show that $\mathbf{Q}(\sqrt{D})$ is subring of $\mathbf{C}$, however, we will omit the proof here as it is easy. In fact, this shows that $\mathbf{Q}(\sqrt{D})$ is an integral domain as any subring of an field is an integral domain. The reason for picking D to be square free (D has prime factorization with exponents at most one, i.e. $D = p_1p_2\cdots p_n$ with all p_i prime and $1 \leq i \leq n$) is so that every element in $\mathbf{Q}(\sqrt{D})$ can be written uniquely in the form $a + b\sqrt{D}$. Moreover, this further gives us that if $a, b \neq 0 \in \mathbf{Q}$, then $a^2 - Db^2 \neq 0$, and furthermore, as $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$, then we can recognize that $(a - b\sqrt{D})/(a^2 - Db^2)$ is the multplicative inverse of $a + b\sqrt{D}$ in $\mathbf{Q}(\sqrt{D})$ if $a + b\sqrt{D} \neq 0$. Thus we have that $\mathbf{Q}(\sqrt{D})$ is a field (called a *quadratic field*).

Continuing our discussion, we can immediately recognize that $\mathbf{Z}[\sqrt{D}]$ is a subring of $\mathbf{Q}(\sqrt{D})$. Now if $D \equiv 4 \pmod 4$ then we can product the slightly larger subset

$$\mathbf{Z}\left[\frac{1 + \sqrt{D}}{2}\right] = \left\{a + b\frac{1 + \sqrt{D}}{2}\colon a, b \in \mathbf{Z}\right\}.$$

This, once again, forms a subring of $\mathbf{Q}\sqrt{D}$. We define $\mathcal{O}_{(\mathbf{Q}\sqrt{D})} = \mathbf{Z}[\omega] = \{a + b\omega\colon a, b \in \mathbf{Z}\}$, where $\omega = \sqrt{D}$ if $D \equiv 2, 3 \pmod 4$ or $\omega = (1 + \sqrt{D})/2$ if $D \equiv 1 \pmod 4$. We call $\mathcal{O}_{(\mathbf{Q}\sqrt{D})}$ the **ring of integers** in the quadratic field $\mathbf{Q}\sqrt{D}$.

Define the *field norm* $N\colon \mathbf{Q}(\sqrt{D}) \to \mathbf{Q}$ by $N(a+b\sqrt{D}) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2 - Db^2 \in \mathbf{Q}$, and as $a, b, D \in \mathbf{Z}$, we also have that $N(a+b(\sqrt{D})) \in \mathbf{Z}$, and so we can begin to talk about the Euclidean aspect to this all. We do this by considering $\mathcal{O}_{(\mathbf{Q}\sqrt{D})}$ as they are integral domains with a norm defined by taking the absolute value of the field norm, i.e. $|N(a+b\sqrt{D})|$, so as to satisfy that $N\colon R \to \mathbf{Z}_{\geq 0}$. In general, however, $\mathcal{O}_{(\mathbf{Q}\sqrt{D})}$ isn't Euclidean; in fact, $\mathcal{O}_{(\mathbf{Q}\sqrt{D})}$ is only Euclidean, using the norm we just defined, for finitely many choices of D, and in, general, for any possible norm on $\mathcal{O}_{(\mathbf{Q}\sqrt{D})}$, and $D < 0$, there are once again finitely many choices of D in which it is Euclidean, and it is an open problem to classify when $\mathcal{O}_{(\mathbf{Q}\sqrt{D})}$ is Euclidean, with whatever norm, for $D > 0$.

Proposition 6.1. $\mathcal{O}_{(\mathbf{Q}\sqrt{-1})} = \mathbf{Z}[\sqrt{-1}] = \mathbf{Z}[i]$ is a Euclidean domain.

Proof. We define the norm $N\colon \mathbf{Z}[i] \to \mathbf{Z}_{\geq 0}$ to be $N(a+bi) = (a+bi)(a-bi) = a^2 + b^2$. Now take $\alpha = a+bi, \beta = c+di \in \mathbf{Z}[i]$ $\beta \neq 0$. Then in the field $\mathbf{Q}(i)$ we have that

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{ac-adi+bci+bd}{c^2+d^2} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{(bc-ad)}{c^2+d^2}i.$$

Now, we define in the clear manner, $\alpha/\beta = r+si$, and clearly $r, s \in \mathbf{Q}$. Let p be an integer closest to the rational number r and let q be an integer closest to the rational number s, so that both $|r-p|$ and $|s-q|$ are at most $1/2$. (It may help to think of the rational numberline here.) The division algorithm follows once we have that

$$\alpha = (p+qi)\beta + \gamma \text{ for some } \gamma \in \mathbf{Z}[i] \text{ with } N(\gamma) \leq \frac{1}{2}N(\beta).$$

Let $\theta = (r-p)+(s-q)i$ and set $\gamma = \beta\theta$. Then $\gamma = \alpha - (p+qi)\beta$, so that $\gamma \in \mathbf{Z}[i]$ is a Gaussian integer and $\alpha = (p+qi)\beta + \gamma$. Since $N(\theta) = (r-p)^2 + (s-q)^2$ is at most $1/4 + 1/4 = 1/2$, and as N is multiplicative, we have $N(\gamma) = N(\beta)N(\theta)$ so $N(\gamma) \leq \frac{1}{2}N(\beta)$. □

Proposition 6.2. Every ideal in a Euclidean domain is principal. More precisely, if I is any nonzero ideal in the Euclidean domain R then $I = (d)$, where d is any nonzero element of I of minimum norm.

Proof. Let A be a Euclidean domain. Then let J be an ideal of A. If J is the zero ideal, then $J = (0)$ and we are done. Let m be the nonzero, minimum element of J with respect to the norm, say, N endowed on A. We many note here that the set $\{N(a)\colon a \in J\}$ indeed has a minimum element by the Well Ordering of $\mathbf{Z}$; recall that $N(a) \in \mathbf{Z}_{\geq 0}$ as $N\colon A \to \mathbf{Z}_{\geq 0}$. So as J is an ideal then $mx \in J$ for $x \in A$; thus $(m) \subseteq J$. Let $\ell \in J$, and so as A is Euclidean, we may write $\ell = mq + r$ for some $q, r \in A$ and $N(r) < N(m)$. We may rewrite this as $\ell - mq = r$, and as J is an ideal, then $\ell - mq \in J$, but then $N(r) < N(m)$ is smaller so this contradicts the minimality of $N(m)$. We must have that $\ell = mq + 0 = mq$, and so every element in J can be written as mt for some $t \in A$. Thus $J \subseteq (m)$, which means $J = (m)$, and so A is a PID. □

6.2. **UFD.**

Definition 6.3. Let R be an integeral domain.

