

1202 Exercise 1 Solutions

Q1. Prove the following basic results about divisibility in \mathbf{Z} , for $a, b, c \in \mathbf{Z}$ (from Propn 1.2 in lectures): **(i)** if $a|b$ and $b|c$, then $a|c$. **(ii)** if $a, b \neq 0$ and $a|b$ and $b|a$ then $a = \pm b$.

Solution (i) If $a|b$ and $b|c$, then there exist m and n such that $b = am$ and $c = bn$. Hence $c = amn$, so $a|c$

(ii) If $a|b$ and $b|a$ then there exist m and n such that $b = am$ and $a = bn$. Then $b = am = bnm$, so $b(1 - nm) = 0$. Since $b \neq 0$, $1 - nm = 0$, i.e. $nm = 1$. But the only two integers that multiply to 1 are 1×1 and -1×-1 . Hence $m = \pm 1$ and so $a = \pm b$.

Q2. (i) Use Euclid's algorithm to find the highest common factor d of 2406 and 330. Also find integers r and s such that $d = 2406r + 330s$.

(ii) Use Euclid's algorithm to find the highest common factor d of 10414 and 9129. Also find integers h and k such that $d = 10414h + 9129k$.

$$\begin{array}{rcll} \text{Solution(i)} & 2406 & = & 330 \times 7 & + & 96 \\ & 330 & = & 96 \times 3 & + & 42 \\ & 96 & = & 42 \times 2 & + & 12 \\ & 42 & = & 12 \times 3 & + & 6 \\ & 12 & = & 6 \times 2 & (+ & 0) \end{array}$$

Hence $hcf(2406, 330) = 6$. Also

$$6 = 42 - 12 \times 3 = 42 - (96 - 42 \times 2) \times 3 = 42 \times 7 - 96 \times 3 = (330 - 96 \times 3) \times 7 - 96 \times 3 = 330 \times 7 - 96 \times 24 = 330 \times 7 - (2406 - 330 \times 7) \times 24 = 330 \times 175 - 2406 \times 24.$$

$$\begin{array}{rcll} \text{* (ii)} & 10414 & = & 9129 \times 1 & + & 1285 \\ & 9129 & = & 1285 \times 7 & + & 134 \\ & 1285 & = & 134 \times 9 & + & 79 \\ & 134 & = & 79 \times 1 & + & 55 \\ & 79 & = & 55 \times 1 & + & 24 \\ & 55 & = & 24 \times 2 & + & 7 \\ & 24 & = & 7 \times 3 & + & 3 \\ & 7 & = & 3 \times 2 & + & 1 \\ & 3 & = & 1 \times 3 & (+ & 0) \end{array}$$

Hence $hcf(10404, 9129) = 1$. Also

$$\begin{aligned} 1 &= 7 - 3 \times 2 = 7 - (24 - 7 \times 3) \times 2 = 7 \times 7 - 24 \times 2 = (55 - 24 \times 2) \times 7 - 24 \times 2 = \\ &55 \times 7 - 24 \times 16 = 55 \times 7 - (79 - 55) \times 16 = 55 \times 23 - 79 \times 16 = (134 - 79) \times 23 - \\ &79 \times 16 = 134 \times 23 - 79 \times 39 = 134 \times 23 - (1285 - 134 \times 9) \times 39 = 134 \times 374 - \\ &1285 \times 39 = (9129 - 1285 \times 7) \times 374 - 1285 \times 39 = 9129 \times 374 - 1285 \times 2657 = \\ &9129 \times 374 - (10414 - 9129) \times 2657 = 9129 \times 3031 - 10414 \times 2657 \end{aligned}$$

Q3. (i) Prove that any prime number > 3 is either of the form $3n + 1$ or $3n + 2$ for some integer n . Show that the product of any set of numbers of the form $3n + 1$ is again of the same form.

(ii) Modify Euclid's proof that there are an infinite number of primes to show that there are an infinite number of primes of the form $3n + 2$ (e.g. 5, 11, 17, 23, 29, 41 etc)

(iii) Does this method work for primes of the form $3n + 1$? Can you find any other cases where this method of proof will work?

Solution. (i) Any integer is of the form $3n$ or $3n + 1$ or $3n + 2$, since you can divide it by 3 and leave a remainder between 0 and 2. Any number of the form $3n$ is not prime (unless it is 3); hence any prime > 3 must be of the form $3n + 1$ or $3n + 2$.

Now $(3n + 1)(3m + 1) = 9nm + 3m + 3n + 1 = 3(3nm + m + n) + 1 = 3r + 1$ is of the required form; by induction, any product of numbers of this form is again of this form. (Formally, let $P(k)$ denote the statement that the product of k numbers of this form is of this form. $k = 1$ is obvious, and we have just proved $k = 2$. Now suppose $P(m)$ holds. Then if we have $m + 1$ numbers of this form a_1, \dots, a_{m+1} , then we can write $a_1 \dots a_{m+1} = (a_1 \dots a_m) a_{m+1}$. By the inductive hypothesis, $a_1 \dots a_m$ is of this form, and now by the case $k = 2$, $(a_1 \dots a_m) a_{m+1}$ is of this form. Thus $P(1)$ is true and also $P(m) \Rightarrow P(m + 1)$, so by induction $P(k)$ is true for all k .)

(ii) Suppose that there are only finitely many primes of the form $3n + 2$, say 2 and p_1, p_2, \dots, p_m . We will derive a contradiction by showing that in fact there is another one. Let $N = 3p_1 p_2 \dots p_m + 2$. This has a prime factorization. Clearly neither 2 nor 3 are factors of N , since N is odd and leaves remainder 2 on division by 3. Hence all the primes occurring in this factorization are of the form $3n + 1$ or $3n + 2$. If they were all of the form $3n + 1$ then their product N would also be of this form, a contradiction. Hence N has at least one prime factor of the form $3n + 2$. This clearly cannot be equal to any of p_1, \dots, p_m , since they do not divide N , nor can it be 2, since N is odd. Hence we have found another prime of the form $3n + 2$.

(iii) This does not work for primes of the form $3n + 1$ since it is not true that a product of some number of primes of the form $3n + 2$ is necessarily of the form $3n + 2$.

However, the same method of proof works for primes of the form $6n + 5$. All primes $p > 6$ are of form $6n + 1$ or $6n + 5$ (since otherwise p would have a factor of 2 or 3); suppose there were only finitely many primes $p > 5$ of the form $6n + 5$, say p_1, \dots, p_n . Then consider $N = 6p_1 \dots p_n + 5$. This does not have a factor of 2, 3 or 5, so all its factors must be of the form $6n + 1$ or $6n + 5$. If they are all of the form $6n + 1$, then N would be of the form $6n + 1$ (since multiplying numbers of the form $6n + 1$ together produces another of the same form), a contradiction. Hence N has at least one prime factor of the form $6n + 5$, which cannot be any of p_1, \dots, p_n , a contradiction.

Q4. Let S be the set of complex numbers of the form $a + b\sqrt{-5}$ ($a, b \in \mathbf{Z}$). If we add or multiply two elements of S we get another element of S , e.g. $(1 + \sqrt{-5})(2 - 3\sqrt{-5}) = 2 - 3 \times -5 + 2\sqrt{-5} - 3\sqrt{-5} = 17 - \sqrt{-5}$. Since S is a subset of \mathbf{C} , all the usual rules, such as $a(b + c) = ab + ac$, apply. We can now define factorization, divisibility, etc, as before e.g. since $(1 + \sqrt{-5})(1 - \sqrt{-5}) = -4$, we have that $1 + \sqrt{-5}$ divides -4 . We call an element $s \neq \pm 1$ of S *irreducible* if it has no non-trivial factorizations (i.e. if $s = ab$ then one of a, b is ± 1) - so irreducible elements here correspond to what we called primes in \mathbf{Z} .

(i) For any $s = a + b\sqrt{-5} \in S$, define the *norm* of s by $N(s) = a^2 + 5b^2$. Show that $N(st) = N(s)N(t)$ and that $N(s) = 1 \Leftrightarrow s = \pm 1$. Prove that there are no elements s of S with $N(s) = 3$.

(ii) Prove that 3 is an irreducible element of S .

(iii) Show that 9 has two different factorisations into the product of 2 irreducible elements in S .

This shows that S does **not** have unique factorization into irreducible elements

Solution. (i) Let $s = a + b\sqrt{-5}$ and $t = c + d\sqrt{-5}$. Then by direct calculation,

$$\begin{aligned} N(st) &= N(ac - 5bd + (ad + bc)\sqrt{-5}) = (ac - 5bd)^2 + 5(ad + bc)^2 \\ &= a^2c^2 - 10abcd + 25b^2d^2 + 5(a^2d^2 + 2abcd + b^2c^2) \\ &= a^2c^2 + 25b^2d^2 + 5a^2d^2 + 5b^2c^2 = (a^2 + 5b^2)(c^2 + 5d^2) \end{aligned}$$

$$= N(s)N(t),.$$

[Or note that $N(s) = (a + b\sqrt{-5})(a - b\sqrt{-5}) = s\bar{s}$, where \bar{s} is the normal complex conjugate of s . Then $N(st) = (st)(\overline{st}) = st\bar{s}\bar{t} = a\bar{s}t\bar{t} = N(s)N(t)$.]

If $N(s) = 1$ then $a^2 + 5b^2 = 1$ and the only solution to this is $b = 0$, $a = \pm 1$.

If $N(s) = 3$ then $a^2 + 5b^2 = 3$ and there are no solutions to this in integers; hence there are no elements of S of norm 3.

(ii) Suppose $3 = st$, $s, t \in S$. Then $9 = N(3) = N(st) = N(s)N(t)$. This is an equation in \mathbf{N} , so $N(s)$ must be 1 or 3 or 9. If $N(s) = 1$ then $s = \pm 1$. $N(s) = 3$ is impossible by (i). If $N(s) = 9$, then $N(t) = 1$ and hence $t = \pm 1$. Thus either s or t is ± 1 and hence 3 has no non-trivial factorisation. Thus 3 is an irreducible element of S .

(iii) In a similar way $2 + \sqrt{-5}$ has norm 9 and hence is an irreducible element of S . Now

$$9 = 3 \times 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$$

gives two different factorizations of 9 as a product of 2 irreducible elements.

Hence S does not have unique factorization into irreducible elements.

1202 2011-12 Exercise 2

1. Learn and write down the definition of a *group*, including the definitions of the terms used.

2. For each of the following sets G and operations \star state, with justification, whether or not (a) \star is associative, (b) there is an identity element, (c) all elements have an inverse, (d) G under \star is a group.

***(i)** $G = \mathbf{R}$, $a \star b = a$

(ii) $G = \mathbf{R}$, $a \star b = \sqrt[3]{a^3 + b^3}$

***(iii)** $G = \mathbf{C}$, $a \star b = a + b + a^2b^2$

(iv) $G = \mathcal{P}(\mathbf{R})$, $A \star B = A \cup B$

***(v)** $G = \mathcal{P}(\mathbf{R})$, $A \star B = A \triangle B$

(here $\mathcal{P}(\mathbf{R})$ denotes the set of all subsets of \mathbf{R} and $A \triangle B = (A \cap B^c) \cup (A^c \cap B)$)

***3** Let G be a finite set and \star an associative binary operation on G with identity element e . Suppose that G satisfies the cancellation laws, i.e. $(f \star g = f \star h \Rightarrow g = h)$ and $(g \star f = h \star f \Rightarrow g = h)$. Prove that G is a group. Give an example to show this need not be true if G is not finite.

4 Write down the group tables for

(i) \mathbf{Z}_4 under addition;

(ii) \mathbf{Z}_3^* under multiplication;

***(iii)** \mathbf{Z}_7 under addition;

***(iv)** \mathbf{Z}_7^* under multiplication.

5*(i) Let p be a prime. Prove that if a is an element of \mathbf{Z}_p^* then $\overline{a^{p-1}} = \overline{1}$, i.e. for any integer a not divisible by p , $a^{p-1} \equiv 1 \pmod{p}$.

(ii) Find $5^{2401} \pmod{13}$

***(iii)** Find $6^{422} \pmod{43}$.

[Hint for (i): Consider the set $S = \{\overline{a}, \overline{2a}, \overline{3a}, \dots, \overline{(p-1)a}\}$ in the group \mathbf{Z}_p^* . Consider the product of all the elements in S and use Proposition 2.8. This result is sometimes called Fermat's Little Theorem - we will prove it again in a different way in lectures.]

*You are advised to attempt all questions. Please hand in the **assessed** question/parts (those marked with a $*$) on Wednesday 2 February at the lecture. Help will be available at the problem class on Friday.*

1202 2011-12 Exercise 2 Solutions

1.(i) A *group* is a set G with a (closed) binary operation \star on G such that

(G1) \star is associative, i.e. for all $a, b, c \in G$, $a \star (b \star c) = (a \star b) \star c$,

(G2) there is an identity element, i.e. there exists $e \in G$ such that $g \star e = e \star g = g$ for all $g \in G$, and

(G3) all elements of G have inverses, i.e. for all $g \in G$, there exists $h \in G$ such that $g \star h = h \star g = e$.

2 (i) $G = \mathbf{R}$, $a \star b = a$. This is clearly a well-defined binary operation.

(a) It is associative: for all $a, b, c \in \mathbf{R}$, $(a \star b) \star c = a \star c = a$ and $a \star (b \star c) = a \star c = a$.

