Universität Konstanz
Fachbereich Mathematik und Statistik
Wintersemester 2010/2011

Dr. Andrew Dolphin
Prof. Dr. Markus Schweighofer

Solutions: Übungsblatt 1 zur Einführung in die Algebra

Aufgabe 1. Welche der folgenden sechs Definitionen des Gruppenbegriffes ist korrekt? Gebe jeweils einen Beweis oder ein Gegenbeispiel! „Eine Gruppe ist ein geordnetes Paar $(G,\cdot)$, wobei G eine Menge ist und $\cdot\colon G \times G \to G$ eine (meist infix oder gar nicht notierte) Abbildung ist derart, daß $(ab)c = a(bc)$ für alle $a,b,c \in G$ gilt und...

(a) $\exists e \in G : ((\forall a \in G : ea = a)\ \&\ (\forall a \in G : \exists b \in G : ab = e))$

(b) $\exists e \in G : ((\forall a \in G : ae = a)\ \&\ (\forall a \in G : \exists b \in G : ab = e))$

(c) $\exists e \in G : ((\forall a \in G : ae = a)\ \&\ (\forall a \in G : \exists b \in G : ba = e))$

(d) $\exists e \in G : ((\forall a \in G : ea = a)\ \&\ (\forall a \in G : \exists b \in G : ba = e))$

(e) $(\forall a,b \in G : \exists x \in G : xa = b)\ \&\ (\forall a,b \in G : \exists y \in G : ay = b)$

(f) $\forall a,b \in G : \exists x,y \in G : xay = b$“

Solution

(a) No. Take any set G with more than 1 element, and take the $(G,\cdot)$ with the operation given by $a \cdot b = b$ for all $a,b \in G$. Then $e \cdot a = a$ for any $e \in G$, and $a \cdot e = e$, so any element is a left identity and every element has a right inverse with respect to any given left identity. But $(G,\cdot)$ is clearly not a group.

(b) Yes. We must prove that if both a right identity and for every element right inverse identity exist with respect to this right inverse, then this identity is also a left identity, and the inverses are also right inverses.

So, there exists $e \in G$ such that $ae = a$ for any $a \in G$, and $b \in G$ such that $ab = e$. Also, there exists $c \in G$ such that $bc = e$. Then

$$bab = be = b$$

$$ba = babc = bc = e.$$

Moreover

$$ea = (ab)a = a(ba) = ae,$$

therefore e is also a right identity, and the right inverses with respect to e given by the assumptions are also left inverses.

(c) Similar to (a).

(d) Similar to (b).

(e) The empty set is a counter example. However this was a misprint, so we assume that G is non-empty.

For all $a \in G$ there exist $y,x \in G$ such that $y \cdot a = a$ and $a \cdot x = a$, and $y_b,x_b \in G$ such that $y_b \cdot a = b$ and $a \cdot x_b = b$ for all $b \in G$.

Hence $b = y_b(ax) = (y_b a)x = bx$, hence x is a right identity for all elements of G. Similarly y is a left identity. We also have that $y = yx = x$ as $x,y \in G$, hence x is both a left and right identity.

Finally, we have that, for all $a \in G$, there exist $b,c \in G$ such that $ba = x = ac$. Hence $c = xc = (ba)c = b(ac) = bx = b$, so the right inverse equals the left inverse for any $a \in G$.

(f) No. The semigroup in (a) is also a counter example here.

Aufgabe 2. Ein geordnetes Paar $(S,\cdot)$ mit einer Menge S und einer (meist infix oder gar nicht notierten) Abbildung $\cdot\colon S \times S \to S$ heißt *Halbgruppe*, wenn $(ab)c = a(bc)$ für alle $a,b,c \in S$ gilt. Eine Halbgruppe $(S,\cdot)$ heißt *Monoid*, wenn es ein $e \in S$ gibt mit $ae = a = ea$ für alle $a \in S$. Zeigen Sie, daß ein endliches Monoid $(S,\cdot)$, in dem die beiden „Kürzungsregeln“

$$\forall a,b,c \in S : (ac = bc \implies a = b) \qquad \text{und} \qquad \forall a,b,c \in S : (ca = cb \implies a = b)$$

gelten, eine Gruppe ist. Ist diese Aussage allgemeiner sogar richtig für endliche Halbgruppen $(S,\cdot)$? Was ist, wenn S unendlich ist?

Solution

Suppose $(S,\cdot)$ is a finite Monoid with identity e. Then, for all $x \in S$, we must have $x^n = x^m$ for some distinct $n,m > 0$. By cancellation, we see that $x^{m-n} = e$, hence every element has an inverse and therefore $(S,\cdot)$ is a group.

Suppose $(S,\cdot)$ is a finite Semigroup (Halbgruppe) with cancellation. For $a \in S$, we define a map $S \to aS$ given by $s \mapsto as$ for all $s \in S$. This map is injective by cancellation, as if $as = at$ then $s = t$ for all $s = t$. It is also surjective. Hence $aS = S$ for all $a \in S$ by the finiteness of S, and similarly $Sa = S$.

In particular, there exists an $e_a \in S$ such that $ae_a = a$. This gives $ae_a a = a^2$, and hence by cancellation, $e_a a = a$. We also have $ae_a x = ax$ for all $x \in G$. Cancellation then gives $e_a x = x$, hence e_a is a left identity on G. One can show it is a right identity similarly.

Finally, $(\mathbb{Z} \setminus \{0\}, \cdot)$ is a Monoid with cancellation, but not a group.

Aufgabe 3. Sei K ein endlicher Körper mit q Elementen. Was ist die Gruppenordnung von $\mathrm{GL}_n(K)$?

Solution

We will count the $n \times n$ matrices whose rows are linearly independent. The first row can be anything other than the zero row, so there are $q^n - 1$ possibilities.

The second row must be linearly independent from the first, which is to say that it must not be a multiple of the first. Since there are q multiples of the first row, there are $q^n - q$ possibilities for the second row.

In general, the ith row must be linearly independent from the first $i-1$ rows, which means that it can't be a linear combination of the first $i-1$ rows. There are q^{i-1} linear combinations of the first $i-1$ rows, so there are $q^n - q^{i-1}$ possibilities for the ith row. Once we build the entire matrix this way, we know that the rows are all linearly independent by choice. Also, we can build any $n \times n$ matrix whose rows are linearly independent in this fashion. Thus, there are $(q^n - 1)(q^n - q)\dots(q^n - q^{n-1}) = \prod_{k=0}^{n-1}(q^n - q^k)$ matrices.