Appendix B

Answers and hints to some exercises

Modular arithmetic and fields

1) Let $E \subset \mathbb{Z}$ be a subset of $\mathbb{Z}$ that is bounded below. We need to show the following:

$$\forall F \subseteq E \qquad F \neq \emptyset \implies F \text{ has a minimal element}$$

Proof. Let $k \in \mathbb{Z}$ be such that $\forall e \in E, e \geqslant k$. Let $F \subseteq E$ be a non-empty subset of E. Note that

$$f \in F \implies f \in E \implies f \geqslant k \implies f - k + 1 \geqslant 1 \implies f - k + 1 \in \mathbb{N}$$

Letting $F' = \{f - k + 1 \mid f \in F\}$ we have that $F' \subseteq \mathbb{N}$ and $F' \neq \emptyset$. Therefore F' has a minimal element, $m' \in F'$ say. Let $m = m' + k - 1$. Then $m \in F$ and for any $f \in F$ we have

$$f - k + 1 \geqslant m' \implies f \geqslant m$$

That is, m is a minimal element of F. □

2) We want to show

$$\forall a, b \in \mathbb{Z} \quad (\gcd(a, b) = 1 \iff (\exists x, y \in \mathbb{Z}, xa + yb = 1))$$

Let $a, b \in \mathbb{Z}$. That $\gcd(a, b) = 1 \implies (\exists x, y \in \mathbb{Z}, xa + yb = 1)$ is Bézout's Theorem (1.6).
For the converse, suppose that $x, y \in \mathbb{Z}$ are such that $xa + yb = 1$ and let $d = \gcd(a, b)$. Since d is a common divisor of a and b we have that $d \mid (xa + yb)$ (Lemma 1.3). But then we have that $d \in \mathbb{N}$ and $d \mid 1$, which implies that $d = 1$.

3) (a) $q = 8, r = 1$ (b) $q = 9, r = 5$ (c) $q = -5, r = 2$

5) Suppose that $qd + r = q'd + r'$ with $0 \leqslant r, r' < d$. Then

$$\begin{aligned} qd + r = q'd + r' &\implies (q - q')d = r' - r && (*) \\ &\implies |(q - q')d| < d \\ &\implies |q - q'| < 1 \\ &\implies q = q' \\ &\implies r = r' && \text{(from } *) \end{aligned}$$

6) Let $x, y, \alpha, \beta \in \mathbb{Z}$ be such that $c = \alpha a = \beta b$ and $xa + yb = 1$. Then

$$\begin{aligned} xa + yb = 1 &\implies x\alpha a + y\alpha b = \alpha \\ &\implies \alpha = x\beta b + y\alpha b \\ &\implies \alpha = b(x\beta + y\alpha) \\ &\implies c = b(x\beta + y\alpha)a \\ &\implies ab \mid c \end{aligned}$$

8) (a) 7 (b) 15 (c) 143 (d) 8 (e) 1

9)

(a) $\gcd(27, 33) = 3 = 5 \times 27 + (-4) \times 33$

(b) $\gcd(27, 32) = 1 = 11 \times 32 + (-13) \times 27$

(c) $\gcd(312, 317) = 13 = 5 \times 377 - 6 \times 312$

13)

(a) For the forward implication

$$[a]_m = [b]_m \implies a \in [b]_m \implies a \equiv b \pmod{m}$$

For the converse, suppose that $a \equiv b \pmod{m}$. Then

$$\begin{aligned} x \in [a]_m &\iff x \equiv a \pmod{m} \\ &\iff x \equiv b \pmod{m} && \text{(transitivity, Lemma 1.16)} \\ &\iff x \in [b]_m \end{aligned}$$

Therefore $[a]_m = [b]_m$.

(b) Suppose that $[a]_m \cap [b]_m \neq \emptyset$ and let $x \in [a]_m \cap [b]_m$. Then $x \equiv a \pmod{m}$ and $x \equiv b \pmod{m}$. Since the congruence relation is transitive (Lemma 1.16), we have $a \equiv b \pmod{m}$ and hence $[a]_m = [b]_m$ by part (a).