(b) There is no identity element. Suppose e was the identity. Then $0 = e \star 0 = e$ and $1 = e \star 1 = e$, so $0 = e = 1$, a contradiction.

(c) Since there is no identity element, there is no question of inverses.

(d) Hence it is not a group.

(ii) $G = \mathbf{R}$, $a \star b = \sqrt[3]{a^3 + b^3}$.

\star is a well-defined binary operation on \mathbf{R} , since each real number has a unique real cube root.

(a) It is associative:

$$(a \star b) \star c = \sqrt[3]{a^3 + b^3} \star c = \sqrt[3]{(\sqrt[3]{a^3 + b^3})^3 + c^3} = \sqrt[3]{a^3 + b^3 + c^3}$$

$$a \star (b \star c) = a \star \sqrt[3]{b^3 + c^3} = \sqrt[3]{a^3 + (\sqrt[3]{b^3 + c^3})^3} = \sqrt[3]{a^3 + b^3 + c^3}$$

(b) The identity element is 0, since $a \star 0 = \sqrt[3]{a^3 + 0^3} = a = 0 \star a$.

(c) Since $a \star (-a) = \sqrt[3]{a^3 + (-a)^3} = 0 = (-a) \star a$, each element a has inverse $-a$.

(d) Thus G is a group.

(iii) $G = \mathbf{C}$, $a \star b = a + b + a^2 b^2$. This is clearly a well-defined binary operation.

(a) \star is not associative. Example is: $(1 \star 1) \star 2 = 3 \star 2 = 41$, while $1 \star (1 \star 2) = 1 \star 7 = 57$

(b) 0 is the identity element, since for all $a \in \mathbf{C}$, $a \star 0 = a = 0 \star a$.

(c) Does each $a \in \mathbf{R}$ have an inverse? Since $a \star x = x \star a$, we just need to solve $a \star x = 0$, i.e. $a + x + a^2 x^2 = 0$. If $a = 0$ this has the obvious solution $x = 0$, so the inverse of 0 is 0. Otherwise we have a quadratic in x , with solution $x = \frac{1}{2a^2}(-1 \pm \sqrt{1 - 4a^3})$. Thus for each $a \neq 0 \in \mathbf{C}$, $a \star \frac{1}{2a^2}(-1 \pm \sqrt{1 - 4a^3}) = 0$, i.e. a has an inverse. Thus every $a \in \mathbf{R}$ has an inverse (in fact, usually more than one inverse).

(d) Thus G is not a group.

(iv) $G = \mathcal{P}(\mathbf{R})$, $A \star B = A \cup B$.

(a) \star is associative, since $A \cup (B \cup C) = (A \cup B) \cup C$ for all sets A, B, C .

(b) \emptyset is the identity, since $A \star \emptyset = A \cup \emptyset = A = \emptyset \star A$ for all $A \in G$.

(c) Not all elements have an inverse, for example, the set $\{0\}$ does not since there is no set X such that $\{0\} \cup X = \emptyset$. (In fact, no element except the empty

set has an inverse.)

(v) $G = \mathcal{P}(X)$, $A \star B = A \Delta B$. This is clearly a well-defined binary operation.

(a) There is a little work in checking that it is associative, i.e. the set identity $A \Delta (B \Delta C) = (A \Delta B) \Delta C$ holds for all A, B, C , and this is most easily shown by a truth table.

First note the truth table for $A \Delta B$:

A	B	$A \Delta B$
T	T	F
T	F	T
F	T	T
F	F	F

A	B	C	$(A \Delta B)$	$(A \Delta B) \Delta C$	$(B \Delta C)$	$A \Delta (B \Delta C)$
T	T	T	F	T	F	T
T	T	F	F	F	T	F
T	F	T	T	F	T	F
T	F	F	T	T	F	T
F	T	T	T	F	F	F
F	T	F	T	T	T	T
F	F	T	F	T	T	T
F	F	F	F	F	F	F

and since the two relevant columns agree, we have $(A \Delta B) \Delta C = A \Delta (B \Delta C)$, so \star is associative.

(b) The identity is \emptyset , since $A \Delta \emptyset = A = \emptyset \Delta A$

(c) Each element is its own inverse, since $A \Delta A = \emptyset$.

(d) Thus G is a group.

***3** Let G have n elements, say $G = \{g_1, \dots, g_n\}$. Let $f \in G$ and consider the set $\{f \star g_1, f \star g_2, \dots, f \star g_n\}$. By the cancellation law, all the elements $f \star g_i$ are distinct and there are n of them; hence $\{f \star g_1, f \star g_2, \dots, f \star g_n\} = G$. Thus one of the $f \star g_i = e$. Similarly there exists j such that $g_j \star f = e$.

Now $g_j \star f \star g_i = g_j \star e = g_j$ and also $g_j \star f \star g_i = e \star g_i = g_i$ (using associativity) and hence $g_i = g_j$ is the inverse of f .

Thus every element has an inverse and so G is a group.

An example showing this does not work for infinite G is the set of non-zero integers under multiplication. This clearly satisfies the cancellation laws, but e.g. 2 has no inverse.

$$4 \text{ (i) } \mathbf{Z}_4 \text{ under } + \begin{array}{cccc} \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{0} & \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{1} & \bar{1} & \bar{2} & \bar{3} & \bar{0} \\ \bar{2} & \bar{2} & \bar{3} & \bar{0} & \bar{1} \\ \bar{3} & \bar{3} & \bar{0} & \bar{1} & \bar{2} \end{array}$$

$$(ii) \mathbf{Z}_3^* \text{ under multiplication: } \begin{array}{ccc} & \bar{1} & \bar{2} \\ \bar{1} & \bar{1} & \bar{2} \\ \bar{2} & \bar{2} & \bar{1} \end{array}$$

$$(iii) \mathbf{Z}_7 \text{ under } + \begin{array}{ccccccc} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{0} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{1} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} & \bar{0} \\ \bar{2} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} & \bar{0} & \bar{1} \\ \bar{3} & \bar{3} & \bar{4} & \bar{5} & \bar{6} & \bar{0} & \bar{1} & \bar{2} \\ \bar{4} & \bar{4} & \bar{5} & \bar{6} & \bar{0} & \bar{1} & \bar{2} & \bar{3} \\ \bar{5} & \bar{5} & \bar{6} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} \\ \bar{6} & \bar{6} & \bar{0} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} \end{array}$$

$$(iv) \mathbf{Z}_7^* \text{ under multiplication: } \begin{array}{cccccc} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{1} & \bar{1} & \bar{2} & \bar{3} & \bar{4} & \bar{5} & \bar{6} \\ \bar{2} & \bar{2} & \bar{4} & \bar{6} & \bar{1} & \bar{3} & \bar{5} \\ \bar{3} & \bar{3} & \bar{6} & \bar{2} & \bar{5} & \bar{1} & \bar{4} \\ \bar{4} & \bar{4} & \bar{1} & \bar{5} & \bar{2} & \bar{6} & \bar{3} \\ \bar{5} & \bar{5} & \bar{3} & \bar{1} & \bar{6} & \bar{4} & \bar{2} \\ \bar{6} & \bar{6} & \bar{5} & \bar{4} & \bar{3} & \bar{2} & \bar{1} \end{array}$$

5(i) Proposition 1.8 states (i) If $f, g, h \in G$, a group, and $fg = fh$ then $g = h$ and (ii) Let G be a group consisting of a finite number of elements g_1, \dots, g_n , and let g be one of these. Then the list gg_1, gg_2, \dots, gg_n contains each element of G exactly once.

Consider the set $S = \{\bar{a}, \bar{2a}, \bar{3a}, \dots, \overline{(p-1)a}\}$ in \mathbf{Z}_p^* . Since \mathbf{Z}_p^* is a group, Proposition 1.8 (ii) shows that S is the set of elements of \mathbf{Z}_p^* , listed in a different order. Hence the product of all the elements of S is equal to the product of all the elements of \mathbf{Z}_p^* , i.e.

$$\bar{a} \times \bar{2a} \times \bar{3a} \times \dots \times \overline{(p-1)a} = \bar{1} \times \bar{2} \times \dots \times \overline{p-1}$$

Now using the various abelian group rules and using the notation $\overline{(p-1)!}$ in the obvious way, we can re-arrange this as

$$\overline{(p-1)!} = \overline{(p-1)!} \times \bar{a}^{p-1}$$

Now by Proposition 1.8 (i), we can cancel $\overline{(p-1)!}$ to get the result.

(ii) By (a) $\bar{5}^{12} \equiv \bar{1}$ in \mathbf{Z}_{13}^* and hence $\overline{5^{2401}} = (\bar{2}^{12})^{200} \times \bar{5} \equiv \bar{5}$, (i.e. $5^{2401} \equiv 5 \pmod{13}$).

(iii) Since 43 is prime, $\overline{6^{42}} = \overline{1}$; also $422 = 42 \times 10 + 2$. Hence $\overline{6^{422}} = (\overline{6^{42}})^{10} \times \overline{6^2} = \overline{6^2} = \overline{36}$. (In other words, $6^{422} \equiv 36 \pmod{43}$.)

1202 2011-2012 Exercise 3

1 Let G be the symmetry group of T . Find all elements of G and find generators and relations for G in the following cases:

- (i) T is a square;
- *(ii) T is a regular pentagon.

2 *(i) Find $\overline{43}^{-1}$ in \mathbb{Z}_{53}^* and hence solve $43x \equiv 4 \pmod{53}$.

(ii) Solve $x^{17} \equiv 3 \pmod{53}$.

*(iii) Show that $x^{13} \equiv 2 \pmod{53}$ has no solution.

3 (i) Show that if $a, b, c \in \mathbb{Z}$ and $a|bc$ and a and b are coprime, then $a|c$.

*(ii) Let G be an abelian group and $g, h \in G$ with $o(g) = m$ and $o(h) = n$, where m and n are coprime. Show that $o(gh) = mn$.

*(iii) Give an example of a (non-abelian) group G and two elements $g, h \in G$ such that $o(g) = 2$ and $o(h) = 3$ but $o(gh) \neq 6$. (So the abelian condition is necessary in (ii)).

4 Write down and learn the conditions usually used to prove that a subset H of G is a subgroup.

5 Determine, with justification, whether or not the given sets H are subgroups of the given group G :

(i) $G = \mathbf{R} - \{0\}$ under \times , $H = \{x \in \mathbf{R} : x \geq 1\}$,

(ii) $G = \mathbf{R} - \{0\}$ under \times , $H = \{2^n : n \in \mathbb{Z}\}$,

(iii) $G = \mathbf{R} - \{0\}$ under \times , $H = \{x \in G : x^2 \in \mathbb{Q}\}$,

*(iv) $G = S(\mathbb{R})$, $H = \{f \in G : f(1) = 1\}$

*(v) $G = S(\mathbb{R})$, $H = \{f \in G : f(1) = 2\}$

*(vi) $G = S(\mathbb{R})$, $H = \{f \in G : f(\{1, 2\}) = \{1, 2\}\}$

(Note: $S(\mathbb{R})$ denotes the group of bijections from \mathbb{R} to \mathbb{R} under composition; if $X \subseteq \mathbb{R}$ then $f(X) = \{f(x) : x \in X\}$.)

*You are advised to attempt all questions. Please hand in the **assessed** questions (the questions marked with a *) on Weds 8 February at the lecture.*

1202 2011-2012 Exercise 3 Solutions

1(i) Here there are 8 obvious symmetries, namely e (the identity), x (rotation by $\pi/2$ anticlockwise), y (rotation by π anticlockwise), z (rotation by $3\pi/2$ anticlockwise), a (reflection in vertical line) b (reflection in horizontal line) c (reflection in line from bottom left to top right) and d (reflection in line from bottom right to top left).

These are in fact all possible symmetries, since corner 1 must go to one of corners 1,2,3, or 4, then corner 2 must go to one of the two adjoining corners (giving $4 \times 2 = 8$ symmetries) and this determines the symmetry.

To get generators and relations, note that $y = x^2$ and $z = x^3$ and that $x^4 = e$, so e.g. $x^3x^3 = x^6 = x^2$. Also calculate:

$$ax =$$

$$ax = c$$

Similarly $ax^2 = b$ and $ax^3 = d$.

Hence the group can be written as $\{e, x, x^2, x^3, a, ax, ax^2, ax^3\}$. Here we know that $x^4 = id$ and that $y^2 = id$ and the only thing more we need to write down

the multiplication table is to know what xa is. Again calculate

So $xa = ax^3$.

Now any product can be calculated fairly easily e.g. $x^2a = x(xa) = x(ax^3) = (xa)x^3 = (ax^3)x^3 = ax^6 = ax^2$.

Thus group has generators x, a and relations $x^4 = e, a^2 = e$, and $xa = ax^3$, i.e. $Symm(T) = \langle x, a : x^4 = a^2 = e, xa = ax^3 \rangle$.

