MATH 551 HOMEWORK 7

SOLUTIONS

(1) **Hungerford III.1.1**

(a) We only need to check that the multiplication is associative and distributative. Since $(ab)c = 0c = 0 = a0 = a(bc)$, the multiplication is associative. Since $a(b + c) = 0 = 0 + 0 = ab + ac$, and $(b + c)a = 0 = ba + ca$, the multiplication is distributative, so G is a ring.

(b) We first check that $(S, +)$ is an abelian group. The additive identity is $\emptyset$, and $A + A = (A - A) \cup (A - A) = \emptyset$, so each set A is its own additive inverse. The addition is abelian by construction. Finally, $A + (B + C) = A + ((B - C) \cup (C - B)) = (A - ((B - C) \cup (C - B))) \cup (((B - C) \cup (C - B)) - A) = ((A \cup B \cup C) - (A \cap B \cup A \cap C \cup B \cap C)) \cup A \cap B \cap C$. Since this is symmetric in A, B and C, it also equals $C + (A + B) = (A + B) + C$, so the addition is associative. Since $A(BC) = (AB)C = A \cap B \cap C$, the multiplication is also associative. Finally, $(A + B)C = C \cap ((A - B) \cup (B - A)) = C \cap (A - B) \cup C \cap (B - A) = (C \cap A - C \cap B) \cap (C \cap B - C \cap A) = C \cap A + C \cap B = CA+CB = AC+BC$, and similarly $A(B+C) = AB+AC$, so the multiplication is distributative. The multiplication is associative with multiplicative identity U.

(2) **Hungerford III.1.16** We need to show that $f(1_R)s = sf(1_R) = s$ for all $s \in S$. Pick $s \in S$. Then $sf(r) = sf(1_Rr) = sf(1_R)f(r)$, so $(s - sf(1_R))f(r) = 0$. Since S has no zero-divisors, and $f(r) \neq 0$, we have $s - sf(1_R) = 0$, so $s = sf(1_R)$. Similarlys $f(r)s = f(r1_R)s = f(r)f(1_R)s$, so $f(r)(s-f(1_R)s) = 0$, and thus $s = f(1_R)s$, and so $f(1_R)$ is a multiplicative identity for S.

(3) **Hungerford III.2.2** If $r, s \in \mathrm{Rad}(I)$, then $r^n, s^m \in I$ for some $n, m \in \mathbb{N}_{>0}$. Without loss of generality $n < m$. Then $(r - s)^{2m} = \sum_{i=0}^{2m} \binom{2m}{i} r^i(-s)^{2m-i}$, by the binomial theorem (this is proved in the book, and is a trivial generalization of the usual binomial theorem). For each $0 \leq i \leq 2m$, either $i \geq n$ or $2m - i \geq m$, so each term, and thus their sum, lies in I. Thus

$r - s \in \mathrm{Rad}(I)$. If $x \in \mathrm{Rad}(I)$,with $x^n \in I$, and $r \in R$, then since R is commutative, $(rx)^n = r^n x^n \in I$, so $\mathrm{Rad}(I)$ is an ideal.

Note: If $I = \mathrm{Rad}(I)$ then I is called a radical ideal. Radical ideals are important objects in elementary algebraic geometry, thanks to Hilbert's Nullstellensatz.

(4) **Hungerford III.2.9**

(a) Let E_{rs} be the matrix with a one in position r, s, and zeroes elsewhere. Let I be a proper ideal of S, and let J be the set of elements of D which appear as the $(1,1)th$ entry of a matrix in I. Since I is an ideal, $A, B \in I$, then $A - B \in I$, and if $A \in I$ then $rA, Ar \in I$, where r is the diagonal matrix with all diagonal entries equal to a constant $d \in D$. This implies that J is an ideal of D. Since D is a division ring, this means that $J = 0$ or $J = D$. Note that $E_{pr}AE_{sq} = a_{rs}E_{pq}$, for all $1 \leq r, s, p, q \leq n$. Taking $p = q = 1$, we conclude that if $J = 0$, we must have $a_{rs} = 0$ for all $1 \leq r, s \leq n$ and all $A \in I$, so $I = 0$. Otherwise $J = D$, so there is some $A \in I$ with $a_{11} = 1_D$. But then $E_{p1}AE_{1q} = E_{pq} \in I$, and since any matrix in S is a linear combination with coefficients in D of matrices of the form E_{pq}, we conclude that in this case $I = S$. So S has no proper nontrivial ideals.