(c) Let $a \in \mathbb{Z}$. By Theorem 1.1 there exists $q, r \in \mathbb{Z}$ such that $a = qm + r$ and $r \in \{0, 1, \dots, m-1\}$. Then note that $a \in [r]_m$ since $m \mid (a - r)$.

14) Suppose that $b, c \in \mathbb{Z}$ are such that $[b]_m[a]_m = [1]_m$ and $[c]_m[a]_m = [1]_m$. Then we have

$$[b]_m = [b]_m[1]_m = [b]_m[c]_m[a]_m = [b]_m[a]_m[c]_m = [1]_m[c]_m = [c]_m$$

15)

$(\mathbb{Z}/7\mathbb{Z}, \times)$

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$(\mathbb{Z}/8\mathbb{Z}, \times)$

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

16)

(a) $3 \equiv 42 \pmod{13}$

(b) $2 \equiv -20 \pmod{11}$

(c) $26 \not\equiv 482 \pmod{14}$

(d) $-2 \equiv 933 \pmod{5}$ as 935 is a multiple of 5.

(e) $-2 \equiv 933 \pmod{11}$ as 935 is a multiple of 11.

(f) As 933 is a multiple of 5 and 11, it is a multiple of 55, hence $-2 \equiv 933 \pmod{55}$.

17)

(a) $6 \pmod{14}$

(b) $7 \pmod{9}$

(c) $0 \pmod{11}$

(d) $933 \equiv -2 \equiv 53 \pmod{55}$

(e) $5 \pmod{10}$

(f) $57102725 \equiv 5+7+1+0+2+7+2+5 \equiv 29 \equiv 2 \pmod 9$

18)

(a) $24 \times 25 \equiv 3 \times 4 \equiv 12 \pmod{21}$

(b) $0 \pmod{210}$

(c) $7 \pmod 9$

(d) $5 \pmod{11}$

(e) $1 \times (2 \times 3) \times (4 \times 5) \times 6 \equiv -1 \times -1 \times -1 \equiv -1 \equiv 6 \pmod 7$

(f) $1 \times 2 \times 3 \times \ldots \times 20 \times 21 \equiv (2 \times 11) \times (3 \times \ldots \times 10) \times (12 \times \ldots \times 21) \equiv 0 \times (\ldots) \times (\ldots) \equiv 0 \pmod{22}$

19) We have that $326 \equiv (3+2+6) \equiv 11 \equiv (1+1) \equiv 2 \pmod 9$, and $4471 \equiv (4+4+7+1) \equiv (16) \equiv 7 \pmod 9$. Therefore $(326 \times 4471) \equiv (2 \times 7) \equiv 14 \equiv 5 \pmod 9$. But $1357546 \equiv (1+3+5+7+5+4+6) \equiv 31 \equiv 4 \pmod 9$. Therefore $326 \times 4471 \neq 1357546$.

20) Consider the possible values of $[x]_m^2 + [y]_m^2 + [z]_m^2$

21)

(a) $\mathbb{Z}/7\mathbb{Z}$ has the set of multiplicative units $\{1,2,3,4,5,6\}$

(b) $\mathbb{Z}/8\mathbb{Z}$ has the set of multiplicative units $\{1,3,5,7\}$

(c) $\mathbb{Z}/12\mathbb{Z}$ has the set of multiplicative units $\{1,5,7,11\}$

(d) $\mathbb{Z}/13\mathbb{Z}$ has the set of multiplicative units $\{1,2,\ldots,12\}$

(e) $\mathbb{Z}/15\mathbb{Z}$ has the set of multiplicative units $\{1,2,4,7,8,11,13,14\}$

22)

(a) 32 in $\mathbb{Z}/27\mathbb{Z}$ has inverse 11 as $1 \equiv 11 \times 32 - 13 \times 27 \equiv 11 \times 32 \pmod{27}$.

(b) 32 in $\mathbb{Z}/39\mathbb{Z}$ has inverse 11.