This completely specifies the multiplication table, which can now be written down if wanted:

	e	x	x^2	x^3	a	ax	ax^2	ax^3
e	e	x	x^2	x^3	a	ax	ax^2	ax^3
x	x	x^2	x^3	e	ax^3	a	ax	ax^2
x^2	x^2	x^3	e	x	ax^2	ax^3	a	ax
x^3	x^3	e	x	x^2	ax	ax^2	ax^3	a
a	a	ax	ax^2	ax^3	e	x	x^2	x^3
ax	ax	ax^2	ax^3	a	x^3	e	x	x^2
ax^2	ax^2	ax^3	a	ax	x^2	x^3	e	x
ax^3	ax^3	a	ax	ax^2	x	x^2	x^3	e

(ii) Label vertices of pentagon 1,2,3,4,5. Let G denote the symmetry group. Possible symmetries are: e (identity) x_i ($i = 1, \dots, 4$), where x_i denotes rotation by $2\pi/5$ anticlockwise, and y_i ($i = 1, \dots, 5$), where y_i denotes reflection in the line through vertex i perpendicular to opposite edge. This gives 10 symmetries, but clearly these are all there are (any symmetry sends vertex 1 to one of 5 places, then vertex 2 to one of the two adjoining places, then all the rest are fixed, i.e. $|G| = 10$).

Thus $G = \{e, x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4, y_5\}$.

The example of the triangle suggests $x = x_1$ and $y = y_1$ might be a good bet for generators. Exactly similar calculations to those for the triangle show that $\{x^i y^j : 0 \leq i \leq 4, 0 \leq j \leq 1\}$ provides a normal form for elements of G (i.e. this lists each element of G exactly once), and that $yx = x^4 y$. We deduce that generators and relations for G are given by

$$G = \langle x, y : x^5 = y^2 = e, yx = x^4 y \rangle.$$

2.(i) To find the inverse of $\overline{43}$ in \mathbb{Z}_{53}^* , we use the Euclidean algorithm:

$$53 = 43 \times 1 + 10$$

$$43 = 10 \times 4 + 3$$

$$10 = 3 \times 3 + 1$$

Hence

$$1 = 10 - 3 \times 3$$

$$= 10 - (43 - 10 \times 4) \times 3$$

$$= 10 \times 13 - 43 \times 3$$

$$= (53 - 43) \times 13 - 43 \times 3$$

$$= 53 \times 13 - 43 \times 16.$$

$$\text{Hence } \overline{43}^{-1} = \overline{-16} = \overline{37}.$$

[Check $37 \times 43 = 1591 = 53 \times 30 + 1 \equiv 1 \pmod{53}$.]

Now if $43x \equiv 4 \pmod{53}$, then $\overline{43x} = \overline{4}$. Multiplying both sides of this equation by $\overline{43}^{-1}$, i.e. $\overline{37}$, we get $\overline{x} = \overline{148} = \overline{42}$. Thus $x \equiv 42 \pmod{53}$.

(ii) If $x^{17} \equiv 3 \pmod{53}$, then $\overline{x^{17}} = \overline{3}$. Hence for any i , $\overline{x^{17i}} = \overline{3^i}$. Choose i so that $17i \equiv 1 \pmod{52}$: this is possible since 17 and 52 are coprime. In general we could use the Euclidean algorithm to find i , but here by inspection, if $i = 3$ then $17i \equiv 51 \equiv -1 \pmod{52}$ and hence if $i = -3$, $17i \equiv 1 \pmod{52}$. Thus by Fermat's Little Theorem, we have $\overline{x} = \overline{x^{-51}} = \overline{x^{17 \times -3}} = \overline{3^{-3}} = \overline{27}^{-1}$. Again we could find this by the Euclidean algorithm, but in fact $27 \times 2 = 54 = 53 + 1$, so $\overline{27}^{-1} = \overline{2}$. Thus $x \equiv 2 \pmod{53}$.

[Check $2^{17} \equiv (2^6)^2 \times 2^5 \equiv 64^2 \times 32 \equiv 11^2 \times 32 \equiv 121 \times 32 \equiv 15 \times 32 \equiv 480 = 53 \times 9 + 3 \equiv 3 \pmod{53}$.]

(iii) If $\overline{x^{13}} = \overline{2}$ then $\overline{x^{13 \times 4}} = \overline{2^4}$, so $\overline{x^{52}} = \overline{16}$. But by Fermat's Little Theorem $\overline{x^{52}} = \overline{1}$, so $\overline{1} = \overline{16}$, a contradiction. Hence the equation has no solution.

3 (i) This could be done as a consequence of unique factorisation. Alternatively: Since a and b are coprime, by the h, k lemma there exist $h, k \in \mathbb{Z}$ such that $ah + bk = 1$. Since $a|bc$, there exists $r \in \mathbb{Z}$ such that $bc = ar$. Then $c = 1c = (ah + bk)c = ahc + bkc = ahc + kar = a(ch + kr)$: hence $a|c$.

(ii) Let G be an abelian group and $g, h \in G$ with $o(g) = m$ and $o(h) = n$. First note that $(gh)^{mn} = g^{mn}h^{mn} = (g^m)^n(h^n)^m = e^n e^m = e$, so by Lemma 2.17, $o(gh) | mn$,

Now suppose $(gh)^i = e$ for some i . Then, since G is abelian, $g^i h^i = e$. Raising both sides to the power m , we get $g^{im} h^{im} = e$, i.e., since g has order m , $h^{im} = e$. Hence, since h has order n , $n | im$. But n and m are coprime, so by (i), $n | i$, say $i = nr$. A similar argument shows that $m | i = nr$. Using part (i) again, $m | r$, say $r = ms$ and hence $i = mns$, so $mn | i$.

Thus we have $(gh)^{mn} = e$ and $(gh)^i = e \Rightarrow mn | i$ and hence by definition of order, $o(gh) = mn$.

(iii) The simplest example here is S_4 . Take $g = (1\ 2)$ and $h = (1\ 3\ 4)$. Then $o(g) = 2$ and $o(h) = 3$, but $gh = (1\ 2)(1\ 3\ 4) = (1\ 3\ 4\ 2)$ and hence $o(gh) = 4 \neq 6 = 2 \times 3$.

4. H is a subgroup of G if and only if (a) $e \in H$, (b) $g, h \in H \Rightarrow gh \in H$, (c) $g \in H \Rightarrow g^{-1} \in H$.

5. (i) $G = \mathbf{R} - \{0\}$ under \times , $H = \{x \in \mathbf{R} : x \geq 1\}$. The identity 1 is in H and H is closed under \times : however, it is not closed under inverses, e.g. $2 \in H$, but $\frac{1}{2} \notin H$. Hence not a subgroup.

(ii) $H = \{2^n : n \in \mathbb{Z}\}$ is a subgroup of $\mathbf{R} - \{0\}$ under \times : $1 = 2^0 \in H$, $a, b \in H \Rightarrow a = 2^m, b = 2^n$ for some $m, n \in \mathbb{Z}$ and hence $ab = 2^{m+n}$ and $a^{-1} = 2^{-m} \in H$.

(iii) $G = \mathbf{R} - \{0\}$ under multiplication, $H = \{x \in \mathbf{R} - \{0\} : x^2 \in \mathbf{Q}\}$. Then H is a subgroup of G : $1 = 1^2$, so $1 \in H$. Also if $h, k \in H$, then $h^2 \in \mathbf{Q}$ and $k^2 \in \mathbf{Q}$ and hence $(h^{-1})^2 = (h^2)^{-1} \in \mathbf{Q}$, so $h^{-1} \in H$ and $(hk)^2 = h^2 k^2 \in \mathbf{Q}$ so $hk \in H$.

(iv) $G = S(\mathbb{R})$, $H = \{f \in G : f(1) = 1\}$. H is a subgroup:

(a) $id(1) = 1$, so $id \in H$.

(b) If $f \in H$, then $f(1) = 1$ and hence $f^{-1}(1) = 1$ and hence $f^{-1} \in H$.

(c) If $f, g \in H$, then $(f \circ g)(1) = f(g(1)) = f(1) = 1$ and hence $f \circ g \in H$.

(v) $G = S(\mathbb{R})$, $H = \{f \in G : f(1) = 2\}$. This is not a subgroup, since $id \notin H$.

*(vi) $G = S(\mathbb{R})$, $H = \{f \in G : f(\{1, 2\}) = \{1, 2\}\}$. This is a subgroup:

(a) $id(1) = 1$, $id(2) = 2$ and hence $id(\{1, 2\}) = \{1, 2\}$ and so $id \in H$.

(b) If $f \in H$, then $f(\{1, 2\}) = \{1, 2\}$. Thus $f(1) = 1$ or 2 and $f(2) = 2$ or 1 ; hence $f^{-1}(1) = 1$ or 2 and $f^{-1}(2) = 2$ or 1 ; hence $f^{-1}(\{1, 2\}) = \{1, 2\}$.

(c) If $f, g \in H$, then similarly $(f \circ g)(\{1, 2\}) = \{1, 2\}$ as required.

1202 2011-2012 Exercise 4

1 (i) Let $C_n = \{e, g, \dots, g^n\}$ ($g^n = e$) be the cyclic group of order n and let H be a subgroup of C_n . By considering $\min\{i > 0 : g^i \in H\}$ show that $H = \langle g^m \rangle$ for some $m|n$.

***(ii)** Find all subgroups of C_{20} , explaining your answer.

2(i) Find h, k , such that $13h + 19k = 1$. Find all solutions to $x \equiv 5 \pmod{13}$, $x \equiv 9 \pmod{19}$.

***(ii)** Find h, k such that $23h + 31k = 1$. Hence find all solutions to $x \equiv 1 \pmod{23}$, $x \equiv 5 \pmod{31}$.

***(iii)** Prove that if n_1, n_2, \dots, n_m are pairwise coprime integers (i.e for all $i \neq j$, n_i and n_j are coprime), then there exists a solution e_i to $x \equiv 1 \pmod{n_i}$, $x \equiv 0 \pmod{n_j}$ for $j \neq i$. Deduce that there is a solution to $x \equiv a_i \pmod{n_i}$ ($i = 1, \dots, m$) for any a_i .

***(iv)** Find a solution to $x \equiv 2 \pmod{7}$, $x \equiv 5 \pmod{11}$, $x \equiv 2 \pmod{19}$.

3 Let G be a group in which $g^2 = e$ for all $g \in G$. Show that G is abelian.

***4** Throughout this question, let G be a group and H and K subgroups of G with $|H| = m$ and $|K| = n$.

(i) Prove that $H \cap K$ is a subgroup of G .

(ii) Prove that if m and n are coprime, then $H \cap K = \{e\}$.

(iii) Prove that if G is abelian, then $HK = \{hk : h \in H, k \in K\}$ is a subgroup of G .

(iv) Prove that if G is abelian and $H \cap K = \{e\}$, then $|HK| = mn$.

PTO

5 Let G be an abelian group of order 77. Prove that G is cyclic, i.e $G = C_{77}$ by showing the following:

- (i) Every non-identity element of G is of order 7, 11 or 77.
- ((ii) If there is an element of order 77, then G is cyclic, so suppose all non-identity elements are of order 7 or 11.
- (iii) Suppose all non-identity elements are of order 7. Show that there exist subgroups H, K of G such that $|H| = |K| = 7$ and $H \cap K = \{e\}$. By Q4, it follows that $|HK| = 49$. This is a contradiction (why?).
- (iv) Similarly if all non-identity elements are of order 11 we get a contradiction.
- (v) Hence there is an element g of order 7 and an element h of order 11. Then $o(gh) = 77$ (why?) and hence G is cyclic.

*Please attempt all questions. Please hand in the **assessed** questions (the questions marked with a *) on Wednesday 22 February at the lecture. There will be a problem class on Friday 10 Feb to help with this sheet.*

1102 2011-2012 Exercise 4 Solutions

1. Let $C_n = \{e, x, x^2, \dots, x^{n-1}\}$, where $x^n = e$.

First note that if $m|n$, say $n = ms$, then $\langle x^m \rangle = \{e, x^m, \dots, x^{(s-1)m}\}$ is a subgroup of C_n .

Now let H be any subgroup of C_n and let m be the least positive integer i such that $x^i \in H$.

We can write $n = mq + r$, where $0 \leq r < m$: then $x^r = x^{n-mq} = x^n(x^m)^{-q} \in H$: hence if $r \neq 0$, we have a contradiction to the definition of m ; hence $r = 0$ and so m divides n , say $n = sm$. Now $\{e, x^m, \dots, x^{m(s-1)}\} \subseteq H$. A similar argument to the above shows that nothing else can be in H : hence $H = \{e, x^m, \dots, x^{m(s-1)}\} = \langle x^m \rangle$.

Hence the subgroups of G are precisely of the form $\langle x^m \rangle$ for $m|n$.

(ii) Subgroups of $C_{20} = \langle x \rangle$ are therefore of the form $\langle x^m \rangle$ for $m|20$, i.e.

$$\langle x \rangle = C_{20},$$

$$\langle x^2 \rangle = \{e, x^2, x^4, x^6, x^8, x^{10}, x^{12}, x^{14}, x^{16}, x^{18}\},$$

$$\langle x^4 \rangle = \{e, x^4, x^8, x^{12}, x^{16}\},$$

$$\langle x^5 \rangle = \{e, x^5, x^{10}, x^{15}\},$$

$$\langle x^{10} \rangle = \{e, x^{10}\},$$

$$\{e\}.$$

[Note that taking other powers of x as generators just produces one of these subgroups again, e.g. $\langle x^{15} \rangle = \{e, x^{15}, x^{30}, x^{45}\} = \{e, x^{15}, x^{10}, x^5\} = \langle x^5 \rangle$.]

