ALGEBRAIC STRUCTURES

XANTCHA

Solutions 23rd April 2014

1. (a) —

   (b) —

   (c) Since $2014 = 2 \cdot 19 \cdot 53$, there is exactly one abelian group of order 2014, the cyclic group $\mathbf{Z}_{2014}$.

   (d) There is, for example, the dihedral group D_{1007}.

2. (a) —

   (b) If $a^2, b^2 \in B$, then also

   $$a^2b^2 = (ab)^2 \in B, \qquad a^2 + b^2 = (a+b)^2 \in B \quad \text{and} \quad -a^2 = a^2 \in B.$$

   (c) If $A = \mathbf{Z}_2[x]$, then $1 = 1^2 \in B$, but $x \cdot 1 = x \notin B$.

   (d) If $A = \mathbf{Z}$, then $1 = 1^2 \in B$, but $1 + 1 = 2 \notin B$.

3. (a) —

   (b) It is known from linear algebra that $\det AB = \det A \det B$.

   (c) Since $\mathrm{SL}_n(\mathbf{C}) = \operatorname{Ker} \det$, it is a normal subgroup. Alternatively, one may show directly that if $\det A = 1$ and M is arbitrary, then

   $$\det MAM^{-1} = \det M \det A \det M^{-1} = \det A = 1,$$

   so that $MAM^{-1} \in \mathrm{SL}_n(\mathbf{C})$.

   (d) The Fundamental Homomorphism Theorem gives

   $$\mathrm{GL}_n(\mathbf{C})/\mathrm{SL}_n(\mathbf{C}) = \mathrm{GL}_n(\mathbf{C})/\operatorname{Ker}\det \cong \operatorname{Im}\det = \mathbf{C}^*.$$

4. (a) —

(b) Since $\mathbf{Z}_4[x]/(x) \cong \mathbf{Z}_4$ is not an integral domain, (x) is neither prime nor maximal.

(c) Since $\mathbf{Z}_4[x]/(2,x) \cong \mathbf{Z}_2$ is a field, $(2,x)$ is both maximal and prime.

(d) Since $\mathbf{Z}_4[x]/(2) \cong \mathbf{Z}_2[x]$ is an integral domain, but not a field, the ideal (2) is prime, but not maximal.

(e) No. Maximal ideals are always prime.

5. (a) —

(b) Factorise

$$\begin{aligned} p(x) &= x^8 - x^2 = x^2(x^6 - 1) = x^2(x^2 - 1)(x^4 + x^2 + 1) \\ &= x^2(x+1)(x-1)(x^2 + x + 1)(x^2 - x + 1). \end{aligned}$$

The roots 0 and ± 1 are rational. The remaining roots are $\pm\frac{1}{2} \pm \frac{1}{2}\sqrt{3}i$. Hence the splitting field is $\mathbf{Q}(\sqrt{3}i)$, which is of degree 2 over $\mathbf{Q}$. Therefore the Galois group is $\mathbf{Z}_2$.

6. (a) —

(b) If $f(x) = ax + b$ and $g(x) = cx + d$ are affine functions, then so is $g \circ f$:

$$g(f(x)) = c(ax + b) + d = acx + (bc + d).$$

Function composition is associative. The identity function $i(x) = x$ is affine. Moreover, $f(x) = ax + b$ has an inverse $f^{-1}(x) = a^{-1} - a^{-1}b$, since

$$\begin{aligned} f^{-1}(f(x)) &= a^{-1}(ax + b) - a^{-1}b = x \\ f(f^{-1}(x)) &= a(a^{-1}x - a^{-1}b) + b = x. \end{aligned}$$

Consequently, A is a group.

(c) This is more or less evident from the definition, since $f(g(x)) = (f \circ g)(x)$ and $i(x) = x$.

(d) Since $x + b$ transforms the point p to $p + b$ and the constant b may be chosen arbitrarily, the orbit of p is $Ap = \mathbf{R}$.

$f(x) = ax + b$ stabilises p if and only if $p = f(p) = ap + b$, which means the stabiliser of p equals

$$A_p = \{ f(x) = ax + p(1 - a) \mid a \neq 0 \}.$$

7. (a) —

(b) Write $q(x) = x^3 + ax^2 + bx + c$. By Viète's Formulæ , there is a relation $\alpha + \beta + \gamma = -a \in \mathbf{Q}$, which means the splitting field is

$$\mathbf{Q}(\alpha, \beta, \gamma) = \mathbf{Q}(\alpha, \beta, -a - \alpha - \beta) = \mathbf{Q}(\alpha, \beta).$$

(c) If $q(x) = (x - 1)^3$, then the splitting field is $\mathbf{Q}(1) = \mathbf{Q}$.

(d) If $q(x) = x^3 - 2$, then the splitting field is

$$\mathbf{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}e^{\frac{4\pi i}{3}}) = \mathbf{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}})$$

which is of degree 6 over $\mathbf{Q}$. However,

$$\mathbf{Q}(\sqrt[3]{2}), \qquad \mathbf{Q}(\sqrt[3]{2}e^{\frac{2\pi i}{3}}) \qquad \text{and} \qquad \mathbf{Q}(\sqrt[3]{2}e^{\frac{4\pi i}{3}})$$

are all of degree 3 over $\mathbf{Q}$, so they must be proper subfields.