Mathematics 301 Algebraic Semigroups Solutions

Professor Peter M. Higgins

November 17, 2019

Solutions and Comments for the Problems

Problem Set 1

1(a) Let $e \in E(S)$ and $a \in S$. Then $ea = e^2a$, whence by left cancellation we obtain $a = ea$, thus showing that e acts as an identity on the left in S.

(b) Let $e, f \in E(S)$. By part (a) and its left-right dual we have $f = ef$ as e is a left identity and $ef = e$ as f is a right identity, so that $f = ef = e$. Hence S has just one idempotent e, which is its identity element, so that S is a (cancellative) monoid.

2. Suppose first that S is a group. Let $a, b \in S$ and consider the equation $b = ax$, which has (unique) solution in $x = a^{-1}b$. Hence $b \in aS$ and since b was arbitrary it follows that $S \subseteq aS$. Since the reverse inclusion is clear we conclude that $aS = S$ for all $a \in S$, which is to say that S is right simple. Reversing order in the previous argument (so that $b = xa$ is solved by $x = ba^{-1}$) we conclude similarly that $Sa = S$ and so S is also left simple. Therefore if S is a group then S is both left and right simple.

Conversely suppose that S is both left and right simple. Take $a \in S$. Then by right simplicity $aS = S$ and there exists $e \in S$ such that $ae = a$. Now take any $b \in S$. By left simplicity $b \in Sa$ so there exists $c \in S$ such that $b = ca$, whence $bx = cax = ca = b$. Therefore e is a right identity element for S. By symmetry S has a left identity f say, whence $e = fe = f$ is the unique identity of S, which is then a monoid. Finally, for any $d \in S$ the equation $dx = e$ is solvable in S. Then $x = xe = xdx$ so that $xd = xdxd = g \in E(S)$. But then there exists $z \in S$ such that $gz = e$ whence $e = gz = g^2z = g(gz) = ge = g$, and so $xd = dx = e$, which is to say that $x = d^{-1}$. We conclude that S is indeed a group.

3(a) Clearly any right ideal containing A but contain all the products of AS^1. On the other hand $(AS^1)S^1 = A(S^1)^2 = AS^1$. Therefore AS^1 is the right ideal generated by A.

(b) Similarly any ideal containing A must contain $S^1(AS^1)$ and $S^1(S^1AS^1)S^1 = (S^1)^2A(S^1)^2 = S^1AS^1$ is the ideal generated by A.

4(a) By definition of function composition we have for any $f, g, h \in \mathcal{T}_X$ that

$$x((f \circ g) \circ h)) = (x(f \circ g))h = (xf)g)h = (xf)(g \circ h) = x(f \circ (g \circ h)$$

so that $(f \circ g) \circ h = (f \circ g) \circ h$ and the operation is associative. Moreover the identity mapping ε on X is a member of $\mathcal{T}_X$ and therefore $\mathcal{T}_X$ is a monoid under function composition.

(b) Let f, g be constant mappings with ranges a and b respectively. Then $x(f \circ g) = (xf)g = ag = b$ for all $x \in X$. Hence $f \circ g = g$, and so the set of constant mappings forms a right zero subsemigroup of $\mathcal{T}_X$ (with function composition from left to right).

Comment Some authors prefer to maintain the calculus convention of composing mappings from right to left. However, in algebra, left to right composition is often used as it is here. In semigroups in particular mappings are often defined as a product of words over an alphabet, in which case left to right is the natural direction to read the composition.

(c) Suppose that $\alpha \in E(\mathcal{T}_X)$. Then for any $x \in X$ we have $x\alpha = x\alpha^2 = (x\alpha)\alpha$, and so we see that α acts identically when restricted to its range. Conversely if $\alpha|_{\text{ran}\alpha}$ is the identity mapping then the previous equation applies and so we conclude that $\alpha \in \mathcal{T}_X$ is idempotent if and only if α acts as the identity mapping when restricted to its range.

(d) Let $\alpha \in I$ and $\beta \in \mathcal{T}_X$. Then $X\beta\alpha \subseteq X\alpha$ so it follows that $|X\beta\alpha| \leq |X\alpha| \leq Y$ so that $\beta\alpha \in I$ and so I is a left ideal of $\mathcal{T}_X$. On the other hand, let $|X\alpha\beta| \leq |X\alpha| \leq Y$ also as, in general the cardinality of the range of any function $f : A \to B$ never exceeds that of its domain. (To see this take any $y \in Af$. Map $y \mapsto x$ where $x \in yf^{-1}$. This defines a one-to-one mapping from Af into A so that $|Af| \leq |A|$.) Hence $\alpha\beta \in I$ also. Therefore I is both a left and a right ideal, and therefore an ideal of $\mathcal{T}_X$.

Comment The converse is also true as these are indeed the only ideals of $\mathcal{T}_X$. To prove this one just shows that the principal ideal generated by a mapping $\alpha \in \mathcal{T}_X$ consists of all mappings of the same rank.

5(a) Clearly if a subsemigroup U of S contains A then, by closure under product and a simple induction on length, it follows that U must contain all products of members of A of any (positive) length. Since this set is by its very definition closed under the taking of products, it follows that the set of all products of members of A is indeed the smallest subsemigroup of S that contains the non-empty set A.

Comment In framing the previous argument we implicitly assume that a product $a_1a_2\cdots a_n$ $(n \geq 1)$ is unambiguous, which is to say that in the cases where $n \geq 3$, the outcome is indepedent of the bracketing of the product. For $n = 3$ this is simply the statement of the Associative law. To show that is true in general requires an induction argument on n, which is itself a useful exercise. As inductive hypothesis we take that for $m < n$ any bracketing of $a_1a_2\cdots a_m$ yields the same outcome as the particular bracketing $a_1(a_2(\cdots(a_m))\cdots)$ and work from there.

(b) We are told that $\langle a\rangle = \{a, a^2, a^3, \cdots\}$ is finite so let a^r be the first power that is repeated in this otherwise infinite list and let m be the least positive integer t such that $a^r = a^{r+t}$. We claim that $\langle a\rangle = S = \{a, a^2, \cdots, a^r, a^{r+1}, \cdots, a^{r+m-1}\}$. By definition of r and m, all the powers $a, a^2, \cdots, a^r$ are distinct from each other and all the listed members of S. Consider the set $K_a = \{a^r, a^{r+1}, \cdots, a^{r+m-1}\}$ and suppose, contrary to what we claim, that $a^{r+t} = a^{r+s}$ where $1 \leq t < s \leq r + m - 1$. Put $d = m - 1 - s \geq 0$. Then $a^{r+t+d} = a^{r+s+d} = a^{r+m-1}$ where $r < r + t + d < r + m - 1$. But then $a^r = a^{r+t+d+1} = a^{r+m}$, contrary to the assumption that m was the least power such that $a^r = a^{r+m}$. Therefore all the listed members of K_a are pairwise distinct and so the list S does indeed consist of m distinct members, which collectively define $\langle a \rangle$.

Next we note that $aK_a = K_a a = \{a^{r+1}, a^{r+2}, \cdots, a^{r+m-1}, a^{r+m} = a^r\} = K_a$, whence it follows that K_a is a subsemigroup of $\langle a \rangle$ that is both left and right simple, whence by Question 2, K_a is an (abelian) group.

(c) Since K_a is a group, there is a unique power t ($r \leq t \leq m-1$) such that a^t is idempotent. By the above argument, for any $a^s \in K_a$ we have that $a^s = a^{s+m}$ and $a^s \neq a^{s+p}$ for any $1 \leq p \leq m-1$. Hence we have

$$a^t = (a^t)^2 = a^{2t} = a^{t+m},$$

so that $m|t$. Hence t is the least integer $p \geq r$ such that $m|p$. In other words t is the unique integer p such that $r \leq p \leq r+m-1$ such that $p \equiv 0 \pmod{m}$, which exists and is unique as $r, r+1, \cdots, r+m-1$ is a set of m consecutive positive integers.

(d) Finally put $s = t+1$ and consider the set $S = \{a^s, a^{2s}, \cdots, a^{ms}\} \subseteq K_a$. We show that the members of the list S are pairwise distinct, and since there are m members listed, it will follow that $S = K_a$ so that K_a is indeed a cyclic group with a^{t+1} as a generator. To this end, suppose that for two members, a^{us} and a^{vs} with $1 \leq u \leq v \leq m$ we have $a^{us} = a^{vs}$. Then since a^t is the identity element of K_a we obtain $a^{ut+u} = a^{vt+v}$, whence $a^{t+u} = a^{t+v}$, whence $u \equiv v \pmod{m}$. This implies that $u = v$ as required to prove our claim. Therefore K_a is indeed a cyclic subgroup of $\langle a \rangle$ with idempotent a^t where $t \geq r$ and $m|t$.

6(a) A simple induction gives $\mathrm{ran}(a^k) = \{k, k+1, \cdots, r+m-1\}$ for all $k = 0, 1, \cdots, r$. Hence the index of a is at least r. On the other hand $a|_{K_a}$ where $K_a = \{r, r+1, \cdots, r+m-1\}$ is a cyclic permutation, whence $a^r = a^{r+m}$ and so r and m are the respective index and period of a.

(b) Let $a^t \in E(\langle a \rangle)$. Then we have $m|t$ and $r \leq t$. Since $r + m = n + 1$ (where $n = |\langle a \rangle|$) we have $m|t$ and $m \geq n + 1 - t$. In this case $t = 8$, $n = 11$ so that $m|8$ and $m \geq 11 + 1 - 8 = 4$. Hence $m = 4$ or $m = 8$, yielding two monogenic semigroups with $r = 8$, $m = 4$, or $r = 4, m = 8$, which we write $S_{8,4}$ and $S_{4,8}$.

(c) The mapping a has two components with vertex sets $\{1, 2, \cdots, 8\}$ and $\{9, 10, 11, 12\}$ respectively. The index of a is the greatest of the two indices of each of the maps represented by these components, which is $\max\{4.3\} = 4$. The period m is the least common multiple of the cycles of each component, which is the $\mathrm{lcm}\{3, 1\} = 3$. Hence $\langle a \rangle = S_{4,3}$.

The idempotent power a^t satisfies $m|t$ and $r \leq t \leq r+m-1$, that is $3|t$ and $4 \leq t \leq 6$, so that $t = 6$. The idempotent of $\langle a \rangle$ is a^6. Since $K_a = \{a^4, a^5, a^6 = e\}$, which is a copy of $\mathbb{Z}_3$, which is the only non-trivial subgroup of $\langle a \rangle$.

7(a) Certainly the mapping defines a binary operation on $\mathbb{C} \setminus \{0\}$. For three complex numbers a, b and c we have

$$(a \circ b) \circ c = |a \circ b|c = (||a|b|)c = (|a||b|)c = |a|(|b|c)$$

$$= |a|(b \circ c) = a \circ (b \circ c),$$

and so we have a semigroup.

(b) $z \in E(S)$ if and only if $z \circ z = |z|z = z$, which is to say that $|z| = 1$.

(c) We need to show that we may always solve the equation $a \circ x = b$ $(a, b \in \mathbb{C} \setminus \{0\})$, which is to say $|a|x = b$, which, since $a \neq 0$, gives the unique solution $x = \frac{b}{|a|}$ and so S is right simple.

Next suppose that $a \circ b = a \circ c$ and so $|a|b = |a|c$, whence $b = c$ and $a \neq 0$. Hence S is also left cancellative.

8(a) Let S be a finite subsemigroup of a group G. Then S inherits cancellativity from the containing group G. Let $a \in S$ and consider the right translation map $\rho_a : S \to Sa$ whereby $x \mapsto xa$. Then ρ_a is one-to-one for if $xa = ya$ $(x, y \in S)$ then $x = y$ by right cancellativity in S. Since ρ_a is clearly onto we have that ρ_a is a bijection, whence $|S| = |Sa|$. (To this point the finiteness hypothesis has not been used.) However, since S is finite and $Sa \subseteq S$ it follows that $Sa = S$ and so S is right simple. By the dual argument, S is also left simple and therefore S is a group by Question 2.

(b) Let $G = (\mathbb{Z}, +)$ and let $S = (\mathbb{N}, +)$ be the subsemigroup of all positive integers. Then S is embedded in a group but is not itself a group.

9(a) Let $\alpha, \beta \in S$. Then $\alpha\beta$ is also one-to-one and $X\alpha\beta \subseteq X\beta$, whence $X \setminus X\alpha\beta \supseteq X \setminus X\beta$ so that $|X \setminus X\alpha\beta| \geq |X \setminus X\beta|$, and so both sets are infinite. Hence $S \leq \mathcal{T}_X$, and indeed this shows that S is a left ideal in the semigroup of all one-to-one mappings on X.

(b) Suppose that α is any one-to-one mapping in $E(\mathcal{T}_X)$. Then by Question 4(c), $\alpha|_{X\alpha}$ is the identity mapping. Suppose that there existed $x \in X \setminus X\alpha$. Then $x\alpha \in X \setminus \{x\}$, whence $x\alpha = (x\alpha)\alpha$, contradicting that α is one-to-one. Hence $X\alpha = X$ and so α is the identity mapping. In particular, it now follows that $\alpha \notin S$ and so S is idempotent-free.

(c) Let $\alpha, \beta \in S$. We construct $\gamma \in S$ such that $\alpha\gamma = \beta$. Necessarily this requires that for each $x \in X$ we put $(x\alpha)\gamma = x\beta$, thus defining γ on $X\alpha$. The sets $Y = X \setminus X\alpha$ and $Z = X \setminus X\beta$ are both countably infinite and so we may take γ to act on $X \setminus X\alpha$ in a one-to-one fashion, mapping onto some infinite subset $W \subseteq Z$ such that $Z \setminus W$ is also infinite. This completes the definition of a mapping γ that satisfies $\alpha\gamma = \beta$ and $|X \setminus X\gamma| = Z \setminus W$, which is infinite. It remains only to check that γ is injective. For $x\alpha, y\alpha \in X\alpha$ $(x, y \in X)$ suppose that $(x\alpha)\gamma = (y\alpha)\gamma$. Then $x\beta = y\beta$ and so $x = y$ as β is one-to-one, whence $x\alpha = y\alpha$, thus showing that γ is one-to-one on $X\alpha$. By construction, γ is also one-to-one on $X \setminus X\alpha$. Finally let $x\alpha \in X\alpha$ and $y \in X \setminus X\alpha$. Then $(x\alpha)\gamma = x\beta \in X\beta$ but $y\gamma \in X \setminus X\beta$ so in particular $(x\alpha)\gamma \neq y\gamma$. Therefore γ is itself one-to-one and so lies in S. Therefore S is right simple.

Next suppose that $\alpha\beta = \gamma\beta$ for some $\alpha, \beta, \gamma \in S$. Then for any $x \in X$ we have $(x\alpha)\beta = (x\gamma)\beta$, whence $x\alpha = x\gamma$ as β is one-to-one. Hence $\alpha = \gamma$ and so S is right cancellative.

Now we consider the equation $\gamma\alpha = \beta$, where α, β are given members of S. For this to be solvable, we must have $X\gamma\alpha = X\beta$, whence $X\beta \subseteq X\alpha$. Clearly it is possible to choose α and β so that this does not hold and so it follows that this equation is not in general solvable and so S is not left simple.

Similarly consider the equation $\alpha\beta = \alpha\gamma$. This shows that $\beta|_{X\alpha} = \gamma|_{X\alpha}$ but clearly β and γ could act differently on some points of the infinite set $X \setminus X\alpha$. Hence α does not in general cancel on the left and so S is not a left cancellative semigroup.

10(a) We do have a binary operation on $S \times T$ so we just need to check associativity. However, with an obvious meaning for the notation we see that

$$((x_1, y_1)(x_2, y_2))(x_3, y_3) = (x_1x_2, y_1y_2)(x_3, y_3) = ((x_1x_2)x_3, (y_1y_2)y_3)$$

$$= (x_1(x_2x_3), y_1(y_2y_3)) = (x_1, y_1)((x_2, y_2)(x_3, y_3)).$$

(b) Let $(a, b) \in L \times R$. Then $(a, b)(a, b) = (a^2, b^2) = (a, b)$, and so $L \times R$ is also a band. Moreover for any $(a, b), (c, d) \in L \times R$ we have:

$$(a, b)(c, d)(a, b) = (ac, bd)(a, b) = (a, d)(a, b) = (a^2, db) = (a, b);$$

whence it follows that every pair in $L \times R$ is an inverse to every pair in $L \times R$.

Problem Set 2

1(a) $A\alpha \le S\alpha$ for if $a\alpha, b\alpha \in A\alpha$ then $a\alpha b\alpha = (ab)\alpha \in A\alpha$ and so ϕ is a mapping into $\mathcal{B}$, and is clearly also inclusion-preserving. To see that ϕ is onto, let $U \le T$. Let $a, b \in U\alpha^{-1}$, so that $a\alpha, b\alpha \in U$, whence $a\alpha b\alpha \in U$, which is equivalent to $(ab)\alpha \in U$, so that $ab \in U\alpha^{-1}$, whence $U\alpha^{-1} \le S$ such that $(U\alpha^{-1})\alpha = U$, and so ϕ is onto.

(b) Our mapping ϕ is now the restriction of the mapping of part (a) to ideals. Let I be an ideal of S. Let $a\alpha \in I\alpha$ $(a \in I)$, $b\alpha \in T$ (remembering α is onto). Then $a\alpha b\alpha = (ab)\alpha \in I\alpha$ as I is a right ideal; dually $b\alpha a\alpha = (ba)\alpha \in I\alpha$ as I is a left ideal. Hence ϕ maps ideals to ideals. Let I now denote an ideal of T, $a \in I\alpha^{-1}, b \in S$. Then $(ab)\alpha = a\alpha b\alpha \in I$ as $a\alpha \in I$, which is a right ideal of T. Thus $ab \in I\alpha^{-1}$, which implies that $I\alpha^{-1}$ is an ideal of S such that $(I\alpha^{-1})\alpha = I$. Therefore ϕ maps onto the set of ideals of T and so ϕ is an inclusion-preserving map from $\mathcal{A}$ onto $\mathcal{B}$.

(c) The composition $\alpha\beta$ is certainly a function from S to V and is also a homomorphism as for any $a, b \in S$ we get that

$$(ab)\alpha\beta = ((ab)\alpha)\beta = (a\alpha b\alpha)\beta$$

as α is a homomorphism. Then since β is also a homomorphism we have the required conclusion as

$$= (a\alpha)\beta(b\alpha)\beta = ((a)\alpha\beta)((b)\alpha\beta).$$

2. Suppose that σ is a congruence on S. Let $a, b, c \in S$ with $a\sigma = b\sigma$. Then since $c\sigma c$ and $a\sigma b$, and $\sigma$is a congruence we obtain $ca\,\sigma\,cb$, and so σ is a left congruence. The dual argument shows that σ is also a right congruence.