2 (i) Go through the usual Euclidean algorithm to get $1 = 13 \times 3 - 19 \times 2$. Hence by Chinese Remainder Theorem, solution to $x \equiv 5 \pmod{13}$ and $x \equiv 9 \pmod{19}$ is given by $c = 13 \times 3 \times 9 - 19 \times 2 \times 5 \pmod{13 \times 19}$, i.e. $c \equiv 161 \pmod{247}$.

(ii) Again Euclidean algorithm:

$$31 = 23 \times 1 + 8$$

$$23 = 8 \times 3 - 1.$$

Hence

$$1 = 8 \times 3 - 23 = (31 - 23) \times 3 - 23 = 31 \times 3 - 23 \times 4.$$

Hence solution to $x \equiv 1 \pmod{23}$ and $x \equiv 5 \pmod{31}$ is $c = 31 \times 3 \times 1 - 23 \times 4 \times 5 \pmod{23 \times 31}$. This yields $x \equiv 346 \pmod{713}$.

(iii) Let $N = n_1 \dots n_m$. Then n_1 and $r_1 = N/n_1 = n_2 \dots n_m$ are coprime. [Suppose a prime number p divides both n_1 and r_1 ; then $p|n_2 \dots n_m$ and since p is prime, $p|n_j$ for some $2 \leq j \leq m$. But then n_1 and n_j are not coprime, contrary to hypothesis.]

Hence by h, k lemma there exist h_1, k_1 such that $n_1 h_1 + r_1 k_1 = 1$. Let $e_1 = r_1 k_1$. Then $e_1 = 1 - n_1 h_1 \equiv 1 \pmod{n_1}$ and $e_1 \equiv 0 \pmod{r_1}$. Since $r_1 = n_2 \dots n_m$ this implies that $e_1 \equiv 0 \pmod{n_i}$ for $2 \leq i \leq m$.

Thus we have found the required e_1 . Clearly an exactly analogous argument produces the required e_i for each i .

Now let $c = \sum_{i=1}^n a_i e_i$. Then mod n_1 we have

$$c = a_1 e_1 + a_2 e_2 + \dots + a_m e_m \equiv a_1 \times 1 + a_2 \times 0 + \dots + a_m \times 0 \equiv a_1.$$

and similarly $c \equiv a_i \pmod{n_i}$ for all i .

(iv) Now suppose $x \equiv 2 \pmod{7}$, $x \equiv 5 \pmod{11}$, $x \equiv 2 \pmod{19}$. The quickest way of doing this is to note that clearly $x \equiv 2 \pmod{7 \times 19}$. $7 \times 19 = 133$, so we need to find h, k such that $11h + 133k = 1$.

$$133 = 11 \times 12 + 1$$

$$\text{Hence } 1 = 133 - 11 \times 12.$$

Hence by Chinese Remainder Theorem, the solution to $x \equiv 2 \pmod{133}$, $x \equiv 5 \pmod{11}$ is

$$x = 133 \times 5 - 11 \times 12 \times 2 = 401 \pmod{1463}.$$

3 Let G be a group in which $g^2 = e$ for all $g \in G$. Then for all $x, y \in G$, $(xy)^2 = e$, i.e. $xyxy = e$. Multiplying on left by x and on right by y , we get $yx = xy$ and hence G is abelian.

4 (i) Suppose $x, y \in H \cap K$. Then $x, y \in H$ and since H is a subgroup, $xy^{-1} \in H$. Similarly $xy^{-1} \in K$ and hence $xy^{-1} \in H \cap K$.

Since H and K are subgroups, $e \in H$ and $e \in K$: hence $e \in H \cap K$.

Hence $H \cap K$ is a subgroup of G .

(ii) $H \cap K$ is a subgroup of G and contained in H ; hence it is a subgroup of H . By Lagrange's Theorem, $|H \cap K|$ divides $|H| = m$. Similarly $|H \cap K|$ divides n . Since m and n are coprime, it follows that $|H \cap K| = 1$ and hence $H \cap K = \{e\}$.

(iii) Let $x_1, x_2 \in HK$, so $x_1 = h_1k_1$ and $x_2 = h_2k_2$ for some $h_i \in H, k_i \in K$. Then $x_1x_2^{-1} = (h_1k_1)(h_2k_2)^{-1} = h_1k_1k_2^{-1}h_2^{-1} = (h_1h_2^{-1})(k_1k_2^{-1})$. Now since H is a subgroup, $h_1h_2^{-1} \in H$ and since K is a subgroup, $k_1k_2^{-1} \in K$. Hence $x_1x_2^{-1} \in HK$. Also $e = ee \in HK$. Thus HK is a subgroup of G .

(iv) We claim all the elements hk ($h \in H, k \in K$) are distinct. For suppose $h_1k_1 = h_2k_2$. Then $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$, so $h_2 = h_1$ and $k_1 = k_2$. Hence there are mn distinct elements of HK , i.e. $|HK| = mn$.

5 (i) By the Corollary to Lagrange's Theorem, the order of any element of G divides $|G| = 77$, and hence must be 1, 7, 11 or 77.

(ii) If there is an g element of order 77, then $|\langle g \rangle| = 77$ and hence $G = \langle g \rangle = C_{77}$. So suppose all non-identity elements are of order 7 or 11.

(iii) Suppose all non-identity elements are of order 7. Let g be an element of order 7, and let $H = \langle g \rangle$, so $|H| = 7$. Pick any element $h \notin H$, and let $K = \langle h \rangle$. Then since $o(h) = 7, |K| = 7$. Now $|H \cap K|$ divides $|H| = 7$; hence $|H \cap K|$ is 1 or 7. If it is 7, then $H = K$, a contradiction: hence $|H \cap K| = 1$. By Q4 (iv), $|HK| = 7 \times 7 = 49$. This is a contradiction, since HK is a subgroup of G and 49 does not divide 77.

(iv) Similarly if all non-identity elements of order 11 we get a contradiction.

(v) Hence there must be an element g of order 7 and an element h of order 11. By Ex 3, Q3(ii), $o(gh) = 77$ and hence $G = C_{77}$.

1202 2011-2012 Exercise 5

1 Learn and write down the definition of $\det A$.

***2** Find $\det(A)$ for the following matrices A over \mathbb{R} :

(i) $A = \begin{pmatrix} 3 & 7 \\ 1 & 4 \end{pmatrix}$ (ii) $A = \begin{pmatrix} 3 & 12 \\ 1 & 4 \end{pmatrix}$ (iii) $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

State whether each matrix is invertible or not, and find the inverse if it is.

3 (i) Prove by direct calculation that $\det(AB) = \det(A)\det(B)$ for any 2×2 matrices A and B .

(ii) Prove by direct calculation that $\det(AB) = \det(A)\det(B)$ for any $n \times n$ matrices A and B . [Optional and not for the faint-hearted. We will prove this result by other means in the lectures.]

4 Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Let S be the unit square with vertices $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Draw a diagram showing S and the image $L_A(S)$ of S under L_A . (Here $L_A(\mathbf{v}) = A\mathbf{v}$.) Calculate the area of $L_A(S)$ and show that $\text{area}(L_A(S))/\text{area}(S) = \pm \det(A)$.

***5** Find the determinants of the following matrices:

(i) $\begin{pmatrix} 3 & -3 & 1 \\ 2 & 7 & 2 \\ 1 & 4 & -1 \end{pmatrix}$ (ii) $\begin{pmatrix} x & y & x \\ y & x & y \\ a & b & c \end{pmatrix}$.

In (ii), state the conditions on x, y, a, b, c for the matrix to be invertible.

***6** Let A_n be the $n \times n$ matrix with entries given by

$$a_{i,i+1} = x \quad (i = 1, \dots, n-1), \quad a_{i+1,i} = y \quad (i = 1, \dots, n-1) \quad \text{and all other entries } 0.$$

(i) Write down A_n for $n = 2, 3, 4$ and in each case evaluate the determinant.

(ii) Find $\det(A_n)$ in the $n \times n$ case by using the formula directly.

[Hint: Suppose $\sigma \in S_n$ contributes a non-zero term to $\det(A)$, i.e. $a_{1,\sigma(1)} \neq 0$, $a_{2,\sigma(2)} \neq 0$, etc. What are the possible values of $\sigma(1)$, $\sigma(2)$, etc? This determinant can be found more easily by other methods which we will see later, but this is an exercise in calculating directly with the definition. You may like to distinguish the cases n odd and n even.]

You are advised to attempt all questions. Please hand in the assessed questions (the questions marked with a *) on Weds 29 February at the lecture.

1202 2011-2012 Exercise 5 Solutions

1. For an $n \times n$ matrix A , $\det(A) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) a_{1,\sigma(1)} a_{2,\sigma(2)} \dots a_{n,\sigma(n)}$.

2. (i) $\det A = \det \begin{pmatrix} 3 & 7 \\ 1 & 4 \end{pmatrix} = 3 \times 4 - 1 \times 7 = 5$. Since this is not zero, A is invertible, with inverse $\frac{1}{5} \begin{pmatrix} 4 & -7 \\ -1 & 3 \end{pmatrix} = \begin{pmatrix} \frac{4}{5} & -\frac{7}{5} \\ -\frac{1}{5} & \frac{3}{5} \end{pmatrix}$.

(ii) $\det A = \det \begin{pmatrix} 3 & 12 \\ 1 & 4 \end{pmatrix} = 3 \times 4 - 1 \times 12 = 0$. Hence A is not invertible.

(iii) $\det A = a^2 + b^2$. Hence A is invertible unless $a = b = 0$ and in this case $A^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$.

3(i) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $B = \begin{pmatrix} x & y \\ z & t \end{pmatrix}$. Then $AB = \begin{pmatrix} ax + bz & ay + bt \\ cx + dz & cy + dt \end{pmatrix}$

$$\begin{aligned} \det(AB) &= (ax + bz)(cy + dt) - (ay + bt)(cx + dz) \\ &= (axcy + bzc y + axdt + bzdt) - (aycx + btcx + aydz + btdz) \\ &= (bzc y + axdt) - (btcx + aydz) \end{aligned}$$

$$\begin{aligned} \det(A) \det(B) &= (ad - bc)(xt - yz) \\ &= (adxt + bcyz) - (bcxt + adyz) \end{aligned}$$

Hence $\det(AB) = \det(A) \det(B)$.

$$\begin{aligned} \text{(ii)} \det(AB) &= \sum_{\sigma \in S_n} \text{sgn}(\sigma) (AB)_{1,\sigma(1)} (AB)_{2,\sigma(2)} \dots (AB)_{n,\sigma(n)} \\ &= \sum_{\sigma \in S_n} \text{sgn}(\sigma) \left(\sum_{i_1=1}^n a_{1,i_1} b_{i_1,\sigma(1)} \right) \left(\sum_{i_2=1}^n a_{2,i_2} b_{i_2,\sigma(2)} \right) \dots \left(\sum_{i_n=1}^n a_{n,i_n} b_{i_n,\sigma(n)} \right) \\ &= \sum_{i_1=1}^n \sum_{i_2=1}^n \dots \sum_{i_n=1}^n a_{1,i_1} a_{2,i_2} \dots a_{n,i_n} \sum_{\sigma \in S_n} \text{sgn}(\sigma) b_{i_1,\sigma(1)} b_{i_2,\sigma(2)} \dots b_{i_n,\sigma(n)}. \end{aligned}$$

Write $X(i_1, \dots, i_n) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) b_{i_1,\sigma(1)} b_{i_2,\sigma(2)} \dots b_{i_n,\sigma(n)}$. We show that if the map $x \mapsto i_x$ is not a permutation, then $X(i_1, \dots, i_n) = 0$. So suppose it is not a bijection: then it is not an injection and hence $i_x = i_y$ for some y . Suppose without loss of generality that $i_1 = i_2$.

Let $\tau = (1 \ 2)$. As σ ranges over S_n so does $\sigma\tau$ and hence

$$\begin{aligned} X(i_1, \dots, i_n) &= \sum_{\sigma \in S_n} \text{sgn}(\sigma\tau) b_{i_1,\sigma\tau(1)} b_{i_2,\sigma\tau(2)} \dots b_{i_n,\sigma\tau(n)} \\ &= - \sum_{\sigma \in S_n} \text{sgn}(\sigma) b_{i_1,\sigma(2)} b_{i_2,\sigma(1)} \dots b_{i_n,\sigma(n)} \\ &= - \sum_{\sigma \in S_n} \text{sgn}(\sigma) b_{i_2,\sigma(2)} b_{i_1,\sigma(1)} \dots b_{i_n,\sigma(n)} \\ &= -X(i_1, \dots, i_n). \end{aligned}$$

Hence $X(i_1, \dots, i_n) = 0$. So the only non-zero contributions come from the case where $x \mapsto i_x$ is a permutation. Write $i(r) = i_r$. Then as σ varies over S_n , so does σi and hence

$$\begin{aligned} X(i_1, \dots, i_n) &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) b_{i(1), \sigma(1)} b_{i(2), \sigma(2)} \dots b_{i(n), \sigma(n)} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma i) b_{i(1), \sigma i(1)} b_{i(2), \sigma i(2)} \dots b_{i(n), \sigma i(n)} \\ &= \operatorname{sgn}(i) \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) b_{1, \sigma(1)} b_{2, \sigma(2)} \dots b_{n, \sigma(n)} \end{aligned}$$

$$\begin{aligned} \text{Hence } \det(AB) &= \sum_{i_1=1}^n \sum_{i_2=1}^n \dots \sum_{i_n=1}^n a_{1, i_1} a_{2, i_2} \dots a_{n, i_n} X(i_1, \dots, i_n) \\ &= \sum_{i \in S_n} a_{1, i(1)} a_{2, i(2)} \dots a_{n, i(n)} X(i(1), \dots, i(n)) \\ &= \sum_{i \in S_n} a_{1, i(1)} a_{2, i(2)} \dots a_{n, i(n)} \operatorname{sgn}(i) \det(B) \\ &= \det(B) \sum_{i \in S_n} \operatorname{sgn}(i) a_{1, i(1)} a_{2, i(2)} \dots a_{n, i(n)} \\ &= \det(B) \det(A). \end{aligned}$$

$$4. L_A\left(\begin{pmatrix} 0 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} 0 \\ 0 \end{pmatrix}, L_A\left(\begin{pmatrix} 1 \\ 0 \end{pmatrix}\right) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ c \end{pmatrix}$$

$$L_A\left(\begin{pmatrix} 0 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} b \\ d \end{pmatrix}, L_A\left(\begin{pmatrix} 1 \\ 1 \end{pmatrix}\right) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} a+b \\ c+d \end{pmatrix}.$$

Thus the image of S is a parallelogram.