- Suppose $r \in R$ is nonzero and is not a unit. Then r is called **irreducible** in R if whenever $r = ab$ with $a, b \in R$, at least one of a or b must be a unit in R. Otherwise, r is said to be **reducible**.
- The nonzero element $p \in R$ is called **prime** in R if the ideal (p) generated by p is a prime ideal. In other words, a nonzero element p is called prime if it is not a unit and whever $p \mid ab$, then either $p \mid a$ or $p \mid b$.
- Two elements a and b of R differing by a unit are said to be **associate** in R (i.e. $a = ub$ for some unit u in R).

We can note here that the reason we define these things in this manner is that we take the ring $\mathbf{Z}$ our motiviation. For example, the conidition of *primeness* comes from Euclid's lemma in $\mathbf{Z}$. And the notion of irreduciblity is what is associated to a prime in $\mathbf{Z}$. The prime $p = 11$ can only be written in the form $11 = 11 \cdot 1$, and so we need a unit, i.e. $1 \in R$ in order to write 11 as a product of more than one integer.

Proposition 6.3. In an integeral domain a prime element is always irreducible.

Proof. Suppose R is an integral domain and let $p \in R$ be prime. If we let p be reducibe, then we can write $p = ab$ where $a, b \in R - R^\times$. This means that $ab \in (p)$ and so either $a \in (p)$ or $b \in (p)$. If we let $a \in (p)$, then $a = pt$ for some $t \in R$, and so $p = ab = (pt)b$, which means that $1 = bt$ and this is a contradiction as we assume $b \notin R^\times$. Similarily, if we let $b \in (p)$, then $b = ps$ for some $s \in R$. Thus, $p = ab = a(ps)$ which implies that $a \in R^\times$; a contradiction. Therefore we must have that p is irreducible. □

Proposition 6.4. In a PID a nonzero element is prime if and only if it is irreducible.

Proof. Let A be a PID. As A is a PID then it is also integral domain, by definition, therefore we're done for the forward direction. Now, let p be irreducibe. If M is an ideal containing (p) then $M = (m)$ is prinicipal, i.e. $(p) \subseteq (m)$. So $p = mx$ for some $x \in A$, but as p is irreducible we must have that either m is a unit or x is a unit. If $m \in A^\times$, then $m\nu = 1$ for some $\nu \in R^\times$, but this then implies that $1 \in (m)$, and so $(m) = A$. Moreover, if $x \in R^\times$ then $xl = 1$ for some $l \in R^\times$, so $p = p \cdot 1 = p(xl)$ so $p = (mx) = plx$, and so $m = pl$; thus $m \in (p)$ so $(m) \subseteq (p)$, which means $(m) = (p)$. Thus (p) is maximal, and so as A is a PID, we have that (p) is a prime ideal. □

Definition 6.4. A **Unique Factorization Domain** (UFD) is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following properties:

(i) r can be written as a finite product of irreducibles p_i of R (not necessarily distinct): $r = p_1 p_2 \cdots p_n$, and
(ii) the decomposition in (i) is *unique up to associates*: namely, if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of the factors so that p_i is associate to q_i, that is, $p_i = q_i \ell$ where $\ell \in R^\times$, for $i = 1, 2, \ldots n$.

Proposition 6.5. In a UFD, a nonezero element is prime if and only if it is irreducible.

Proof. By the Proposition 5.3., we have the forward direction already done. Let A be a UFD and let ℓ be irreducible in A and assume that $\ell \mid ab$ for some $a, b \in A$. Then we may write $ab = \ell k$ for some $k \in A$. Writing a and b as a product of irreducibles, then we have two characterization of ab and so we must have that the irreducible ℓ must be associate to one of the irreducibles in either a or b. WLOG, let ℓ be associate to one of the irreducibles in the factorization of a, and so we may write $a = (u\ell)p_1 p_2 \cdots p_n$ for $u \in A^\times$ and some (possibly empty set of) irreducibles $p_1, \ldots, p_n$. Thus $a = \ell(up_1 p_2 \cdots p_n)$ and so $\ell \mid a$. □

6.3. **Polynomial Rings.** Recall that the polynomial ring $R[x]$ in the indeterminate x with coefficients from R is the set of all formal sums $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ with $n \geq 0$ and each $a_i \in R$. Addition of polynomials is done "componentwise":

$$\sum_{i=0}^{n} a_i x^i + \sum_{i=0}^{n} b_i x^i = \sum_{i=0}^{n} (a_i + b_i) x^i.$$

Multiplication may at first seem odd without actually computing what multiplication might look like for some two polynomials: take $f, g \in R[x]$ with $f = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0$ and $g = b_m x^m + a_{m-1}x^{m-1} + \cdots + b_1 x + b_0$. Then

$$fg = (a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} + a_n x^n)(b_0 + b_1 x + \cdots + b_{m-1}x^{m-1} + b_m x^m) \tag{1}$$

$$= (a_0 b_0 + a_0 b_1 x + \cdots a_0 b_{m-1} x^{m-1} + a_0 b_m x^m) + a_1 b_0 x + a_1 b_1 x^2 + \cdots + a_1 b_{m-1} x^m + a_1 b_m x^{m+1} + \cdots \tag{2}$$

$$= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_2 b_0 + a_1 b_1)x^2 + \cdots \tag{3}$$

This continues going on, however, this multiplication can be described by

$$fg = \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{i=0}^{m} b_i x^i\right) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i b_{k-i}\right) x^k.$$

Proposition 6.6. Let R be an integral domain. Then

(i) $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x))$ if $p(x), q(x) \in R[x]$ and both polynomials are nonzero,
(ii) $(R[x])^\times = R^\times$, and
(iii) $R[x]$ is an integral domain.

Proof. (i) This is obvious.

(ii) If $p(x), q(x) \in R[x]$ such that $p(x)q(x) = 1$, then we need for the degrees of the polynomials to match up, i.e. $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)) = \deg(1) = 0$. Thus we must have that $p(x)$ and $q(x)$ are both constant polynomials. Lastly, let $p(x) = a$ and $q(x) = b$, and so $ab = 1$; thus $p(x) = a \in R^\times$ and same goes for $b = q(x)$. For the other direction, if we have $st = 1$ for $s, t \in R^\times$, then this is trivially in the units of $R[x]$ as s, t are "polynomials" of degree 0.