Conversely suppose that σ is both a left and a right congruence on S. Let $a, b, c, d \in S$ such that $a\sigma b$ and $c\sigma d$. Then since σ is a left congruence we have $ac\,\sigma\,bc$. Since σ is a right congruence then we have $bc\,\sigma\,bd$. Finally since σ is transitive we obtain $ac\,\sigma\,bc\,\sigma\,bd$ implies that $ac\,\sigma\,bd$, thus demonstrating that σ is a congruence on S.

3(a) Clearly kerϕ is an equivalence relation. Suppose that $(a, b), (c, d) \in$kerϕ. Then $(ac)\phi = a\phi c\phi = b\phi d\phi = (bd)\phi$, which is to say that $(ac, bd) \in$ kerϕ and so kerϕ is a congruence on it domain S.

(b) We first need to check that this multiplication is well-defined, meaning that it is independent of the representatives chosen for the ρ-classes. So, suppose that $a\rho c$ and $b\rho d$. Then $ab\,\rho\,cd$ (as ρ is a congruence), or in the alternative notation, $\rho_{ab} = \rho_{cd}$, so the class that results from the operation does not depend on the representive chosen for each congruence class. Associativity also needs to be checked:

$$(a\rho\, b\rho)c\rho = (ab)\rho\, c\rho = ((ab)c)\rho = (a(bc))\rho = a\rho\,(bc)\rho = a\rho(b\rho\, c\rho).$$

(c) By definition of multiplication in S/ρ we have $(ab)\rho^\natural = (ab)\rho = a\rho\, b\rho = a\rho^\natural b\rho^\natural$, so that $\rho^\natural$ is a homomorphism from S to S/ρ, which is clearly onto as every member of S/ρ has the form $a\rho$ for some $a \in S$. Finally

$$\ker(\rho^\natural) = \{(a, b) : a\rho^\natural = b\rho^\natural\} = \{(a, b) : a\rho = b\rho\} = \rho.$$

4. That ker(α) is a congruence was shown in Question 3(a). We require that $\rho^\natural\psi = \alpha$, which is to say that ψ is necessarily defined to act as $(a\rho)\psi = a\alpha$. We check ψ is thereby well-defined. Suppose that $a\rho = b\rho$, which is to say that $(a, b) \in$ kerα, whence $a\alpha = b\alpha$, so the action of ϕ is independent of the representative chosen for $a\rho$. Clearly ψ is a surjective mapping onto $T = S\alpha$; and as for being one-to-one, suppose that $(a\rho)\psi = (b\rho)\psi$. Then $a\alpha = b\alpha$, which is to say that $(a, b) \in$ ker$\alpha = \rho$. Hence $a\rho = b\rho$, and we conclude that ψ is indeed a bijection. Finally we need to check that ψ is a homomorphism. However

$$((a\rho)(b\rho))\psi = ((ab)\rho)\psi = (ab)\alpha = a\alpha b\alpha = ((a\rho)\psi)((b\rho)\psi);$$

therefore ψ is indeed an isomorphism $\psi : S/\rho \to T$ and is the unique such isomorphism that satisfies $\rho^\natural\psi = \alpha$. This completes the proof.

5. First we check that ρ/σ is a well-defined relation on S/σ. Suppose that $(a\sigma, b\sigma) \in \rho/\sigma$ so that $a\rho b$. Suppose now that $a\sigma = c\sigma$ and $b\sigma = d\sigma$. Then since $\sigma \subseteq \rho$ we have that $c\,\rho\,a\,\rho\,b\,\rho\,d$, so that $c\rho d$ and so $(c\sigma, d\sigma) \in \rho/\sigma$. This shows that the membership of ρ/σ is independent of the representatives chosen for the σ-classes involved in the definition. Hence ρ/σ is a well-defined relation on S/σ.

That ρ/σ is an equivalence relation on S/σ follows immediately from the fact that σ and ρ are equivalence relations: for instance, as regards transitivity let us suppose that $(a\sigma, b\sigma), (b\sigma, c\sigma) \in S/\sigma$ with $(a, b) \in \rho$ and $(b, c) \in \rho$. Then $(a\sigma, c\sigma) \in \sigma$ as σ is transitive and $(a, c) \in \rho$ as ρ is transitive, whence $(a\sigma, c\sigma) \in \rho/\sigma$.

To show that ρ/σ is a congruence let us take $(a\sigma, b\sigma), (c\sigma, d\sigma) \in \rho/\sigma$. Then, since σ is a congruence we have $ac\,\sigma bd$, and since $\sigma \subseteq \rho$ we have $a\rho b$ and $c\rho d$. Since ρ is a congruence this gives that $(ac)\rho(bd)$ and so $((ac)\sigma, (bd)\sigma) \in \rho/\sigma$, which is what was required to show that ρ/σ is itself a congruence on S/σ.

Next we check that $(\rho/\sigma)^\natural$ maps surjectively onto S/ρ. Let $a\rho \in S/\rho$. Then

$$(a\sigma)(\rho/\sigma)^\natural = (a\sigma)(\rho/\sigma) = a\rho,$$

which is well-defined as $\sigma \subseteq \rho$. This shows that $(\rho/\sigma)^\natural$ maps surjectively onto S/ρ.

The kernel of $(\rho/\sigma)^\natural$ is the set of pairs $(a\sigma, b\sigma)$ such that

$$(a\sigma)(\rho/\sigma)^\natural = (b\sigma)(\rho/\sigma)^\natural \Leftrightarrow a\rho b \Leftrightarrow (a\sigma, b\sigma) \in \rho/\sigma,$$

which is to say that $\ker(\rho/\sigma)^\natural = \rho/\sigma$, as required. Hence by the First isomorphism theorem we have that $(S/\sigma)/(\rho/\sigma) \cong S/\rho$.

6(a) Let $a, b \in e\rho$. Then

$$(ab^{-1})\rho = (a\rho)(b^{-1}\rho) = (b\rho)(b^{-1}\rho) = (bb^{-1})\rho = e\rho,$$

which shows that $ab^{-1} \in N = e\rho$. Hence $e\rho$ is a subgroup N of G. Moreover N is normal as for any $a \in N$ and $b \in G$ we have

$$(b^{-1}ab)\rho = b^{-1}\rho a\rho b\rho = b^{-1}\rho e\rho b\rho = (b^{-1}eb)\rho = e\rho$$

so that $b^{-1}ab \in N$. Finally for $a, b \in G$ we have

$$a\rho b \Leftrightarrow ab^{-1}\rho bb^{-1} = e,$$

which is to say that $a\rho b$ if and only if $ab^{-1} \in N$. Hence the set of ρ-classes coincide with the set of all cosets of the normal subgroup $N = e\rho$.

(b) Conversely let N be a normal subgroup of G and define a relation ρ on G by $a\rho b$ if and only if $ab^{-1} \in N$. Then $a\rho a$ as $aa^{-1} = e \in N$; if $a\rho b$ then $ab^{-1} \in N$, whence $(ab^{-1})^{-1} = ba^{-1} \in N$, as N is closed under the taking of inverses, and so ρ is symmetric. Next if $a\rho b\rho c$ then $ab^{-1}, bc^{-1} \in N$, whence so is $ab^{-1}bc^{-1} = ac^{-1}$, whence $a\rho c$ and so ρ is transitive and therefore is an equivaence relation. Next let $a\rho b$ and take any $c \in G$. Then $(ac)(bc)^{-1} = acc^{-1}b^{-1} = ab^{-1} \in N$ so that $ac\rho bc$ and so ρ is a right congruence. Also $(ca)(cb)^{-1} = cab^{-1}c^{-1} \in N$ as $ab^{-1} \in N$ and N is normaland so closed under conjugation. Hence ρ is also a left congruence and therefore ρ is a congruence by Question 2. Moreover $a\rho e \Leftrightarrow ae^{-1} = a \in N$, whence we have that $e\rho = N$, as required to complete the proof.

7(a) It is clear that all the defining properties of congruence are inherited by arbitrary intersections. For example let $\rho = \cap_{i\in I}\rho_i$ over some index set I, where each ρ_i is a congruence on some semigroup S. Let $a\rho b$ and $c\rho d$. Then $a\rho_i b$ and $c\rho_i d$ for all $i \in I$. Since ρ_i is a congruence on S, it follows that $ac\rho_i bd$. Since this holds for all $i \in I$, it follows that $ab\rho cd$ as well.

We do have to note that $\rho \neq \emptyset$, which follows as each ρ_i contains the equality congruence on S, whence S does also. (And this is necessary to verify that ρ is a reflexive relation on S).

(b) This follows almost immediately from part (a), we just need to note that there is at least one congruence, namely the universal congruence $S \times S$, in the intersection in question.

8. By Question 7, the least congruence containing R exists (and we denote it by R^*). Suppose that $a \to \cdots \to b$ is a sequence of elementary R-transitions from a to b $(a, b \in S)$ of length $n \geq 0$. We prove by induction on n that aR^*b, the claim being true for $n = 0$ be reflexivity of R. If $n = 1$ then $a = xcy$, $b = xdy$, and $cR^S d$ for some $c, d \in S$ and $x, y \in S^1$. Since $R^S \subseteq R^*$ (as $R \subseteq R^*$ and R^* is reflexive and symmetric), if follows that cR^*d. Then since R^* is a congruence, it follows that $a = xcyR^*xdy = b$. Finally let $n \geq 2$ so that the sequence has the form $x \to t \to \cdots \to b$ say. By the $n = 1$ case we have xR^*t and by induction we have tR^*b. Then we have aR^*tR^*b and since $R^*$is transitive, it follows that aR^*b, completing the proof in this direction.

To show the converse we assign the symbol R_1 to the relation defined by aR_1b if and only if there is a sequence of elementary R-transitions from a to b. By above we have $R \subseteq R_1 \subseteq R^*$. Since R^* is the smallest congruence on S that contains R, it follows that to complete the proof we need only show that R_1 is a congruence.

By taking $n = 0$ we see that aR_1a, so that R_1 is reflexive. Next, since the reverse of each elementary R-transition is also an elementary R-transition, it follows that $b \to \cdots \to a$ by the reverse sequence of transitions so that bR_1a and hence R_1 is symmetric. Next suppose that is a sequence of elementary R-transitions $b \to \cdots \to c$ say. Then by following $a \to \cdots \to b$ by $b \to \cdots \to c$ we have a sequence of elementary R-transitions $a \to \cdots \to c$, thus showing that R_1 is transitive. Therefore R_1 is an equivalence relation on S that contains R. Finally, once more consider the sequence $a \to \cdots \to b$ and take any $c \in S^1$. Each elementary R-transition in the sequence has the form $xty \to xsy$ for some $(x, y \in S^1$ and $tR^S s)$. Then $xt(yc) \to xs(yc)$ is also an elementary R-transition, and so, replacing each transition is the original sequence by that where each term in the sequence is multiplied on the right by c gives a sequence of elementary R-transitions from ac to bc, thus showing that R_1 is a right congruences on S. By symmetry, R_1 is also a left congruence on S, and therefore R_1 is a congruence on S whence we conclude that $R_1 = R^*$.

9. Consider our candidate

$$E^\flat = \{(a, b) \in S \times S : (\forall\, x, y \in S^1)\, (xay, xby) \in E\}.$$

We need to show that $E^\flat \subseteq E$, that $E^\flat$ is a congruence, and finally that if $\rho \subseteq E$ is a congruence then $\rho \subseteq E^\flat$. To this end, let us take $(a, b) \in E^\flat$.

Putting $x = y = 1$ in the definition of $E^\flat$ we get that $(a, b) \in E$, and so $E^\flat \subseteq E$. For any $a \in S$ we have $(xay, xay) \in E$ as E is reflexive and so $(a, a) \in E^\flat$ and so $E^\flat$ is reflexive. Now suppose that $(a, b) \in E^\flat$ so that $(xay, xby) \in E$ for all $x, y \in S^1$. Since E is symmetric, it follows that $(xby, xay) \in E$ for all $x, y \in S^1$ and so $(b, a) \in E^\flat$ and $E^\flat$ is therefore symmetric. Next suppose that $aE^\flat bE^\flat c$ say, so that $(xay, xby) \in E$ and $(xby, xcy) \in E$ for all $x, y \in S^1$. Since E is transitive, it follows that $(xay, xcy) \in E$ and therefore $(a, c) \in E^\flat$ and therefore $E^\flat$is transitive and therefore is an equivalence relation contained in E. Now suppose that $(a, b) \in E^\flat$ and take any $c \in S^1$. Then $(xay, xby) \in E$ for all $x, y \in S^1$. In particular $(xacy, xbcy) \in E$ for all $x, y \in S^1$ so that $(ac, bc) \in E^\flat$. It follows that $E^\flat$ is a right congruence and by the dual argument, also a left congruence and therefore $E^\flat$ is indeed a congruence that is contained in E.

Now let ρ be any congruence on S such that $\rho \subseteq E$. Suppose that $(a, b) \in \rho$. Then since ρ is a congruence contained in E it follows that $(xay, xby) \in \rho \cap E$ for all $x, y \in S^1$. Therefore $\rho \subseteq E^\flat$. This completes the proof that $E^\flat$ is the largest congruence contained in the equivalence relation E on S.

10(a) We have that $e = fe$ as f is a left identity, while equally we have $fe = f$ as e is a right identity. Therefore $e = fe = f$ and so $e = f$ and e is the unique identity element of S, which is therefore a monoid.

(b) We have that $e = fe$ as e is a right zero element, while equally $fe = f$ as f is a left zero element. Therefore $e = fe = f$ and e is the unique zero element of S.

(c) Let ρ be any equivalence relation on a null semigroup S with zero element e. Then for any $(a, b), (c, d) \in \rho$ we have $ac = e = bd$ and so $(ac, bd) \in \rho$. Therefore ρ is also a congruence on S. Now take any $a\rho, b\rho$ in S/ρ. Then $(a\rho)(b\rho) = (ab)\rho = e\rho$ for all $a\rho, b\rho \in S/\rho$. Therefore S/ρ is indeed itself a null semigroup in which all products equal the zero class, $e\rho$.

Problem Set 3

1(a) For any $e \in E$ we have $e \leq e$ as $e = e^2$. Suppose that $e \leq f$ and $f \leq e$ $(e, f \in E)$. Then $e = ef = fe$ and $f = fe = ef$, so that $e = ef = f$ and so $\leq$ is anti-symmetric. Finally let $e \leq f$ and $f \leq g$. Then $e = ef = fe$ and $f = fg = gf$. Then $eg = (ef)g = e(fg) = ef = e$ and $ge = g(fe) = (gf)e = fe = e$. Hence $e \leq g$ and so $\leq$ is transitive. Therefore $\leq$ is indeed a partial order on $E(S)$.

(b) If $e \leq f$ then $fef = f(ef) = fe = e$. Conversely if $e = fef$ then $ef = fef^2 = fef = e$ and $fe = f^2ef = fef = e$ so that $e \leq f$.

2. We will need to make use of the observation that if $a \leq b$ then $x = a \wedge c \leq b \wedge c = y$. To see this we note that $x \leq b$ and $x \leq c$ so that $x \leq y$ and y is the greatest lower bound of b and c.

We need to show that $x = (a \wedge b) \wedge c = y = a \wedge (b \wedge c)$. Now $a \wedge b \leq a$ and so $x \leq a$. Also $a \wedge b \leq b$ and so $x = (a \wedge b) \wedge c \leq b \wedge c$, whence $x \leq a \wedge (b \wedge c) = y$; a similar argument shows that $y \leq x$ and therefore the meet operation is associative and clearly $a \wedge b = b \wedge a$ and $a \wedge a = a$. Therefore $(S, \wedge)$ defines a commutative band. Furthermore $a \leq b$ if and only if $a = a \wedge b$ and so the natural partial order on $(S, \wedge)$ is the order $\leq$ of the semilattice.

3. Let B be a commuative band and let $\leq$ be the natural partial order on B. Let $e, f \in B$ then $e \cdot ef = ef$ and $ef \cdot e = fe \cdot e = fe = ef$. It follows that $ef \leq e$ and equally $ef \leq f$ so that $ef \leq e \wedge f$. Now let $g \leq e$ and $g \leq f$. Then $g \cdot ef = ge \cdot f = gf = g$ and $ef \cdot g = g \cdot ef = g$ also and so $g \leq ef$. Therefore $ef = e \wedge f$, and so B is a semilattice. Moreover the product in S coincides with the meet operation in the semilattice of the natural partial order of B.

4(a) For $a \in G$, the inverse a^{-1} satisfies the required definition of regularity as: $aa^{-1}a = ae = a$ and $a^{-1}aa^{-1} = ea^{-1} = a^{-1}$. Therefore a group is a regular semigroup.

(b) We have $a = axa$. Then

$$a(xax)a = (axa)xa = axa = a; \;\; (xax)a(xax) = x(axa)(xax) = x(axa)x = xax;$$

therefore $xax \in V(a)$.

(c) Let $\alpha \in \mathcal{T}_X$. For any $y \in X\alpha$, choose $x \in y\alpha^{-1}$ and put $y\beta = x$. For $y \in X \setminus X\alpha$ put $y\alpha = z$ where $z \in X$ is arbitrary. Then for any $t \in X$ we have $t\alpha\beta\alpha = x\alpha$ where $x \in (t\alpha)\alpha^{-1}$ so that $x\alpha = t\alpha$ and therefore $t\alpha\beta\alpha = t\alpha$ for all $t \in X$. Therefore $\alpha = \alpha\beta\alpha$ and the result now follows from part (b).

(d) Let $\alpha : S \to T$ be a homomorphism. Then $S\alpha \leq T$ by Question 1(a) of Set 2. Let $y \in S\alpha$ so that $y = x\alpha$ say. Let $x' \in V(x)$ and denote $x'\alpha$ by y'. Then

$$yy'y = (x\alpha)(x'\alpha)(x\alpha) = (xx'x)\alpha = x\alpha = y;$$

whence it follows that y is regular. Therefore $S\alpha$ is a regular subsemigroup of T.

(e) For any given $a = (a_i)_{i \in I}$ in S, clearly $(x_i)_{i \in I} \in V(a)$, where $x_i \in V(a_i)$ for all $i \in I$.

Comment Clearly the converse also holds in that S is regular implies the same of each component in the direct product.