(c) 17 in $\mathbb{Z}/41\mathbb{Z}$ has inverse $-12 \equiv 29 \pmod{41}$.

(d) 18 in $\mathbb{Z}/33\mathbb{Z}$ has no inverse as $3 = \gcd(18,33)$.

(e) 200 has inverse 41 in $\mathbb{Z}/911\mathbb{Z}$.

23) 52

25) We need to show that

$$(x+y=0) \wedge (x+z=0) \implies y=z$$

Suppose that $x+y=x+z=0$. We have

$$\begin{aligned}
x+y=0 &\implies (x+y)+z=0+z \\
&\implies (y+x)+z=z && \text{(addition is commutative, property of additive identity)} \\
&\implies y+(x+z)=z && \text{(addition is associative)} \\
&\implies y+0=z && (x+z=0) \\
&\implies y=z && \text{(property of additive identity)}
\end{aligned}$$

27) Suppose that $1=0$, and let $a \in R$. Then $a = 1 \times a = 0 \times a = 0$. Therefore $R=\{0\}$.

29) For example, $(\sqrt[3]{2})^2$ is not in the set. Set $\alpha = \sqrt[3]{2}$ and suppose that $\alpha^2 = a + b\alpha$ for some $a, b \in \mathbb{Q}$. Then

$$2 = \alpha^3 = a\alpha + b\alpha^2 = a\alpha + b(a+b\alpha) = ab + (a+b^2)\alpha.$$

It would follow that $\alpha = (2 - ab)/(a + b^2)$ and so that α is rational, which we know to be false.
If we take the set of all $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ with $a, b, c \in \mathbb{Q}$ then we do obtain a field.

30)

$$[1]_7 = [3]_7^6 \quad [2]_7 = [3]_7^2 \quad [3]_7 = [3]_7^1 \quad [4]_7 = [3]_7^4 \quad [5]_7 = [3]_7^5 \quad [6]_7 = [3]_7^3$$

31) The polynomial X, for example, does not have a multiplicative inverse.

32) Showing closure under addition and subtraction is relatively straightforward. It is reasonably easy to convince yourself of closure under multiplication. The problem is with multiplicative inverses. (I do not recommend attempting detailed proofs of all of the axioms!)
To see that

$$c_{-k}t^{-k} + c_{-k+1}t^{-k+1} + \cdots + c_0 + c_1 t + \cdots + c_s t^s + \dots$$

has an inverse, assume that $c_{-k} \neq 0$ and write the above as $c_k t^{-k} g$ where g is a power series involving only non-negative powers of t and with constant term 1. Now show g has an inverse in this set of power series.

33) The polynomial $X^2 + 1$ has no root in the field $\mathbb{Q}[\sqrt{2}]$.

35) (a) $m = 57, n = 36$ (b) 5 is relatively prime to 36 (c) 32 15 24 18 (d) $d = 29$ (e) 49 8

36) (a) $n = 40$ (b) (c) 17 14 48 25 17 15 2 15 (d) $d = 27$, rosebud

Linear algebra I

37) Suppose that $A, B, C \in M_n(K)$. Suppose that $A \sim B$ and $B \sim C$. Let $P, Q \in \mathrm{GL}(K)$ be such that $B = P^{-1}AP$ and $C = Q^{-1}BQ$. Then we have

(a) $A \sim A$ since $A = I^{-1}AI$

(b) $B \sim A$ since $B = P^{-1}AP \implies (P^{-1})^{-1}BP^{-1} = A$

(c) $A \sim C$ since $C = Q^{-1}P^{-1}APQ = (PQ)^{-1}A(PQ)$

38) Let $P \in \mathrm{GL}_n(K)$ and fix a basis $\mathcal{B}'$ for V. Since P is invertible, its columns form a basis for $M_{n,1}$. Let $b_j \in V$ be such that $[b_j]_{\mathcal{B}'}$ is the j-th column of P. Then $\mathcal{B} = \{b_1, \dots, b_n\}$ is linearly independent and therefore a basis for V. Finally note that $[\mathrm{Id}_V]_{\mathcal{B}',\mathcal{B}} = P$.