(iii) Suppose we have $f(x), g(x) \neq 0 \in R[x]$ such that $f(x)g(x) = 0$. Then we write out $f = a_n x^n + \cdots + a_1 x + a_0$ and $g = b_m x^m + \cdots + b_1 x + b_0$, and if we have that $fg = 0$, then each polynmoial coefficient must be 0, and in particular, for the term $a_n b_m x^{n+m}$ in the product, we have that $a_n b_m = 0$, so as R is an integral domain, we either have that $a_n = 0$ or $b_m = 0$. WLOG, if we have $a_n = 0$, then we have that the original degree of f is not n, which is a contradiction. Therefore one of our original polynomials must be zero and thus $R[x]$ is an integral domain. □

If we consider localization, i.e. the quotient field of $R[x]$, then the quotient field, say, K of $R[x]$ consists of all quotients $p(x)/k(x)$ where $k(x)$ is not the zero polynomial. The quotient field K is called the field of rational functions in x with coefficients in R.

Proposition 6.7. Let I be an ideal of the ring R and let $(I) = I[x]$ denote the ideal of $R[x]$ generated by I (the set of polynomials with coefficients in I). Then

$$R[x]/(I) \simeq (R/I)[x].$$

In particular, if I is a prime ideal of R then (I) is a prime ideal of $R[x]$.

Proof. Define the map $\varphi\colon R[x] \to (R/I)[x]$ by taking a polynomial $\varphi(f) = \varphi(a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_0) = (a_n + I)x^n + (a_{n-1} + I)x^{n-1} + \cdots + (a_1 + I)x + (a_0 + I)$. This map can be easily realized to be a homomorphism (think of terms simply as $\overline{a_i x^n}$) and surjective. Now if we consider the kernel of the map, then we have

$$\ker(\varphi) = \{q \in R[x] \colon \varphi(q) = I\}.$$

A polynomial in $R[x]$ that's in the kernel of φ can clearly be seen to need coefficients in I, and so $\ker(\varphi) = I[x]$. As the map is surjective as a homomorphism, then $R[x]/I[x] \simeq (R/I)[x]$. □

Example 6.1. If we let $R = \mathbf{Z}$ and take the ideal $n\mathbf{Z} = (n)$ of $\mathbf{Z}$. Then the above proposition gets us that $\mathbf{Z}[x]/n\mathbf{Z}[x] \simeq (\mathbf{Z}/n\mathbf{Z})[x]$. Moreover as $\mathbf{Z}/p\mathbf{Z} \simeq \mathbf{F}_p$ is a field then $\mathbf{Z}/p\mathbf{Z}[x]$ is an integral domain (as well as a Euclidean domain). The last remark could've been also realized another way: $p\mathbf{Z} = (p)$ is a prime ideal of $\mathbf{Z}$ and so $\mathbf{Z}/p\mathbf{Z}$ is an integral domain and by Proposition 5.6. (iii), we have that $(\mathbf{Z}/p\mathbf{Z})[x]$ is an integral domain.

6.3.1. *Polynomial Rings Over Fields.*

Theorem 6.1. Let F be a field. The polynomial ring $F[x]$ is a Euclidean domain. Specifically, if $a(x)$ and $b(x)$ are two polynomials in $F[x]$ with $b(x)$ nonzero, then there are *unique* $q(x)$ and $r(x)$ in $F[x]$ such that

$$a(x) = q(x)b(x) + r(x) \text{ with } r(x) = 0 \text{ or } \deg(r(x)) < \deg(b(x))$$

Corollary 6.1. If F is field, then $F[x]$ is a PID and UFD.

Remark 6.2. Recall that F is a field if and only if $F[x]$ is a PID. Furthermore, if R is any commutative ring such that $R[x]$ is a Euclidean domain, then R is a field.

6.3.2. *Polynomial Rings that are UFD.* Recall that if we have an integral domain R then we can embed it into its field of fraction, say, F, so that $R[x] \subseteq F[x]$ is a subring and $F[x]$ is a Euclidean domain (and hence a PID and UFD). A motivation towards using $F[x]$ rather than $R[x]$ is that, well, we have more ready machinery in $F[x]$, and as $R[x] \subseteq F[x]$ then we can approach some questions about $R[x]$ in $F[x]$. For example, if we have $p(x) \in R[x]$. Then $p(x) \in F[x]$ and as $F[x]$ is a UFD we can factor $p(x)$ uniquely into a product of irreducibles in $F[x]$. In general $R[x]$ is not a UFD, and so if R is an integral domain that isn't a UFD, then $R[x]$ cannot be a UFD as well.

Proposition 6.8 (Gauss' Lemma)**.** Let R be a UFD with field of fractions F and let $p(x) \in R[x]$. If $p(x)$ is reducible in $F[x]$ then $p(x)$ is reducible in $R[x]$. More precisely, if $p(x) = A(x)B(x)$ for some nonconstant polynomials $A(x), B(x) \in F[x]$, then there are nonzero elements $r, s \in F$ such that $rA(x) = a(x)$ and $sB(x) = b(x)$ both lie in $R[x]$ and $p(x) = a(x)b(x)$ is a factorization in $R[x]$.

Corollary 6.2. Let R be a UFD, let F be its field of fractions and let $p(x) \in R[x]$. Suppose the greatest common divisor of the coefficients of $p(x)$ is 1. Then $p(x)$ is irreducible in $R[x]$ if and only if it is irreducible in $F[x]$. In particular, if $p(x)$ is a monic polynomial that is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$.

Proof. By Gauss' Lemma, we have that if $p(x)$ is irreducible in $R[x]$, then $p(x)$ is irreducible in $F[x]$ (contrapositive). Now for the other direction, irreducible in $F[x] \implies$ irreducible in $R[x]$, we do this again by contrapostive: suppose $p(x)$ is reducible in $R[x]$, and so let $p(x) = a(x)b(x)$, where $a(x), b(x) \in R[x] - R^\times$, as the gcd of all the coefficents is one. This factorization of $p(x)$ is once again reducible in $F[x]$ (note here that no information of reducibility is lost when transfering this over to the quotient field as we can write $p(x) = \frac{a(x)b(x)}{1}$ and $1 \in R[x]$, so $p(x)$ remains reducible). □

Theorem 6.2. R is a UFD if and only if $R[x]$ is a UFD.

Corollary 6.3. If R is a UFD, then a polynomial ring in an arbitrary number variables with coefficients in R is also a UFD.

6.4. **Irreducibility of Polynomials.**

Proposition 6.9. Let F be a field and let $p(x) \in F[x]$. Then $p(x)$ has a factor of degree one if and only if $p(x)$ has a root in F.

Proof. Suppose that $p(x)$ has a factor of degree one, i.e. $p(x)$ has a linear factor. Now as were working with a field F, we may assume the factor is monic, and so the linear factor is of the form $(x - \alpha)$ with $\alpha \in F$. But clearly if $\alpha = x$, then we get that $p(\alpha) = 0$, i.e. α is a root in F. Now suppose we have that $p(\ell) = 0$ for some $\ell \in F$. Then we may write $p(x) = q(x)(x-\ell) + r$ and r is constant as we needed $\deg(x-\ell) = 1 >$ "$\deg(r)$". So then $p(\ell) = q(\ell)(\ell-\ell) + r = 0 + r = r$, and so then $r = 0$ and $(x - \ell)$ is a linear factor of $p(x)$. □

Proposition 6.10. A polynomial of degree two or three over a field F is irreducible if and only if it has no roots in F.