5(a) By Question 4(a), any group G is regular and has a unique idempotent e, that being the identity element of G. Conversely suppose that S is regular with a unique idempotent e. Let $a \in S$ and let $x \in V(a)$. Then $(ax)^2 = (axa)x = ax$ and $(xa)^2 = (xax)a = xa$. Hence $ax = xa = e$, and $ae = axa = a$ and $ea = axa = a$ and so S is a monoid with identity e. Moreover x is the inverse of a with respect to e and therefore S is a group.

(b) Let S be a finite semigroup. Certainly if S is a group then S is cancellative. Conversely suppose that S is cancellative. We prove that S is a group by checking that S is both left and right simple, and by symmetry it is enough to verify that S is left simple, which is to say that $S = Sa$ for all $a \in S$. Now $\rho_a : S \to Sa$ whereby $x \mapsto xa$ is an injective map for, by right cancellativity, if

$xa = ya$ then $x = y$. Hence $Sa \subseteq S$ and $|Sa| = |S|$. However, since S is finite this implies that $Sa = S$, thus completing the proof.

(c) Part (b) does not hold in general: for example $(\mathbb{N}, +)$ is a cancellative (and commutative) semigroup that is not a group.

6. We have ρ is reflexive as $(a, b)\rho(a, b) \Leftrightarrow ab = ba$; suppose that $(a, b)\rho(c, d)$ so that $ad = bc \Rightarrow cb = da$ so that $(c, d)\rho(a.b)$ and so ρ is symmetric. As for transitivity we take $(a, b)\rho(c, d)\rho(e, f)$ say so that $ad = bc$ and $cf = de$. Hence $afc = acf = ade = bce = bec$ so that $af = be$, as S is cancellative, and so $(a, b)\rho(e, f)$, thus establishing ρ as an equivalence relation.

To show that ρ is a congruence, it follows by commutativity that is suffices to show that ρ is a right congruence. Suppose then that $(a, b)\rho(c, d)$ and let $(e, f) \in F$. We have $ad = bc$ so that

$$aedf = adef = bfce \Leftrightarrow (ae, bf)\rho(ce, df) \Leftrightarrow ((a, b)(e, f))\rho((c, d)(e, f)),$$

as required. Thus ρ is a congruence and so F/ρ is commutative, with $(1, 1)\rho$ as identity element. Furthermore F/ρ is a group, as for any $(a, b)\rho \in F/\rho$ we have

$$(a, b)\rho(b, a)\rho = (ab, ba)\rho = (ab, ab)\rho = (1, 1)\rho.$$

Finally we verify that the mapping ϕ where $a \mapsto (a, 1)\rho$ embeds S into the abelian group F/ρ. That ϕ is injective is immediate from the definition of ρ. Furthermore ϕ is a morphism:

$$(ab)\phi = (ab, 1)\rho = (a, 1)\rho(b, 1)\rho = a\phi b\phi.$$

Let $S = (\mathbb{N}, +)$, so $S^1 = \mathbb{N} \cup \{0\}$. We have $F = S^1 \times S^1$ and so

$$(a, b)\rho(c, d) \Leftrightarrow a + d = b + c \Leftrightarrow a - b = c - d.$$

We thus have a well-defined bijection ϕ between F/ρ and $(\mathbb{Z}, +)$ where $(a, b)\phi = a - b$. Moreover ϕ is an isomorphism:

$$((a, b)+(c, d))\rho = (a+c, b+d)\rho \mapsto a+c-(b+d) = (a-b)+(c-d) = ((a, b)\rho)\phi((c, d))\phi.$$

For the embedding of S where $a \mapsto (a, 0)\rho$ and $(a, 0)\rho\phi = a - 0 = a$, we see that this is just the standard embedding of $(\mathbb{N}, +) \to (\mathbb{Z}, +)$.

Next let $S = (\mathbb{N}, \cdot)$ so that $F = \mathbb{N} \times \mathbb{N}$ and $(a, b)\rho(c, d) \Leftrightarrow ad = bc$, which is to say $\frac{a}{b} = \frac{c}{d}$. This is the usual embedding of $(\mathbb{N}, \cdot)$ into $(\mathbb{Q}^+, \cdot)$ of positive fractions, with $a \in \mathbb{N}$ identified with $(a, 1) = \frac{a}{1}$ in $F/\rho \cong (\mathbb{Q}^+, \cdot)$.

7(a) Let $S = G \times E$. Then for any $(a, e), (b, f) \in G \times E$ we have $(a, e)(a^{-1}b, f) = (aa^{-1}b, ef) = (b, f)$, showing that S is right simple. To show that S is left cancellative we suppose that

$$(c, g)(a, e) = (c, g)(b, f)$$

$$\Rightarrow (ca, ge) = (cb, gf) \Rightarrow (ca, e) = (cb, f)$$

whence $a = b$ as G is cancellative and $e = f$, whence S is indeed left cancellative and therefore S is a right group.

(b) We now suppose that S is a right group. Take $a \in S$. Since S is right simple, for any $b \in S$ there exists $x \in S$ such that $a = bx$ and taking $b = a$ this give $a = ax$, whence $a = ax = ax^2$. By left cancellativity we have that $x = x^2$ is an idempotent. Therefore $E(S) \neq \varnothing$.

(c) Next let $e, f \in E(S)$. Then there exists $x \in S$ such that $ex = f$. Hence $ef = e \cdot ex = ex = f$, so that $E(S)$ is a right zero semigroup.

(d) Now take $e \in E(S)$ and $b \in S$. Then there exists $x \in S$ such that $ex = b$, whence $eb = e \cdot ex = ex = b$.

(e) Certainly $Se \leq S$. If $xe \in Se$ then $e \cdot xe = xe$ (by (d)) and $xe \cdot e = xe$, so that e is the identity element of Se. Finally let $xe \in Se$. Then there exists $y \in S$ such that $xey = e$, whence $xe \cdot ye = e^2 = e$, and so $ye = (xe)^{-1}$ and Se is a group.

(f) Let $a \in S$ and take $e \in E(S)$ such that $a = ae$, (e exists as shown in (b)). Define $\phi : S \to G \times E$ by $a \mapsto (af, e)$. Supppose that $a\phi = b\phi$, so that $af = bf$ and $ae = a$, $be = b$. Then, since $e = fx$ for some $x \in S$ we obtain

$$a = ae = afx = bfx = be = b,$$

and so ϕ is injective.

For each $a \in S$, the right identity e for a is unique, for if $a = ae = ag$, then $e = g$ by left cancellativity. Now take $(af, e) \in G \times E$. Then $(ae)\phi = (aef, e) = (a, e)$ and so ϕ is surjective. Finally let $a\, b \in S$ with $a = ae$ and $b = bfg(e, g \in E(S))$. Then

$$(ab)\phi = (abf, g) \text{ (as } abg = ab) = (afbf, eg)$$

as $fbf = bf$ and Sf is a group with identity f,

$$= (af, e)(bf, g) = a\phi b\phi.$$

Therefore ϕ is a required isomorphism and so $S \cong G \times E$.

8(a) If S is a right group then $S \cong G \times E$ say and thus is right simple and contains at least one idempotent. Conversely, if S has these properties then since $S = eS$ for all $e \in E(S)$, it follows that every idempotent of S is a left identity. Now suppose that $ca = cb$ $(a, b, c \in S)$. Then take $e \in E(S)$ and write $e = cx$. Put $f = xc$, then

$$f^2 = xcxc = xec = xc = f$$

so that $f \in E(S)$. Then

$$a = fa = xca = xcb = fb = b.$$

Hence S is left cancellative and right simple, and thus S is a right group.

(b) Let $S = G \times E$ by a right group and consider the equation $(a, e)(x, g) = (b, f)$. This gives $ax = b$ and $eg = f$, whence $x = a^{-1}b$ and $g = f$, so the solution of our equation is indeed unique. Conversely, given that $ax = b$ is uniquely solvable in S, it follows that S is right simple. Putting $b = a$ gives $ax = a = ax^2$ so that $x \in E(S)$, by uniqueness of solution. Hence $E(S) \neq \varnothing$ and it follows from (i) that S is a right group.

(c) Since the direct product of two regular semigroups is easily seen to be regular, it follows that right group $G \times E$ is regular and left cancellative. Conversely let S be a regular and left cancellative semigroup. For each $e \in E(S)$ and $a \in S$ we have $e \cdot a = e \cdot ea$ whence $a = ea$ by left cancellativity and so each idempotent is a left identity in S. Now take $a, b \in S$. Let $a' \in V(a)$. Then $aa' \in E(S)$ so that putting $x = aa'$ we have $a = xb$ and so it follows that $aS = S$ for all $a \in S$. Therefore S is a right group.

9. Clearly ρ is an equivalence relation. Suppose that $a\rho b$ and $c \in S$. Either $a = b$ in which case $ac = bc$. Otherwise $a, b \in I$ whence $ac, bc \in I$ as I is a right ideal. This shows that ρ is a right congruence. Dually, ρ is a left congruence and therefore ρ is a congruence on S.

10(a) Let $a, b \in S$. We need to check that $(ab)\Phi = a\Phi b\Phi$, which is to say that $\rho_{ab} = \rho_a\rho_b$. Take any $x \in S$, then

$$x\rho_{ab} = x(ab) = (xa)b = x\rho_a\rho_b.$$

(b) Let S be a null semigroup with zero element z. For any $a, x \in S$ we have $x\rho_a = xa = z$. Hence $\rho_a = \rho_b$ for all $a, b \in S$. In particular, Φ is not one-to-one unless $|S| = 1$.

(c) If we replace S by S^1 then Φ is still a homomorphism as in (a). Suppose that $\rho_a = \rho_b$. Then $a = 1a = 1\rho_a = 1\rho_b = 1b = b$. Therefore $a = b$, whence it follows that Φ is indeed one-to-one and so Φ acts to embed S into the full transformation semigroup $\mathcal{T}_S^1$. Therefore any semigroup may be embedded in a full transformation semigroup $\mathcal{T}_X$. Moreover, if S is finite, we may take $\mathcal{T}_X$ to be finite also.

Problem Set 4

1(a) $a \in \text{dom}\alpha\beta$ if and only if there exists $b, c \in X$ such that $a\alpha = c$ and $c\beta = b$. Hence $a\alpha \in \text{dom } \beta$ and $a\alpha \in \text{ran } \alpha$ so it follows that $\text{dom}\alpha\beta \subseteq (\text{ran}\alpha \cap \text{dom}\beta)\alpha^{-1}$. Conversely suppose that $a \in (\text{ran}\alpha \cap \text{dom}\beta)\alpha^{-1}$. Then $a\alpha \in \text{ran}\alpha \cap \text{dom } \beta$. Hence $a\alpha\beta$ is defined and so $a \in \text{dom } \alpha\beta$ giving the reverse inclusion and we conclude that $\text{dom}\alpha\beta = (\text{ran}\alpha \cap \text{dom}\beta)\alpha^{-1}$. Therefore

$$\text{ran } \alpha\beta = (\text{ran } \alpha \cap \text{dom}\beta)\alpha^{-1}\alpha = \text{ran } \alpha \cap \text{dom } \beta.$$

(b) Let $\Phi : \mathcal{PT}_X \to \mathcal{T}_{X \cup \{0\}}$ be the mapping whereby $\alpha \mapsto \alpha_1$ where $x\alpha_1 = x\alpha$ if $x \in \text{dom}\alpha$ and otherwise $x\alpha_1 = 0$. In particular $0\alpha_1 = 0$. Suppose that $\alpha_1 = \beta_1$ for some $\alpha, \beta \in \mathcal{PT}_X$. Then if $x \in \text{dom}\alpha$ then $x\alpha \in X$ and

$x\alpha = x\alpha_1 = x\beta_1 = x\beta$ (as $x\alpha \neq 0$) so that $x \in$ dom β and $x\alpha = x\beta$. On the other hand if $x \notin \text{dom}\alpha$ then $x\alpha_1 = 0 = x\beta_1$, whence $x \notin \text{dom}\beta$. This all serves to show that $\alpha = \beta$ and so Φ is one-to-one.

Now let $\alpha_1 \in \mathcal{T}_{X\cup\{0\}}$ with $0\alpha_1 = 0$. Let $\alpha \in \mathcal{PT}_X$ be defined by $\text{dom}\alpha = \{x \in X : x\alpha_1 \neq 0\}$ and for $x \in \text{dom}\alpha$ put $x\alpha = x\alpha_1$. Then, by construction $\alpha\Phi = \alpha_1$. Hence Φ is a bijection of $\mathcal{PT}_X$ onto the set of all members of $\mathcal{T}_{X\cup\{0\}}$ which fix 0. Finally we need to check that Φ is a homomorphism. Let $\alpha, \beta \in \mathcal{PT}_X$. If $x(\alpha\beta)_1 \neq 0$ then $x(\alpha\beta)_1 = x\alpha\beta$, which occurs iff $x \in (\text{ran}\alpha \cap \text{dom}\beta)\alpha^{-1}$. On the other hand, $x\alpha_1\beta_1 \neq 0$ iff $x \in \text{dom}\alpha$ and $x\alpha \in \text{dom}\beta$ (in which case $x(\alpha\beta)_1 = x\alpha\beta$). But $x \in \text{dom}\alpha$ and $x\alpha \in \text{dom}\beta$ iff $x \in (\text{ran}\alpha)\alpha^{-1} \cap (\text{dom}\beta)\alpha^{-1} = (\text{ran}\alpha \cap \text{dom}\beta)\alpha^{-1}$, whence it follows that $(\alpha\beta)_1 = \alpha_1\beta_1$. Therefore Φ is indeed a required isomorphism.

Comment Note that we have used the fact that for any function f and sets A and B we have $(A \cap B)f^{-1} = Af^{-1} \cap Bf^{-1}$. Clearly we have containment from left to right while if $x \in Af^{-1} \cap Bf^{-1}$ then $xf \in A \cap B$, whence $x \in (A \cap B)f^{-1}$.

(c) For each $x \in X_n$ we have n choices for $x\alpha$ and since different choices give different functions it follows that $|T_n| = n^n$.

By (b) $|\mathcal{PT}_n| = |\{\alpha \in \mathcal{T}_{X\cup\{0\}} : 0\alpha = 0\}|$. Hence when constructing a member of the latter set we have for each $x \in X$, a choice of $n+1$ possible images (as $x\alpha = 0$ is always possible) giving $(n+1)^n$ choices in all. Therefore $|\mathcal{PT}_n| = (n+1)^n$.

(d) We know that $\mathcal{T}_X$ is regular, and identifying $\mathcal{PT}_X$ with the semigroup of all mappings in $\mathcal{T}_{X\cup\{0\}}$ which fix 0, we need only observe that when taking an inverse β of such a mappping in $\mathcal{T}_{X\cup\{0]}$ we may insist that $0\beta = 0$.

2. Certainly $\mathcal{I}_X \subseteq \mathcal{PT}_X$ and since the composition of partial one-to-one mappings will yield another (partial) one-to-one mapping, it follows that $\mathcal{I}_X \leq \mathcal{PT}_X$. Since α^{-1} is a (partial) one-to-one function it follows that α^{-1} is the only member $\beta \in \mathcal{I}_X$ such that $\alpha\beta\alpha = \alpha$ and $\beta = \beta\alpha\beta$. A mapping $\varepsilon \in \mathcal{I}_X$ if and only if $x\varepsilon = x$ for all $x \in \text{dom}\varepsilon$ and so an idempotent can be identified by its domain (which equals its range). If we write ε_A for the idempotent in $\mathcal{I}_X$ with domain A we then see that $\varepsilon_A\varepsilon_B = \varepsilon_{A\cap B}$. Therefore the semilattice of idempotents of $\mathcal{I}_X$ is the semilattice of the power set of X under intersection.

3. (i) implies (ii). Since S is regular, it follows that $S^1a = Sa$. Now $Sa = Saa^{-1}a \subseteq Sa^{-1}a \subseteq Sa$. It follows that $Sa = Saa^{-1}$ and $aa^{-1} \in E(S)$. Similarly $aS = aa^{-1}S$, so that each right and each left ideal have an idempotent generator (and this is true for any regular semigroup). Suppose now that $Se = Sf$ where $e, f \in E(S)$. Then there exist $x, y \in S$ such that $xe = f$ and $yf = e$. Then

$$e = yf = yf^2 = ef = fe = xe \cdot e = xe = f.$$

The dual argument shows that each left principal ideal has a unique idempotent generator.

(ii) implies (iii). Let $a \in S$ and take $a', a'' \in V(a)$. Then $aS = aa'S = aa''S$ and $Sa = Sa'a = Sa''a$. Since idempotent generators are unique, we have

$aa' = aa''$ and $a'a = a''a$. Hence

$$a' = a'aa' = a''aa' = a''aa'' = a''$$

and so each element has a unique inverse.

(iii) implies (i). Let $e, f \in E(S)$ and $x = (ef)^{-1}$. One checks that xe and fx are both inverse to ef:

$$xe \cdot ef \cdot xe = xefxe = xe;\ ef \cdot xe \cdot ef = efxef = ef;$$

$$fx \cdot ef \cdot fx = fxefx = fx;\ ef \cdot fx \cdot ef = efxef = ef.$$

Thus by uniqueness of inverses we have $x = xe = fx$, whence $x^2 = xe \cdot fx = x$. But then $x = x^{-1} = ef$, whence $ef \in E(S)$. By a similar argument, $fe \in E(S)$. Next we show that ef and fe are mutually inverse:

$$ef \cdot fe \cdot ef = efef = ef;\ fe \cdot ef \cdot fe = fefe = fe.$$

However, since $ef \in E(S)$, it follows that ef is its own unique inverse. Hence $ef = fe$ and therefore $E(S)$ is commutative, and so is a semilattice.

4(a) By uniqueness of inverses, it suffices to show that the given candidate for inverse in each case satisfies the equations for inverses. We certainly have $aa^{-1}a = a$ and $a^{-1}aa^{-1} = a^{-1}$ so that $(a^{-1})^{-1} = a$. Similarly we see that through the commutation of idempotents that:

$$ab \cdot b^{-1}a^{-1} \cdot ab = a(bb^{-1})(a^{-1}a)b = (aa^{-1}a)(bb^{-1}b) = ab;$$

$$b^{-1}a^{-1} \cdot ab \cdot b^{-1}a^{-1} = b^{-1}(a^{-1}a \cdot bb^{-1})a^{-1} = b^{-1}bb^{-1}a^{-1}aa^{-1} = b^{-1}a^{-1};$$

which shows that $(ab)^{-1} = b^{-1}a^{-1}$.