39) Let $\{u_1, \dots, u_k\}$ be a basis for $\ker(f)$. Extend to a basis $\mathcal{B} = \{u_1, \dots, u_k, v_1, \dots, v_m\}$ of V. For each $1 \leqslant i \leqslant m$ define $w_i = f(v_i)$. Then $\{w_1, \dots, w_m\}$ is linearly independent since

$$\begin{aligned}
\sum_{i=1}^{m} \alpha_i w_i = 0 \implies \sum_{i=1}^{m} \alpha_i f(v_i) = 0 \implies f(\sum_{i=1}^{m} \alpha_i v_i) = 0 \implies \sum_{i=1}^{m} \alpha_i v_i \in \ker(f) \\
\implies \sum_{i=1}^{m} \alpha_i v_i = \sum_{j=1}^{k} \beta_j u_j \implies \sum_{i=1}^{m} \alpha_i v_i + \sum_{j=1}^{k} (-\beta_j) u_j = 0 \\
\implies \forall i, \quad \alpha_i = 0 \quad \text{(since } \mathcal{B} \text{ is linearly independent)}
\end{aligned}$$

Extend to a basis $\mathcal{B}' = \{b_1, \dots, b_k, w_1, \dots, w_m\}$ of V. Then $[f]_{\mathcal{B}',\mathcal{B}}$ is a diagonal matrix with the diagonal entries being k zeros followed by m ones.

40) Note that, from the definition of an eigenvalue, there exists $v \in V_\lambda \setminus \{0\}$. In particular, $V_\lambda \neq \emptyset$. Now let $u, v \in V_\lambda$ and $k \in K$. Then $f(u + v) = f(u) + f(v) = \lambda u + \lambda v = \lambda(u + v)$ and $f(ku) = kf(u) = k\lambda u = \lambda ku$. Therefore $u + v \in V_\lambda$ and $ku \in V_\lambda$. It follows that V_λ is a subspace. Since $V_\lambda \setminus \{0\} \neq \emptyset$, $V \neq \{0\}$ and therefore $\dim(V_\lambda) \geqslant 1$.

41) Let P be an invertible matrix such that $B = P^{-1}AP$. Then

$$Bu = \lambda u \implies PBu = \lambda Pu \implies APu = \lambda Pu$$

Since P is invertible, $u \neq 0 \implies Pu \neq 0$. Therefore, if u is an eigenvector for B having eigenvalue λ, then Pu is an eigenvector for A having eigenvalue λ. Reversing the roles of A and B, we can conclude that λ is an eigenvalue for A iff λ is an eigenvalue for B.

42) We need to show that $f(f(v)) = \lambda f(v)$. Note that $f(f(v)) = f(\lambda v) = \lambda f(v)$. Therefore $f(V_\lambda) \subseteq V_\lambda$.

44) The proofs given for $1 \implies 2$ and $2 \implies 3$ did not assume that V is finite dimensional. We need only prove $3 \implies 1$.
Assume that $\mathcal{B}$ and $\mathcal{C}$ are as in 3. Since $\mathcal{B} \cup \mathcal{C}$ is a spanning set, we have that $V = U + W$. It remains to show that $U \cap W = \{0\}$.
Let $v \in U \cap W$. Then, since $v \in U$ we have $v = \sum_{i=1}^m \beta_i b_i$ for some $m \in \mathbb{N}$, $\beta_i \in K$ and $b_i \in \mathcal{B}$. Similarly, $v = \sum_{j=1}^n \gamma_j c_i$ for some $n \in \mathbb{N}$, $\gamma_j \in K$ and $c_j \in \mathcal{C}$. Then

$$\begin{aligned} \sum_{i=1}^m \beta_i b_i = \sum_{j=1}^n \gamma_j c_i &\implies \sum_{i=1}^m \beta_i b_i + \sum_{j=1}^n (-\gamma_j) c_i = 0 \\ &\implies \forall i \forall j \quad (\beta_i = 0 \text{ and } \gamma_j = 0) && \text{(since } \mathcal{B} \cup \mathcal{C} \text{ is linearly indepemdent)} \\ &\implies v = 0 \end{aligned}$$