Proof. Let $f \in F[x]$ with f having degree two or three. If f has a root α in F, then f is divisible by $(x - \alpha)$, and so f is reducible. Now, for the other direction, if f is reducible in $F[x]$, then it has a factor of degree 1, which is of the form $ax + b$. Then $-b/a$ is a root of f. □

Proposition 6.11 (Rational Root Theorem)**.** Let $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial of degree n with integer coefficients. If $r/s \in \mathbf{Q}$ is in lowest terms (i.e. r and s are relatively prime integers) and r/s is a root of $p(x)$, then r divides the constant term and s divides the leading coefficient of $p(x)$: $r \mid a_0$ and $s \mid a_n$. In particular, if $p(x)$ is a monic polynomial with integer coefficents and $p(d) \neq 0$ for all integers d diving the constant term of $p(x)$, then $p(x)$ has no roots in $\mathbf{Q}$.

Proof. Suppose that $r/s \in \mathbf{Q}$ and $\gcd(r, s) = 1$ with $p(r/s) = 0$. Then $p(r/s) = 0 = a_n(r/s)^n + a_{n-1}(r/s)^{n-1} + \cdots + a_1(r/s) + a_0$, and so $0 = a_n r^n + a_{n-1}r^{n-1}s + \cdots + a_0 s^n$, which can be rewritten as $a_n r^n = s(-a_{n-1}r^{n-1} - \cdots - a_0 s^{n-1})$. Hence $s \mid a_n r^n$. So, as $\gcd(r, s) = 1$, we must have that $s \mid a_n$. Solving the equation for $a_0 s^n$ would've given us that $r \mid a_0$. □

Corollary 6.4. If $f(x) = p_n x^n + p_{n-1}p^{n-1} + \cdots + p_1 x + p_0$ is a monic polynomial, then the rational roots of $f(x)$ must be integers

Proof. By the rational root theorem, if $r = a/b$ is a root of $f(x)$, then $b \mid p_n = 1$ so $b = 1$, and so then $a/b = a/1 = a \in \mathbf{Z}$. □

Example 6.2. For any prime p the polynomials $x^2 - p$ and $x^3 - p$ are irreducible in $\mathbf{Q}[x]$, as they are degree less than or equal to three and it's obvious that they have no rational roots. The fact that $x^2 - p$ is irreducible in $\mathbf{Q}[x]$ provides with the fact that $\sqrt{2}$ is irrational for the case of $p = 2$. However, using the previous proposition, and supposing we had a hypothetical root in $r/s \in \mathbf{Q}$, then we would need for $r \mid p$ and $s \mid 1$, and so this would mean that we need have the choice between the roots ± 1 or $\pm p$, but in either case case, when substituted into either equation, we don't produce a zero. (Looking back at this it would've been easier to simply observe that as the quadratic and cubic are monic and have integer coefficients, then we would only need to look at the divisors of $-p$, which are ± 1 and $\pm p$, and neither provide zeros for either polynomial. Thus they are irreducible.)

Proposition 6.12. Let I be a proper ideal in the integral domain R and let $p(x)$ be a nonconstant monic polynomial in $R[x]$. If the image of $p(x)$ in $(R/I)[x]$ cannot be factored in $(R/I)[x]$ into two polynomials of smaller degree, then $p(x)$ is irreducible in $R[x]$.

Proof. Suppose $p(x)$ cannot be factored in $(R/I)[x]$ but that $p(x)$ is reducible in $R[x]$, in aim of contradiction. Then there are monic polynomials $a(x)$ and $b(x)$ in $R[x]$ such that $p(x) = a(x)b(x)$. By the isomorphism between $R[x]/I[x] \simeq (R/I)[x]$. reducing the coefficients modulo I, gives a factorization in $(R/I)[x]$ with nonconstant factors, which is a contradiction. Thus $p(x0$ is irreducible. □

Proposition 6.13 (Eisenstein's Criterion)**.** Let P be a prime ideal of the integral domain R and let $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial in $R[x]$ (here $n \geq 1$). Suppose $a_{n-1}, \ldots, a_1 a_0$ are all elements of P and suppose a_0 is not an element of P^2. Then $f(x)$ is irreducible in $R[x]$

7. Assortment of Exercises since last Midterm

7.1. 8.1: Euclidean Domains.

Exercise 7.1 (3.)**.** Let R be a Euclidean domain. Let m be the minimum integer in the set of norms of nonzero elements of R. Prove that every nonzero element of R of norm m is a unit. Deduce that a nonzero element of norm zero (if such an element exists) is a unit.

Proof. If we let S denote the set of all all norms of nonzero elements of R, then the elements in S belong to $\mathbf{Z}_{>0}$, and so using the well-ordering principle, we have a minmimum element, which we will call m; that is, $m < N(a)$ of m. Let $x \neq 0 \in R$, and $N(x) = m$. Then, as R is Euclidean, we can write $1 = ax + r$ where $a, r \in R$ and $N(r) < N(x) = m$, which forces $r = 0$ because of the minimality of m. Thus we have that $ax = 1$ and x is a unit.

Suppose $\ell \neq 0 \in R$ such that $N(\ell) = 0$. Then, in a similar manner, we can write $1 = b\ell + r$ where $b, r \in R$ and $N(r) < N(\ell) = 0$, which means that $r = 0$, and ℓ is hence a unit. □

Exercise 7.2 (10.)**.** Prove that the quotient ring $\mathbf{Z}[i]/I$ is finite for any nonzero ideal of I of $\mathbf{Z}[i]$.

Proof. By Proposition 1 in D&F in 8.1., we have that I is generated by an element in I with minimum norm in I, say, α, and so $I = (\alpha)$. An element in $\mathbf{Z}[i]/I$ is written as $\ell + (\alpha)$ for some $\ell \in \mathbf{Z}[i]$. Now let $x = \alpha q + r$ for some $q, r \in \mathbf{Z}[i]$ and $N(r) < N(\alpha)$. Then this is exactly a representation of $\mathbf{Z}[i]/I$, and so $x = r + (\alpha)$, and as we have $N(r) < N(\alpha)$, and $N(\alpha)$ is just some integer, then there is only going to be finitely many choices of r, as $\mathbf{Z}[i]$ is Euclidean, and then we will have a finite list of different representations of x, i.e. $r_1 + (\alpha), r_2 + (\alpha), \ldots, r_k + (\alpha)$ for $N(r_i) < N(\alpha)$ for $1 \leq i \leq k$. Thus as we have finitely many representations of elements in $\mathbf{Z}[i]/I$, then we have that $\mathbf{Z}[i]/I$ is finite. □

7.2. **8.2 PID.**

Exercise 7.3 (3.)**.** Prove that a quotient of a PID by a prime ideal is again a PID.

