1 MATH 210A Notes

A brief review of some asasorted resuls and definitions

1. If m and n are integers, $m > 0$, then there exists unique integers q and r, $0 \leq r < m$, such that $n = qm + r$.

2. If m and n are integers, the greatest common factor of m and n (denoted (m, n)) is the largest positive integer, g, such that $g \mid m$ and $g \mid n$.

   If m and n are positive integers, then there exists integers x and y such that $(m, n) = mx + ny$.

   m and n are relatively prime iff $(m, n) = 1$ iff there exists integers x and y such that $mx + ny = 1$.

3. Assume that $a = 2^{t_1} \cdot 3^{t_2} \cdots p_k^{t_k}$ and $b = 2^{w_1} \cdot 3^{w_2} \cdots p_k^{w_k}$ are the prime factorizations of a and b. Then $a \mid b$ iff for all i, $t_i \leq w_i$. If $u_i = \min\{t_i, w_i\}$ and $v_i = \max\{t_i, w_i\}$, then $(a, b) = 2^{u_1} \cdot 3^{u_2} \cdots p_k^{u_k}$ and $\text{lcm}(a, b) = [a, b] = 2^{v_1} \cdot 3^{v_1} \cdots p_k^{v_k}$.

1.1 Group Theory

Assume that $(G, *)$ is a group, and that $(H, *)$ is a subgroup. Define R on G by aRb iff $ab^{-1} \in H$. Then R is an equivalence relationon G, and if $a \in G$, then $Ha = \{ha : h \in H\} = [a]_R$. Since R is an equivalnce relation, and since equivalence classes are either equal or dijoint, aRb iff bRa iff $ab^{-1} \in H$ iff $ba^{-1} \in H$ iff $a = hb$ for some $h \in H$ iff $b = ga$ for some $g \in H$ iff $a \in Hb$ iff $b \in aH$ iff $Ha = Hb$ iff $Ha \cap Hb \neq \varnothing$.

Recall that an equivalence reltion induces a partition on the set. The set of equivalnce classes of G with respect to R is denoted G/H (the set of right cosets of H in G). If the number of cosets is finite, then the number of cosets of H is G is called the **index of** H in G, denoted $[G : H]$.

If N is a subgroup of G, then N is called **a normal subgroup** of G, denoted $N \triangleleft G$, iff for all $g \in G$ and for all $n \in N$, $gng^{-1} \in N$. If $*$ is an associative relation on S, and R is an equivalence relation on S, then R is called a **congruence relation** on S with respect to $*$ iff for all $a, b, c, d \in S$, aRb and cRd implies $(a * b)R(c * d)$. For example, congruence mod n is a congruence relation on $\mathbb{Z}$ with repect to $+$ and $*$.

If $N \triangleleft G$ and R is an equivalence relation on G defined by aRb iff $ab^{-1} \in N$, then R is a congruence relation on G with respect to $*$. Moreover, the set of equivalence classes of G with respect to R, G/N is a group with respect to $\odot$.

A group $(G, *)$ **acts on** a set S iff there exists $\varphi : G \times S \to S$ such that for all $g, h \in G$ and $s \in S$: $\varphi((g * h, s)) = \varphi(g, \varphi((h, s)))$ and $\varphi((e, s)) = s$.

