Observe that if a legal move changes X to Y, then $A(Y) = A(X), B(Y) = B(X)$. This follows easily from the equation $\alpha^2 + \alpha + 1 = 0$, which in turn follows from the tables. Thus the pair $(A(X), B(X))$ is invariant under any sequence of legal moves.

The starting position X has $A(X) = B(X) = 1$. Therefore any position Y that arises during the game must satisfy $A(Y) = B(Y) = 1$. If the game ends with a single peg on (x, y) then $\alpha^{x+y} = \alpha^{x-y} = 1$. Now $\alpha^3 = 1$, so α has order 3 in the multiplicative group of nonzero elements of $\mathbb{GF}(4)$. Therefore $x+y, x-y$ are multiples of 3, so x, y are multiples of 3. Thus the only possible end positions are $(-3,0), (0,-3), (0,0), (0,3), (3,0)$. Experiment (by symmetry, only $(0,0)$, the traditional finish, and $(3,0)$ need be attempted; moreover, the same penultimate move must lead to both, depending on which peg is moved) shows that all five of these positions can be obtained by a series of legal moves.

EXERCISES

19.1 For which of the following values of n does there exist a field with n elements?

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 17,\ 24,\ 312,\ 65536,$$
$$65537,\ 83521,\ 103823,\ 2^{13466917} - 1$$

(*Hint:* See 'Mersenne primes' under 'Internet' in the References.)

19.2 Construct fields having 8, 9, and 16 elements.

19.3 Let ϕ be the Frobenius automorphism of $\mathbb{GF}(p^n)$. Find the smallest value of $m > 0$ such that ϕ^m is the identity map.

19.4 Show that the subfields of $\mathbb{GF}(p^n)$ are isomorphic to $\mathbb{GF}(p^r)$ where r divides n, and there exists a unique subfield for each such r.

19.5 Show that the Galois group of $\mathbb{GF}(p^n) : \mathbb{GF}(p)$ is cyclic of order n, generated by the Frobenius automorphism ϕ. Show that for finite fields the Galois correspondence is a bijection, and find the Galois groups of

$$\mathbb{GF}(p^n) : \mathbb{GF}(p^m)$$

whenever m divides n.

19.6 Are there any composite numbers r that divide all the binomial coefficients $\binom{r}{s}$ for $1 \leq s \leq r-1$?

19.7 Find generators for the multiplicative groups of $\mathbb{GF}(p^n)$ when $p^n = 8$, 9, 13, 17, 19, 23, 29, 31, 37, 41, and 49.

19.8 Show that the additive group of $\mathbb{GF}(p^n)$ is a direct product of n cyclic groups of order p.

19.9 By considering the field $\mathbb{Z}_2(t)$, show that the Frobenius monomorphism is not always an automorphism.

19.10* For which values of n does $\mathbb{S}_n$ contain an element of order $e(\mathbb{S}_n)$?
(*Hint:* Use the cycle decomposition to estimate the maximum order of an element of $\mathbb{S}_n$, and compare this with an estimate of $e(\mathbb{S}_n)$. You may need estimates on the size of the nth prime: for example, 'Bertrand's Postulate', which states that the interval $[n, 2n]$ contains a prime for any integer $n \geq 1$.)

* 19.11* Prove that in a finite field every element is a sum of two squares.

19.12 Mark the following true or false.

(a) There is a finite field with 124 elements.

(b) There is a finite field with 125 elements.

(c) There is a finite field with 126 elements.

(d) There is a finite field with 127 elements.

(e) There is a finite field with 128 elements.

(f) The multiplicative group of $\mathbb{GF}(19)$ contains an element of order 3.

(g) $\mathbb{GF}(2401)$ has a subfield isomorphic to $\mathbb{GF}(49)$.

(h) Any monomorphism from a finite field to itself is an automorphism.

(i) The additive group of a finite field is cyclic.