(b) Since $ef = fe$ we have $Sef \subseteq Sf$ and $Sef = Sfe \subseteq Se$ so that $Sef \subseteq Se \cap Sf$. Conversely let $x = ae = bf \in Se \cap Sf$. Then $x = bf = bf \cdot f = aef \in Sef$ so that $Se \cap Sf \subseteq Sef$ and therefore $Sef = Se \cap Sf$. Since $a = aa^{-1}a$ we have $Sa = Saa^{-1}a \subseteq Sa^{-1}a \subseteq Sa$ so that $Sa = Sa^{-1}a$. Replacing a by a^{-1} we then have $Sa^{-1} = S(a^{-1})^{-1}a^{-1} = Saa^{-1}$.

5. By Question 4(b) we have dom$\rho_a = Sa^{-1} = Saa^{-1}$. For any $x \in Saa^{-1}$ we may write $x = yaa^{-1}$ whence $x\rho_a = yaa^{-1}a = ya$ so that ran$\rho_a \subseteq Sa = Sa^{-1}a$, again by 4(b). Replacing a by a^{-1} we have $\rho_{a^{-1}} : Sa^{-1}a \to Saa^{-1}$. Hence for any $x \in Saa^{-1}$ so that $x = yaa^{-1}$ we have

$$x\rho_a\rho_{a^{-1}} = yaa^{-1}aa^{-1} = yaa^{-1} = x$$

and by the same argument with a replaced by a^{-1} we obtain that $x\rho_{a^{-1}}\rho_a = x$ for all $x \in Sa^{-1}a$. Therefore ρ_a, $\rho_{a^{-1}}$ are both bijections, so that $\rho_a, \rho_{a^{-1}} \in \mathcal{I}_X$ and $\rho_{a^{-1}} = \rho_a^{-1}$, $\rho_a = \rho_{a^{-1}}^{-1}$.

6. Suppose that $\rho_a = \rho_b$. Then the domains of these mappings are equal, so that $Saa^{-1} = Sbb^{-1}$ and then $aa^{-1} = bb^{-1}$ by uniqueness of idempotent

generators. Since $a^{-1} \in Saa^{-1}$ it follows that $a^{-1}\rho_a = a^{-1}\rho_b$, which is $a^{-1}a = a^{-1}b$.

$$a = aa^{-1}a = aa^{-1}b = bb^{-1}b = b.$$

7. To show that Φ is a homomorphism it is enough to show that $\mathrm{dom}\rho_{ab} = \mathrm{dom}\rho_a\rho_b$ (meaning that the result follows at once from this and associativity of S). First we have $\mathrm{dom}\rho_{ab} = Sab(ab)^{-1}$. On the other hand $\mathrm{dom}\rho_a\rho_b = (\mathrm{ran}\rho_a \cap \mathrm{dom}\rho_b)\rho_a^{-1}$

$$= (Sa^{-1}a \cap Sbb^{-1})\rho_a^{-1} = Sa^{-1}abb^{-1}\rho_a^{-1} = Sabb^{-1}a^{-1} \text{ (as } Sa^{-1}a = Sa)$$

$$= Sab(ab)^{-1} = \mathrm{dom}\rho_{ab}.$$

8. We have $a \in E(S/\rho)$ where S is regular. Put $e = axa$ where $x \in V(a^2)$. Then $e \in E(S)$ as

$$e^2 = axa \cdot axa = a \cdot xa^2x \cdot a = axa = e.$$

Moreover

$$e\rho = (axa)\rho = a\rho x\rho a\rho = a^2\rho x\rho a^2\rho = (a^2xa^2)\rho = a^2\rho = a\rho.$$

9. Let $\alpha : S \to T$ be a homomorphism from an inverse semigroup S onto a semigroup T. Certainly T is regular, and to show T is inverse it is then enough to show that if $e, f \in E(T)$ then $ef = fe$. By Lallement's lemma, since $T \cong S/\mathrm{ker}\alpha$, there exist idempotents $g, h \in E(S)$ such that $g\alpha = e$ and $h\alpha = f$. Then

$$ef = g\alpha h\alpha = (gh)\alpha = (hg)\alpha = h\alpha g\alpha = fe.$$

10. The final statement is demonstrated as follows:

$$aea' = aea'aa' = a(ea'a)^2a' = aea'aea'aa' = aea'aea',$$

with a similar line of proof to show that $a'ea$ is idempotent.

(i) implies (ii). Let $a, b \in S$ with $a' \in V(a)$, $b' \in V(b)$. Since S is orthodox we have

$$ab \cdot b'a' \cdot ab = aa'abb'a'abb'b = a(a'abb')^2b = aa'abb'b = ab$$

and similarly we may show that $b'a'abb'a' = b'a'$.

(ii) implies (iii). Since $xe, ex \in E(S)$ it follows from the given property that $ex^2e \in V(xe^2x)$. But $x = xe^2x$, which is inverse to ex^2e, and thus

$$x = x(ex^2e)x = (xex)(xex) = x^2.$$

(iii) implies (i). Let $e, f \in E(S)$ and take $x \in V(ef)$. Then $ef \in V(fxe)$ and $fxe \in E(S)$ as

$$ef \cdot fxe \cdot ef = efxef = ef, \ fxe \cdot ef \cdot fxe = fxe;$$

$$(fxe)^2 = fxe \cdot fxe = fxe.$$

It follows that $ef \in E(S)$ by the given property.

Problem Set 5

1. All Green's relations are equivalence relations. Let $a \,\mathcal{L}\, b$ and let $c \in S^1$. Then $S^1a = S^1b$, whence $S^1ac = S^1bc$ so that $ac \,\mathcal{L}\, bc$, thus showing thast $\mathcal{L}$ is a right congruence. Dually, $\mathcal{R}$ is a left congruence.

Comment This result does not imply that $\mathcal{H} = \mathcal{L} \cap \mathcal{R}$ is a congruence. Generally it is not.

2. Take $(a, b) \in \lambda \circ \rho$ so there exists $c \in S$ with $a \,\lambda\, c \,\rho\, b$, whence there exists $u, v \in S^1$ such that $a = uc$ and $b = cv$. It follows that $av = ucv = ub = d$, say. But $a \,\lambda\, c$ implies that $av \,\lambda\, cv$ as λ is a right congruence, which is to say $av \,\lambda\, d$, in other words $d \,\lambda\, b$. Dually $c \,\rho\, b$ implies $uc \,\rho\, ub$, which is $a \,\rho\, d$. Hence $a \,(\rho \circ \lambda)\, b$ and so $\lambda \circ \rho \subseteq \rho \circ \lambda$. Dually $\rho \circ \lambda \subseteq \lambda \circ \rho$. Therefore $\lambda \circ \rho = \rho \circ \lambda$, as required.

Comment In particular of course, we have the crucial equation $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$.

3(a) If $a \,\mathcal{L}\, b$ then $S^1a = S^1b$, whence $S^1aS^1 = S^1bS^1$, so that $\mathcal{L} \subseteq \mathcal{J}$. Dually $\mathcal{R} \subseteq \mathcal{J}$, whence $\mathcal{D} \subseteq \mathcal{J}$, as $\mathcal{D} = \mathcal{L} \vee \mathcal{R}$, is the smallest equivalence relation on S that contains $\mathcal{L} \cup \mathcal{R}$.

(b) Consder the relation $\mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$ by the Comment after Question 2. Since $\mathcal{L}$ and $\mathcal{R}$ are each relexive, for any $a \in S$ we have $a \,\mathcal{L}\, a \,\mathcal{R}\, a$ so that $\mathcal{L} \circ \mathcal{R}$ is reflexive. Suppose now that $a \,(\mathcal{L} \circ \mathcal{R})\, b$. Then there exists $c \in S$ such that $a \,\mathcal{L}\, c \,\mathcal{R}\, b$ so that $b \,(\mathcal{R} \circ \mathcal{L})\, a$. But by the comment of Question 2 we have $b \,(\mathcal{L} \circ \mathcal{R})\, a$, showing that $\mathcal{L} \circ \mathcal{R}$ is symmetric.

To see that $\mathcal{L} \circ \mathcal{R}$ is transitive, first note that $\mathcal{L} \circ \mathcal{L} = \mathcal{L}$ and $\mathcal{R} \circ \mathcal{R} = \mathcal{R}$ as, if $a \,\mathcal{L}\, c \,\mathcal{L}\, b$ then $S^1a = S^1c = S^1b$ so that $S^1a = S^1b$, with a similar remark applying to the $\mathcal{R}$ relation. Then since relational composition is itself associative we obtain:

$$(\mathcal{L} \circ \mathcal{R}) \circ (\mathcal{L} \circ \mathcal{R}) = (\mathcal{L} \circ \mathcal{R}) \circ (\mathcal{R} \circ \mathcal{L}) = \mathcal{L} \circ (\mathcal{R} \circ \mathcal{R}) \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R} \circ \mathcal{L}$$

$$= (\mathcal{L} \circ \mathcal{L}) \circ \mathcal{R} = \mathcal{L} \circ \mathcal{R},$$

which shows that $\mathcal{L} \circ \mathcal{R}$ is also transitive and is therefore an equivalence relation. Since $\mathcal{L}$ and $\mathcal{R}$ are reflexive, we conclude that $\mathcal{L} \circ \mathcal{R}$ is an equivalence relation that contains $\mathcal{L} \cup \mathcal{R}$. Since any equivalence relation that contains $\mathcal{L} \cup \mathcal{R}$ must contain $\mathcal{L} \circ \mathcal{R}$ (in order to be transitive) and since $\mathcal{D}$ is, by definition $\mathcal{L} \vee \mathcal{R}$, we conclude that $\mathcal{D} = \mathcal{L} \circ \mathcal{R} = \mathcal{R} \circ \mathcal{L}$.

(c) Suppose now that $a \,\mathcal{D}\, b$. This is equivalent to $a \,(\mathcal{L} \circ \mathcal{R})\, b$, which is to say that there exists $c \in S$ such that $a \,\mathcal{L}\, c \,\mathcal{R}\, b$. Dually $a \,\mathcal{D}\, b$ may be expressed as saying there exists $d \in S$ such that $a \,\mathcal{R}\, d \,\mathcal{L}\, b$.

4. Let $a_1, a_2 \in L$ and $b_1, b_2 \in R$. Since $\mathcal{L}$ is a right congruence, $a_1b_1 \,\mathcal{L}\, a_2b_1$. Since $\mathcal{R}$ is a left congruence, we have $a_2b_1 \,\mathcal{R}\, a_2b_2$, which is to say that $a_1b_1 \,\mathcal{L}\, a_2b_1 \,\mathcal{R}\, a_2b_2$. Therefore $a_1b_2 \,\mathcal{D}\, a_2b_2$, from which it follows that LR is contained in a single $\mathcal{D}$-class.

5(a) Let $\alpha, \beta \in \mathcal{T}_X$. There there exists $\gamma \in \mathcal{T}_X$ such that $\gamma\alpha = \beta$ implies that $X\beta = (X\gamma)\alpha \subseteq X\alpha$. Conversely assume that $X\beta \subseteq X\alpha$. Define $\gamma \in \mathcal{T}_X$ as follows: for each $y \in X\beta$, γ maps $y\beta^{-1}$ upon a single element in $y\alpha^{-1}$. Then $\gamma\alpha = \beta$. It follows that $L_\beta \leq L_\alpha$ iff $X\beta \subseteq X\alpha$. In particular we see then that $\alpha \,\mathcal{L}\, \beta$ iff $X\alpha = X\beta$.

(b) If $\alpha\gamma = \beta$, then for any $(x, y) \in \ker\alpha$ we have

$$x\beta = x\alpha\gamma = y\alpha\gamma = y\beta,$$

which implies that $\ker\beta \subseteq \ker\alpha$. Conversely suppose that $\ker\beta \subseteq \ker\alpha$. Define γ on $X\alpha$ by $x\alpha\gamma = x\beta$ $(x \in X)$. To see that γ is well-defined, suppose that $x\alpha = y\alpha$. Then $x\beta = y\beta$ by hypothesis. Define γ to act in any way on $X \setminus X\alpha$. Then by construction $\alpha\gamma = \beta$.

Hence $R_\beta \leq R_\alpha$ iff $\ker\beta \subseteq \ker\alpha$. It follows that $\alpha \,\mathcal{R}\, \beta$ iff $\ker\alpha = \ker\beta$.

(c) This is immediate from (a) and (b) as $\mathcal{H} = \mathcal{L} \cap \mathcal{R}$.

(d) Let $\alpha, \beta \in \mathcal{T}_X$. If $\alpha \,\mathcal{D}\, \beta$, then $\alpha \,\mathcal{L}\, \gamma \mathcal{R}\, \beta$ for some $\gamma \in \mathcal{T}_X$. By (a), α and γ have the same range, and so share a common rank; similarly by (b), β and γ have the same kernel, and so the same rank. Hence $\text{rank}\alpha = \text{rank}\beta$. Conversely, suppose that $\text{rank}\alpha = \text{rank}\beta$. Then $|X\alpha| = |X/\ker\beta|$, and so there exists $\gamma \in \mathcal{T}_X$ with $\ker\gamma = \ker\beta$ and $X\alpha = X\gamma$, whence $\alpha \,\mathcal{L}\, \gamma \,\mathcal{R}\, \beta$, and so $\alpha \,\mathcal{D}\, \beta$.

(e) Since $\mathcal{D} \subseteq \mathcal{J}$ is always true, if follows from (d) that it is enough to prove that if $J_\beta \leq J_\alpha$ then $\text{rank}\beta \leq \text{rank}\alpha$. However $J_\beta \leq J_\alpha$ implies that $\beta = \gamma\alpha\delta$ say $(\gamma, \delta \in \mathcal{T}_X)$. Hence

$$|X\beta| = |X\gamma\alpha\delta| \leq |X\alpha\delta| \leq |X\alpha|,$$

which yields the claim.

6. That ρ_s maps L_a into L_b follows as $\mathcal{L}$ is a right congruence: $c \,\mathcal{L}\, a$ implies $cs \,\mathcal{L}\, ax = b$. Let $x \in L_a$; then there exists t in S^1 such that $x = ta$, whence

$$x\rho_s\rho_{s'} = xss' = tass' = tbs' = ta = x.$$

By applying the same argument to L_b and $\rho_{s'}$ we see that $\rho_s|_{L_a}$ and $\rho_{s'}|_{L_b}$ are mutually inverse bijections.

Finally note that if $x \in L_a$ and $y = x\rho_s = xs$, then $ys' = x$, so that $y \mathcal{R} x$. Similarly, $\rho_{s'}|_{L_b}$is $\mathcal{R}$-class preserving.

7. *Green's Lemma* (left hand version) Let $a \,\mathcal{L}\, b$ $(a, b \in S)$ and take $s, s' \in S^1$ such that $sa = b$ and $s'b = a$. Then the mappings $\lambda_s|R$ and $\lambda_{s'}|R_b$ are mutually inverse, $\mathcal{L}$-class preserving bijections of R_a onto R_b and of R_b onto R_a respectively.

Now let $H_a = L_a \cap R_a$ and $H_b = L_b \cap R_b$ be two $\mathcal{H}$-classes within the same $\mathcal{D}$-class of S. Let $H_c = L_b \cap R_a$. By Green's lemma, there exists an $\mathcal{R}$-class preserving bijection $\rho_a : L_a \to L_b$, so it follows that $H_a\rho_a = R_a \cap L_b = H_c$. Hence $\rho_a|_{H_a}$ is a bijection onto H_c. By the dual of Greens' lemma, it follows that there exists a bijection $\lambda_b : H_c \to H_b$. Therefore the composition mapping $\rho_a\lambda_b : H_a \to H_b$ is a bijection between two arbitrary $\mathcal{H}$-classes within a given $\mathcal{D}$-class. In particular, any two $\mathcal{H}$-classes within the same $\mathcal{D}$-class of a semigroup S share the same cardinality.

8(a) Since $ab \in R_a \cap L_b$, by Green's lemma ρ_b is an $\mathcal{R}$-class preserving bijection of L_a onto L_{ab} so there exists $c \in R_b \cap L_a$ such that $c\rho_b = cb = b$. Since $c\,\mathcal{R}\,b$ there exists $u \in S$ such that $c = bu$. It follows that $bub = cb = b$ and thus $c^2 = bubu = bu = c$, so that $c \in E(S) \cap R_b \cap L_a$, as claimed.

(b) and (c). Conversely, if $e = e^2 \in R_b \cap L_a$ then $b = ex$ say and so $eb = e^2x = ex = b$. Dually we get $ae = a$.

From $e\,\mathcal{R}\,b$ and the fact that $\mathcal{R}$ is a left congruence we deduce that $a = ae\,\mathcal{R}\,ab$ and from $e\,\mathcal{L}\,a$ and the fact that $\mathcal{L}$ is a right congruence we obtain $b = eb\,\mathcal{L}\,ab$. This shows that $ab \in R_a \cap L_b$.

9. (i) implies (ii). Let $e \in H \cap E(S)$. Putting $a = b = e$ we get $ab = e^2 = e \in H$.

(ii) implies (i). Let $a, b \in H$ such that $ab \in H$. By Miller and Clifford's theorem we have $ab \in R_a \cap L_b (= R_a \cap L_a = H)$ iff $R_b \cap L_a (= R_a \cap L_a = H)$ contains an idempotent e, as required.

(i) & (ii) implies (iii). Since there exists $a, b \in H$ such that $ab \in H$, it follows from Miller and Clifford that H is a subsemigroup of S and H contains an idempotent e and that by Green's lemma it follows that for each $c \in H$, $\rho_c|_H$ and $\lambda_c|_H$ are bijections of H. In particular, there exists $p, q \in H$ such that $cp = qc = e$, thus showing that H is a subgroup of S.

Now let G be any subgroup of S such that $G \cap H \neq \emptyset$. Since the $\mathcal{H}$-relation within a group is universal, it follows that G is contained within a single $\mathcal{H}$-class of S, whence $G \subseteq H$. Hence H contains every subgroup that meets H. In particular H is a maximal subgroup of S.

(iii) implies (i). Since the $\mathcal{H}$-class H is a group, H contains an idempotent e.

10. Let H_e and H_f be two $\mathcal{H}$-classes within the same $\mathcal{D}$-class with $e, f \in E(S)$. Take $a \in R_e \cap L_f$. Then $ea = a$ and $a'a = f$ for some $a' \in S$. As above, the mapping $\rho_a\lambda_{a'}$ defines a bijection of H_e onto H_f in which e is mapped to $a'ea = a'a = f$. Note that $aa'a = af = a$, whence $aa' \in E(S)$ and $aa'\mathcal{R}a$. Hence for any $z \in R_a$ we have $aa'\mathcal{R}z$ and thus $aa'z = z$. In particular for any $y \in H_e$, $aa'y = y$.

In order to complete the proof we verify that the bijection of H_e onto H_f whereby $x \mapsto a'xa$ is a homomorphism. To see this, take any $x, y \in H_e$. We obtain

$$a'xya = a'x(aa'y)a = (a'xa)(a'ya)$$

as required.