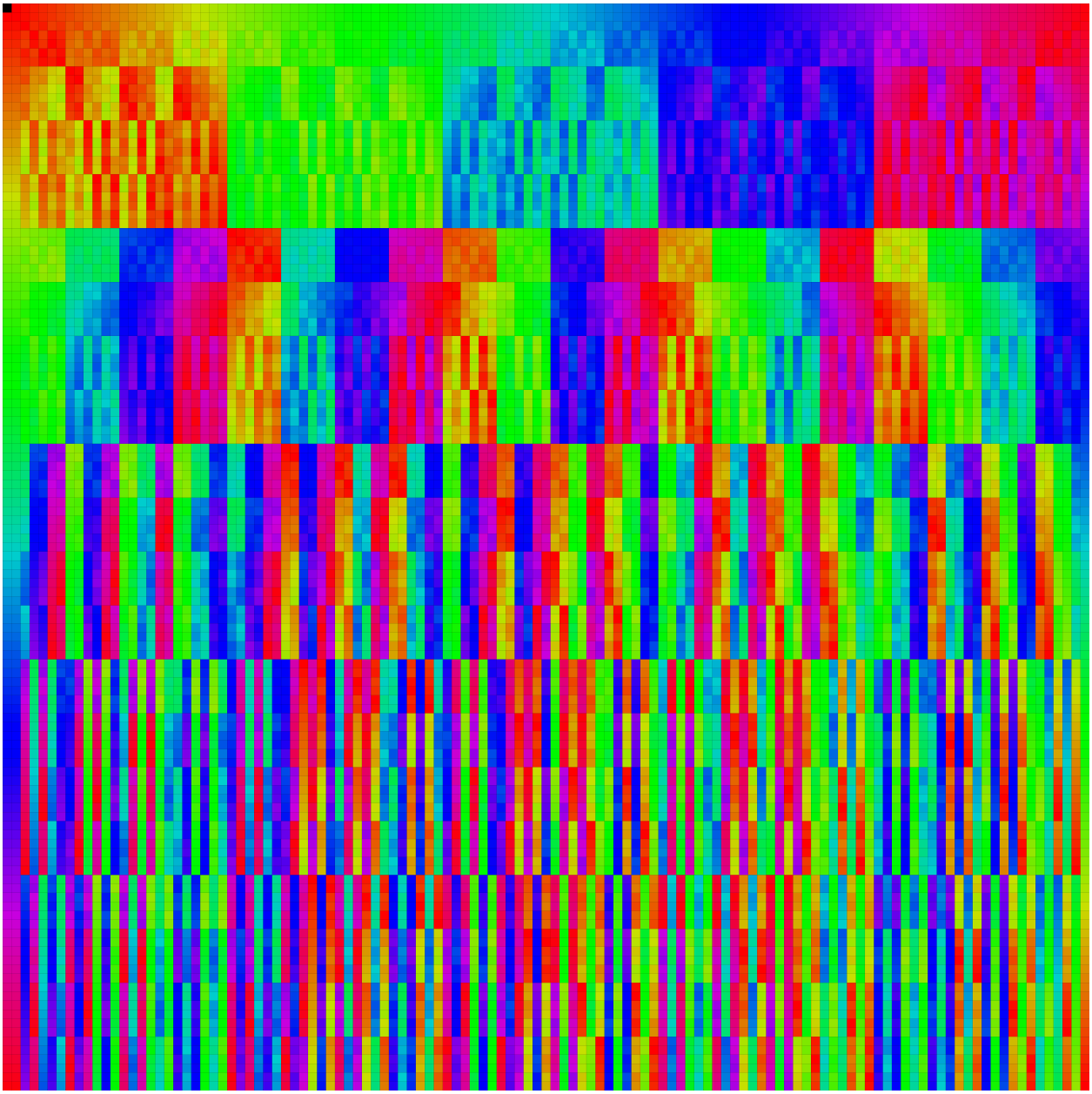

Figure 1: Group Action

Example 1.1. Assume that $(K, *)$ is a group, and $H \subseteq_g K$. Define $\varphi : H \times K \to K$ by $\varphi((h, b)) = h * b$. Then to show that H acts on K, we let $a, b \in H$ and $c \in K$. By definition of φ we have that

$$\begin{aligned}\varphi((a * b, c)) &= (a * b) * c \\ &= a * (b * c) \\ &= a * \varphi((b, c)) \\ &= \varphi((a, \varphi((b, c)))).\end{aligned}$$

Satisfying the first condition. Finally, note that $\varphi((e, c)) = e * c = c$. Therefore, K acts on S. Here φ is called the action of **left translation**.