Area of $L_A(S)$ can be calculated as $2 \times$ (area of OYR - area of OZX - area of ZTRX - area of ZTY) $= 2[\frac{1}{2}(a+b)(c+d) - \frac{1}{2}ac - bc - \frac{1}{2}bd] = ac + bc + ad + bd - ac - 2bc - bd = ad - bc = \det(A)$.

Hence $\text{area}(L_A(S))/\text{area}(S) = (ad - bc)/1 = \det(A)$. (In fact $\pm \det A$, depending whether or not L_A involves a reflection.)

$$*5 \det \begin{pmatrix} a & b & c \\ d & e & f \\ g & h & i \end{pmatrix} = aei + bfg + cdh - ceg - bdi - afh.$$

$$(i) \det \begin{pmatrix} 3 & -3 & 1 \\ 2 & 7 & 2 \\ 1 & 4 & -1 \end{pmatrix} = -21 - 6 + 8 - 7 - 24 - 6 = -56.$$

$$\text{(ii) } \det \begin{pmatrix} x & y & x \\ y & x & y \\ a & b & c \end{pmatrix} = x^2c + y^2a + xyb - x^2a - y^2c - xyb = (c-a)x^2 + (a-c)y^2 = (c-a)(x^2 - y^2) = (c-a)(x-y)(x+y).$$

The matrix is invertible if and only if the determinant is not zero, i.e. if and only if $a \neq c$ and $x \neq y$ and $x \neq -y$

$$\mathbf{6} \text{ (i) } A_2 = \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix}, \text{ so } \det(A_2) = -xy.$$

$$A_3 = \begin{pmatrix} 0 & x & 0 \\ y & 0 & x \\ 0 & y & 0 \end{pmatrix} \text{ so } \det(A_3) = 0.$$

$A_4 = \begin{pmatrix} 0 & x & 0 & 0 \\ y & 0 & x & 0 \\ 0 & y & 0 & x \\ 0 & 0 & y & 0 \end{pmatrix}$. Hence the only term from the $4! = 24$ products to be non-zero is that associated to $\sigma = (12)(34)$ and hence

$$\det(A_4) = \text{sgn}(\sigma)a_{12}a_{21}a_{34}a_{43} = x^2y^2.$$

(ii) In the $n \times n$ case, $\det A_n = \sum_{\sigma \in S_n} \text{sgn}(\sigma)a_{1,\sigma(1)}a_{2,\sigma(2)} \dots a_{n,\sigma(n)}$. The non-zero contributions to this sum come from σ which satisfy $a_{1,\sigma(1)} \neq 0$, $a_{2,\sigma(2)} \neq 0$, etc. From the form of A this means that

$$\sigma(1) = 2$$

$$\sigma(2) = 1 \text{ or } 3,$$

$$\sigma(3) = 2 \text{ or } 4$$

...

$$\sigma(n-1) = n-2 \text{ or } n.$$

$$\sigma(n) = n-1.$$

Looking at $\sigma(i)$ for odd i , we see that $\sigma(1) = 2$, $\sigma(3) \neq 2$, so $\sigma(3) = 4$, $\sigma(5) \neq 4$, so $\sigma(5) = 6$, etc. If n is odd, this yields $\sigma(n) = n+1$, impossible, so there are no non-zero terms, and $\det(A_n) = 0$.

If n is even, look at $\sigma(i)$ for even i . $\sigma(n) = n-1$; then $\sigma(n-2) \neq n-1$, so $\sigma(n-2) = n-3$, etc. Thus the only non-zero term comes from

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n-1 & n \\ 2 & 1 & 4 & 3 & \dots & n & n-1 \end{pmatrix} = (1 \ 2)(3 \ 4) \dots (n-1 \ n)$$

Thus for even n , $\det(A) = \text{sgn}(\sigma)a_{1,\sigma(1)} \dots a_{n,\sigma(n)} = (-1)^{n/2}a_{12}a_{21} \dots a_{n-1,n}a_{n,n-1} = (-xy)^{n/2}$.

1202 2011-2012 Exercise 6

1 Find the determinant of the following matrices using row/column ops and/or expanding along rows/columns:

$$(i) \begin{pmatrix} 1 & 2 & 0 & 3 & -1 \\ 2 & 3 & 0 & 1 & 1 \\ 0 & -1 & 0 & 2 & 1 \\ 1 & 1 & 3 & 1 & 1 \\ 0 & 0 & 0 & 3 & 4 \end{pmatrix} \quad (ii)^* \begin{pmatrix} 1 & 3 & 1 & -2 & -1 \\ 0 & 1 & 1 & 2 & 1 \\ 1 & 2 & 0 & -2 & 0 \\ 0 & 1 & 3 & 1 & 1 \\ 1 & 4 & 0 & 3 & 0 \end{pmatrix}$$

2* Let $A = \begin{pmatrix} x & y & z \\ z & x & y \\ y & z & x \end{pmatrix}$. Find $\det A$ as a product of irreducible factors (over \mathbb{R}).

Is the matrix $\begin{pmatrix} 151 & -271 & 120 \\ 120 & 151 & -271 \\ -271 & 120 & 151 \end{pmatrix}$ invertible?

3(i) Let $A = \begin{pmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^3 & b^3 & c^3 & d^3 \end{pmatrix}$. Find $\det A$ as a product of linear factors.

(ii)* Let A be the $n \times n$ matrix with entry $a_{ij} = x_j^{i-1}$. Prove that $\det(A) = \prod_{i < j} (x_j - x_i)$.

4 Let A_n be the $n \times n$ matrix given by $a_{ii} = 5$, $a_{ij} = 2$ if $j = i \pm 1$, and all other $a_{ij} = 0$. Let $d_n = \det A_n$. Find d_1, d_2, d_3 . Express d_{n+2} in terms of d_n and d_{n+1} and hence prove that $d_n = \frac{1}{3}(4^{n+1} - 1)$.

5* Let A_n be the $n \times n$ matrix given by $a_{ii} = 2$ and $a_{ij} = x$ ($i \neq j$), and let $d_n = \det A_n$. Find d_1, d_2, d_3 . Find and prove a formula for d_n . For which values of x is A_n invertible?

[Hint: use row and/or column operations.]

6 Re-do Q6 from Ex 5 using row and column operations and induction.

You are advised to attempt all questions. Please hand in the **assessed** questions (the questions marked with a *) on Wednesday 7 March at the lecture

1202 2011-2012 Exercise 6 Solutions

1.(i) Below we use the following;

- (1) is expanding down 3rd column; (2) is taking twice row 1 from row 2;
 (3) is expanding down 1st column; (4) is taking row 1 from row 2;
 (5) is expanding down first column.

$$\det \begin{pmatrix} 1 & 2 & 0 & 3 & -1 \\ 2 & 3 & 0 & 1 & 1 \\ 0 & -1 & 0 & 2 & 1 \\ 1 & 1 & 3 & 1 & 1 \\ 0 & 0 & 0 & 3 & 4 \end{pmatrix} \stackrel{(1)}{=} -3 \det \begin{pmatrix} 1 & 2 & 3 & -1 \\ 2 & 3 & 1 & 1 \\ 0 & -1 & 2 & 1 \\ 0 & 0 & 3 & 4 \end{pmatrix}$$

$$\stackrel{(2)}{=} -3 \det \begin{pmatrix} 1 & 2 & 3 & -1 \\ 0 & -1 & -5 & 3 \\ 0 & -1 & 2 & 1 \\ 0 & 0 & 3 & 4 \end{pmatrix} \stackrel{(3)}{=} -3 \det \begin{pmatrix} -1 & -5 & 3 \\ -1 & 2 & 1 \\ 0 & 3 & 4 \end{pmatrix}$$

$$\stackrel{(4)}{=} -3 \det \begin{pmatrix} -1 & -5 & 3 \\ 0 & 7 & -2 \\ 0 & 3 & 4 \end{pmatrix} \stackrel{(5)}{=} 3 \det \begin{pmatrix} 7 & -2 \\ 3 & 4 \end{pmatrix} = 3(28 + 6) = 102.$$

(ii) Below we use the following:

- (1) is taking row 1 from row 3 and from row 5;
 (2) is expanding down 1st column;
 (3) is adding row 1 to row 2, taking row 1 from row 3 and taking row 1 from row 4;
 (4) is expanding down 1st column
 (5) is expanding down third col.

$$\det \begin{pmatrix} 1 & 3 & 1 & -2 & -1 \\ 0 & 1 & 1 & 2 & 1 \\ 1 & 2 & 0 & -2 & 0 \\ 0 & 1 & 3 & 1 & 1 \\ 1 & 4 & 0 & 3 & 0 \end{pmatrix} \stackrel{(1)}{=} \det \begin{pmatrix} 1 & 3 & 1 & -2 & -1 \\ 0 & 1 & 1 & 2 & 1 \\ 0 & -1 & -1 & 0 & 1 \\ 0 & 1 & 3 & 1 & 1 \\ 0 & 1 & -1 & 5 & 1 \end{pmatrix}$$

$$\stackrel{(2)}{=} \det \begin{pmatrix} 1 & 1 & 2 & 1 \\ -1 & -1 & 0 & 1 \\ 1 & 3 & 1 & 1 \\ 1 & -1 & 5 & 1 \end{pmatrix} \stackrel{(3)}{=} \det \begin{pmatrix} 1 & 1 & 2 & 1 \\ 0 & 0 & 2 & 2 \\ 0 & 2 & -1 & 0 \\ 0 & -2 & 3 & 0 \end{pmatrix} \stackrel{(4)}{=} \det \begin{pmatrix} 0 & 2 & 2 \\ 2 & -1 & 0 \\ -2 & 3 & 0 \end{pmatrix}$$

$$\stackrel{(5)}{=} 2 \det \begin{pmatrix} 2 & -1 \\ -2 & 3 \end{pmatrix} = 8$$

$$2. \det \begin{pmatrix} x & y & z \\ z & x & y \\ y & z & x \end{pmatrix} = \det \begin{pmatrix} x+y+z & y & z \\ x+y+z & x & y \\ x+y+z & z & x \end{pmatrix}$$

(here we added column 2 and column 3 to column 1)

$$= (x + y + z) \det \begin{pmatrix} 1 & y & z \\ 1 & x & y \\ 1 & z & x \end{pmatrix} = (x + y + z) \det \begin{pmatrix} 1 & y & z \\ 0 & x - y & y - z \\ 0 & z - y & x - z \end{pmatrix}$$

(here we took $x + y + z$ out of column 1 and then took row 1 from row 2 and row 3)

$$= (x + y + z) \det \begin{pmatrix} x - y & y - z \\ z - y & x - z \end{pmatrix} = (x + y + z)[(z - y)(x - z) + (y - z)^2]$$

$$= (x + y + z)[x^2 + y^2 + z^2 - xy - xz - yz].$$

[The second factor is irreducible over \mathbb{R} , i.e. cannot be factorized any further. Suppose it did factorize: then it would clearly have to be the product of two linear factors, say $x^2 + y^2 + z^2 - xy - xz - yz = (ax + by + cz)(dx + ey + fz)$. This can be shown to be impossible either by equating coefficients or more easily by setting e.g. $y = 1$ and $z = 0$ to get $x^2 - x + 1 = (ax + b)(dx + e)$, which is impossible as $x^2 - x + 1 = 0$ has non-real roots. It is not asked for in the question, but in fact this does factorize over \mathbb{C} : $x^2 + y^2 + z^2 - xy - xz - yz = (x + \omega y + \omega^2 z)(x + \omega^2 y + \omega z)$, where $\omega = e^{2\pi i/3}$ is a complex cube root of unity. These factors can be found from the determinant of the original matrix e.g. adding ω times column 2 and ω^2 times column 3 to column 1 and then taking out a factor from column 1 yields the factor $x + \omega y + \omega^2 z$.]

The matrix $B = \begin{pmatrix} 151 & -271 & 120 \\ 120 & 151 & -271 \\ -271 & 120 & 151 \end{pmatrix}$ is of this form with $x = 151$, $y = -271$ and $z = 120$. Since $x + y + z = 151 - 271 + 120 = 0$, $\det B = 0$ and hence B is not invertible.