45) Let $V_1 = \{v \in V : f(v) = -v\}$ and $V_{-1} = \{v \in V : f(v) = -v\}$. We need to show that $V = V_1 + V_{-1}$ and that $V_1 \cap V_{-1} = \{0\}$. For the second note that

$$v \in V_1 \cap V_{-1} \implies v = -v \implies 2v = 0 \implies v = 0$$

The last implication above requires the hypothesis that $2 \neq 0$ in the field of scalars.
We need now to show that $V = V_1 + V_{-1}$. Note that since $X^2 - 1$ is the minimal polynomial of f, we have that $f^2 = \mathrm{Id}_V$. Given any $v \in V$ we have that $v = 2^{-1}(v + f(v)) + 2^{-1}(v - f(v))$ (we have again used that $2 \neq 0$). Finally, note that $2^{-1}(v + f(v)) \in V_1$ and $2^{-1}(v - f(v)) \in V_{-1}$ since

$$f(2^{-1}(v + f(v))) = 2^{-1} f((v + f(v))) = 2^{-1}(f(v) + f^2(v)) = 2^{-1}(f(v) + v) = 2^{-1}(v + f(v))$$

and

$$f(2^{-1}(v - f(v))) = 2^{-1} f((v - f(v))) = 2^{-1}(f(v) - f^2(v)) = 2^{-1}(f(v) - v) = -2^{-1}(v - f(v))$$

If $\mathcal{B}$ is a basis for V_1 and $\mathcal{C}$ is a basis for V_{-1}, then $[f]_{\mathcal{B}\cup\mathcal{C}}$ will be diagonal with all diagonal entries ± 1.

47) From Theorem 2.18, there are $q(X), r(X) \in K[X]$ such that $p(X) = q(X)(X - k) + r(X)$ and $\deg(r(X)) = 0$. We need to show that $r(X) = 0$. Let $a \in K$ be such that $r(X) = a$. Then

$$p(k) = q(k)(k - k) + a \implies 0 = q(k)0 + a = a$$

Therefore $r(X) = 0$ and $p(X) = q(X)(X - k)$.

48)

(a) $\frac{1}{b-a}(X - a) + \frac{1}{a-b}(X - b) = 1$

(b) First we will show that $(X - a)$ is prime. That is, we show that

$$\forall p(X), q(X) \in K[X] \quad (X - a) \mid p(X)q(X) \implies (X - a) \mid p(X) \vee (X - a) \mid q(X) \qquad (*)$$

To prove this we have

$$\begin{aligned} (X - a) \mid p(X)q(X) &\implies p(X)q(X) = (X - a)r(X) && \text{(for some } r(X) \in K[X]) \\ &\implies p(a)q(a) = 0 \\ &\implies p(a) = 0 \vee q(a) = 0 && \text{(using that } K \text{ is a field)} \\ &\implies (X - a) \mid p(X) \vee (X - a) \mid q(X) && \text{(by Exercise 47)} \end{aligned}$$

Using $(*)$, the desired result can then be established using induction on m. Here's the outline.

$$\begin{aligned} d(X) \mid (X - a)^m &\implies d(X)e(X) = (X - a)^m && \text{(some } e(X) \in K[X]) \\ &\implies (X - a) \mid d(X)e(X) \\ &\implies (X - a) \mid d(X) \vee (X - a) \mid e(X) \end{aligned}$$

and

$$\begin{aligned}
(X-a) \mid d(X) &\implies d(X) = d'(X)(X-a) && \text{(some } d'(X) \in K[X]\text{)}\\
&\implies d'(X)e(X) = (X-a)^{m-1} &&\\
&\implies d'(X) = (X-a)^{k'} && \text{(for some } 1 \leqslant k' \leqslant m-1\text{)}\\
&\implies d(X) = (X-a)^{k} && \text{(with } 2 \leqslant k \leqslant m\text{)}
\end{aligned}$$

and

$$\begin{aligned}
(X-a) \mid e(X) &\implies e(X) = e'(X)(X-a) && \text{(some } e'(X) \in K[X]\text{)}\\
&\implies d(X)e'(X) = (X-a)^{m-1} &&\\
&\implies d(X) = (X-a)^{k} && \text{(for some } 1 \leqslant k \leqslant m-1\text{)}
\end{aligned}$$