Problem Set 6

1(a) Let $a \in \mathrm{Reg}(S)$ with $a' \in V(a)$. Then since $(aa')a = a$ it follows that $a\mathcal{R}aa'$ and $aa' \in E(S)$ as $(aa')^2 = (aa'a)a' = aa'$. Dually $a\mathcal{L}a'a$ and $a'a \in E(S)$.

(b) Suppose that for some $b \in R_a$ we have $a\mathcal{R}e$ for some $e \in E(S)$ so that $e = by$ say $(y \in S^1)$. Then $b = eb = byb$ so that $yby \in V(b)$. From this observation, its left-right dual, and part (a), it follows that if $a \in S$ is regular, then all members of $R_a \cup L_a$ are regular.

Now take any $b \in D_a$ and let $c \in R_a \cap L_b$ (which exists, as all the intersections of an $\mathcal{R}$-class and an $\mathcal{L}$-class within a $\mathcal{D}$-class is an $\mathcal{H}$-class and all $\mathcal{H}$-classes within the same $\mathcal{D}$-class are equicardinal). Then it follows from the previous paragraph that c is regular, so that all members of L_c are also regular. In particular this applies to b. Therefore we may conclude that if D contains one regular element a then all members of D are regular.

(c) Let $(a, a') \in V(S)$. Then we have $a\mathcal{R}aa'\mathcal{L}a'$ so that $(a, a') \in \mathcal{D}$. It follows that $V(a) \subseteq D_a$.

2. Let $a \in S$ and suppose that $b \in V(S)$. Then $a\mathcal{R}ab\mathcal{L}b$ and $a\mathcal{L}ba\mathcal{R}b$. Hence we have idempotents $e = ab$ and $f = ba$ such that $e \in R_a \cap L_b$ and $f \in L_a \cap R_b$, thus proving the theorem in the forward direction.

Conversely suppose that we are given that there are idempotents e and f where $e \in R_a \cap L_b$ and $f \in L_a \cap R_b$. By Miller and Clifford's theorem $ab \in H_e$ and $ba \in H_f$. By Green's lemma, ρ_a defines a bijection of L_b onto L_a and thus there exists a unique $x \in H_b$ such that $xa = f$. Since $af = a$ it follows that $axa = af = a$. Furthermore, $ax \in E(S)$ and since λ_a defines an $\mathcal{L}$-class-preserving bijection from R_b onto R_a it follows that $ax \in H_e$, and so $ax = e$. But then $x = xe = xax$. We conclude that x is the unique inverse of a in H_b.

3(a) Since $SL \subseteq L$ and $RS \subseteq R$ it follows more particularly that $RL \subseteq L \cap R$. Suppose now that S is regular and that $a \in L \cap R$. Take $b \in V(a)$. Then $ba \in L$ and so $a = a \cdot ba \in RL$.

(b) Suppose that $a\mathcal{L}b$ so there exists $x, y \in S^1$ such that $xa = b$ and $yb = a$. But then $yxa = yb = a$, whence $(yx)^2a = yxa$, whence by right cancellativity $yx = (yx)^2$ so that $yx \in E(S^1)$. However, since $E(S) = \varnothing$, it follows that $yx = 1$ and so $x = y = 1$ and $a = b$. Therefore all $\mathcal{L}$-classes of a right cancellative semigroup without idempotents are trivial.

4. H is the $\mathcal{H}$-class of $\mathcal{T}_X$ of all α such that $\mathrm{ker}\alpha = \Pi$ and $X\alpha = Y \subseteq X$. Let $\varepsilon \in E(H)$. Thus $Y = X\varepsilon$, $\Pi = \Pi_\varepsilon = \mathrm{ker}\varepsilon$, and $\varepsilon^2 = \varepsilon$. Let $x \in X$. Since $x\varepsilon = (x\varepsilon)\varepsilon$ it follows from $\Pi = \Pi_\varepsilon$ that $(x, x\varepsilon) \in \Pi$. On the other hand, if $(y, y') \in \Pi$, with $y, y' \in Y$ then $y = y\varepsilon = y'\varepsilon = y'$. It follows that each class of Π contains exactly one element $y \in Y$, and that ε maps every element of $y\Pi^\natural$ $(y \in Y)$ onto y.

Conversely assume that Y is a transversal of Π. Then the member $\varepsilon \in \mathcal{T}_X$ that maps each element each class C of Π to $y \in Y \cap C$ is an idempotent element of H and so H is a group (by Question 9, Set 5).

We continue under the assumption that H is a group with idempotent ε, which is then the identity element of the group H. We now show that $\alpha \in H$ induces a permutation of Y in that $\alpha|_Y \in \mathcal{G}_Y$. Certainly $Y\alpha \subseteq Y$. Moreover $\alpha|_Y$ is one-to-one for if $y\alpha = y'\alpha$ $(y, y' \in Y)$ then $(y, y') \in \Pi$, and so $y = y'$. Also $\alpha|_Y$ is onto Y (which does not follow immediately as there is no assumption that Y is finite) for given $y \in Y = X\alpha$, there exists $x \in X$ such that $x\alpha = y$. Then $x\varepsilon \in Y$ and since $(x, x\varepsilon) \in \Pi$, we get $(x\varepsilon)\alpha = x\alpha = y$. Hence $\alpha|_Y \in \mathcal{G}_Y$, the symmetric group on Y. Moreover every element $\phi \in \mathcal{G}_Y$ is induced in this way by some element α of H, namely that defined by $x\alpha = (x\varepsilon)\phi$. Furthermore α is unique in this regard for if $y\alpha = y\beta$ for all $y \in Y$ with $\alpha, \beta \in H$ then $x\varepsilon\alpha = x\varepsilon\beta$ for all $x \in X$, and so $\alpha = \varepsilon\alpha = \varepsilon\beta = \beta$. Hence the mapping $\alpha \mapsto \phi = \alpha|_Y$ is a one-to-one mapping of H onto $\mathcal{G}_Y$. To see this is a homomorphism (and hence an isomorphism of$H$ onto $\mathcal{G}_Y$) we need to check that if $\alpha, \beta \in H$ then $(\alpha|_Y)(\beta|_Y) = (\alpha\beta)|_Y$. However this follows immediately from the fact that $Y\alpha \subseteq Y$ (indeed $Y\alpha = Y$).

5. Following the hint, we put $f = eb'b$ where $b' \in V(b)$. Then since $a \in \mathrm{Reg}(S)$ it follows that L_a is regular and there exists an idempotent $e\mathcal{L}a$ (can take $e = a'a$ for any $a' \in V(a)$) and then $ae = a$. Since $L_a \geq L_b$ we have that $b = xa$ for some $x \in S^1$. Hence

$$f^2 = eb'b \cdot eb'b = eb'xaeb'b = eb'xab'b = eb'bb'b = eb'b = f,$$

so that $f \in E(S)$. Moreover $f\mathcal{L}b$ as $f = (eb')b$ and $bf = xa \cdot eb'b = xab'b = bb'b = b$. Finally $e \geq f$ as $ef = e \cdot eb'b = eb'b = f$ and $fe = eb'be = eb'xae = eb'xa = eb'b = f$.

6(a) We have $a = bx$ for some $x \in S^1$. Take $b' \in V(b) \cap U$ so that $a = bx = bb'bx = bb'a$, and since $b'a \in U$, this shows that $R'_a \leq R'_b$.

(b) If $a \leq_{\mathcal{L}'} b$ then $a = ub$ for some $u \in U \leq S$ so that $a \leq_{\mathcal{L}} b$. It follows that $\mathcal{L}' \subseteq \mathcal{L} \cap (U \times U)$, with similar inequalities for $\mathcal{R}$ and $\mathcal{H}$. Next let $a, b \in \mathrm{Reg}(U)$ with $R_a = R_b$ (respectively $L_a = L_b, H_a = H_b$) then by (a) we have $R'_a = R'_b$ (respectively $L'_a = L'_b, H'_a = H'_b$). Hence if U is regular then $\mathcal{G}' = \mathcal{G} \cap (U \times U)$ for $\mathcal{G} \in \{\mathcal{L}, \mathcal{R}, \mathcal{H}\}$.

7. Let $a, b \in D$. Since D is a $\mathcal{D}$-class of$S$, there exists $c \in D$ such that $a\mathcal{L}^S c\mathcal{R}^S b$. Since D is a regular subsemigroup of S, we have by Question 6(b) that $a\mathcal{L}^D c\mathcal{R}^D b$, showing that D has a single $\mathcal{D}$-class.

8. In any semigroup S we have $\mathcal{D} \subseteq \mathcal{J}$. Conversely suppose that S is finite and that $a\mathcal{J}b$ for some $a, b \in S$. Then there exists $u, v, x, y \in S^1$ such that $a = ubv$ and $b = xay$. Hence for any $n \geq 1$ we have $a = (ux)^n a(yv)^n$ and $b = (xu)^n b(vy)^n$. Since S is finite, it follows that we may choose n such that each of these powers is idempotent (as, in general, if x^k and y^l are idempotent then x^{kl} and y^{lk} are both idempotent). Then $a(yv)^n = (ux)^n a(yv)^{2n} = (ux)^n a(yb)^n = a$; similarly $a = (ux)^n a$, $b = (xu)^n b = b(vy)^n$. Put $c = xa$, so that $a = (ux)^{n-1}uc$

and so $a\mathcal{L}c$. Now $cy = xay = b$. Moreover

$$c = xa = x(ux)^{n+1}a(yv)^{n+1} = (xu)^{n+1}xay(vy)^n v = (xu)^{n+1}b(vy)^n v$$
$$= (xu)^{n+1}b(vy)^{2n}v = b(vy)^{n-1}v,$$

and this final equation allows us to conclude that $a\mathcal{L}c\mathcal{R}b$, whence $a\mathcal{D}b$ and therefore $\mathcal{J} \subseteq \mathcal{D}$. Therefore, in a finite semigroup S, $\mathcal{D} = \mathcal{J}$.

9. Let D be a $\mathcal{D}$-class of S. As was shown in Question 9 Set 5, any subgroup G of a semigroup S is contained in a single $\mathcal{H}$-class, which is then a maximal subgroup of S. Since S is a union of groups, it follows that D consists of (disjoint) $\mathcal{H}$-classes each of which are mutually isomorphic groups. For any $a, b \in D$ it follows that $ab \in R_a \cap L_b$ and in particular D is a regular subsemigroup of S. By Question 7, it follows that D is itself a regular semigroup consisting of a single $\mathcal{D}$-class. (We say that such a semigroup is *bisimple*; a semigroup with a single $\mathcal{J}$-class is called *simple.*)

10(a) Since $\mathcal{D} \subseteq \mathcal{J}$ it follows that $\mathcal{D}^* \subseteq \mathcal{J}^*$. To show that $\mathcal{J}^* \subseteq \eta$ it follows, since η is a congruence, that it is enough to show that $\mathcal{J} \subseteq \eta$. To this end take $a\mathcal{J}b$ in S so there exists $x, y, u, v \in S^1$ such that $a = xby$ and $b = uav$. But then

$$a = xby\,\eta\,xb^2y\,\eta\,xbyb = ab\eta ba\,\eta\,uava\,\eta ua^2v\,\eta uav\,\eta\,b,$$

as required. Therefore in any semigroup we have $\mathcal{D}^* \subseteq \mathcal{J}^* \subseteq \eta$.

Comment There reverse containment, $\eta \subseteq \mathcal{J}^*$ is generally false: for example, taking $S = (\mathbb{N}^+, +)$ we see that $\mathcal{J}^*$ is trivial but η is universal.

(b) This is checked directly:

$$ef \cdot fye \cdot ef = efyef = ef;\; fye \cdot ef \cdot fye = f(yefy)e = fye;$$

hence $fye \in V(ef)$ and fye is itself an idempotent.

Comment Since the inverse x of an idempotent e is always the product of two idempotents, as $x = xex = (xe)(ex)$ it follows from (b) that in a regular semigroup it is always the case that $V(E) = E^2$. Indeed an extension of the previous argument shows that in a regular semigroup $V(E^n) = E^{n+1}$. In particular it follows that the idempotent-generated subsemigroup of a regular semigroup is itself regular.

(c) It is enough to show that $\eta_0 \subseteq \mathcal{D}^*$ for, given this we have by part (a) that

$$\eta = \eta_0^* \subseteq (\mathcal{D}^*)^* = \mathcal{D}^* \subseteq \mathcal{J}^* \subseteq \eta,$$

giving equality throughout.

Now for any $a \in S$ take $a' \in V(S)$. Then $a\mathcal{D}aa'$, whence $a^2\mathcal{D}^*aa'a = a$ so that $(a, a^2) \in \mathcal{D}^*$. Now take $e, f \in E(S)$ and let $y \in V(ef)$. By (b) we have $fye \in V(ef)$ and so

$$ef\mathcal{D}fye \Rightarrow fefe\mathcal{D}^*f^2ye^2 = fye.$$

But then

$$fe\mathcal{D}^*(fe)^2 = f(ef)f\mathcal{D}^*f(fye)e = fye\mathcal{D}^*ef.$$

Finally take $a, b \in S$. Then

$$ab\mathcal{D}^* aa'bb'\mathcal{D}^* bb'aa'\mathcal{D}^* ba,$$

thus showing that $\eta_0 \subseteq \mathcal{D}^*$ as required. Therefore, in a regular semigroup, $\mathcal{D}^* = \mathcal{J}^* = \eta$.

Problem Set 7

1(a) Suppose that S has only one ideal, which must then by S itself. For any $a \in S$, S^1aS^1 is an ideal, so it follows that for all $a, b \in S$, we have $S^1aS^1 = S = S^1bS^1$. Hence $a\mathcal{J}b$ and so S consists of a single $\mathcal{J}$-class. Conversely suppose that $a\mathcal{J}b$ for all $a, b \in S$, which is to say that $S^1aS^1 = S^1bS^1$ for all $a, b \in S$. Since $b \in S^1bS^1$ it follows that $b \in S^1aS^1$, whence it follows that $S^1aS^1 = S$ for all $a \in S$. Now let I be any ideal of S and take any $a \in I$. Then we have $S = S^1aS^1 \subseteq I \subseteq S$. Therefore the only ideal I of S is S itself.

(b) Suppose that $SaS = S$ for all $a \in S$. Then $S^1aS^1 = S$ for all $a \in S$ so that S is a simple semigroup. Conversely suppose that S is simple. For any $a \in S$, SaS is an ideal of S so that $SaS = S$.

(c) Suppose that S has a zero element 0 and that the only ideals of S are S and $\{0\}$. Given that $S^2 \neq \{0\}$, then in particular S is not a two-element null semigroup.

Conversely suppose that S has a zero element, the only ideals of S are S and $\{0\}$ and that S is not a two-element zero semigroup.

Take $a \in S$ and suppose that $S \setminus a$ is an ideal of S. Then $S \setminus a = \{0\}$ so that $S = \{a, 0\}$. Moreover, $a^2 = a$ as otherwise $S^2 = \{0\}$ and S is a two-element null semigroup. (Hence in this case S is the two-element semilattice.) Otherwise, for every $a \in S \setminus \{0\}$, $S \setminus a$ is not an ideal of S. It follows that for any non-zero member a of S, $a = xy$ for some $x, y \in S$. In particular $S^2 \neq \{0\}$. Therefore, the additional restriction that $S^2 \neq \{0\}$ is equivalent to the additional restriction that S is not the two-element null semigroup.

2(a) If $ea = a$ then $e^2a = ea$, whence $e^2 = e$. Any idempotent in a cancellative semigroup is the identity (Question 1, Set 1); contradicting hypothesis. Dually $ae = a$ is impossible.

If $\mathcal{D}$ were non-trivial then at least one of $\mathcal{R}$ and $\mathcal{L}$ is non-trivial. Let us suppose that $\mathcal{R} \neq \iota$ (the argument is dual in case $\mathcal{L} \neq \iota$). Then there exists a and b with $a \neq b$ such that $a\mathcal{R}b$ in S. Hence there exists $x, y \in S$ such that $ax = b$ and $by = a$, whence $a = a(xy)$, which we have shown is impossible in S.

(b) Let $A, X \in S$ with

$$A = \begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix}, \ X = \begin{bmatrix} x & 0 \\ y & 1 \end{bmatrix}$$

$$\Rightarrow AX = \begin{bmatrix} ax & 0 \\ bx+y & 1 \end{bmatrix} \in S,$$

Hence S is a semigroup without identity element as one may check that $AJ = A$ implies $j = I_2 \notin S$. Next suppose that $AX = AY$, so we have products according to

$$AX = AY = \begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} \begin{bmatrix} u & 0 \\ v & 1 \end{bmatrix} = \begin{bmatrix} au & 0 \\ bu+v & a \end{bmatrix};$$

then $au = ax$, so that $u = x$; $bx + y = bu + v$ then gives $y = v$ (since $u = x$), so S is left cancellative.

If $XA = YA$, which is to say

$$\begin{bmatrix} xa & 0 \\ ya+b & 1 \end{bmatrix} = \begin{bmatrix} ua & 0 \\ va+b & 1 \end{bmatrix},$$

then $xa = ua$, whence $x = u.ya + b = va + b$, so that $y = v$. Therefore S is a cancellative semigroup without identity and so, by part (a), S is $\mathcal{D}$-trivial.

(c) Yet S is $\mathcal{J}$-simple. We require x, y, u, v which solve

$$\begin{bmatrix} x & 0 \\ y & 1 \end{bmatrix} \begin{bmatrix} a & 0 \\ b & 1 \end{bmatrix} \begin{bmatrix} u & 0 \\ v & 1 \end{bmatrix} = \begin{bmatrix} c & 0 \\ d & 1 \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} xa & 0 \\ ya+b & 1 \end{bmatrix} \begin{bmatrix} u & 0 \\ v & 1 \end{bmatrix} = \begin{bmatrix} c & 0 \\ d & 1 \end{bmatrix}$$

$$\Leftrightarrow \begin{bmatrix} xau & 0 \\ (ya+b)u+v & 1 \end{bmatrix} = \begin{bmatrix} c & 0 \\ d & 1 \end{bmatrix}$$

$$\Leftrightarrow a \cdot xu = c; \ (ya+b)u + v = d.$$

Solving the second equation gives:

$$y = \frac{1}{a}(\frac{d-v}{u} - b) = \frac{d-v-bu}{au}.$$

We require that

$$d - v - bu > 0 \Leftrightarrow v + bu < d \Leftrightarrow u < \frac{d-v}{b}.$$

Choose v such that $0 < v < d$, then take u such that $0 < u < \frac{d-v}{b}$. Then $y = \frac{d-v-bu}{au}$; $x = \frac{c}{au}$.