3.(i) Direct method using row/column ops

Operations are:

- (1) is take col 1 from col 2, col 3 and col 4
- (2) is expand along first row
- (3) is divide col 1 by $b - a$, col 2 by $c - a$, col 3 by $d - a$
- (4) is take col 1 from col 2 and col 3
- (5) is expand along first row
- (6) is divide col 1 by $c - b$, col 2 by $d - b$
- (7) is take col 1 from col 2
- (8) is expand along first row.

$$\det \begin{pmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^3 & b^3 & c^3 & d^3 \end{pmatrix} \stackrel{(1)}{=} \det \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & b - a & c - a & d - a \\ a^2 & b^2 - a^2 & c^2 - a^2 & d^2 - a^2 \\ a^3 & b^3 - a^3 & c^3 - a^3 & d^3 - a^3 \end{pmatrix}$$

$$\begin{aligned}
 (2) &= \det \begin{pmatrix} b-a & c-a & d-a \\ b^2-a^2 & c^2-a^2 & d^2-a^2 \\ b^3-a^3 & c^3-a^3 & d^3-a^3 \end{pmatrix} \\
 (3) &= (b-a)(c-a)(d-a) \det \begin{pmatrix} 1 & 1 & 1 \\ b+a & c+a & d+a \\ b^2+ab+a^2 & c^2+ac+a^2 & d^2+ad+a^2 \end{pmatrix} \\
 (4) &= (b-a)(c-a)(d-a) \det \begin{pmatrix} 1 & 0 & 0 \\ b+a & c-b & d-b \\ b^2+ab+a^2 & c^2-b^2+ac-ab & d^2-b^2+ad-ab \end{pmatrix} \\
 (5) &= (b-a)(c-a)(d-a) \det \begin{pmatrix} c-b & d-b \\ c^2-b^2+ac-ab & d^2-b^2+ad-ab \end{pmatrix} \\
 (6) &= (b-a)(c-a)(d-a)(c-b)(d-b) \det \begin{pmatrix} 1 & 1 \\ a+b+c & a+b+d \end{pmatrix} \\
 (7) &= (b-a)(c-a)(d-a)(c-b)(d-b) \det \begin{pmatrix} 1 & 0 \\ a+b+c & d-c \end{pmatrix} \\
 (8) &= (b-a)(c-a)(d-a)(c-b)(d-b)(d-c)
 \end{aligned}$$

OR briefer method (better for generalizing to $n \times n$ in (ii))

$$\text{Let } f(a, b, c, d) = \det \begin{pmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^3 & b^3 & c^3 & d^3 \end{pmatrix}.$$

If $b = a$ then clearly the determinant is zero, since it has the first two columns the same; hence $f(a, a, c, d) = 0$; it follows that $b - a$ divides f . Similarly for $c - a$, $d - a$, $c - b$, $d - b$ and $d - c$.

$$\text{Hence } f(a, b, c, d) = (b-a)(c-a)(d-a)(c-b)(d-b)(d-c)g(a, b, c, d).$$

But clearly all terms in f have total degree 6 (using definition of determinant, f is sum of terms like $1 \times b \times d^2 \times c^3$); hence g is in fact a constant.

Now there is exactly one term bc^2d^3 occurring in the determinant (the main diagonal) and bc^2d^3 also appears with coefficient +1 in $(b-a)(c-a)(d-a)(c-b)(d-b)(d-c)$; hence $g = 1$.

$$\text{So } f(a, b, c, d) = (b-a)(c-a)(d-a)(c-b)(d-b)(d-c).$$

(ii) Let $f(x_1, \dots, x_n) = \det A$. Note that if $x_i = x_j$ then two columns are the same and hence $f = 0$. This means that $(x_j - x_i)$ divides f for all $i \neq j$. Hence $\prod_{i < j} (x_j - x_i)$ divides f , say $f(x_1, \dots, x_n) = \prod_{i < j} (x_j - x_i)g(x_1, \dots, x_n)$. Clearly all terms in f are of total degree $1 + 2 + \dots + (n-1) = \frac{1}{2}n(n-1)$ and $\prod_{i < j} (x_j - x_i)g(x_1, \dots, x_n)$ is the product of $\frac{1}{2}n(n-1)$ linear terms, hence of the

same degree. Thus g is of degree 0, i.e. a constant.

One term in the determinant is obtained by multiplying all the terms on the main diagonal, which produces $x_2x_3^2\dots x_n^{n-1}$; the corresponding term in $\prod_{i<j}(x_j - x_i)$ is given by taking the first term in each bracket, yielding $x_2x_3^2\dots x_n^{n-1}$; hence the constant g is 1 and so $\det A = \prod_{i<j}(x_j - x_i)$.

$$4. d_1 = \det(5) = 5 = \frac{1}{3}(4^2 - 1).$$

$$d_2 = \det \begin{pmatrix} 5 & 2 \\ 2 & 5 \end{pmatrix} = 21 = \frac{1}{3}(4^3 - 1).$$

$$d_3 = \det \begin{pmatrix} 5 & 2 & 0 \\ 2 & 5 & 2 \\ 0 & 2 & 5 \end{pmatrix} = 85 = \frac{1}{3}(4^4 - 1).$$

$$\text{Now } d_{n+2} = \det \begin{pmatrix} 5 & 2 & 0 & 0 & \dots & 0 \\ 2 & 5 & 2 & 0 & \dots & 0 \\ 0 & 2 & 5 & 2 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ 0 & 0 & 0 & 0 & \dots & 5 \end{pmatrix}.$$

$$= 5 \det \begin{pmatrix} 5 & 2 & 0 & 0 & \dots & 0 \\ 2 & 5 & 2 & 0 & \dots & 0 \\ 0 & 2 & 5 & 2 & \dots & 0 \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot \\ 0 & 0 & 0 & 0 & \dots & 5 \end{pmatrix} - 2 \det \begin{pmatrix} 2 & 2 & 0 & \dots & 0 \\ 0 & 5 & 2 & \dots & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \dots & \cdot \\ 0 & 0 & 0 & \dots & 5 \end{pmatrix}$$

$$= 5d_{n+1} - 4d_n.$$

$$\text{Hence } d_{n+2} = 5d_{n+1} - 4d_n.$$

Now prove by induction that $d_n = \frac{1}{3}(4^{n+1} - 1)$.

Statement is true for $n = 1, 2, 3$ (checked at beginning of question). Suppose holds for $n < k + 2$. Then

$$\begin{aligned} d_{k+2} &= 5d_{k+1} - 4d_k \\ &= 5 \times \frac{1}{3}(4^{k+2} - 1) - 4 \times \frac{1}{3}(4^{k+1} - 1) \\ &= \frac{1}{3}(5 \times 4^{k+2} - 4 \times 4^{k+1} - 5 + 4) \\ &= \frac{1}{3}((20 - 4) \times 4^{k+1} - 1) \\ &= \frac{1}{3}(4^{k+3} - 1). \end{aligned}$$

Thus the statement holds for $n = k + 2$. By induction, it is true for all n .

$$5. A_1 = (2), \text{ so } d_1 = 2.$$

$$A_2 = \begin{pmatrix} 2 & x \\ x & 2 \end{pmatrix}, \text{ so } d_2 = 4 - x^2.$$

$$A_3 = \begin{pmatrix} 2 & x & x \\ x & 2 & x \\ x & x & 2 \end{pmatrix}, \text{ so } d_3 = 8 - 2x^3 - 6x^2.$$

Now consider $d_n = \det A_n$. Do the following column operations: take the first column from each of the others. This leaves the determinant unchanged, and changes the matrix as follows:

$$\begin{pmatrix} 2 & x & x & \dots & x \\ x & 2 & x & \dots & x \\ x & x & 2 & \dots & x \\ \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \dots & \cdot \\ x & x & x & \dots & 2 \end{pmatrix} \longrightarrow \begin{pmatrix} 2 & x-2 & x-2 & \dots & x-2 \\ x & 2-x & 0 & \dots & 0 \\ x & 0 & 2-x & \dots & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \dots & \cdot \\ x & 0 & 0 & \dots & 2-x \end{pmatrix}$$

Now add each of rows 2,3,...,n to the first row. This again leaves the determinant unchanged and changes matrix as follows

$$\begin{pmatrix} 2 & x-2 & x-2 & \dots & x-2 \\ x & 2-x & 0 & \dots & 0 \\ x & 0 & 2-x & \dots & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \dots & \cdot \\ x & 0 & 0 & \dots & 2-x \end{pmatrix} \longrightarrow \begin{pmatrix} 2+(n-1)x & 0 & 0 & \dots & 0 \\ x & 2-x & 0 & \dots & 0 \\ x & 0 & 2-x & \dots & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \dots & \cdot \\ x & 0 & 0 & \dots & 2-x \end{pmatrix}$$

But this matrix is lower triangular, so has determinant $(2+(n-1)x)(2-x)^{n-1}$.

Thus $d_n = (2+(n-1)x)(2-x)^{n-1}$, and the matrix A_n is invertible (for $n \geq 2$) as long as $x \neq 2$ and $x \neq -2/(n-1)$.

6 Let $d_n = \det A_n$. Then $d_n = \det \begin{pmatrix} 0 & x & 0 & 0 & \dots & 0 & 0 \\ y & 0 & x & 0 & \dots & 0 & 0 \\ 0 & y & 0 & x & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \dots & 0 & x \\ 0 & 0 & 0 & 0 & \dots & y & 0 \end{pmatrix}.$

Expanding along the first row, we get

$$d_n = -x \det \begin{pmatrix} y & x & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & x & 0 & \dots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \dots & \cdot & \cdot \\ 0 & 0 & 0 & 0 & \dots & y & 0 \end{pmatrix}$$

Now expanding down first column yields $d_n = -xy d_{n-2}$.

Since $d_1 = 0$ and $d_2 = -xy$ it is now easy to prove by induction that $d_n = 0$ (n odd) and $d_n = (-xy)^{n/2}$ (n even).

This is probably easier than the method using the definition in Ex Sheet 5.

1202 2011-2012 Exercise 7

1 (i) Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be invertible. Show that the solution to

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$$

is given by $x_i = \frac{\det A_i}{\det A}$, where A_i is the matrix obtained from A by replacing the i^{th} column by $\begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$.

[Hint: multiply equation on left by $A^{-1} = \frac{1}{\det A} \text{adj}A$]

*(ii) Now let A be an $n \times n$ invertible matrix. Show that the solution to $A\mathbf{x} = \mathbf{p}$ is given by $x_i = \frac{\det A_i}{\det A}$, where A_i is the matrix obtained from A by replacing the i^{th} column by \mathbf{p} .

(iii) Use result of part (ii) to find the value of y in the solution to

$$\begin{pmatrix} 1 & 2 & 7 \\ 2 & 1 & 3 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

*(iv) Use the result of part (ii) to find x_1 in the solution to

$$\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_n^2 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \dots & a_n^{n-1} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

where the a_i are distinct real numbers.

[Note: this is called *Kramer's Rule*. For (iv) you may find Ex 6, Q3 helpful.]

PTO

***2** Let $A = \begin{pmatrix} 1/4 & 3/4 \\ 3/4 & 1/4 \end{pmatrix}$.

(i) Find eigenvalues and eigenvectors for A and hence find an invertible matrix P such that $P^{-1}AP = D$ (diagonal).

(ii) Find a formula for A^n ($n \in \mathbf{Z}$); also find a matrix B such that $B^3 = A$.

(iii) Solve the following simultaneous differential equations:

$$\frac{dx_1}{dt} = (1/4)x_1 + (3/4)x_2$$

$$\frac{dx_2}{dt} = (3/4)x_1 + (1/4)x_2$$

given that $x_1(0) = 1/3$, $x_2(0) = 2/3$.

***3** Let $A \in M_n(\mathbf{R})$ be a matrix such that $A^2 = I$.

(i) Show that the only possible eigenvalues of A are 1 and -1.

(ii) Show directly that $E_1 \cap E_{-1} = \{0\}$.

(iii) Show that $\mathbf{R}^n = E_1 + E_{-1}$. [Hint: What is $A(\mathbf{v} + A\mathbf{v})$?]

(iv) Let $\{\mathbf{v}_1, \dots, \mathbf{v}_r\}$ be a basis for E_1 and let $\{\mathbf{w}_1, \dots, \mathbf{w}_s\}$ be a basis for E_{-1} . Prove that $\{\mathbf{v}_1, \dots, \mathbf{v}_r, \mathbf{w}_1, \dots, \mathbf{w}_s\}$ is a basis for \mathbf{R}^n .

(v) Deduce that A is diagonalizable. What are the possible forms of the diagonal matrix to which A is similar?

4 Let $A \in M_n(\mathbf{R})$ be a matrix such that $A^2 = 0$ (such a matrix is called *nilpotent*). Show that if A is diagonalisable then $A = 0$. Give an example of a non-zero 2×2 nilpotent matrix.

You are advised to attempt all questions. Please hand in the assessed questions (i.e. Q1 (ii), (iv), Q2 and Q3 on Wednesday 14 March at the lecture.