Proof. Suppose that A is a PID, and let (p) be a prime ideal of A. Then $A/(p)$ is a field as (p) is maximal, and so we have that the only ideals of $A/(p)$ are (0) and $(1) = R$. Thus $A/(p)$ is a PID. □

Exercise 7.4 (5.)**.** Let R be the quadratic integer ring $\mathbf{Z}[\sqrt{-5}]$. Define the ideals $I_2 = (2, 1 + \sqrt{-5})$, $I_3(3, 2 + \sqrt{-5})$, and $I_1 = (3, 2 - \sqrt{-5})$.

Proof. We will only show one of the ideals is not principal for (a), as the rest follow pretty easily using the same structure as proving for it one of the ideals: Suppose that I_2 is a principal ideal, that is, let $I_2 = (2, 1 + \sqrt{-5}) = (\alpha)$. Then we have that $2 = \alpha x$ and $1 + \sqrt{-5} = \alpha y$ for some $x, y \in \mathbf{Z}[\sqrt{-5}]$. So then $N(2) = 4 = N(\alpha)N(x)$ and $N(1 + \sqrt{-5}) = 1^2 + 5 = 6 = N(\alpha)N(y)$. Thus we have that $N(\alpha) = 1$ or 2, as $N(\alpha) \mid 4$ and $N(\alpha) \mid 6$. When $N(\alpha) = 1$, then α is a unit, so $(\alpha) = R$, and so we can write $1 = 2s + (1 + \sqrt{-5})t$ for some $s, t \in \mathbf{Z}[\sqrt{-5}]$. Moreover, $(1 + \sqrt{-5}) = 2s(1 + \sqrt{-5}) + 6t = 2(s + s(1 + \sqrt{-5}) + 3t)$, and so the LHS and RHS don't align as the RHS has coefficent divisible by 2, but the LHS does not. Thus we cannot have $N(\alpha) = 1$. If $N(\alpha) = 2$, then $a^2 + 5b^2 = 2$, which clearly has no integral solutions. Thus we cannot have $N(\alpha) = 2$, either. So then we have that $(\alpha) \neq I_2$, and so I_2 cannot be principal.

□

7.3. **Polynomial Rings that are UFDS.**

Exercise 7.5 (1.)**.** Let R be an integral domain with quotient field F and let $p(x)$ be a monic polynomial in $R[x]$. Assume that $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ of smaller degree than $p(x)$. Prove that if $a(x) \notin R[x]$ then R is not a UFD. Deduce that $\mathbf{Z}[2\sqrt{2}]$ is not a UFD.

Proof. Let $p(x)$ be a monic polynomial in $R[x]$. Moreover, let $p(x) = a(x)b(x)$ where $a(x)$ and $b(x)$ are monic polynomials in $F[x]$ of smaller degree than $p(x)$. Now suppose that $a(x) \notin R[x]$. In aim of contradiction, assume that $R[x]$ is a UFD. By Gauss, as $p(x)$ is reducible in $F[x]$, then it is reducible in $R[x]$ as well, and specifically: there are some $r, s \in F$ such that $ra(x)$, $sb(x) \in R[x]$ and $p(x) = (rs)a(x)b(x)$. Since $p(x)$, $a(x)$, and $b(x)$ are all monic polynomials then we must have that $rs = 1$ and so $r, s \in R$ and both are units. As r is a unit in R, then $a(x) = rr^{-1}a(x) \in R[x]$ □

Exercise 7.6 (4.)**.** Let $R = \mathbf{Z} + x\mathbf{Q}[x] \subset \mathbf{Q}[x]$ be the set of polynomials in x with rational coefficients whose constant term is an integer.

(a) Prove R is an integral domain domain and its units are ± 1.
(b) Show that the irreducibles in R are $\pm p$ where p is a prime in $\mathbf{Z}$ and polynomials $f(x)$ that are irreducible in $\mathbf{Q}[x]$ and have constant term ± 1. Prove that these irreducibles are prime in R.
(c) Show that x cannot be written as the product of irreducibles in R (in particular, x is not irreducible) and conclude that R is not a UFD.
(d) Show that x is not prime in R and describe the quotient ring $R/(x)$.

Proof. For (a): Note that we aren't given initally that R is a ring. However, it easy to see show that R is closed under subtraction and multiplication and it is also trivially nonempty, and so R is a subring of $\mathbf{Q}[x]$ and so it is an integral domain. Suppose that we have $(n + xf(x))(m + xg(x)) = 1$ for some $n, m \in \mathbf{Z}$ and $f, g \in \mathbf{Q}[x]$. Looking at this through the scope of being a subring of $\mathbf{Q}[x]$ the degree norm is multiplicative and so $N((n + xf(x))(m + xg(x))) = N(n + xf(x)) + N(m + xg(x)) = N(1) = 0$. And so we must have consants on the LHS that are integers, and so the only possible units are those of $\mathbf{Z}$; that is, ± 1.

For (b): We will about showing that $\pm$ satisfies irreducibility: Suppose $f(X)$ is of the form $\pm p$ where p is prime in $\mathbf{Z}$. If we had that $f(X)$ can be written as a product $f(X) = a(X)b(X)$ for some $a(X), b(X) \in R$, then the degree terms would need to add to zero, as $\pm p$ is constant. And so $f(X)$ gives rise to a product of integers. As primes in $\mathbf{Z}$ are irreducible, then we have that either $a(X)$ or $b(X)$ is a unit, and so we can conclude that $f(X)$ is irreducible. Other part is hard...

For (c): We have that $\frac{1}{n}x$ and n for $n \neq 0 \in \mathbf{Z}$ are non unit elements in R that give a product of x, and so x is not irreducible in R. Now suppose that we could write x as a product of irreducibles, that is, $x = p_1(x)p_2(x)\cdots p_n(x)$ for irreducible elements $p_i(x)$ in R, but $N(x) = 1 = N(p_1(x)p_2(x)\cdots p_n(x)) = N(p_1(x)) + N(p_2(x)) + \cdots + N(p_n(x))$ and so we must have at most one polynomial with degree 1 on the RHS and all others must be of degree 0. WLOG, let $\deg(p_1(x)) = 1$. So then we can write $p_1(x) = ax + b$ for $a \in \mathbf{Q}$ and $b \in \pm 1$. For the other $p_i(x)$ terms with

$i > 1$, $p_i(x) = p_i$ as an irreducible in $\mathbf{Z}$ (using part (b)). However this cannot happen as we would need the product $p_2(x)p_3(x)\cdots p_n(x) = p_1p_2p_3\cdots p_n$ to multiply to a polynomial with 0 constant term, and so x is not a product of irreducibles of R. Thus we have that R is not a UFD. □

For (d): Consider once again $\frac{1}{n}x$ and n, which are both in R, but neither of whom are in (x). But $(x/n)\cdot n = x \in (x)$. Thus (x) is not a prime ideal. We know immediately that $R/(x)$ cannot be an integral domain.