3(a) The number of minimal ideals of S is either 0 or 1 for if M and N were two minimal ideals of S then MN is an ideal of S and $MN \subseteq M \cap N$. In particular $M \cap N \neq \emptyset$ and is an ideal contained in each of the minimal ideals M and N, which is only possible of $M = N$.

(b) Let I be an ideal of the kernel K of S. Then

$$I \supseteq KIK \supseteq S^1KIKS^1 \supseteq K \supseteq I,$$

where the third containment is so because S^1KIKS^1 is an ideal of S and K is the minimal ideal of S. Therefore $I = K$, which is therefore a simple semigroup.

(c) Let S be a finite semigroup, which then has finitely many ideals $I_1, \cdots, I_k$. Then $K = I_1 \cdots I_k$ is an ideal of S and $K \subseteq I_i$ for all $1 \leq i \leq k$ and so K is the kernel of S. From (b) it now follows that every finite semigroup S has a simple kernel.

(d) Suppose that S is 0-simple. Then S^2 is an ideal of S, $S^2 \neq \{0\}$, whence $S^2 = S = S^3$. For any $\in S$, SaS is an ideal of S, which implies that $SaS = S$ or $SaS = \{0\}$. The subset $I = \{x \in S : SxS = \{0\}\}$ is an ideal of S containing 0, whence $I = \{0\}$, as otherwise $I = S$ and $S^3 = S^2 = \{0\}$. Hence $SaS = S$ for all $a \in S \setminus \{0\}$. Conversely suppose that S has a zero 0 and that for all non-zero a we have $SaS = S$. Let I be a non-zero ideal of S and take $a \in I$. The $I \supseteq SaS = S$. This serves to show that S is indeed a 0-simple semigroup.

4. If $M^2 \neq \{0\}$ then $M^2 = M = M^3$. Take $a \in M \setminus \{0\}$. Then S^1aS^1 is an ideal of S and is not $\{0\}$, whence $S^1aS^1 = M$. Thus

$$MaM \subseteq S^1aS^1 = M = M^3 = M(S^1aS^1)M = (MS^1)a(S^1M) = MaM,$$

and so $MaM = M$, which proves the result.

5. Let $\mu : I \to I/J$ be the natural homomorphism of I onto I/J so that $a\mu = a$ if $a \in I \setminus J$ and $a\mu = J$ if $a \in J$. Then, quite generally, there is a one-to-one order-preserving correspondence between the set of ideals of S lying between J and I and the ideals of I/J. We are given here that there are no ideals of S strictly between J and I, and therefore the only ideals of J/I are J and I. Hence I/J is a 0-minimal ideal of I/J and so by Question 4, I/J is either 0-simple or a null semigroup (which is the case iff $I^2 \subseteq J$).

6. Let $J = J_a$ be a $\mathcal{J}$-class of S and write $J(a) = S^1aS^1$ for the principal ideal generated by a. Let $I_a = \{b \in J(a) : J_b < J_a\}$. If I_a is empty then $J(a) = S^1aS^1 = J_a$ is the kernel of S. Otherwise I_a is an ideal of S contained in $J(a)$. Moreover, suppose that B were an ideal of S such that $I_a \subseteq B \subset J(a)$ and let $b \in B$. Then clearly $J_b < J_a$ and so $b \in I_a$. Since b was arbitrary we infer that $B = I_a$. Therefore the factor semigroup $J(a)/I_a$ is either 0-simple or null.

Comment The semigroups K and $J(a)/I_a$ are called *principal factors* of S. A semigroup is called *semisimple* if none of its principal factors are null. A principal factor J/I can be thought of as the $\mathcal{J}$-class J together with 0 and for any $a, b \in J$ the product of a and b is ab if $ab \in J$ and is 0 otherwise.

7(a) Let $a \in S$ and take $x \in V(a)$ such that $ax = xa$. Then $ax \in E(S)$ and $a\mathcal{R}ax = xa\mathcal{L}a$, which is to say that $a\mathcal{H}ax$ and so H_a is a group $\mathcal{H}$-class. Since a was arbitrary, it follows that S is a union of groups. Conversely, suppose that S is a union of groups. For $a \in S$ let x be the inverse of a in a subgroup of S that contains a. Then $ax = xa$, which shows that S is completely regular.

(b) Let D be a $\mathcal{D}$-class of a completely regular semigroup S. Since each $\mathcal{H}$-class is then a group, it follows by the location theorem that for any $a, b \in S$, we have $ab \in R_a \cap L_b$. In particular, $ab \in D$ so that D is a regular subsemigroup of S. Then by Question 7 of Set 6, it follows that D is a regular bisimple semigroup. Let $e, f \in E(D)$ and suppose that $e \leq f$. Then $e = ef \in R_e \cap L_f$ and $e = fe \in R_f \cap L_e$. Hence $f \in H_e$, whence $e = f$ as an $\mathcal{H}$-class has at most one idempotent. Hence all idempotents of D are primitive idempotents, whence D is a completely simple semigroup.

Finally, we note that all $\mathcal{H}$-classes of D are $\mathcal{H}$-classes of S and by Question 10 of Set 5, all are mutually isomorphic subgroups of D.

8(a) First we show that $\eta_0 = \{(a, a^2), (ab, ba),\ a, b \in S\} \subseteq \mathcal{J}$. Now since S is a union of groups, it follows that $a\mathcal{H}a^2$, so certainly $a\mathcal{J}a^2$. Then

$$J_{ab} = J_{(ab)^2} = J_{a(ba)a} \leq J_{ba};$$

equally of course, $J_{ba} \leq J_{ab}$ and so we conclude that $ab\mathcal{J}ba$. Therefore $\eta_0 \subseteq \mathcal{J}$. It follows that if we show that $\mathcal{J}$ is a congruence on S we may conclude that $\eta \subseteq \mathcal{J}$ and that $S/\mathcal{J}$ is a semilattice. By symmetry, it is enough to show that $\mathcal{J}$ is a right congruence on S. To this end, let us take $a\mathcal{J}b$ and $c \in S$. Then there exists $x, y, u, v \in S^1$ such that $b = xay$ and $a = ubv$. Then

$$J_{ca} = J_{cubv} \leq J_{cub} = J_{bcu} \leq J_{bc} = J_{cb};$$

by the same argument, we obtain $J_{cb} \leq J_{ca}$ and so $J_{ca} = J_{cb}$, thereby establishing that $\mathcal{J}$ is a right congruence, and therefore, as already observed, is thus a congruence on S.

(b) Since $\mathcal{J} \subseteq \eta$ is always true in any semigroup (Question 10, Set 6) and that for a completely regular semigroup $\eta \subseteq \mathcal{J}$ by part (a), it follows that $\mathcal{J} = \eta$ for a completely regular semigroup.

9. Let S be a simple and completely regular semigroup. We show that S is completely simple by showing that any $e \in E(S)$ is a primitive idempotent. To this end, suppose that $e, f \in E(S)$ with $f \leq e$. Take $z, t \in S$ such that $e = zft$. Put $x = ezf$ and $y = fte$. Then

$$xfy = ezf^3te = e(zft)e = e^3 = e \text{ and } ex = xf = x,\ fy = ye = y.$$

Since S is completely regular, we have $x \in H_g$ for some $g \in E(S)$. Thus $gx = xg = x$ and therefore there exists $x* \in H_g$ such that $xx* = x * x = g$. From $xf = x$ it follows that $x * xf = xx*$, whence $gf = g$. We also have

$$gf = gef = gxfyf = ef = f.$$

Hence $g = f$. Therefore $f = fe = ge = gxfy = xfy = e$, as required.

10. We need to show that $\mathcal{D} = \mathcal{J}$. Since each $\mathcal{J}$-class J is an η-class of S, it follows that J is a regular subsemigroup of S and a union of groups. By Question 6, J is a simple semigroup, and so is completely simple by Question 9. It follows that J is indeed a $\mathcal{D}$-class, and that S is a semilattice of completely simple semigroups. I

Problem Set 8

1 (i) implies (ii). Let D be a $\mathcal{D}$-class of S. Since S is regular, D contains at least one idempotent. Suppose that $e\mathcal{D}f$ with $e, f \in E(S)$. Then there exists $a \in S$ such that $e\mathcal{L}a\mathcal{R}f$, and thus for some $x \in S^1$, $e = xa$ whence, since idempotents are central, $e = xa = xfa = fxa = fe = ef$; similarly we may show that $f = ef$, so that $e = f$.

(ii) implies (iii). The given condition implies that each $\mathcal{D}$-class is a group $\mathcal{H}$-class. Since $\mathcal{D} \subseteq \eta$, it follows that each η-class is a union of groups, and so S is also. It follows now that S is a semilattice of groups.

(iii) implies (iv). Let S be a semilattice Y of groups G_α $(\alpha \in Y)$ and for each $\alpha \in Y$, let e_α be the identity of G_α. Then the mappings $\phi_{\alpha,\beta} : G_\alpha \to G_\beta$ $(\alpha \geq \beta)$ defined by

$$a_\alpha \phi_{\alpha,\beta} = a_\alpha e_\beta \ (a_\alpha \in G_\alpha)$$

is a homomorphism as, using that $\alpha\beta = \beta$ we get

$$(a_\alpha b_\alpha)\phi_{\alpha,\beta} = (a_\alpha b_\alpha)e_\beta = a_\alpha b_\alpha e_\beta^2 = a_\alpha e_\beta b_\alpha e_\beta = a_\alpha \phi_{\alpha,\alpha\beta} b_\alpha \phi_{\alpha,\alpha\beta};$$

$$a_\alpha \phi_{\alpha,\alpha} = a_\alpha e_\alpha = a_\alpha;$$

and so $\phi_{\alpha,\alpha}$ acts identically on S_α. For $\alpha \geq \beta \geq \gamma$ we have

$$a_\alpha \phi_{\alpha,\beta} \phi_{\beta,\gamma} = a_\alpha e_\beta e_\gamma = a_\alpha e_\gamma = a_\alpha \phi_{\alpha,\gamma};$$

and for any $\alpha, \beta \in Y$ we have

$$(a_\alpha \phi_{\alpha,\alpha\beta})(b_\beta \phi_{\beta,\alpha\beta}) = a_\alpha e_{\alpha\beta} b_\beta e_{\alpha\beta} = a_\alpha b_\beta e_{\alpha\beta}^2 = a_\alpha b_\beta e_{\alpha\beta} = a_\alpha b_\beta.$$

Hence the mappings $\phi_{\alpha,\beta}$ satisfy the requirements for a family of strong homomorphisms that define the original multiplication of S, so that S is indeed a strong semilattice of groups $S = (Y, G_\alpha, \phi_{\alpha\beta} : \alpha \geq \beta \in Y)$.

(iv) implies (i). If S is a strong semilattice of groups $S(Y, G_\alpha; \phi_{\alpha,\beta})$, then S is certainly regular. The idempotents of S are the identity elements $e_{\alpha,\alpha}$ of the groups G_α. If $e_\alpha \in E(S)$ and $b_\beta \in G_\beta$ then, writing $\gamma = \alpha\beta$ we have

$$e_\alpha b_\beta = (e_\alpha \phi_{\alpha,\gamma})(b_\beta \phi_{\beta,\gamma}) = e_\gamma (b_\beta \phi_{\beta,\gamma}) = b_\beta \phi_{\beta,\gamma} = (b_\beta \phi_{\beta,\gamma}) e_\gamma$$

$$= (b_\beta \phi_{\beta,\gamma})(e_\alpha \phi_{\alpha,\gamma}) = b_\beta e_\alpha,$$

and so every idempotent of S is central.

2. Suppose that S is a semilattice of groups. Then S is regular and so for any $a \in S$ there exists $x \in S$ such that $a = axa$. Next, for any $b \in S$ let e be the group identity of H_{ab} so that $ae, eb \in H_{ab}$ Put $y = e(be)^{-1}ab(ea)^{-1}e$, were inversion is in the group H_{ab}. Then

$$bya = be(be)^{-1}ab(ea)^{-1}ea = e(ab)e = ab.$$

Conversely, if S satisfies the given equations then S is certainly regular. Take $a \in S$ and $e \in E(S)$. Then there exists $y \in S$ such that $ae = eya$ and so $eae = e^2ya = eya = ae$. Similarly there exists $z \in S$ such that $ea = aze$ and so $eae = aze^2 = aze = ea$. Therefore $ea = eae = ae$ and so idempotents are central in S and therefore S is a semilattice of groups.

3. Suppose that S is a strong semilattice of abelian groups $S = S(Y, G_\alpha, \phi_{\alpha,\beta})$. Then S is regular and for any $a, b \in S$ we have

$$ab = (a\phi_{\alpha,\alpha\beta})(b\phi_{\beta,\alpha\beta}) = (b\phi_{\beta,\alpha\beta})(a\phi_{\alpha,\alpha\beta}) = ba$$

and so S is a commutative regular semigroup. Conversely suppose that S is a commutative regular semigroup. Then S is regular and idempotents are central and so S is a strong semilattice of groups, which must be abelian as S is commutative.

4(a) Suppose that the identity $a = aba$ holds in S. Putting $b = a$ and $b = a^2$ gives $a = a^3$ and $a = a^4$. Then from $a = a^3$ we get $a^2 = a^4 = a$ so that $a = a^2$ and S is a band. Now suppose that $ab = ba$. Then

$$a = aba = aab = ab = ba = bba = bab = b.$$

Conversely suppose that S is nowhere commutative. Then $a \cdot a^2 = a^2 \cdot a$ so that $a = a^2$ by the given property. Then $a \cdot aba = aba = aba \cdot a$ so that, again since S is nowhere commutative, we have $a = aba$.

5(a) First S is a semigroup as for a triple product we have:

$$((a,b)(c,d))(e,f) = (a,d)(e,f) = (a,f) = (a,b)(c,f) = (a,b)((c,d)(e,f))$$

and therefore the given binary operation is associative. Next

$$(a,b)(c,d)(a,b) = (a,d)(a,b) = (a,b)$$

and so S satisfies the identity $a = aba$ $(a, b \in S)$ and S is a rectangular band as defined in Question 4.

(b) Since S is a rectangular band, it follows as shown in Question 4 that S is a band. Since a band is a union of (trivial) groups, it follows that S is a semilattice of completely simple semigroups. However the identity $a = aba$ implies that $a \in J_b$ for all $a, b \in S$, which is to say that S is simple. Hence the structure semilattice of S is trivial and so S is a completely simple semigroup all of whose groups are trivial. Therefore $a = L_a \cap R_a$ for all $a \in S$. Let T be the rectangular band defined on $L \times R$ where L and R respectively the respective collections of $\mathcal{L}$- and $\mathcal{R}$-classes of S in the fashion of part (a). For an arbitrary semigroup, the mapping ϕ where $a \mapsto L_a \cap R_a$ is a surjection from S onto $S/\mathcal{H}$. Since S is $\mathcal{H}$-trivial, in this case ϕ is a bijection from S onto the semigroup T. Indeed ϕ is an isomorphism as

$$a\phi b\phi = (L_a, R_a)(L_b, R_b) = (L_a, R_b) = (ab)\phi.$$

6. Since a band B is a union of groups, B is a semilattice of completely simple semigroups. Since each subgroup of S is trivial, it follows that each of these completely simple semigroups satisfies $a = aba$ and so is a rectangular band, which is to say that B is a semilattice of rectangular bands.

7. Let $\phi : S \to (\mathbb{Z}, +)$ be defined by $w\phi = |w|_x - 2|w|_y$, where $|w|_x$, $|w|_y$ denote the number of $x's$ and $y's$ respectively in the word w.

Before checking that ϕ is an isomorphism, we verify that S is commutative and in order to show that, it is enough to check that x and y commute with one another. Now in S:$y = y \cdot xyx$, so that $xy = xyx \cdot yx = yx$. We conclude any $w \in S$ has a representation in the form $x^a y^b$ $(a, b \geq 0)$.

First, ϕ is well-defined: this follows as the word xyx is such that $(xyx)\phi = 0$. Also ϕ is a morphism as

$$(w_1w_2)\phi = |w_1w_2|_x - 2|w_1w_2|_y = |w_1|_x + |w_2|_x - 2|w_1|_y - 2|w_2|_y$$

$$= (|w_1|_x - 2|w|_y) + (|w_2|_x - 2|w_2|_y) = w_1\phi + w_2\phi.$$

Next, ϕ is onto as any integer may be written (not uniquely) in the form $n-2m$ $(n \geq 0, m \geq 0)$. Then $(x^n y^m)\phi = n - 2m$.

And ϕ is one-to-one . Suppose that $w_1\phi = w_2\phi$. We may write $w_1 = x^{a_1}y^{b_1}$, $w_2 = x^{a_2}y^{b_2}$. Assume without loss of generality that $a_1 \leq a_2$ so we may write $a_2 = a_1 + t$ say. Then

$$a_1 - 2b_1 = a_1 + t - 2b_2 \Rightarrow b_2 = b_1 + \frac{t}{2}.$$

Hence $t = 2s$ for some $s \geq 0$. But then

$$w_1 = w_1(xyx)^s = x^{a_1+2s}y^{b_1+s} = w_2.$$

Therefore ϕ is indeed an isomorphism, as required.

8(a) Observe that for any $n \in \mathbb{N}^0$ we have $n\alpha\beta = (n+1)\beta = n$ so that $\alpha\beta = \varepsilon$, the identity mapping. However $0\beta\alpha = \max\{-1, 0\}\alpha = 0\alpha = 0 + 1 = 1$, so that $\beta\alpha \neq \varepsilon$. For the final assertion we need to check that the mapping from M to S whereby $a\phi = \alpha$ and $b\phi = \beta$ induces a homomorphism ϕ from M to S, meaning that for any word $w = a_1 \cdots a_k \in M$ $(a_i \in \{a, b\})$ we may defined $w\phi = a_1\phi \cdots a_k\phi$, as from this it follows that S is a homomorphic image of M. Now two words w and z in the alphabet $\{a, b\}$ represent equal members of M if and only if we may pass from w to z by inserting or deleting copies of the word $ab = 1$ a finite number of times. It follows by induction on the number of transitions that we need only consider the case where the transition is of the form $w = uv \mapsto uabv = z$. However since $a\phi b\phi = \alpha\beta = \varepsilon$, this follows immediately.

(b) To show that any member of M may be expressed uniquely in the form $b^m a^n$ $(m, n \geq 0)$ it is enough to show that any member of M of the form $b^k a^l b^p a^q$ $(k, l, p, q \geq 0)$ has the required form. However, since $ab = 1$ the term $a^l b^p = a^{l-p}$ if $l \geq p$ in which case our product simplifies to $b^k a^{l-p+q}$, which is of the stated form. On the other hand if $p \leq l$ we get $a^l b^p = b^{p-l}$ and our product becomes $b^{k+p-l}a^q$, as required.