1202 2011-2012 Exercise 7 Solutions

$$1 \text{ (i)} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} p_1 \\ p_2 \end{pmatrix}$$

Multiply on the left by $A^{-1} = \frac{1}{\det A} \text{adj} A = \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$ to get

$$\begin{aligned} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} &= \frac{1}{\det A} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} p_1 \\ p_2 \end{pmatrix} \\ &= \frac{1}{\det A} \begin{pmatrix} dp_1 - bp_2 \\ -cp_1 + ap_2 \end{pmatrix} \end{aligned}$$

Now $A_1 = \begin{pmatrix} p_1 & b \\ p_2 & d \end{pmatrix}$, so $\det A_1 = dp_1 - bp_2$.

$A_2 = \begin{pmatrix} a & p_1 \\ c & p_2 \end{pmatrix}$, so $\det A_2 = ap_2 - cp_1$.

$$\text{Hence } \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \frac{1}{\det A} \begin{pmatrix} \det A_1 \\ \det A_2 \end{pmatrix}.$$

(ii) Let A be an $n \times n$ invertible matrix. Suppose that $A\mathbf{x} = \mathbf{p}$. Then $(\text{adj} A)A\mathbf{x} = (\text{adj} A)\mathbf{p}$, so $(\det A)\mathbf{x} = (\text{adj} A)\mathbf{p}$

Looking at the i^{th} component of this last equation we get

$$(\det A)x_i = \sum_j (\text{adj} A)_{ij} p_j = \sum_j C_{ji} p_j, \text{ where } C_{ji} \text{ is the } (j, i)\text{-cofactor of } A.$$

Now consider the matrix A_i obtained from A by replacing the i^{th} column by \mathbf{p} . Note that the (j, i) cofactor of A_i is the same as that of A , i.e. C_{ji} , because A and A_i differ only in i^{th} column. Hence expanding down the i^{th} column of A_i yields $\det A_i = \sum_j p_j C_{ji}$. Thus $(\det A)x_i = \det A_i$, i.e. $x_i = \frac{\det A_i}{\det A}$. (Note this makes sense: since A is invertible, $\det A \neq 0$.)

(iii)

$$\begin{pmatrix} 1 & 2 & 7 \\ 2 & 1 & 3 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}.$$

$$\det A_2 = \det \begin{pmatrix} 1 & 0 & 7 \\ 2 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} = 1$$

$$\det A = \det \begin{pmatrix} 1 & 2 & 7 \\ 2 & 1 & 3 \\ 0 & 1 & 1 \end{pmatrix} = 1 + 14 - 3 - 4 = 8.$$

Hence A is invertible and so by part (ii) the solution is given by $y = \det A_2 / \det A = 1/8$.

$$(iv) \text{ Let } A = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_n^2 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \dots & a_n^{n-1} \end{pmatrix}, \mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ \vdots \\ x_n \end{pmatrix} \text{ and } \mathbf{p} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

By (ii), the solution to $A\mathbf{x} = \mathbf{p}$ has $x_i = \det A_i / \det A$.

By Ex 6, Q3, $\det A = \prod_{1 \leq i < j \leq n} (a_j - a_i)$.

$$\det A_1 = \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 0 & a_2 & a_3 & \dots & a_n \\ 0 & a_2^2 & a_3^2 & \dots & a_n^2 \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 0 & a_2^{n-1} & a_3^{n-1} & \dots & a_n^{n-1} \end{pmatrix} = \det \begin{pmatrix} a_2 & a_3 & \dots & a_n \\ a_2^2 & a_3^2 & \dots & a_n^2 \\ \vdots & \vdots & \dots & \vdots \\ a_2^{n-1} & a_3^{n-1} & \dots & a_n^{n-1} \end{pmatrix} = a_2 \dots a_n \det \begin{pmatrix} 1 & 1 & \dots & 1 \\ a_2 & a_3 & \dots & a_n \\ \vdots & \vdots & \dots & \vdots \\ a_2^{n-2} & a_3^{n-2} & \dots & a_n^{n-2} \end{pmatrix}$$

But this is just the $(n-1) \times (n-1)$ version of A with parameters a_2, \dots, a_n , so $\det A_1 = a_2 \dots a_n \prod_{2 \leq i < j \leq n} (a_j - a_i)$.

Hence $x_1 = a_2 \dots a_n \prod_{2 \leq i < j \leq n} (a_j - a_i) / \prod_{1 \leq i < j \leq n} (a_j - a_i) = \prod_{j=2}^n (a_j / (a_j - a_1))$.

***2** $A = \begin{pmatrix} 1/4 & 3/4 \\ 3/4 & 1/4 \end{pmatrix}$.

(i) $c_A(t) = \det \begin{pmatrix} t - 1/4 & -3/4 \\ -3/4 & t - 1/4 \end{pmatrix} = (t - 1/4)^2 - (3/4)^2 = (t - 1)(t + 1/2)$.
Hence eigenvalues are 1 and $-1/2$.

Corresponding eigenvectors:

For $\lambda = 1$, we solve $A\mathbf{v} = \mathbf{v}$, i.e. $\begin{pmatrix} -3/4 & 3/4 \\ 3/4 & -3/4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. It is easy to get that the general solution is $\left\{ \begin{pmatrix} \alpha \\ \alpha \end{pmatrix} : \alpha \in \mathbf{R} \right\}$. Hence an eigenvector can be chosen as $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

For $\lambda = -1/2$, we solve $A\mathbf{v} = -\frac{1}{2}\mathbf{v}$, i.e. $\begin{pmatrix} -3/4 & -3/4 \\ -3/4 & -3/4 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. It is

easy to get that the general solution is $\left\{ \begin{pmatrix} -\alpha \\ \alpha \end{pmatrix} : \alpha \in \mathbf{R} \right\}$. Hence an eigenvector can be chosen as $\begin{pmatrix} -1 \\ 1 \end{pmatrix}$.

Thus a basis of eigenvectors is $\left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\}$. Let $P = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$. Then P is invertible and $P^{-1}AP = \begin{pmatrix} 1 & 0 \\ 0 & -1/2 \end{pmatrix}$.

Check:

P is invertible, since $\det P = 2 \neq 0$. Also

$$AP = \begin{pmatrix} 1/4 & 3/4 \\ 3/4 & 1/4 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1/2 \\ 1 & -1/2 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1/2 \end{pmatrix}$$

Hence $AP = PD$, as required.

$$\begin{aligned} \text{(ii) Now } A^n &= (PDP^{-1})^n = PD^nP^{-1} \\ &= \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & (-1/2)^n \end{pmatrix} (1/2) \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \\ &= (1/2) \begin{pmatrix} 1 & -(-1/2)^n \\ 1 & (-1/2)^n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \\ &= (1/2) \begin{pmatrix} 1 + (-1/2)^n & 1 - (-1/2)^n \\ 1 - (-1/2)^n & 1 + (-1/2)^n \end{pmatrix} \end{aligned}$$

$B^3 = A$ iff $(P^{-1}BP)^3 = P^{-1}AP = D$. One solution to this is clearly

$$P^{-1}BP = \begin{pmatrix} 1 & 0 \\ 0 & -1/\sqrt[3]{2} \end{pmatrix} \text{ and hence}$$

$$\begin{aligned} B &= P \begin{pmatrix} 1 & 0 \\ 0 & -1/\sqrt[3]{2} \end{pmatrix} P^{-1} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1/\sqrt[3]{2} \end{pmatrix} (1/2) \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \\ &= (1/2) \begin{pmatrix} 1 & 1/\sqrt[3]{2} \\ 1 & -1/\sqrt[3]{2} \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \\ &= (1/2) \begin{pmatrix} 1 - 1/\sqrt[3]{2} & 1 + 1/\sqrt[3]{2} \\ 1 + 1/\sqrt[3]{2} & 1 - 1/\sqrt[3]{2} \end{pmatrix} \end{aligned}$$

(Of course, you could also get this from the formula found for A^n ; this needs a (very small) amount of justification.)

$$\text{(iii) The equations are: } \begin{aligned} \frac{dx_1}{dt} &= (1/4)x_1 + (3/4)x_2 \\ \frac{dx_2}{dt} &= (3/4)x_1 + (1/4)x_2 \end{aligned}$$

Write $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ and let $A = \begin{pmatrix} 1/4 & 3/4 \\ 3/4 & 1/4 \end{pmatrix}$. Then we can write these equations as

$$\mathbf{x}' = A\mathbf{x}$$

where the $'$ denotes differentiation with respect to t . Now make a change of variable $\mathbf{x} = P\mathbf{y}$. Then the equation becomes: $P\mathbf{y}' = AP\mathbf{y}$, so $\mathbf{y}' = (P^{-1}AP)\mathbf{y}$,

i.e.

$$\mathbf{y}' = D\mathbf{y}$$

Writing this out, we have

$$\begin{pmatrix} dy_1/dt \\ dy_2/dt \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -1/2 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} \text{ i.e. } \begin{aligned} \frac{dy_1}{dt} &= y_1 \\ \frac{dy_2}{dt} &= -(1/2)y_2 \end{aligned}$$

This has solutions $y_1 = Ae^t$, $y_2 = Be^{-t/2}$. Hence $\mathbf{y} = \begin{pmatrix} Ae^t \\ Be^{-t/2} \end{pmatrix}$.

Now $\mathbf{x}(0) = \begin{pmatrix} 1/3 \\ 2/3 \end{pmatrix}$; it follows that

$$\mathbf{y}(0) = P^{-1} \begin{pmatrix} 1/3 \\ 2/3 \end{pmatrix} = (1/2) \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1/3 \\ 2/3 \end{pmatrix} = \begin{pmatrix} 1/2 \\ 1/6 \end{pmatrix}$$

Hence $A = 1/2$, $B = 1/6$, and so $\mathbf{y} = \begin{pmatrix} (1/2)e^t \\ (1/6)e^{-t/2} \end{pmatrix}$. Thus

$$\mathbf{x} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \mathbf{y} = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} (1/2)e^t \\ (1/6)e^{-t/2} \end{pmatrix} = \begin{pmatrix} (1/2)e^t - (1/6)e^{-t/2} \\ (1/2)e^t + (1/6)e^{-t/2} \end{pmatrix}$$

3(i) $A^2 = I$. If λ is an eigenvalue of A , then there exists an eigenvector \mathbf{v} such that $A\mathbf{v} = \lambda\mathbf{v}$. Then $\mathbf{v} = I\mathbf{v} = A^2\mathbf{v} = A(A\mathbf{v}) = A(\lambda\mathbf{v}) = \lambda(A\mathbf{v}) = \lambda^2\mathbf{v}$. Since $\mathbf{v} \neq \mathbf{0}$, $\lambda^2 = 1$ and so $\lambda = \pm 1$.

(ii) $E_1 = \{\mathbf{v} \in \mathbf{R}^n : A\mathbf{v} = \mathbf{v}\}$ and $E_{-1} = \{\mathbf{v} \in \mathbf{R}^n : A\mathbf{v} = -\mathbf{v}\}$. Now if $\mathbf{v} \in E_1 \cap E_{-1}$ then $A\mathbf{v} = \mathbf{v}$ (since $\mathbf{v} \in E_1$) and $A\mathbf{v} = -\mathbf{v}$ (since $\mathbf{v} \in E_{-1}$); hence $\mathbf{v} = -\mathbf{v}$ and so $\mathbf{v} = \mathbf{0}$. Thus $E_1 \cap E_{-1} = \{\mathbf{0}\}$.

(iii) By defn $E_1 + E_{-1} \subseteq \mathbf{R}^n$. Suppose $\mathbf{v} \in \mathbf{R}^n$. Then $\mathbf{v} = \frac{1}{2}(\mathbf{v} + A\mathbf{v}) + \frac{1}{2}(\mathbf{v} - A\mathbf{v})$ and $\frac{1}{2}(\mathbf{v} + A\mathbf{v}) \in E_1$ (since $A(\mathbf{v} + A\mathbf{v}) = A\mathbf{v} + A^2\mathbf{v} = A\mathbf{v} + \mathbf{v}$) and $\frac{1}{2}(\mathbf{v} - A\mathbf{v}) \in E_{-1}$ (since $A(\mathbf{v} - A\mathbf{v}) = A\mathbf{v} - A^2\mathbf{v} = A\mathbf{v} - \mathbf{v} = -\mathbf{v} - A\mathbf{v}$). It follows that $E_1 + E_{-1} = \mathbf{R}^n$.

(iv) We claim $\{\mathbf{v}_1, \dots, \mathbf{v}_r, \mathbf{w}_1, \dots, \mathbf{w}_s\}$ is a basis for \mathbf{R}^n . If $\mathbf{v} \in \mathbf{R}^n = E_1 + E_{-1}$, then $\mathbf{v} = \mathbf{u} + \mathbf{w}$, where $\mathbf{u} \in E_1$ and $\mathbf{w} \in E_{-1}$. Since $\{\mathbf{v}_1, \dots, \mathbf{v}_r\}$ is a basis for E_1 , there exist $\alpha_i \in \mathbf{R}$ such that $\mathbf{u} = \sum_i \alpha_i \mathbf{v}_i$. Since $\{\mathbf{w}_1, \dots, \mathbf{w}_s\}$ is a basis for E_{-1} , there exist $\beta_i \in \mathbf{R}$ such that $\mathbf{w} = \sum_i \beta_i \mathbf{w}_i$. Hence $\mathbf{v} = \mathbf{u} + \mathbf{w} = \sum_i \alpha_i \mathbf{v}_i + \sum_i \beta_i \mathbf{w}_i$, i.e. \mathbf{R}^n is spanned by $\{\mathbf{v}_1, \dots, \mathbf{v}_r, \mathbf{w}_1, \dots, \mathbf{w}_s\}$.