Exercise 7.7 (2.)**.** Prove that if $f(x), g(x)$ are polynomials with rational coefficients whose product $f(x)g(x)$ has integer coefficients, then the product of any coefficient of $g(x)$ with any coefficient of $f(x)$ is an integer.

Proof. Suppose that $f(x), g(x) \in \mathbf{Q}[x]$ and $f(x)g(x) \in \mathbf{Z}[x]$. By Gauss' lemma, there exists $r, s \in \mathbf{Q}$ such that $rf(x), sg(x) \in \mathbf{Z}[x]$, so then we have that $(rf(x))(sg(x)) = (rs)f(x)g(x) = f(x)g(x)$, and so we have that $s = r^{-1}$. Thus for for the coefficents of $f(x)$ and $g(x)$, say, we have coefficients a_i of $f(x)$ and coefficients b_j for $g(x)$, then $ra_i, r^{-1}b_j \in \mathbf{Z}$ and so $ra_ir^{-1}b_j = a_ib_j \in \mathbf{Z}$. □

7.4. **9.4: Irreducibility Criteria.**

Exercise 7.8 (1.)**.** .

(a) $x^2 + x + 1$ in $\mathbf{Z}/2\mathbf{Z}[x]$.
(b) $x^3 + x + 1$ in $\mathbf{Z}/3\mathbf{Z}[x]$.
(c) $x^4 + 1$ in $\mathbf{Z}/5\mathbf{Z}[x]$.
(d) $x^4 + 10x^2 + 1$ in $\mathbf{Z}[x]$.

Proof. For (a): it suffices to check all cases: $0^2 + 0 + 1 = 1$ and $1^2 + 1 + 1 = 3 = 1$, and so by Proposition 10. (308) in D&G, this polynomial is irreducible.

For (b): once again, it suffices to check all cases: $0^3 + 0 + 1 = 1, 1^3 + 1 + 1 = 0$, and $3^2 + 3 + 1 = 1$, and so this polynomial is reducible and can be factored as $(x-1)(x^2 + x + 2) = x^3 + x - 2$ and $1 \equiv -2 \pmod 3$ so $x^3 + x - 2 \equiv_3 x^3 + x + 1$. Thus $x^3 + x + 1 = (x-1)(x^2 + x + 2)$.

For (c): Observe that $1 \equiv -4 \pmod 5$, and so $x^4 + 1 = x^4 - 4 = (x^2 + 2)(x^2 - 2)$; thus $x^4 + 1$ is reducible in $\mathbf{Z}/5\mathbf{Z}[x]$.

For (d): Let $p = x^4 + 10x^2 + 1$. We're going to take $p \in \mathbf{Q}[x]$. By the the rational root test and the collorary that follows, if we have a root of p, then it must be an integer. But clearly p doesn't have integral solutions. Thus by Proposition 6.9., we don't have a linear factor. Now suppose that p is reducible, that is, $p = x^4 + 10x^2 + 1 = (x^2 + ax + b)(x^2 + cx + d)$, then expanding this out gives us: $p = x^4 + x^3c + x^2d + ax^3 + ax^2c + adx + x^2b + bcx + bd = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd$. This then implies the following list conditions, by matching coefficients: $(a + c) = 0, b + d + ac = 10, ad + bc = 0, bd = 1$. So, in particular, $a = -c$ and $b, d = \pm 1$, which implies that, using $b + d + ac = 10$, we get either $2 - a^2 = 10$ or $-2 - a^2 = 10$, so then $a^2 = -8$ or $a^2 = -12$, and in either case this doesn't work as $a \in \mathbf{Z}$. Thus p is irreducible. □

8. First Midterm:

Exercise 8.1. Let $\varphi\colon G \to G'$ be a group homomorphism, and let $H' \trianglelefteq G'$. Show that $\varphi^{-1}(H') \trianglelefteq G$.

Proof. The set is nonempty as $\varphi(1) = 1 \in \varphi^{-1}(H')$. Now take $x, y \in \varphi^{-1}(H')$. Then as $\varphi(y) = h$ for some $h \in H'$, then $\varphi(1) = \varphi(y)\varphi(y^{-1}) = h\varphi(y^{-1}) = 1$, and so we have that $\varphi(y^{-1}) = h^{-1} \in H'$. Thus we trivially get that $\varphi(xy^{-1}) = \varphi(x)\varphi(y^{-1}) \in H'$. So we have that $\varphi^{-1}(H') \leq G$. For normality, take $g \in G$ and $\varphi(a \in G) = k \in H'$. As H' is normal for G', then we have $\varphi(gkg^{-1}) = \varphi(g)k\varphi(g^{-1}) \in H'$. Thus $\varphi^{-1}(H') \trianglelefteq G$. □

Exercise 8.2. Let G be a finite group of order p, a prime. Show that $G \simeq \mathbf{Z}/p\mathbf{Z}$.

Proof. As G has order p, then there exists an element, say, $q \in G$ such that $q^p = 1$. Thus we have a cyclic subgroup $\langle q\rangle$ with order p, and so we have that $|\langle q\rangle = p \mid p$. (The only other subgroup of G would be $\{1\}$, the trivial subgroup.) This forces G to be cyclic and so let $\langle x\rangle = G$. Now we define $\varphi\colon G \to \mathbf{Z}/p\mathbf{Z}$ by $\varphi(x^i) = \overline{i}$ for some $x^i \in G$, and $0 \leq i \leq p$. This map is trivially seen to be surjective. Now let $x^i, x^j \in G$. Then $\varphi(x^i \cdot x^j) = \varphi(x^{ij}) = \overline{ij} = \overline{i}\cdot\overline{j} = \varphi(x^i)\varphi(x^j)$, and so we have a homomorphism. Now, $\ker\varphi = \{x^i \in G\colon \varphi(x^j) = \overline{1} = \overline{p}\}$. Thus $\ker\varphi$ has only one element in G that maps to $\overline{1}$ is $x^p = 1$ (by the nature of how the map is defined). So φ is injective and we have an isomorphism $G \simeq \mathbf{Z}/p\mathbf{Z}$. □

Exercise 8.3. Let $H \trianglelefteq G$ and $K \leq G$, where G is a group. Show that $HK = \{hk\colon h \in H, k \in K\}$ is a subgroup of G.

