Groups, Fields, and Vector Spaces

Homework #1 (2018-2019), Answers

Q1: Group or not a group?

Which of the following are groups? If a group, is it commutative? Finite or infinite? If infinite, is it discrete or continuous? If not a group, where does it fail?

A. The even integers $\{... -6, -4, -2, 0, 2, 4, 6...\}$*, under multiplication*
Not a group. It fails to be a group because it doesn't contain the identity element

B. The set of all translations of 3-space, under composition
It's a commutative group; infinite; continuous

C. The set of all rotations of 3-space, under composition
It's a non-commutative group; infinite; continuous

D. The set of all $N \times N$ *matrices with integer entries, under matrix addition*
It's a commutative group, infinite, discrete

E. The set of all $N \times N$ *matrices with integer entries, under matrix multiplication*
Not a group. Some elements, for example, the matrix with all 0 entries, don't have inverses.

F. The set of all 2×2 *matrices with integer entries and determinant 1, under matrix multiplication*
It's a non-commutative group, infinite, discrete

G. Complex numbers, under addition
It's a commutative group, infinite, continuous

H. Complex numbers, under multiplication
Not a group. 0 has no inverse.

Q2. Modular arithmetic

For two integers x and y, we say $x = y$ *(mod k) if x and y differ by an integer multiple of k. So, for example, 3+4=2 (mod 5) and 6*9=10 (mod 11).*

A. Show that the integers $\{0,1,\ldots k-1\}$ *form a group under addition (mod k).*
Addition (mod *k*) inherits associativity and the identity element (0) from ordinary multiplication. To show that there's an additive inverse for an integer *x*, we note that $x+(k-x)=k$, so $x+(k-x)=0 \pmod{k}$, so $k-x$ is the additive inverse of *x*.

B. For what integers k do the integers $\{1,\dots k-1\}$ *form a group under multiplication (mod k)?*
It is a group if, and only if, *k* is prime.

Multiplication (mod *k*) inherits associativity and the identity element (1) from ordinary multiplication. To determine whether there's a multiplicative inverse for an integer *x*, we seek another integer *y* for which $xy = 1$ (mod *k*). This means that $xy = 1 + ka$ for some integer *a*, or, that $xy - ka = 1$. But if *x* and *k* have a common factor greater than 1, say *r*, then $xy - ka$ also has *r* as a common factor, so $xy = 1$ (mod *k*) cannot be solved, and *x* does not have an inverse. This means that if *k* is not a prime, then $\{1,\dots,k-1\}$ is not a group under multiplication (mod *k*).

Conversely, we can show that if *k* is a prime, then $\{1,\dots,k-1\}$ is a group. One way to see this is as follows. Consider (for $1 \le x \le k-1$) all powers of *x*, $x^1, x^2, \dots, x^q, \dots$, and reduce each of them (mod *k*) to numbers $< k$. Since there are only a finite number of possibilities in $1 \le x \le k-1$, eventually there have to be repeats. If this repeat occurs for the integer exponents *a* and *b* ($a < b$), then $x^a = x^b$ (mod *k*). This in turn means that $x^a = x^b + Nk$ for some integer *N*. Since *k* is prime, *x* cannot divide *k*, and therefore x^a must divide *N*. So $1 = x^{b-a} + N'k$ for some integer N', i.e., $x^{b-a} = 1$ (mod *k*). This in turn means that x^{b-a-1} is the multiplicative inverse of *x*.