Example 1.2. Assume that $(G, *)$ is a group, and $S = G$. Define $\varphi : G \times S \to S$ by $\varphi((g, s)) = g * s * g^{-1}$. Then we want to show that G acts on S. Let $a, b \in G$ and $c \in S$. Then by definition of φ, it follows that

$$\begin{aligned}\varphi(a * b, c) &= (a * b) * c * (a * b)^{-1} \\ &= (a * b) * c * (b^{-1} * a^{-1}) \\ &= a * (b * c * b^{-1}) * a^{-1} \\ &= a * \varphi(b, c) * a^{-1} \\ &= \varphi(a, \varphi(b, c)),\end{aligned}$$

as desired. Finally, we have that $\varphi(e, c) = e * c * e^{-1} = c$. Therefore, G acts on S. Also, φ is called the **action of conjugacy**.

Assume that $s \in S$. Let $G_S = \{g \in G : \varphi(g, s) = s\}$, then $G_S \subseteq_g G$ and G_S is called the **stabilizer** of s in G, or the **isotropy group** of s.

Assume that $s \in S$. Let $G(s) = \{\varphi(g, s) : g \in G\}$. Then $G(s)$ is called the **orbit** of s in S, and $\{G(s) : s \in S\}$ is a partition of S.

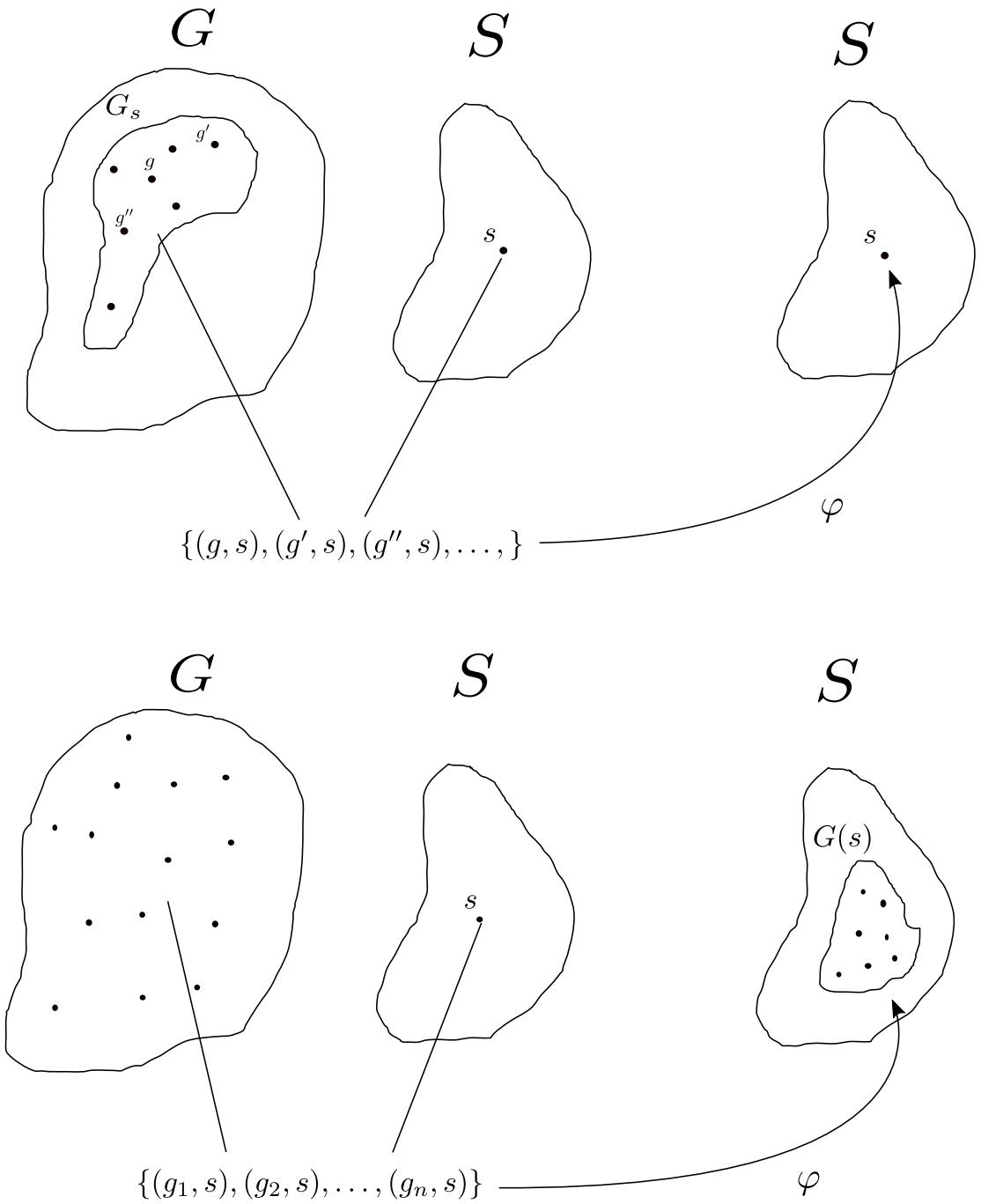

Figure 2: Stabilizer and Orbit

Example 1.3. For left translation, let $a \in K$, then

$$H_a = \{g \in H : \varphi(g, a) = a\} = \{g \in H : g * a = a\} = \{e\}$$

is the isotropy group of K. And

$$H(a) = \{\varphi(g, a) : g \in H\} = \{g * a : g \in H\} = Ha$$

is the orbit of a in K. Hence, the set of orbits under the action of left translation is the set of left cosets.

Example 1.4. For conjugacy, let $s \in S$. Then the isotropy group of s is

$$G_s = \{g \in G : \varphi(g, s) = s\} = \{g \in G : g * s * g^{-1} = s\} = \{g \in G : g * s = s * g\}.$$

This set is also known as the **centralizer** or the **normalizer** of s, and is denoted as $N(s)$. Finally, the orbit of s in S is

$$G(s) = \{\varphi(g, s) : g \in G\} = \{g * s * g^{-1} : g \in G\}.$$

This set is referred to as the set is referred to as the conjugates of S, or the **conjugacy class** of S, denoted $c(S)$.

Define a relation R on S by aRb iff there exists $s \in S$ such that $a \in G(s)$ and $b \in G(s)$. Then R is an equivalence relation on S, and $\{G(s) : s \in S\}$ is the set of equivalence classes of R on S.