Proof. Note that HK is trivially nonempty as $0 \cdot 0 \in HK$. Let $x = h_1k_1 \in HK$ and $y = h_2k_2 \in HK$. Then , consider $y^{-1} = (h_2k_2)^{-1} = k_2^{-1}h_2^{-1}$. Then $xy^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1}$, and let $k_1k_2^{-1} = k_3$. As $H \trianglelefteq G$ and $K \leq G$, we have that $h_1k_2h_2^{-1} = h_1h_2k_2 \in HK$. Thus HK is a subgroup of G. □

Exercise 8.4. Consider the action of a group G on a set X, and let $x_0 \in X$. Show that there is a bijection between G/G_{x_0} and $G \cdot x_0$.

Proof. Define $\varphi\colon G\cdot x_0 \to G/G_{x_0}$ given by, for all $g\in G$, $\varphi(g\cdot x)=gG_{x_0}$, and $\cdot$ in the LHS is the group action on X. Suppose that $g\cdot x = h\cdot x$ for some $g,h\in G$. Then we have that $h^{-1}g\cdot x = 1\cdot x = x$, which means that $h^{-1}g\in G_{x_0}$, so then $gG_{x_0}=hG_{x_0}$; thus we have that φ is well defined. Let $\varphi(g_1\cdot x)=\varphi(g_2\cdot x)$, then $g_1G_{x_0}=g_2G_{x_0}$, and so we have that $g_2^{-1}g_1\in G_{x_0}$. This means that $g_2^{-1}g_1\cdot x = x$, so then we may write $g_2\cdot x = g_2\cdot(g_2^{-1}g_1\cdot x)=(g_2g_2^{-1}g_1)\cdot x = g_1\cdot x$, and so we conclude that φ is injective. Moreover, we can see, by definition of our map, that φ is clearly surjective. Therefore we have a bijection. □

Exercise 8.5. Let G be a group and let x and y be two elements of G such that $|xy|=n$. Show that $|yx|=n$.

Proof. So, $(xy)(xy)\cdots(xy)=1$ for n many xy terms, which implies that $x(yx)(yx)\cdots(yx)y=1$, where there are $n-1$ many yx terms. So then $(yx)(yx)\cdots(yx)=(yx)^{n-1}=x^{-1}y^{-1}=(yx)^{-1}$, and hence $(yx)^{n-1}(yx)=(yx)^n=1$. Thus $|yx|=n$. □

Exercise 8.6. Let G be a p-group of order p^2. We wish to classify the possible group structures on G up to isomorphism.

(a) Case 1: Suppose G contains an element of order p^2. Conclude.
(b) Case 2: Suppose that G does not contain an element of order p^2:
(b)(i) Show that $Z(G)$ contains a subgroup H of order p
(b)(ii) Show that G contains another subgroup K of order p, $K\neq H$. Then show that $G=HK$.
(b)(iii) Show that $H\times K\simeq G=HK$. Conclude.

Proof. For part (a): If G contains an element of order p^2, then G is cyclic, as G would be generated by that element as order of cyclic group generated by that element would be $p^2=|G|$, and so $G\simeq Z/p^2\mathbf{Z}$.

(b): Suppose that G does not contain an element of order p^2.

(i): The easiest approach would be to show that the center of $Z(G)$ has an element of order p: The center of a p-group is known to be G non trivial so let us pick an element $x\in Z(G)-\{1\}$. Then consider the subgroup cyclic subgroup $\langle x\rangle$ of G. By Lagrange, we must have that $|\langle x\rangle| \mid p^2$, and so we have a couple of choices: $|\langle x\rangle|=1,p$, or p^2. We cannot have the case of $|\langle x\rangle|=1$ as then would make $x=1$. Now if $|\langle x\rangle|=p^2$, then this would generate the whole group and so we would have an element of p^2 in G. Thus we must have that $|\langle x\rangle|=p$, which is exactly what we want. Thus we have an element of the center, and so a subgroup of $Z(G)$, with order p. Lastly, as we picked $x\in Z(G)$, then we have that $\langle x\rangle \trianglelefteq G$ Let $H=\langle x\rangle$

(ii) We want to show that another subgroup of order p exists, excluding H. So, take $g\in G-H\neq\varnothing$. In a similar fashion to (ii), by Lagrange, we have that $|g|=p$, and let $\langle g\rangle=K$, and $K\neq H$. Then, as H is normal in G, then $HK\leq G$. Additionally, $|HK|=|H||K|=p^2=|G|$, and so $HK=G$.

(iii): Define the map $\varphi\colon H\times K\to HK=G$ defined by $a\times b\mapsto ab$. As $x\in Z(G)$, we have that every element of H commutes with every element of K, and so we easily get a homomorphism: take $(a,b),(c,d)\in H\times K$, then $\varphi((a,b),(c,d))=\varphi(ac,bd)=(ac)(bd)=a(bc)d=(ac)(cd)=\varphi(a,b)\varphi(c,d)$. If $\varphi(h,k)=1$ for some $h\in H$ and $k\in K$, then we have that k is the inverse of h and so $k\in H$ and as we havea a trivial intersection, then $k=1$, which forces $h=1$ as well. So φ is injective and thus a bijection as the order of the domain and codomain of φ are the same. Thus $H\times K\simeq HK=G$. □

Exercise 8.7. Let H and K be two normal subgroups of a finite group G. Recall that such conditions are more than sufficient to make $HK\leq G$.

(a) Assume that the orders of H are K are coprime. Show that $H\times K\simeq HK$.
(b) Let G be a group of order 33. Determine the possible group structures on G up to isomorphism.

