ISOMORPHISMS BETWEEN SEMIGROUPS OF INTEGERS

PAGE PAINTER

1. **Introduction.** Let j and k be positive integers. Let G_j be the multiplicative group of residue classes mod j whose elements are relatively prime to j, and denote its elements by R_1', R_2', $\cdots$, $R_{\phi(j)}'$. We will always identify R_1' with the identity element, the class of all integers congruent to 1 mod j. Let R_i be the set of positive integers in R_i', and note that R_1 is a semigroup under multiplication. Similarly G_k has elements S_1', S_2', $\cdots$, $S_{\phi(k)}'$ where S_i is the set of positive integers in S_i'. Again S_1 is a semigroup.

For the case $j=1$ and $k=2$, any one-to-one mapping of the primes onto the odd primes can be extended to an isomorphism of $R_1 = \{1, 2, 3, \cdots\}$ onto $S_1 = \{1, 3, 5, \cdots\}$. However, the semigroup $\{1, 4, 7, \cdots\}$ corresponding to the identity element of G_3 is not isomorphic to the above semigroups since unique factorization holds in the former cases but not in the latter ($100 = 10 \cdot 10 = 25 \cdot 4$). Our main result is that G_j is isomorphic to G_k (written $G_j \sim G_k$) if and only if $R_1 \sim S_1$. The problem of the existence of isomorphisms between these infinite semigroups is thereby reduced to a solvable problem.

2. **Isomorphisms.**

THEOREM. *$G_j \sim G_k$ if and only if $R_1 \sim S_1$.*

PROOF. Assume $G_j \sim G_k$. We may choose our notation so that the class S_i' is the image of the class R_i'. Thus the isomorphism induces a mapping α such that $\alpha(R_i) = S_i$. We use α to define a mapping of the integers in R_1 onto the integers in S_1 as follows: for each $i = 1, 2, \cdots, \phi(j)$ set up a one-to-one correspondence between the primes in R_i and the primes in S_i. Now given any element a in R_1, write its decomposition into prime factors $p_1 p_2 p_3 \cdots$ (these factors must be in the sets R_i), and map these primes onto their corresponding primes q_1, q_2, q_3, $\cdots$ in the sets S_i. In this way we define a mapping $a \to q_1 q_2 q_3 \cdots$. It is easy to show that this gives an isomorphism of R_1 onto S_1.

Before proving the converse, we note that if $F_j = \{H_1', H_2', \cdots\}$ is a subgroup of G_j, where H_i is again the set of positive integers in H_i', then $H = H_1 \cup H_2 \cup \cdots$ is a semigroup under multiplication. Let $F_k = \{I_1', I_2', \cdots\}$ be a subgroup of G_k, and let $I = I_1 \cup I_2 \cup \cdots$. The above proof is easily generalized to show that if $G_j \sim G_k$ and $F_j \sim F_k$, then $H \sim I$. The converse is false since it is always true that

Received by the editors March 30, 1966.

$R_1 \cup R_2 \cup \cdots \cup R_{\phi(j)} \sim S_1 \cup S_2 \cup \cdots \cup S_{\phi(k)}$ (unique factorization holds in both semigroups).

Conversely assume $R_1 \sim S_1$. Let p be any prime such that $(p, j) = 1$, and let t be the least positive integer such that $p^t \equiv 1 \pmod{j}$. Then p^t is a member of R_1, and its image under the R_1 to S_1 isomorphism is some product of primes $q_1 q_2 \cdots q_n$. Let v be the least positive integer such that $q_1^v \equiv 1 \pmod{k}$. Under the R_1 to S_1 isomorphism p^{tv} maps onto $(q_1 q_2 \cdots q_n)^v = q_1^v (q_2 \cdots q_n)^v$. Since the only factorization of p^{tv} into irreducible elements of R_1 contains v irreducible factors each p^t, $(q_1 q_2 \cdots q_n)^v$ must factor uniquely into v identical factors in S_1. But $(q_1 q_2 \cdots q_n)^v$ has an irreducible factor q_1^v in S_1, so we conclude that p^t maps onto q_1^v. Furthermore all the q_i are equal and $n = v$.

Now let p_0 be another prime, different from p, such that $p_0 \equiv p \pmod{j}$. Then t is the least positive integer such that $p_0^t \equiv 1 \pmod{j}$, and under the R_1 to S_1 isomorphism p_0^t maps onto q_0^w, where q_0 is a prime different from q_1. Consequently $(p p_0^{t-1})^t$ maps onto $q_1^v q_1^{w(t-1)}$. Since this expression must be a tth power, we have $t \mid v$. Similarly we can show that $v \mid t$, so that $t = v$.

We now see that the R_1 to S_1 isomorphism can be embedded in a larger mapping ψ by defining $\psi(p) = q_1$, $\psi(p_0) = q_0$: similarly every prime p_i (not a divisor of j) maps onto a prime q_i (not a divisor of k), where the R_1 to S_1 isomorphism maps $p_i^{\phi(j)}$ onto $q_i^{\phi(j)}$. If a is any positive integer relatively prime to j, write its decomposition into prime factors $p_1 p_2 p_3 \cdots$, and define $\psi(a) = \psi(p_1)\psi(p_2)\psi(p_3) \cdots$.

Let a and b be elements of R_i. Then both $a b^{\phi(j)-1}$ and $b^{\phi(j)}$ are in R_1. Since ψ, restricted to R_1, is the R_1 to S_1 isomorphism, both of these products are mapped by ψ into S_1. Now it is easy to show that $\psi(a)$ and $\psi(b)$ are in the same set S_i (ψ preserves congruence), and that ψ maps R_i onto S_i. Hence we can define a mapping of G_j onto G_k by defining the image of R_i' to be S_i', where ψ maps R_i onto S_i. It is easy to verify that this gives an isomorphism of G_j onto G_k.

3. **Monomorphisms and epihomomorphisms.** We can always define an isomorphism of R_1 into S_1 by setting up a one-to-one mapping of the primes into the primes of S_1 and extending the mapping to the product of primes as before. By defining a mapping of the primes in R_1 onto S_1 and by extending this mapping so that any prime not in R_1 maps onto 1, we have a homomorphism of R_1 onto S_1. However, there are many examples where there is no isomorphism of G_j into G_k and where there is no homomorphism of G_j onto G_k e.g. G_5 and G_8. Hence the theorem cannot be generalized to the case of monomorphisms or to the case of epihomomorphisms.

UNIVERSITY OF CALIFORNIA, DAVIS