To show uniqueness, suppose that $b^k a^l = b^m a^n$ say. Then $\beta^k \alpha^l = \beta^m \alpha^n$ and so $(0)\beta^k \alpha^l = l = (0)\beta^m \alpha^n = n$, so that $l = n$. Multiplying both sides on the right by β^l then gives $\beta^k = \beta^m$. Hence $k\beta^k = 0 = k\beta^m$, whence $k \leq m$. By a symmetric argument, $m \leq k$ also and so $k = m$, and the form of the product is unique. It follows that that the homomorphism from M onto S induced by $a \mapsto \alpha$ and $b \mapsto \beta$, is an isomorphism as $(b^m a^n)\phi = (b^k a^l)\phi$ is to say that $\beta^m \alpha^n = \beta^k \alpha^l$, whence, by what we have just proved, $m = k$ and $n = l$. Therefore S is a faithful representation of the bicyclic monoid M.

9(a) Consider the product $b^k a^l \cdot b^m a^n$. First, if $l \leq m$ the product becomes $b^k b^{m-l} a^n = b^{k+m-l} a^n$. On the other hand, if $m \leq l$ the product simplifies to $b^k a^{l-m} a^n = b^k a^{l-m+n}$. In both cases the product is described by the formula

$$b^k a^l \cdot b^m a^n = b^i a^j, \text{ where } i = k + m - \min\{l, m\}, \ j = l + n - \min(l, m).$$

(b) Next, by the previous product formula in M we have $(b^m a^n)^2 = b^m a^n$ if and only if $m = m+m-\min(m, n)$ and $n = n+n-\min(m, n)$, which respectively give the inequalities $m \leq n$ and $n \leq m$. Therefore $b^m a^n \in E(M)$ if and only if $m = n$.

10(a) Take any two members $b^i a^m$ and $b^i a^n$ of the set $\{b^i a^j : 0 \leq j\}$ $i \geq 0\}$. If $m \leq n$ then we have $b^i a^m \cdot a^{n-m} = b^i a^n$. On the other hand, if $n \leq m$ then $b^i a^m b^{m-n} = b^i a^{m-(m-n)} = b^i a^n$. In either case we see follows that $b^i a^m \leq_{\mathcal{R}} b^i a^n$, and so by symmetry that $b^i a^m \mathcal{R} b^i a^n$. Conversely suppose that $b^k a^i \leq_{\mathcal{R}} b^m a^n$ so that $b^k a^l = b^m a^n \cdot b^i a^j$ say. It then follows by Question 9(a) that $k = m + i - \min(i, n) \leq m$. It follows that if $b^k a^i \mathcal{R} b^m a^n$ then $k = m$. This all serves to show that the set $R_{b^i} = \{b^i a^j : 0 \leq j\}$, as claimed.

Next take any two members $b^k a^j$ and $b^m a^j$ of the set $\{b^i a^j : 0 \leq i\}$ $j \geq 0$. If $k \leq m$ then we have $b^{m-k} b^k a^j = b^m a^j$. On the other hand, if $m \leq k$ then $a^{k-m} b^m a^j = a^k b^j$. It follows similarly to the previous paragraph that $b^k a^j \mathcal{L} b^m a^j$ and therefore $L_{a^j} = \{b^i a^j : 0 \leq i\}$, as claimed. Now suppose that $x = b^i a^j \mathcal{H} b^m a^n = y$. Then we have $y \mathcal{R} b^m \mathcal{R} x$ and $x \mathcal{L} a^j \mathcal{L} y$, whence it follows that $i = m$ and $j = n$. Therefore M is $\mathcal{H}$-trivial.

Finally for any two members $x = b^i a^j$ and $y = b^m a^n$ in M we have $b^i a^j \mathcal{L} b^m a^j \mathcal{R} b^m a^n$ and so $x \mathcal{D} y$ and therefore M is bisimple.

(b) We have from part (a) that M is a bisimple monoid, whence M is regular (as it has idempotents, in particular the identity of M). Indeed the idempotents of M form a chain as for any two idempotents $e = b^m a^m$ and $f = b^n a^n$, with $m \leq n$ we have

$$ef = b^m a^m \cdot b^n a^n = b^m b^{n-m} a^n = b^n a^n = f = b^n a^{n-m} a^m = b^n a^n b^m a^m = fe.$$

This shows $e \leq f$ if and only if $m \leq n$, from which it follows that $E(M)$ is an infinite descending chain with maximum element $1 = b^0 a^0$. In particular it now follows that M is a bisimple inverse monoid.

Problem Set 9

1(a) Since $SaS = S$ for all $a \in S \setminus \{0\}$ and $S^2 \neq 0$, it follows that $S^n \neq \{0\}$ for all $n \geq 1$. Since S it finite, it follows that $E(S)$ contains at least one non-zero idempotent. Again by finiteness, some non-zero idempotent e is 0-minimal in the natural partial oder, which is to say that e is a primitive idempotent.

(b) Since S is 0- simple, S has a unique non-zero $\mathcal{J}$-class. Since S is finite, $\mathcal{J} = \mathcal{D}$, whence it follows that S has a unique non-zero $\mathcal{D}$-class D. Then we have by part (a) that D contains an idempotent e and so $D = D_e$ is a regular $\mathcal{D}$-class. Therefore S is regular.

2(a) If $ab \neq 0$ then $a\mathcal{D}^{\mathcal{T}_{S^1}}ab\mathcal{D}^{\mathcal{T}_{S^1}}b$. It follows that $\text{rank}(a) = \text{rank}(ab) = \text{rank}(b)$ so that Xa is a transversal of ab and $Xab = Xb$, which is to say that $a\mathcal{R}^{\mathcal{T}_{S^1}}ab\mathcal{L}^{\mathcal{T}_{S^1}}b$. Since S is regular, if follows that $a\mathcal{R}ab\mathcal{L}b$ in S.

(b) It follows that if $ab \neq 0$ that $L_a \cap R_b$ contains an idempotent, and so is a group $\mathcal{H}$-class.

3(a) Let e be the identity of $H_{1,1}$ so that $eq_\lambda = q_\lambda$ and $r_i e = r_i$. It follows by Greens lemma that $\phi_{i,\lambda}$ is a bijection from $H_{1,1}$, onto $H_{i,\lambda}$.

(b) By part (a) there is a one-to-one correspondence between the triples $(a; i, \lambda)$ and the members of S via the bijection $(a; i, \lambda) \mapsto a\phi_{i,\lambda} = r_i a q_\lambda$.

(c) Take any two members of $H_{i,\lambda}$, $x = r_i a q_\lambda$ $y = r_j b q_\mu$ say. Then

$$xy = r_i(aq_\lambda r_j b)q_\mu \tag{1}$$

We now seek to represent the multiplication of S in terms of the triples of part (b). If $xy \neq 0$ then $H_{j,\mu}$is a group so that $q_\lambda r_\mu \neq 0$ as this product lies in the group $H_{1,1}$. By (1) it follows that

$$(a; i, \lambda)(b; j, \mu) = (c; i, \mu)$$

where $c = aq_\lambda r_j \mu$. On the other hand, $xy = 0$ if and only if $q_\lambda r_j = 0$, which occurs if and only if $H_{j,\mu}$ is not a group. In this case $(q_\lambda r_i; i, \mu) = (0; i, \mu) = 0$. Hence, in either case, we may represent multiplication in S in terms of the corresponding triples via the rule:

$$(a; i, \lambda)(b; j, \mu) = (ap_{\lambda,i}b; i, \mu), \text{ where } p_{\lambda,j} = q_\lambda r_j.$$

4(a) Since $ap_{\lambda,j}b \in G^0$, we have a binary operation on the set of triples in which any product involving the class of 0, which consists of all triples of the form $(0; i, \lambda)$, equals 0. It just remains to show that the product is associative. Hence consider a typical product of the form:

$$((a; i, \lambda)(b; j, \mu))(c; k, \nu) = (ap_{\lambda,j}b; i, \mu)(c; k, \nu) = (ap_{\lambda,j}bp_{\mu,k}c; i, \nu)$$

$$= (a; i, \lambda)(bp_{\mu,k}c; j, \nu) = (a; i, \lambda)((b; j, \mu)(c; k, \nu)),$$

showing that our product is associative and so $M^0[G,I,\Lambda,P]$ is a semigroup.

(b) Suppose that row λ of the $\Lambda \times I$ matrix P was a row of zeros. Then for any $x=(a;i,\lambda)$ and any $y=(b;j,\mu)$ we have

$$xy=(ap_{\lambda,j}b;i,\mu)=(0;i,\mu)=0$$

as $p_{\lambda,j}=0$. In particular, there is no $y \in S$ such that $xyx=x$ so that x is not regular. Similarly if column i of P consisted only of zeros we have

$$xy=(ap_{\lambda,j}b;i,\mu)=(0;i,\mu)=0$$

as $p_{\lambda,j}=0$ and agains x is not regular. Therefore if S is regular then P is regular, meaning that P has no zero row or zero column. Conversely, suppose that every row and every column of P contains at least one non-zero entry. Let $x=(a;i,\lambda)\neq 0$ say. We wish to find $y=(b;j,\mu)\in S$ such that $x=xyx$ in order to conclude that x, and so S, is a regular semigroup. Now

$$xyx=(ap_{\lambda,j}bp_{\mu,i}a;i,\lambda);$$

by hypothesis, we may choose μ and j so that $p_{\lambda,j}\neq 0$ (as row λ of P has a non-zero entry) and $p_{\mu,i}\neq 0$ (as column i of P has a non-zero entry). We now put $ap_{\lambda,j}bp_{\mu,i}a=a$, which has a unique solution in

$$b=p_{\lambda,j}^{-1}a^{-1}p_{\mu,i}^{-1}\in G.$$

This identifies an inverse for x and thus completes the proof that S is regular if and only if P is a regular matrix.

(c) By Question 1, any finite 0-simple semigroup S is regular. Hence by Question 4(b) S is isomorphic to a regular Rees matrix semigroup.

5(a) Let $b\in eS\setminus\{0\}$ and write $e=xby$, for some $x,y\in S^1$, which is possible as S is 0-simple and $b\neq 0$. Then consider $f=byexe$. We have, since $eb=b$ that

$$f^2=byexe\cdot byexe=bye(xby)exe=bye^3xe=byexe=f$$

and so $f\in E(S)$. Note that by Question 1(b) of Set 3, $f\leq e$ is equivalent to $f=fef$, and this is the case as:

$$fef=byexe\cdot e\cdot byexe=(byexe)^2=f^2=f.$$

(b) Since e is a primitive idempotent and $f\leq e$, this implies either that $f=0$ or $f=e$. However

$$xfby=(x\cdot by)exe\cdot by=e^2xeby=exeby=exby=e^2=e.$$

If $f=0$ this would give that $e=0$, which is not the case. Therefore $e=f$.

(c) Since $e\in R$ we have $R\cup\{0\}\subseteq eS$. Conversely take any $b\in eS\setminus\{0\}$ so that $e=eb$. By part (b) we have $e=f=byexe$, showing that $e\in bS$ also, whence $eS\subseteq bS^2=bS$ and since $bS\subseteq eS^2=eS$ it follows that $b\mathcal{R}e$. Therefore $R\cup\{0\}=eS$.

(d) Suppose that R' were a non-zero right ideal of S with $R' \subseteq R \cup \{0\}$. Take any $a \in R' \setminus \{0\}$ and $x \in R$. We have $x\mathcal{R}a$ and thus $x = au \in R'$, which shows that $R \subseteq R'$. Therefore if follows that $R' = R \cup \{0\}$. Therefore $R \cup \{0\}$ is a 0-minimal right ideal of S.

6(a) Now $S = SeS = S(R \cup \{0\})$. Hence for any $x \in S$ we have $x \in c(R \cup \{0\})$ for some $c \in S$ so that $x = cr$ for some $r \in R \cup \{0\}$. If $x = 0$ then $R_x = \{0\}$ and we take $c = 0$ to conclude that $R_x \cup \{0\} = c(R \cup \{0\}) = ceS$. Otherwise assume that $x \neq 0$ and take any $y \in R_x$ so that $y \in c(R \cup \{0\}S \subseteq c(R \cup \{0\})$. Then $R_x \cup \{0\} \subseteq c(R \cup \{0\})$.

Conversely, let $y = cs$ for some $s \in R \cup \{0\}$. Clearly if $s = 0$ then $y = 0$ and $y \in c(R \cup \{0\})$. Otherwise $r\mathcal{R}s$ and since $\mathcal{R}$ is a left congruence it follows that $x = cr\mathcal{R}cs = y$ and so $y \in R_x \cup \{0\}$ in the general case as well. Therefore for any $x \in S$ there exists $c \in S$ such that $R_x \cup \{0\} = c(R \cup \{0\}) = ceS$.

(b) By part (a), we may write $R_x \cup \{0\}$ as ceS for some $c \in S$. Take any $y = ces$ for some $s \in S$. Then $es \in R \cup \{0\}$ so by the minimality of the right ideal $R \cup \{0\}$ we have that $esS = R \cup \{0\}$ so that $yS = cesS = c(R \cup \{0\}) = R_x \cup \{0\}$, thereby showing that $R_x \cup \{0\}$ is a 0-minimal right ideal for any $x \in S \setminus \{0\}$, as required.

7(a) Let $a, b \in S \setminus \{0\}$. Then $aSb \neq \{0\}$ for otherwise we would deduce that $S = \{0\}$ as follows:

$$S = S^2 = SaS \cdot SbS = S(aSb)S = S\{0\}S = \{0\}.$$

Take any $c \in aSb \setminus \{0\}$. Since $c \in aS \cap Sb$ we have, by Question 6 and its dual, that $aS \cup \{0\}$ and $Sb \cup \{0\}$ are respectively right and left minimal ideals so that $a\mathcal{R}c\mathcal{L}b$, which is to say that $a\mathcal{D}b$, so that S is 0-bisimple. The non-zero $\mathcal{D}$-class D has a (primitive) idempotent and so D is regular.

(b) If $ab \neq 0$ then $R_{ab} \leq R_a$ and $L_{ba} \leq L_b$, whence by 0-minimality of right and left principal ideals in S it follows that $a\mathcal{R}ab\mathcal{L}b$, as required.

(c) Given part (b), the connstruction of the Rees matrix semigroup representation of a completely 0-simple semigroup (as in Questions 2 and 3) may now be repeated as for the finite 0-simple case, resulting in a representation of S in the form $M^0[H_{1,1}; I, \Lambda, P]$ as before.

8. Without loss of generality, we show that the row and column indexed by the symbol 1, can be taken to have the required form. Since $H_{1,1}$ is a group, we may put $r_1 = q_1 = e$, so $p_{1,1} = q_1 r_1 = e^2 = e$. We need to show that we may choose the other r_i and q_λ such that $q_1 r_i = e$ if $H_{r_i,1}$is a group, and $q_\lambda r_1 = e$ if H_{1,q_λ} is a group. (If the $\mathcal{H}$-classes in question are not groups, choices may be made arbitrarily and the product and corresponding matrix entry is 0).

However if $H = H_{r_i,1}$ is a group, it follows by Green's Lemma that $\lambda_{q_1}|_H$ is a bijection onto $H_{1,1}$, from which it follows that there exists $r_i \in H_{r_i,1}$ such that $q_1 r_i = e$. Dually q_λ can be chosen so that $q_\lambda r_1 = e$.

9(i) Let e, f are each non-zero idempotents of S and suppose that $e \leq f$ so that $e = ef = fe$. Since $ef \neq 0$ it follows by Question 7 we have $ef\mathcal{L}f\mathcal{R}fe$, whene $e\mathcal{H}f$, which implies that $e = f$. It follows that no two distinct non-zero idempotents are comparable in the natural partial order, and therefore every non-zero idempotent of S is primitive.

(ii) Let $a\mathcal{H}b$ and let $c \in S$. Then either $ac = bc = 0$ or $ac, bc \in R_a \cap L_b$. In either case, $ac\mathcal{H}bc$. The dual argument to this shows that $\mathcal{H}$ is also a left congruence, and therefore $\mathcal{H}$ is a congruence on a completely 0-simple semigroup.

(iii) Let ρ be a congruence on S. Suppose that $(0, a) \in \rho$ with $a \neq 0$. Take any $b \in S$ so there exists $x, y \in S$ such that $b = xay$ so the $b\rho = x\rho a\rho y\rho = 0\rho$. Hence ρ is the universal congruence and S/ρ is trivial. Since any non-trivial homomophic image is isomorphic to S/ρ for some congruence ρ on S, we continue under the hypothesis that no such a exists. But then the equation $b\rho = x\rho a\rho y\rho$ shows that S/ρ is 0-simple. Finally take any two non-zero idempotents $e\rho, f\rho$. Since S is regular we may appeal to Lallement's lemma, to allow the assumption that $e, f \in E(S)$. If $e\rho = e\rho f\rho = f\rho e\rho$ then we have $e\rho = (ef)\rho = (fe)\rho$. Hence $(fe)\rho = (f^2e)\rho = f\rho(fe)\rho = f\rho(ef)\rho = (fef)\rho$. It follows that $ef, fe \neq 0$ so that H_e, H_f, H_{ef}, H_{fe} are all non-zero groups. But then $fef \in H_f$. Hence $e\rho = (fef)\rho\mathcal{H}f\rho$ and so $e\rho$ and $f\rho$ are $\mathcal{H}$-related idempotents in S/ρ so that $e\rho = f\rho$. It follows that $e\rho$ is a primitive idempotent in S/ρ and therefore S/ρ is indeed a completely 0-simple semigroup.

10. Clearly $S = M^0[G, I, I; \Delta]$ is a regular 0-simple semigroup. Suppose that $x = (a; i, \lambda) \in E(S)$. Now $x^2 \neq 0$ implies that $i = \lambda$ and $a^2 = a$ so that $a = e$, the identity of G and conversely $(e, i, i) \in E(S)$. What is more $(e; i, i)(e, j, j) = (e, j, j)(e, i, i) = 0$ unless $i = j$. In particular idempotents commute with each other so that S is an inverse semigroup.

Conversely suppose that $S = M^0[G, I, \Lambda, P]$ is an inverse semigroup, so that P is a certainly a regular matrix. Let R_i and L_λ denote the respective $\mathcal{R}$- and $\mathcal{L}$-class of S defined by $i \in I$ and $\lambda \in \Lambda$ respectively. The mapping that maps $i \mapsto \lambda$ where $R_i \cap L_\lambda$ is a group is a bijection from I to Λ as each $\mathcal{R}$- and $\mathcal{L}$-class of S contains a unique idempotent. Hence we may take $\Lambda = I$ and so P is an $I \times I$ square regular matrix. Furthermore, we may insist that $H_{i,i}$ is the unique group $\mathcal{H}$-class in $R_i \cap L_i$.