Proof. Consider the map $\varphi\colon H\times K\to HK$ defined by $\varphi\colon(a,b)\mapsto ab$. Let $(a,b)=(c,d)\in H\times K$. Then $(ac^{-1},bd^{-1})=(1,1)$, which implies that $\varphi(ac^{-1},bd^{-1})=(ac^{-1})(bd^{-1})=1$, so then $ab=cd$, so the map is well defined. Moreover, the map is clearly surjective. Now we consider $\ker\varphi=\{(a,b)\in H\times K\colon \varphi(a,b)=1\}$, so $ab=1$, which means that $b^{-1}ab=b^{-1}\in K$, and as $H\trianglelefteq G$, then $b^{-1}ab=b^{-1}\in H$. As $H\cap K=\{1\}$, then we must have that $b^{-1}=1$, so then $bb^{-1}=b1=b$, and $ab=1\implies ab(b^{-1})=a=1\cdot 1=1$; thus $a=1$ and $b=1$, so the kernel must only have $(1,1)$ in it, and φ is hence injective. Lastly we need to show that φ is a homomorphism: Suppose $(a,b),(c,d)\in H\times K$, then $\varphi((a,b),(c,d))=\varphi(ac,bd)=(ac)(bd)\stackrel{?}{=}a(cb)d=(ab)(cd)=\varphi(a,b)\varphi(c,d)$, which is what we essentially need to show, i.e. that H commutes with any element in K. Now take $h\in H$ and $k\in K$, then do we have that $hk=kh$ if and only if $hkh^{-1}k^{-1}=1$. So then

$$hkh^{-1}k^{-1}=(hkh^{-1})k^{-1}\in HK \tag{4}$$

$$=h(kh^{-1}k^{-1})\in HK, \tag{5}$$

as H and K are normal, and so $hkh^{-1}k^{-1}\in H\cap K$, but the intersection is trivial and so we have that $hkh^{-1}k^{-1}=1$, so $hk=kh$ and φ is a homomorphism. Therefore $H\times K\simeq HK$.

(b): As G has order $33 = 11 \cdot 3$, then we have that $n_{11} \mid 3$ and $n_{11} \equiv 1 \pmod 3$ and so this forces $n_{11} = 1$, and we have that $n_3 \mid 11$ and $n_3 \equiv 1 \pmod 3$ which forces $n_3 = 1$. This means that we have a unqiue, normal 11-Sylow subgroups, say, P, and a unique, normal 3-Sylow subgroup Q. As both are normal, and we have an obvious trivial intersection, we have that $G \simeq P \times Q \simeq \mathbf{Z}/11\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z} \simeq \mathbf{Z}/33\mathbf{Z}$. □

9. Ring Theory Exercises and Notes done long ago

Exercise 9.1. All maximal ideals are prime ideals.

Proof. Suppose $\mathfrak{m}$ is a maximal ideal of a ring R. Then there are no other ideals contained between $\mathfrak{m}$ and R, i.e., if $\mathfrak{n}$ is an ideal of R such that $\mathfrak{m} \subseteq \mathfrak{n} \subseteq R$, then $\mathfrak{n} = \mathfrak{m}$ or $\mathfrak{n} = R$. Take $a, b \in R$, and suppose $ab \in \mathfrak{m}$. Suppose $\mathfrak{m}$ isn't a prime ideal, so $a \notin \mathfrak{m}$ and $b \notin \mathfrak{m}$. Consider the ideal $(a) + \mathfrak{m}$ generated by a and $\mathfrak{m}$. Since the ideal $(a) + \mathfrak{m}$ is strictly larger than $\mathfrak{m}$, we must have $R = (a) + \mathfrak{m}$ by the maximality of $\mathfrak{m}$. Since $1 \in R$, then $1 = ar + m$ for $r \in R$ and $m \in \mathfrak{m}$, and similarly for $(b) + \mathfrak{m}$, $1 = bs + n$ for $s \in R$ and $n \in \mathfrak{m}$. But then

$$1 \cdot 1 = (ar + m)(bs + n) = arbs + arn + bsm + nm = (ab)rs + (ar)n + (bs)m + (nm),$$

and so since $ab, n, m \in \mathfrak{m}$, the sum of this expression must be in $\mathfrak{m}$, i.e., $1 \in \mathfrak{m}$, and hence $\mathfrak{m} = R$. Since a maximal ideal is proper by definition, this is a contradiction. Thus, $\mathfrak{m}$ must be prime. □

Exercise 9.2. Let $\mathfrak{p}$ be a prime ideal of a ring R — that is, $\mathfrak{p}$ is a proper ideal such that if $ab \in \mathfrak{p}$ for $a, b \in R$, then $a \in \mathfrak{p}$ or $b \in P$. Prove that if $abc \in \mathfrak{p}$ for $a, b, c \in R$, then at least one of the three elements must be in $\mathfrak{p}$. More generally, use induction to prove that if $a_1 a_2 a_3 \cdots a_n \in \mathfrak{p}$ for $a_i \in R$, then at least one of the factors a_i must be in $\mathfrak{p}$.

Proof. Suppose $\mathfrak{p}$ is a prime ideal of a ring R.

For the case of three elements: Let $a, b, c \in R$ and $abc \in \mathfrak{p}$. Then $(ab)c \in \mathfrak{p}$ implies that $ab \in \mathfrak{p}$ or $c \in \mathfrak{p}$, and so $a \in \mathfrak{p}$, $b \in \mathfrak{p}$, or $c \in \mathfrak{p}$.

As hinted, we proceed with a view of induction. Suppose $a_1 a_2 a_3 \cdots a_n \in \mathfrak{p}$ for $a_i \in R$. Then the case of $n = 2$ holding is obviously true, and we also just did the case of $n = 3$. Suppose that the statement is true for $n = k - 1$. Then

$$a_1 a_2 a_3 \cdots a_k = (a_1 a_2 a_3 \cdots a_{k-1}) a_k \in \mathfrak{p},$$

so, since $\mathfrak{p}$ is prime, $a_1 a_2 \cdots a_{k-1} \in \mathfrak{p}$ or $a_k \in \mathfrak{p}$. If $a_k \in \mathfrak{p}$, then we're done. Otherwise, if $a_1 a_2 a_3 \cdots a_{k-1} \in \mathfrak{p}$, then, by the induction hypothesis, one of the elements $a_1, a_2, \ldots, a_{k-1}$ is in $\mathfrak{p}$. □

Exercise 9.3. Any finite integral domain must be a field

Proof. Suppose D is a finite integral domain with α elements, i.e., $|D| = \alpha$. Let $a_1, a_2, \ldots, a_\alpha$ be elements of D. Fix an arbitrary element $\ell \in D$ such that $\ell \neq 0$. Then, we claim that $\ell a_1, \ell a_2, \ldots, \ell a_\alpha$ are all distinct. Suppose that they aren't, for aim of contradiction. So, $\ell a_i = \ell a_j$ for $i \neq j$, but then $\ell(a_i - a_j) = 0$, so we have that $a_i = a_j$ — a contradiction. Thus they must all be distinct. Moreover, since D has only α elements, one of which is the identity 1, one of the α products has to be 1. Therefore, we can say that some ℓa_i, must be the element 1, and hence a_i is the inverse of ℓ. □

Exercise 9.4. Let I be an ideal of a ring R that is contained in a prime ideal Q. Use Zorn's lemma to prove that there is a prime ideal $\mathfrak{p}$ of R such that

$$I \subseteq \mathfrak{p} \subseteq Q,$$

and there are *no* prime ideals between I and $\mathfrak{p}$. We will can such a prime $\mathfrak{p}$ a **minimal prime over** I.