ALGEBRAIC STRUCTURES

Xantcha

Solutions 2nd April 2013

1. (a) —

   (b) M is the set of inversible matrices. Matrix multiplication is always associative, and products and inverses of inversible matrices are inversible. The identity matrix I is the neutral element.

   The group is not abelian, for

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

   (c) M contains six elements:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

   It must therefore be isomorphic to the third symmetric (or dihedral) group.

   (d) The axioms for a group action are immediate:

$$A \cdot B \begin{pmatrix} x \\ y \end{pmatrix} = (AB) \begin{pmatrix} x \\ y \end{pmatrix}$$

   and

$$Ix = x.$$

   (e) Since

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

and

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

but

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix},$$

the orbits are $\{(1,0),(0,1),(1,1)\}$ and $\{(0,0)\}$.

2. (a) —
   (b) The polynomial $x^6 + 9x + 6$ is irreducible by Eisenstein's Criterion, applied at the prime 3. Therefore the factor ring is a field.
   (c) The simple extension $\mathbf{Q}(\theta)$ is isomorphic to the factor ring $\mathbf{Q}[x]/(x^6 + 9x + 6)$, with θ corresponding to the coset $x + (x^6 + 9x + 6)$. Polynomial divison yields

   $$x^6 + 9x + 6 = (1 + x)(x^5 - x^4 + x^3 - x^2 + x + 8) - 2,$$

   and hence

   $$(1+x)\cdot\frac{x^5 - x^4 + x^3 - x^2 + x + 8}{2} = \frac{1}{2}(x^6+9x+6)+1 \equiv 1 \mod x^6+9x+6.$$

   The inverse of $1 + \theta$ is $\frac{\theta^5-\theta^4+\theta^3-\theta^2+\theta+8}{2}$.

3. (a) —
   (b) One may consider the example

   $$\langle (13)(24) \rangle \trianglelefteq \langle (1234) \rangle \trianglelefteq D_4.$$

   Explicitly, these subgroups are

   $$\langle (13)(24) \rangle = \{(), (13)(24)\}$$
   $$\langle (1234) \rangle = \{(), (1234), (13)(24), (4321)\}.$$

   Since each group has index 2 in the succeeding one, every group is normal in the next. However, $\langle (13)(24) \rangle$ is not normal in D_4, for

   $$(12) \circ (13)(24) \circ (12)^{-1} = (14)(23) \notin \langle (13)(24) \rangle.$$

4. (a) —
   (b) The multiplicative identity is the constant function 1.

   F is not an integral domain, and therefore also not a field. Construct two non-zero functions f_- and f_+, chosen so that $f_+ = 0$ on the interval $(-\infty, 0]$ and $f_- = 0$ on the interval $[0, \infty)$. Then $f_- f_+ = 0$.

(c) C is not an ideal. The product of a constant function with an arbitrary function is not constant.

(d) If $f(0) = 0$ and g is arbitrary, then $(fg)(0) = f(0)g(0) = 0$, so Z is an ideal.

The factor ring $F/Z \cong \mathbf{R}$. Consider the homomorphism

$$\varphi\colon F \to \mathbf{R}, \quad f \mapsto f(0).$$

It is clearly onto, and its kernel is precisely Z. The Fundamental Homomorphism Theorem gives:

$$F/Z = F/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi = \mathbf{R}.$$

5. (a) —

(b) One easily verifies the following properties of the symmetric difference:

I. Associativity: $(A \sqcap B) \sqcap C = A \sqcap (B \sqcap C)$ is the set of elements belonging to exactly one or all three of A, B, C.

II. Commutativity: $A \sqcap B = B \sqcap A$.

III. Identity: $A \sqcap \varnothing = A$.

IV. Inverse: $A \sqcap A = \varnothing$.

Hence $P(X)$ is an abelian group in which the empty set is the identity and every set is its own inverse.

(c) Number the elements: $X = \{x_1, \ldots, x_n\}$. There is an homomorphism $\varphi\colon \mathbf{Z}_2^n \to P(X)$ given by

$$(e_1, \ldots, e_n) \mapsto \{\, x_k \mid e_k = 1 \,\}.$$

The homomorphism property is verified thus:

$$\begin{aligned}
\varphi(e_1, \ldots, e_n) \sqcap \varphi(f_1, \ldots, f_n) &= \{\, x_k \mid e_k = 1 \,\} \sqcap \{\, x_k \mid f_k = 1 \,\} \\
&= \{\, x_k \mid (e_k = 1 \ \vee\ f_k = 1) \ \wedge\ \neg(e_k = f_k = 1) \,\} \\
&= \{\, x_k \mid e_k + f_k = 1 \,\} \\
&= \varphi(e_1 + f_1, \ldots, e_n + f_n).
\end{aligned}$$

The inverse of φ^{-1} maps A to the vector $(e_1, \ldots, e_n)$, where $e_k = 1$ if $x_k \in A$ and $e_k = 0$ if $x_k \notin A$. Hence we have an isomorphism of groups $\mathbf{Z}_2^n \cong P(X)$.

6. (a) —

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	1	$-i$
k	k	j	i	1

TABLE 1: Multiplication table for the Split-Quaternions.

(b) One easily finds the multiplication table in Table 1.

(c) S is not commutative, since $ij = k \neq -k = ji$. It will also have zero divisors: $(j+1)(j-1) = j^2 - 1 = 0$.

(d) Define the isomorphism $S \to \mathbf{R}^{2\times 2}$ by

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad i \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad j \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad k \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Since these four matrices constitute a basis for $\mathbf{R}^{2\times 2}$, and they satisfy the defining relations for the split-quaternions, this will be an isomorphism.

7. (a) —

(b) The factorisation is

$$p(x) = x^6 - 64 = (x^3-8)(x^3+8) = (x-2)(x^2+2x+4)(x+2)(x^2-2x+4).$$

The quadratic polynomials are clearly irreducible, since their roots are $-1 \pm \sqrt{-3}$ and $1 \pm \sqrt{-3}$, respectively.

(c) To find the Galois group, we observe that an automorphism of the splitting field $\mathbf{Q}(\sqrt{-3})$ is uniquely determined by its value on $\sqrt{-3}$. Since $\sqrt{-3}$ must map to $\pm\sqrt{-3}$, the automorphism group is isomorphic with $\mathbf{Z}_2$.