Example 1.5. For left-translation, the above relation yields the set $\{H(s) : s \in K\} = \{Hs : s \in K\}$. This set is the collection of left cosets of H in K.

Example 1.6. For conjugacy, we have that aRb iff $\exists t \in S$ such that $a, b \in G(t)$ iff $\exists g, h \in G$ such that $\varphi(g, t) = a$ and $\varphi(h, t) = b$ iff $a = gtg^{-1}$ and $b = hth^{-1}$ iff $t = g^{-1}ag = h^{-1}bh$ iff $(hg^{-1})a(hg^{-1})^{-1} = b$ iff $b = \varphi((hg^{-1}), a)$. In this case, we would call a and b conjugates.

1.2 The Relationships Between G_s and $G(s)$

Assume that $t \in G(s)$, say that $t = \varphi(g, s)$, then $G_t = gG_sg^{-1}$.

Proof. Let $t \in G(s)$ with $t = \varphi(g, s)$ for some $g \in G$. We want to show that $gG_sg^{-1} \subseteq G_t$ and $G_t \subseteq gG_sg^{-1}$. To show the former, we let $x \in gG_sg^{-1}$. Then $x = ghg^{-1}$, where $\varphi(h, s) = s$. □

Additionally, we have that

$$|G(s)| = \frac{|G|}{|G_s|}.$$

Proof. Define $\theta : G/G_s \to G(s)$ by $\theta(G_s a) = \varphi(a^{-1}, s)$. Then we first want to show that θ is a function. Before we do this, however, let us review the objects at play here and what is is we are trying to prove, as well as how exactly we are going to prove it. So what it is that we are showing is that for a given $s \in S$, the number of elements in the orbit of S is the same as the number of elements of G divided by the number of elements in the stabilizer.

Intuitively, the stabilizer of $s \in S$ is the subgroup of G whose elements are those that 'fix' the element s under the action φ. Whereas the orbit of $s \in S$ is the subset of S whose elements are those which are mapped to under the action φ given input $g \in G$ and fixed s. So what this result is saying, is that the cardinality of the stabilizer divides the cardinality of G and the result of this division is a number denoting the size of the orbt.

□