Choose $r_i \in H_{i,1}$ arbitrarily. Then, again by Green's Lemma we may choose $q_i \in H_{1,i}$ such that $q_i r_i = e$ (remembering that $H_{i,i}$ is a group). With these choices we have that Δ is then the identity matrix, as specified.

Problem Set 10

1. Suppose that S is a 0-direct union of completely 0-simple semigroups and let $e, f \in E(S)$ for $f \neq 0$ and suppose that $e \leq f$. If $e\mathcal{J}f$ then e and f are members of the same 0-completely simple semigroup so that $e \neq 0$ and so $f \leq e$ also and so e and f are primitive. Otherwise$ef = 0$ and so $e = 0$ and f is

primitive. We conclude that all non-zero idempotents of S are primitive.

Conversely suppose that S is regular with all non-zero idempotents are primitive. Take any two non-zero $\mathcal{J}$-classes, which can be denoted by J_e and J_f for some $e, f \in E(S)$ as S is regular. Suppose that $\{0\} \neq J_f \leq J_e$ $(e, f \in E)$. Then $f = xey$ say; put $g = eyfxe$. Now

$$g^2 = eyfxe \cdot eyfxe = eyfxeyfxe = eyf^3xe = eyfxe = g.$$

Next note that $eg = ge = g$ and if $g = 0$ then $0 = xgy = xeyfxey = f^3 = f$, which is not the case. Thus we have $g \leq e$ so that $g = e$ as e is primitive. Therefore $J_e \leq J_f$ and so $J_e = J_f$. Hence no two distinct non-zero $\mathcal{J}$-classes J_1 and J_2 are comparable, whence $J_1J_2 = \{0\}$. Each subsemigroup $J_e \cup \{0\}$ is then 0-simple with a primitive idempotent e and so is completely 0-simple. Therefore S is a 0-disjoint union of completely 0-simple semigroups. (We almost must admit the possibility that S is completely simple, and so has no zero element.)

2. (i) $\Rightarrow$ (ii) Suppose that S is completely simple. Let $a = (x; i, \lambda), b = (y; j\mu)$ and suppose that $aba = a$ whence $xp_{\lambda,j}yp_{\mu,i}x = x \Leftrightarrow xp_{\lambda,j} = p_{\mu,i}^{-1}y^{-1}$. Certainly we have $bab\mathcal{H}b$ and indeed$bab = (yp_{\mu,i}xp_{\lambda,j}y; j, \mu)$. But

$$yp_{\mu,i}xp_{\lambda,j}y = yp_{\mu,i}p_{\mu,i}^{-1}y^{-1}y = y$$

so that $bab = b$.

(i) $\Rightarrow$(iii) Since S is completely simple we have $xa\mathcal{L}a\mathcal{R}ax$ it follows that if $ax = bx$ and $ya = yb$ then $a\mathcal{H}b$. Let $x = (u; k, \sigma)$, $a = (r; i, \lambda), b = (s; i, \lambda)$. Then $ax = bx$ implies that $rp_{\lambda,k}u = sp_{\lambda,k}u \Rightarrow r = s$ and so $a = b$. Therefore S is weakly cancellative.

(iii) $\Rightarrow$(i) Suppose that S is regular and weakly cancellative. Suppose that $e \leq f$ for $e, f \in E(S)$. Then $e = ef = fe$. Hence $e^2 = ef = fe$. Putting $e = a, b = f$ and $x = y = e$ we have $ax = e^2 = fe = bx$ and $ya = e^2 = ef = yb$. Hence by weak cancellativity we have $a = b$, which is to say that $e = f$. Hence every idempotent is primitive. By Question 1, it follows that S is a 0-direct union of completely simple semigroups. However, if S has a zero 0 and $a \in S$ then $a0 = 0^2 = 0 = 0a$ and weak cancellativity implies that $a = 0$. Hence it follows that S is in fact completely simple.

(iii) $\Rightarrow$(ii) Let $a = aba$. Then $b \cdot a = bab \cdot a$ and $a \cdot b = a \cdot bab$ so by weak cancellativity it follows that $b = bab$.

(ii) implies (i) Suppose that $P(a) = V(a)$ for all a in the regular non-trivial semigroup S and that S has two comparable non-zero idempotents, $e \leq f$ say. Then $e = efe$ so that $f \in P(e) = V(e)$ and then $f = fef = e$. It follows that all non-zero idempotents in S are primitive. By above we then have that S^0 is a 0-disjoint union of completely 0-simple semigroups. Moreover 0 must be adjoined for if $0 \in S$, we have $0 = 0e0$ for all $e \in S$ whence by hypothesis $e \in V(0)$ so that $e = 0$, from which it would follows that $S = \{0\}$. Therefore S is completely simple.

3. Let $S = G \times R$ be the direct product of a group with identity element e

and a rectangular band R. Let $(g,r),(h,s)\in G\times R$. Then

$$(g^{-1},s)(g,r)(h,s)=(g^{-1}gh,srs)=(h,s)$$

thus showing that $(h,s)\leq_{\mathcal{J}}(g,r)$ and by symmetry the opposite inequality also holds and so S is simple. Next, the idempotents of S are exactly the members of S of the form (e,a) $(a\in R)$. Suppose that $(e,a)\leq(e,b)$ in the natural partial order on $E(S)$. Then $(e,a)=(e.a)(e,b)=(e,ab)$ and $(e,a)=(e,b)(e,a)=(e,ba)$, whence it follows that $ab=ba$ for all $a,b\in R$. Since R is nowhere commutative, this implies that $a=b$ and so S is simple with a primitive idempotent and so is completely simple. Finally S is also orthodox as $(e,a)(e,b)=(e,ab)\in E(S)$ so the product of two idempotents is idempotent.

Comment Alternatively, it is easy to show that in general the direct product of completely simple semigroups is completely simple. We can then apply this to $G\times R$.

Conversely suppose that S is a completely simple orthodox semigroup $S=M[G,I,\Lambda,P]$. As in Question 8 of Set 9 we may choose $H_{1,1}=G$. We may also find a suitable sandwich matrix P by choosing $r_i=e_{i,1}$ and $q_\lambda=e_{1,\lambda}$, where $e_{i,1}$ and $e_{1,\lambda}$ are the respective identity elements of the groups $H_{i,1}$ and $H_{1,\lambda}$ This choice can be made for any completely simple semigroup but under the additional assumption of orthodoxy we get $p_{\lambda,i}=q_\lambda r_i=e_{1,\lambda}e_{i,1}=e$, the identity element of the group $G=H_{1,1}$ and this holds for all $i\in I$ and $\lambda\in\Lambda$. But then

$$(a;i,\lambda)(b;j,\mu)=(ap_{\lambda,j}b;i,\mu)=(aeb;i,\mu)=(ab;i,\mu).$$

It now follows that S is isomorphic to the rectangular group $T=G\times R$ where R is the rectangular band defined on $I\times\Lambda$: specifically et $\phi:S\to T$ be the mapping whereby $(a;i,\lambda)\phi=(a,(i,\lambda))$. Then ϕ is clearly a bijection between the two semigroups. We just need to show that ϕ is a homomorphism in order to complete the proof and this now follows immediately:

$$((a;i,\lambda)(b;j,\mu))\phi=(ab;i,\mu)\phi=(ab;(i,\mu))=(a;(i,j))(b;j,\mu))=(a;i,\lambda)\phi(b;j,\mu)\phi.$$

4. Suppose that S is a 0-rectangular band and take $x,y\in S$. If $xyx\neq 0$ then $x\mathcal{H}xyx$ but since $\mathcal{H}$ is trivial in S it follows that $xyx=x$, thus establishing (i). As for (ii), take $x,y\in S\setminus\{0\}$ and suppose that $xSy=\{0\}$. Since $S=SyS$ this gives that $\{0\}=xSy=xSyS=xS$, which contradicts that $x\in\text{Reg}(S)$. Therefore $xSy=\{0\}$ implies $0\in\{x,y\}$.

Conversely suppose that S satisfies the given pair of conditions (i) and (ii). Take any $x\in S\setminus\{0\}$. Then by (ii) $xSx\neq\{0\}$ so that there exists $y\in S$ such that $xyx\neq 0$ whence $xyx=x$ by (i). In particular, this shows that S is regular. Let $e,f\in E(S)\setminus\{0\}$ with $e\leq f$. Then $e=fef=f$ by (i). It follows that all non-zero idempotents of S are primitive and so S is a 0-direct union of completely 0-simple semigroups. Suppose that $x\in S\setminus\{0\}$ and $y\notin J_x$ for some $y\in S$. Then $xSy=0$, whence by (ii) if follows that $y=0$ and so S is completely 0-simple.

Finally let G be a non-zero subgroup of S with identity element e and let $a \in G$. Then $a = eae \neq 0$, whence $a = eae = e$ by (i). Hence all subgroups of S are trivial, and so S is therefore a 0-rectangular band.

5. Throughout let $x, y, z \in \mathbb{R}^{>0}$.

(i)

$$(x \circ y) \circ z = \sqrt{x^2 + y^2} \circ z = \sqrt{(\sqrt{x^2 + y^2})^2 + z^2} = \sqrt{x^2 + y^2 + z^2}$$

$$= \sqrt{x^2 + (\sqrt{y^2 + z^2})^2} = x \circ (\sqrt{y^2 + z^2}) = x \circ (y \circ z).$$

(ii)

$$(x \circ y) \circ z = (\frac{xy}{x+y} \circ z) = \frac{\frac{xyz}{x+y}}{\frac{xy}{x+y} + z} = \frac{xyz}{xy + xz + yz} = \frac{\frac{xyz}{y+z}}{x + \frac{yz}{y+z}} = x \circ (y \circ z);$$

or we note that

$$\frac{xy}{x+y} = (\frac{1}{x} + \frac{1}{y})^{-1} \text{ so that}$$

$$(x \circ y) \circ z = ((\frac{1}{x} + \frac{1}{y})^{-1})^{-1} + \frac{1}{z}))^{-1} = (\frac{1}{x} + \frac{1}{y} + \frac{1}{z})^{-1} = ((\frac{1}{x} + (\frac{1}{y} + \frac{1}{z})^{-1})^{-1}$$

$$= x \circ (y \circ z).$$

(iii) Note that $e^x + e^y - 2 > 0$ as $x, y > 0$ so that $\ln(e^x + e^y - 2)$ is well-defined. Then

$$(x \circ y) \circ z = \ln(e^x + e^y - 2) \circ z = \ln(e^{\ln(e^x + e^y - 2)} + e^z - 2) = \ln(e^x + e^y - 2 + e^z - 2)$$

$$= \ln(e^x - 2 + (e^y + e^z - 2)) = \ln(e^x + e^{\ln(e^y + e^z - 2)} - 2) = x \circ (\ln(e^y + e^z - 2)) = x \circ (y \circ z).$$

6(a) The general check for associativity of $\circ$ is as follows:

$$(x \circ y) \circ z = f^{-1}(f(f^{-1}(f(x) + f(y))) + f(z)) = f^{-1}((f(x) + f(y) + f(z))$$

$$= f^{-1}((f(x) + (f(y) + f(z))) = f^{-1}(f(x) + f(f(^{-1}(f(y) + f(z))) = x \circ (y \circ z).$$

(b) Hence both $(S, +)$ and $(S, \circ)$ are semigroups. Indeed the permutation $f : (S, \circ) \to (S, +)$ is not only a bijection but an isomorphism as

$$f(x \circ y) = f(f^{-1}(f(x) + f(y)) = f(x) + f(y).$$

(c) In 6(a) we take $f(x) = x^2$ as our bijection on $\mathbb{R}^+$ for then we get $x \circ y = \sqrt{x^2 + y^2}$. As for (ii), we take $f(x) = x^{-1} = f^{-1}(x)$, as then $x \circ y = (\frac{1}{x} + \frac{1}{y})^{-1}$.

Comment Note that this operation arises when resistances are added in parallel circuits, an operation that is clearly seen to be associative in that physical situation.

For (iii), let $f(x) = e^x - 1$, a bijection on $\mathbb{R}^+$ as the rule defines a one-to-one continuous function on $\mathbb{R}^{\geq 0}$ that is strictly increasing and unbounded with minimum $f(0) = 0$. We can therefore define a semigroup operation on $\mathbb{R}^{\geq 0}$ (giving a semigroup isomorphic to $(\mathbb{R}^{\geq 0}, +)$ with $f : \mathbb{R}^{\geq 0} \to \mathbb{R}^{\geq 0}$ an isomorphism) by the rule:$x \circ y = f^{-1}(f(x) + f(y))$. In this case $f^{-1} : \mathbb{R}^+ \to \mathbb{R}^+$ with $f^{-1}(x) = \ln(x + 1)$. Then for any $x, y \in \mathbb{R}^+$ we have

$$x \circ y = \ln((e^x - 1) + (e^y - 1) + 1) = \ln(e^x + e^y - 1) \tag{2}$$

$$\Rightarrow f(x \circ y) = e^{\ln(e^x+e^y-1)} - 1 = e^x + e^y - 2. \tag{3}$$

Comment In particular we see each of these semigroups is a copy of the semigroup of positive real numbers under addition.

8(a) If the homomorphism ϕ exists then it must satisfy $x\phi = x\alpha$ for all $x \in X$. Therefore ϕ must be defined by

$$(x_1 \cdots x_n)\phi = x_1\phi \cdots x_n\phi = x_1\alpha \cdots x_n\alpha.$$

It follows that in order to complete the proof it suffices to show that if two words $u = x_1 \cdots x_n = y_1 \cdots y_m = v$ $(x_i, y_j \in X)$ are equal in F_X then $u\phi = v\phi$. However $u = v$ if and only if $m = n$ and $x_i = y_i$ for all $1 \leq i \leq n$ so this follows immediately.

(b) Let S be any semigroup and let X be any generating set of S (for instance, we may take $X = S$). By (a) there is a homomorphism $\phi : F_X \to S$ such that $x\phi = x$ for all $x \in X$. Since $\langle X \rangle = S$, it follows that ϕ is also surjective. Therefore every semigroup S is the homomorphic image of the free semigroup F_X for any generating set X of S.

Comment We say that the homomorphism ϕ is the homomorphism *induced by* the inclusion mapping $\iota : X \to S$.

(c) We have injections $\iota_1 : X \to F_X$ and $\iota_2 : X \to G$. Hence there are unique homomorphisms $\phi_1 : F_X \to G$ and $\phi_2 : G \to F_X$ such that $\iota_1\phi_1 = \iota_2$ and $\iota_2\phi_2 = \iota_1$. But then $\iota_1 = \iota_1\phi_1\phi_2$ and so $\phi_1\phi_2$ is the unique homomorphism $\alpha : F_X \to F_X$ such that $\iota_1\alpha = \iota_1$. However, since the identity mapping ε on F_X clearly has this property, it follows that $\phi_1\phi_2 = \varepsilon$. By symmetry, $\phi_2\phi_1$ is the identity mapping on G so that ϕ_1 and ϕ_2 are then mutually inverse mappings, which are homomorphisms, and therefore isomorphisms between F_X and G. Therefore F_X is unique up to isomorphism.

8. In general, $U\phi^{-1}$ is a subsemigroup of S. Let V be a subsemigroup of $U\phi^{-1}$ of mimimum cardinality such that $V\phi = U$. Let $v \in V$ so that $v\phi = u \in U$. Then vV is a subsemigroup of V. Hence $(vV)\phi = v\phi V\phi = uU = U$ as U is right simple since U is a group. Since $|vV| \leq |V|$ and since $|V|$ is the minimum cardinal of subsemigroups of S that maps onto U under ϕ, it follows that $|vV| = |V|$ and so $vV = V$ by finiteness. By symmetry it follows equally that $Vv = V$ so that V is indeed a group, as required.

9(a) We have $a = xy(xyxy)'xyx$ and $b = y(xyxy)'xy$ and so

$$aba = xy(xyxy)'xyx \cdot y(xyxy)'xy \cdot xy(xyxy)'xyx = xy(xyxy)'xyx = a;$$

$$bab = y(xyxy)'xy \cdot xy(xyxy)'xyx \cdot y(xyxy)'xy = y(xyxy)'xy = b,$$

which is to say that $(a,b) \in V(S)$.

(b) Now since $(xy)\phi = (cd)\phi = ((cdcd))\phi = (xyxy)\phi$, and so we obtain:

$$a\phi = (xy(xyxy)'xyx)\phi = (xyxy(xyxy)'xyxyx)\phi = (xyxy)\phi x\phi = (xyx)\phi = cdc = c;$$

$$b\phi = (y(xyxy)'xy)\phi = (y(xyxy)(xyxy)'(xyxy))\phi = (yxyxy)\phi = d(cd)^2 = d.$$

(c) In particular, if $c = d = f \in E(T)$ we have that $a, b \in V(S)$ are such that $a\phi = b\phi = f$. But then $ab = e \in E(S)$ and

$$e\phi = (ab)\phi = a\phi b\phi = f^2 = f.$$

10. Let $n \geq 0$ and consider

$$(-n)\alpha = (n-2n)\alpha = n\alpha + (-2n)\alpha = n\beta + (-2n)\alpha$$

$$(-2n+3n)\beta + (-2n)\alpha = (-2n)\beta + (3n)\beta + (-2n)\alpha$$
$$= (-2n)\beta + (3n)\alpha + (-2n)\alpha = (-2n)\beta + (3n-2n)\alpha$$
$$= (-2n)\beta + n\alpha = (-2n)\beta + n\beta = (-2n+n)\beta = (-n)\beta.$$

It follows that α and β agree on all integers and so $\alpha = \beta$.

Comment Let $\iota : (\mathbb{N}, +) \to (\mathbb{Z}, +)$ be the inclusion mapping where $x\iota = x$. It follows that if $\alpha, \beta : \mathbb{Z} \to X$ are semigroup homomorphisms such that $\iota\alpha = \iota\beta$ then $\alpha = \beta$. In general if $\gamma : S \to T$ is a homomorphism such that whenever $\alpha, \beta : T \to X$ are such that $\gamma\alpha = \gamma\beta$ then $\alpha = \beta$ we say that such a left cancellable homomorphism is an *epimorphism*. Certainly any surjective homomorphism is an epimorphism but, as this example shows, not every epimorphism is surjective. This is so in the category of Semigroups but in the category of Groups, all epimorphisms are necessarily surjective.