(b) We assume for this that $n \geq 2$. Then $E_{12}E_{21} = 0$, so S has zero divisors. Since 0 is a maximal ideal by the first part, and division rings have no zero divisors, this means that $S/0$ is not a division ring, despite being the quotient of S by a maximal ideal. Since 0 is the only proper ideal of S, and S has an identity, if A, B are ideals of S with $AB \subseteq 0$, then at least one of A and B is 0, so 0 is prime. However $E_{12}E_{21} \in \langle 0 \rangle 0$, but neither is the zero matrix.

(5) **Fall 2003**. *Let r and n be positive integers, let G be a group generated by r elements, and let S be the set of subgroups of G with index at most n.*

(a) *Show that S is finite.* Let the r generators of G be $g_1, \ldots, g_r$. Let H be a subgroup of G with index at most n. Construct the directed graph $\mathcal{G}$ whose vertices are the cosets of H, and there is an edge from aH to bH if $bH = g_i aH$. Note that the underlying undirected graph of $\mathcal{G}$ is connected, since there is a path from H to aH given by the way of writing a as a word in the g_i. In addition, every such path gives a word that is an element of aH. The graph $\mathcal{G}$ determines H, since a word $a \in G$ lies in H if and only if the corresponding path in $\mathcal{G}$ starting at H ends at H. Thus it suffices to show that the set of possible graphs $\mathcal{G}$ is finite. This is immediate, as each $\mathcal{G}$ is a connected directed graph with a distinguished vertex (H), at most n vertices, and with the out-degree of each vertex equal to r, and there are only finitely many such graphs.

(b) *Suppose that $r = 2$ and $n = 10$. Give an upper bound for the cardinality of S.* By the first part, we need only to bound the number of connected directed graphs with a distinguished vertex (H) and at most 10 vertices, where every vertex has out-degree 2. This is bounded by the number of directed graphs on 10 vertices where every vertex has out-degree 2 (since a connected graph on fewer than 10 vertices can be extended to a graph on 10 vertices with the original graph as a connected component by adding extra vertices each of which has r loops to itself). There are 10^{20} such labelled graphs (since at each of the 10 vertices, there are 10 choices for the other endpoint of each of the two edges leaving that edge. There are more such labelled graph than graphs with a distinguished vertex, so 10^{20} is an upper bound for the number of subgroups of G of index at most 10.

(6) **Spring 2005**. *Suppose that the symmetric group S_4 acts transitively on a finite set X having 8 elements. How many different subgroups of S_4 can occur as stabilizers of points of X?*

Let $x \in X$, and $G = S_4$. Since the group action is transitive, $|Gx| = 8$, so since $|Gx| = [G : G_x]$, we have $|G_x| = 3$, so the stabilizer of any point of x is a subgroup of S_4 of order 3. Such groups are generated by an element of order three, which is a 3-cycle. All such 3-cycles π can be the stabilizer in some action on a set of size 8, by letting S_4 act by left translation on the left cosets of $\langle \pi \rangle$, and all stabilizers arise in this fashiion. For example, let $H = \langle (123) \rangle$, and let S_4 act by left translation on the left cosets of H. These cosets are $H, (12)H, (14)H, (14)(23)H, (13)(24)H, (24)H, (12)(34)H, (34)H$, whose stabilizers are $H, H, \langle (234) \rangle, \langle (234) \rangle, \langle (134) \rangle, \langle (134) \rangle, \langle (124) \rangle, \langle (124) \rangle$, respectively. All other cases are conjugate to this, so we see that all four groups of order 3 in S_4 occur as stabilizers of points of X.