ALGEBRAIC STRUCTURES

Xantcha

Solutions 16th December 2013

1. (a) —

   (b) $48 = -12$ has clearly order 5.

   (c) Clearly each element of $\langle 8, 30 \rangle$ is even, so $\langle 8, 30 \rangle \leqslant \langle 2 \rangle$. Conversely, $2 = 4 \cdot 8 - 30 \in \langle 8, 30 \rangle$, so in fact

   $$\langle 8, 30 \rangle = \langle 2 \rangle = \{ 0, 2, 4, \ldots, 58 \}.$$

   (d) The group $\mathbf{Z}_{60}^*$ consists of those elements with multiplicative inverses modulo 60. These are the numbers relatively prime to 60, and there are 16 of those:

   $$1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ 49,\ 53,\ 59.$$

2. (a) —

   (b) A is closed under multiplication since

   $$2^a 3^b \cdot 2^c 3^d = 2^{a+c} 3^{b+d}.$$

   Also $1 = 2^0 3^0 \in A$ and $(2^a 3^b)^{-1} = 2^{-a} 3^{-b} \in A$. Therefore A is a subgroup of $\mathbf{Q}^+$.

   (c) Define a map

   $$\varphi\colon \mathbf{Z} \times \mathbf{Z} \in A, \quad (a, b) \mapsto 2^a 3^b.$$

   This is an homomorphism since

   $$\varphi(a, b)\varphi(c, d) = 2^a 3^b \cdot 2^c 3^d = 2^{a+c} 3^{b+d} = \varphi(a + c, b + d).$$

   It is surjective by the very definition of A, and also injective, since $1 = \varphi(a, b) = 2^a 3^b$ implies $a = b = 0$.

3. (a) —

   (b) K is a field if and only if the polynomial $p(x) = x^4 + x + 1$ is irreducible over $\mathbf{Z}_2$. It has no linear factors, since $p(0) = p(1) = 1$. To search for quadratic factors, we try

$$x^4 + x + 1 = (x^2 + ax + b)(x^2 + cx + d),$$

   and are led to the system of equations

$$\begin{cases} a + c &= 0 \\ b + ac + d &= 0 \\ ad + bc &= 1 \\ bd &= 1. \end{cases}$$

   From the first and last of these equations, we deduce $a = c$ and $b = d = 1$, which does not satisfy the third equation. Hence $p(x)$ is irreducible and K is a field.

   Every element of K can be uniquely represented by a cubic polynomial:

$$a + bx + cx^2 + dx^3 + (p(x)), \qquad a, b, c, d \in \mathbf{Z}_2.$$

   Therefore the order of K is $2^4 = 16$.

   (c) The multiplicative group of any finite field is cyclic.

   (d) The extension $\mathbf{Z}_2 \leqslant K$ is finite (it has degree 4), and so necessarily algebraic.

4. (a) —

   (b) Calculate:

$$\pi(x, y) + \pi(z, w) = x + y + z + w = \pi(x + z, y + w).$$

   (c) Since $\pi(x, 0) = x$, the image of π is all of $\mathbf{R}$. The kernel is the set of all $(t, -t)$, where $t \in \mathbf{R}$.

   (d) The kernel is the line of all $(t, -t)$, where $t \in \mathbf{R}$, and so the cosets will be lines parallel to it. The coset containing (x, y) is the set

$$\{\, (x, y) + (t, -t) \mid t \in \mathbf{R} \,\}.$$

5. (a) —

   (b) By the Tower Isomorphism Theorem,

$$\begin{aligned} \mathbf{C}[x]/(x^3 - 1)\Big/(x - 1 + (x^3 - 1)) &= \mathbf{C}[x]/(x^3 - 1)\Big/(x - 1)/(x^3 - 1) \\ &\cong \mathbf{C}[x]/(x - 1) \cong \mathbf{C} \end{aligned}$$

   is a field, and therefore $(x - 1 + (x^3 - 1))$ is maximal (and prime).

(c) One has

$$(x-1+(x^3-1))(x^2+x+1+(x^3-1)) = x^3-1+(x^3-1) = 0+(x^3-1),$$

but neither of the factors is in $(0+(x^3-1))$.

(d) The ideals of $\mathbf{C}[x]/(x^3-1)$ are of the form $(p(x))/(x^3-1)$, where $(p(x))$ is an ideal of $\mathbf{C}[x]$ that contains x^3-1, which means that $p(x) \mid x^3-1$. When that is the case,

$$\mathbf{C}[x]/(x^3-1)\Big/(p(x))/(x^3-1) \cong \mathbf{C}[x]/(p(x)).$$

This is an integral domain precisely when $(p(x))$ is a maximal ideal of $\mathbf{C}[x]$, which holds if and only if $p(x)$ is irreducible. It is a field precisely when $(p(x))$ is a prime ideal of $\mathbf{C}[x]$, which holds if and only if $p(x)$ is irreducible *or* zero. Hence the only possibility for a prime ideal which is not maximal is given by $p(x) = 0$, but $p(x)$ is not a divisor of x^3-1.

(e) Maximal ideals are always prime.

6. (a) —

(b) Factorise:

$$x^5-x^4-x+1 = (x-1)(x^4-1) = (x-1)^2(x+1)(x-i)(x+i).$$

The splitting field is $\mathbf{Q}(i)$. Any automorphism of $\mathbf{Q}(i)$ fixing $\mathbf{Q}$ must permute $\pm i$. Consequently, the Galois group contains precisely two elements: the identity map and the complex conjugation map. It is isomorphic to $\mathbf{Z}_2$.

(c) Obviously.

7. (a) Calculate:

$$\varphi(xy) = (xy)^3 = x^3y^3 = \varphi(x)\varphi(y)$$
$$\varphi(x+y) = (x+y)^3 = x^3+3x^2y+3xy^2+y^3 = x^3+y^3 = \varphi(x)+\varphi(y)$$
$$\varphi(1) = 1^3 = 1.$$

(b) We show that φ is injective. Suppose $0 = \varphi(z) = z^3$ for some $z \neq 0$. Then

$$(z+1)^3 = z^3+3z^2+3z+1 = 1,$$

so that $z+1$ is inversible. By the assumption on L, also z will be inversible. But it cannot be, since $z^3 = 0$. This contradiction shows that φ is injective. Since the ring L is finite, φ must then also be bijective.

(c) φ is a permutation on the finite set L, and so φ^n is the identity map for some n. Then $x = \varphi^n(x) = x^{3^n}$ for all x.

(d) Using that $x^{3^n} = x$, we compute:

$$(x^{3^n-1}+1)^2 = x^{2\cdot 3^n-2} + 2x^{3^n-1} + 1 = x^{3^n-1} + 2x^{3^n-1} + 1 = 1.$$

(e) We prove that an arbitrary $x \neq 0$ is inversible. We have $x^{3^n-1} \neq 0$, for $x^{3^n-1} = 0$ would imply $x = x^{3^n} = 0$.

By part (d), $x^{3^n-1} + 1$ is inversible, from which it follows, using the assumption on L, that x^{3^n-1} is also inversible.

The element x cannot be a zero divisor, for $xy = 0$ would imply $x^{3^n-1}y = 0$, and therefore $y = 0$, since x^{3^n-1} is inversible.

By part (c), $x(x^{3^n-1} - 1) = 0$, and, x not being a zero divisor, it must be that $x^{3^n-1} = 1$, and so x is inversible.