Now suppose $\sum \alpha_i \mathbf{v}_i + \sum \beta_j \mathbf{w}_j = \mathbf{0}$. Then $\sum \alpha_i \mathbf{v}_i = -\sum \beta_j \mathbf{w}_j \in E_1 \cap E_{-1} = \{\mathbf{0}\}$. Hence $\sum \alpha_i \mathbf{v}_i = \mathbf{0}$ and $\sum \beta_j \mathbf{w}_j = \mathbf{0}$. Since $\{\mathbf{v}_1, \dots, \mathbf{v}_r\}$ is a basis for E_1 , it is LI, and hence all $\alpha_i = 0$. Similarly all $\beta_j = 0$. Thus $\{\mathbf{v}_1, \dots, \mathbf{v}_r, \mathbf{w}_1, \dots, \mathbf{w}_s\}$ is LI.

Thus $\{\mathbf{v}_1, \dots, \mathbf{v}_r, \mathbf{w}_1, \dots, \mathbf{w}_s\}$ is a basis for \mathbf{R}^n .

(v) $\mathbf{v}_1, \dots, \mathbf{v}_n$ is a basis for \mathbf{R}^n consisting of eigenvectors, and hence by basic criterion (3.4) A is diagonalisable.

If $P^{-1}AP = D$, then the diagonal entries of D are the associated eigenvalues,

i.e. 1's and/or -1's, so $D = \begin{pmatrix} \pm 1 & 0 & 0 & \dots & 0 \\ 0 & \pm 1 & 0 & \dots & 0 \\ \cdot & \cdot & \cdot & \dots & \cdot \\ \cdot & \cdot & \cdot & \dots & \cdot \\ 0 & 0 & 0 & \dots & \pm 1 \end{pmatrix}$

4 Suppose $A^2 = 0$ and A is diagonalisable, say $P^{-1}AP = D = \text{diag}(\lambda_1, \dots, \lambda_n)$. Then $D^2 = (P^{-1}AP)^2 = P^{-1}AP.P^{-1}AP = P^{-1}A^2P = P^{-1}0P = 0$. But $D^2 = \text{diag}(\lambda_1^2, \dots, \lambda_n^2)$ and hence each $\lambda_i^2 = 0$. Then each $\lambda_i = 0$ and hence $D = 0$. It follows that $A = PDP^{-1} = 0$.

The easiest example of a non-zero 2×2 nilpotent matrix is $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

1202 2011-2012 Exercise 8

1 For each of the following matrices A , find the characteristic polynomial and the dimension of each eigenspace, and determine if A is diagonalizable (over \mathbf{R}). For those that are, give an invertible matrix P such that $P^{-1}AP$ is diagonal.

(i) $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}$

(ii) $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix}$

* (iii) $\begin{pmatrix} 2 & 0 & 1 \\ 0 & 2 & -2 \\ -2 & -1 & 3 \end{pmatrix}$

* (iv) $\begin{pmatrix} 0 & 3 & 1 \\ 2 & 1 & 1 \\ -6 & -9 & -5 \end{pmatrix}$

***2** Two $n \times n$ matrices A and B are said to be *simultaneously diagonalisable* if there exists an invertible P such that $P^{-1}AP$ and $P^{-1}BP$ are both diagonal.

(i) Prove that if A and B are simultaneously diagonalisable then $AB = BA$.

(ii) Let D be an $n \times n$ diagonal matrix with distinct entries on the diagonal, and X an $n \times n$ matrix such that $XD = DX$. Prove that X is diagonal.

(iii) Let A and B be two $n \times n$ matrices such that $AB = BA$ and suppose that A has n distinct eigenvalues. Prove that A and B are simultaneously diagonalizable.

(iv) Let $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$. Is it possible to simultaneously diagonalise A and B ? If so, find a matrix P that achieves this, and check it works.

*You are advised to attempt all questions. Please hand in the **assessed** questions (the questions marked with a *) on Wednesday 21 March at the lecture.*

1202 2011-2012 Exercise 8 Solutions

$$1 \text{ (i) } A = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}, \quad c_A(t) = \det \begin{pmatrix} t & -1 & 0 \\ 0 & t & -1 \\ 0 & 0 & t \end{pmatrix} = t^3.$$

Hence A has only one eigenvalue, namely 0, with algebraic multiplicity 3.

It is easy to find the corresponding eigenspace: it is just the set $\begin{pmatrix} \alpha \\ 0 \\ 0 \end{pmatrix}$. Hence the geometric multiplicity is 1. Since $1 \neq 3$, A is not diagonalizable.

$$(ii) A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix}$$

$$c_A(t) = \det \begin{pmatrix} t-1 & -1 & 0 \\ 0 & t-2 & -1 \\ 0 & 0 & t-3 \end{pmatrix} = (t-1)(t-2)(t-3).$$

Hence A has three eigenvalues 1,2,3, each with algebraic multiplicity 1. It follows immediately that A is diagonalizable. Now to find corresponding eigenvectors.

$$\lambda = 1; \text{ we solve } A\mathbf{v} = \mathbf{v}, \text{ i.e. } \begin{pmatrix} 0 & -1 & 0 \\ 0 & -1 & -1 \\ 0 & 0 & -2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Reducing to RRE form gives

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \text{ This yields one eigenvector, } \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Similarly the eigenvector corresponding to the eigenvalue 2 can be taken as $\begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}$ and that corresponding to 3 to be $\begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}$. The matrix P is given by

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix}$$

We can check that P is invertible (since $\det P = 2 \neq 0$) and that

$$\begin{aligned}
 AP &= \begin{pmatrix} 1 & 1 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 2 & 6 \\ 0 & 0 & 6 \end{pmatrix} \\
 &= \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{pmatrix} = PD
 \end{aligned}$$

as required.

$$\begin{aligned}
 \text{(iii)} \quad c_A(t) &= \det(tI - A) = \det \begin{pmatrix} t-2 & 0 & -1 \\ 0 & t-2 & 2 \\ 2 & 1 & t-3 \end{pmatrix} \\
 &= (t-2)^2(t-3) + 2(t-2) - 2(t-2) = (t-2)^2(t-3).
 \end{aligned}$$

Hence eigenvalues are $\lambda_1 = 3$ and $\lambda_2 = 2$ with algebraic multiplicities $f_1 = 1$ and $f_2 = 2$.

The eigenspace corresponding to 3 must in fact be 1-dimensional (since $1 \leq e_1 \leq f_1 = 1$).

Consider $\lambda_2 = 2$. The eigenspace is the set of solutions to $A\mathbf{v} = 2\mathbf{v}$, i.e. solutions to

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & -2 \\ -2 & -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

This is easily seen to be $\left\{ \begin{pmatrix} -\alpha \\ 2\alpha \\ 0 \end{pmatrix} : \alpha \in \mathbf{R} \right\}$ with basis $\left\{ \begin{pmatrix} -1 \\ 2 \\ 0 \end{pmatrix} \right\}$.

Hence this eigenvalue has geometric multiplicity $e_2 = 1$; since this is not equal to f_2 , the matrix is not diagonalizable.

$$\begin{aligned}
 \text{(iv)} \quad c_A(t) &= \det(tI - A) = \det \begin{pmatrix} t & -3 & -1 \\ -2 & t-1 & -1 \\ 6 & 9 & t+5 \end{pmatrix} \\
 &= t(t-1)(t+5) + 18 + 18 + 9t - 6(t+5) + 6(t-1) \\
 &= t^3 + 4t^2 - 5t + 36 + 9t - 36 \\
 &= t(t^2 + 4t + 4) \\
 &= t(t+2)^2
 \end{aligned}$$

Hence eigenvalues are $\lambda_1 = 0$, $\lambda_2 = -2$ with algebraic multiplicities $f_1 = 1$, $f_2 = 2$. Now to find eigenspaces.

$\lambda_1 = 0$. Corresponding eigenspace is given by solutions to $A\mathbf{v} = \mathbf{0}$, i.e.

$$\begin{pmatrix} 0 & 3 & 1 \\ 2 & 1 & 1 \\ -6 & -9 & -5 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Row-reducing, we get

$$\begin{pmatrix} 0 & 3 & 1 & 0 \\ 2 & 1 & 1 & 0 \\ -6 & -9 & -5 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 3 & 1 & 0 \\ 2 & 1 & 1 & 0 \\ 0 & -6 & -2 & 0 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 & 3 & 1 & 0 \\ 2 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

This is not quite in RRE form, but it is easy enough to read off the complete

solution: so the eigenspace is $\left\{ \begin{pmatrix} -\alpha \\ -\alpha \\ 3\alpha \end{pmatrix} : \alpha \in \mathbf{R} \right\}$, with a basis consisting of

the single eigenvector, e.g. $\begin{pmatrix} 1 \\ 1 \\ -3 \end{pmatrix}$.

Now for $\lambda_2 = -2$. Corresponding eigenspace is given by solutions to $A\mathbf{v} = -2\mathbf{v}$, i.e.

$$\begin{pmatrix} 2 & 3 & 1 \\ 2 & 3 & 1 \\ -6 & -9 & -3 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

Row-reducing, we get

$$\begin{pmatrix} 1 & 3/2 & 1/2 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \text{ Here there are 2 free variables, } y \text{ and } z, \text{ so the eigenspace}$$

is $\left\{ \begin{pmatrix} -(3/2)\alpha - (1/2)\beta \\ \alpha \\ \beta \end{pmatrix} : \alpha, \beta \in \mathbf{R} \right\}$.

Now $\begin{pmatrix} -(3/2)\alpha - (1/2)\beta \\ \alpha \\ \beta \end{pmatrix} = \alpha \begin{pmatrix} -3/2 \\ 1 \\ 0 \end{pmatrix} + \beta \begin{pmatrix} -1/2 \\ 0 \\ 1 \end{pmatrix}$ and hence a basis is

$\left\{ \begin{pmatrix} -3 \\ 2 \\ 0 \end{pmatrix}, \begin{pmatrix} -1 \\ 0 \\ 2 \end{pmatrix} \right\}$.

Thus geometric multiplicities (i.e. dimensions of the eigenspaces) are $e_1 = 1$ and $e_2 = 2$: since the geometric and algebraic multiplicities agree, A is diagonalizable. Let P be the matrix whose columns are made up from the bases of the eigenspaces, i.e.

$$P = \begin{pmatrix} 1 & -3 & -1 \\ 1 & 2 & 0 \\ -3 & 0 & 2 \end{pmatrix} \text{ and } P^{-1}AP = D = \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix}$$

Check: $\det P \neq 0$ so P is invertible.

$$\begin{aligned} AP &= \begin{pmatrix} 0 & 3 & 1 \\ 2 & 1 & 1 \\ -6 & -9 & -5 \end{pmatrix} \begin{pmatrix} 1 & -3 & -1 \\ 1 & 2 & 0 \\ -3 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 0 & 6 & 2 \\ 0 & -4 & 0 \\ 0 & 0 & -4 \end{pmatrix} \\ &= \begin{pmatrix} 1 & -3 & -1 \\ 1 & 2 & 0 \\ -3 & 0 & 2 \end{pmatrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & -2 \end{pmatrix} = PD \end{aligned}$$

2. (i) Suppose A and B are simultaneously diagonalizable, i.e. if there exists an invertible P such that $P^{-1}AP$ and $P^{-1}BP$ are both diagonal. Clearly any two diagonal matrices commute, so $P^{-1}AP.P^{-1}BP = P^{-1}BP.P^{-1}AP$, i.e. $P^{-1}ABP = P^{-1}BAP$ and hence $AB = BA$.

(ii) Suppose $XD = DX$, where $D = \text{diag}(\lambda_1, \dots, \lambda_n)$ (all λ_i distinct), and $X = (x_{ij})$. Then comparing (i, j) entries of XD and DX we get

$$x_{ij}\lambda_j = \lambda_i x_{ij}, \text{ i.e. } x_{ij}(\lambda_i - \lambda_j) = 0.$$

Now for $i \neq j$, $\lambda_i - \lambda_j \neq 0$, and hence $x_{ij} = 0$, i.e. X is diagonal.

(iii) Now suppose $AB = BA$. By hypothesis, there exists an invertible P such that $P^{-1}AP = D$ is diagonal with distinct entries, say $\lambda_1, \dots, \lambda_n$. Write $E = P^{-1}BP$. Then $DE = P^{-1}AP.P^{-1}BP = P^{-1}ABP = P^{-1}BAP = ED$.

By (ii), E is diagonal, and hence P simultaneously diagonalises A and B .

(iv) $A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, $B = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix}$. Hence $AB = \begin{pmatrix} 8 & 7 \\ 7 & 8 \end{pmatrix} = BA$ and hence by the above, A and B can be simultaneously diagonalised.

We easily find eigenvalues for A , which are 1 and 3, with corresponding eigenvectors $\mathbf{v}_1 = \begin{pmatrix} 1 \\ -1 \end{pmatrix}$ and $\mathbf{v}_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Hence if $P = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ then

$$P^{-1}AP = D = \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix}.$$

Now check that $BP = \begin{pmatrix} 3 & 2 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 \\ -1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$,

i.e. $P^{-1}BP = E = \begin{pmatrix} 1 & 0 \\ 0 & 5 \end{pmatrix}$.