50) $(X-2)(X+1)$, X^2+X-1, X^3-1, $(X-1)^3$

51) The minimal polynomial of either matrix is $(X-1)(X-2)$.
The characteristic polynomials are $(X-1)^2(X-2)^2$ and $(X-1)^3(X-2)$, respectively.

52) Check by direct computation that $A^2-2A-8I_3=0$. Since this polynomial has distinct roots, it must be the minimal polynomial of the matrix. Note that

$$A^2-2A-8I=0 \implies A\frac{1}{8}(A-2I)=I$$

The above calculation shows that A^{-1} exists and is equal to $\frac{1}{8}(A-2I)$.

53) If the minimal polynomial has non-zero constant term, use the idea of the previous question to show there is an inverse.

If the minimal polynomial has zero constant term, then it is of the form $m(X)=Xp(X)$ for some polynomial $p(X)$. Since $p(f)\neq 0$, there is a vector v such that $w=p(f)(v)\neq 0$. But $f(w)=f(p(f)(v))=m(f)(v)=0$. If f had an inverse f^{-1} we could deduce that $w=f^{-1}(f(w))=f^{-1}(0)=0$ which is a contradiction.

54) You can do this by taking a power of an appropriate matrix. But the 'slick' way to do it is to use the linear transformation f which corresponds to A, using the standard basis $\{e_1,\ldots,e_n\}$. Note that $f(e_i)$ can be written as a linear combination of those e_j with $j<i$. Now show that $f^2(e_i)$ can be written as a linear combination of those e_j with $j<i-1$ and then work out what happens for $f^n(e_i)$.

55)

(a) The characteristic polynomial is $(X-2)^3$. The only eigenvalue is 2.

(b) The minimal polynomial is $(X-2)^2 \in \mathbb{F}_5[X]$

(c) $\mathcal{B}=\{(1,0,1),(-2,1,0),(1,0,0)\}$

$$[f]_{\mathcal{B}} = \begin{bmatrix} 2 & 0 & 3\\ 0 & 2 & 2\\ 0 & 0 & 2\end{bmatrix}$$

56) Let P be an invertible matrix such that $B=P^{-1}AP$. Using standard properties of the determinant, we have

$$\begin{aligned}
c_A(X) &= \det(XI-A) = \det(P^{-1}P)\det(XI-A) = \det(P^{-1})\det(XI-A)\det(P)\\
&= \det(P^{-1}(XI-A)P) = \det(XP^{-1}IP-P^{-1}AP) = \det(XI-P^{-1}AP)\\
&= \det(XI-B)\\
&= c_B(X)
\end{aligned}$$

58) Suppose that $T:V\to V$ is nilpotent, and let $n\in\mathbb{N}$ be minimal with the property that that $T^n=0$. Since $T^{n-1}\neq 0$, there exists $v\in V$ such that $w=T^{n-1}(v)\neq 0$. However, $T(w)=T^n(v)=0$.

63)

$$\begin{bmatrix}-2 & 1\\ 0 & -2\end{bmatrix}, \begin{bmatrix}2 & 0 & 0\\ 0 & -1 & 1\\ 0 & 0 & -1\end{bmatrix}, \begin{bmatrix}-2 & 0 & 0\\ 0 & -2 & 0\\ 0 & 0 & 4\end{bmatrix}$$

64) Recall that $J(a,n)$ represents the Jordan block with size n and diagonal entry a.

(a) one $J(0,2)$ plus two $J(-1,2)$ **or** one $J(0,2)$ plus one $J(-1,2)$ plus two $J(-1,1)$

(b) two $J(3,2)$ plus one $J(3,1)$ **or** one $J(3,2)$ plus three $J(3,1)$

(c) two $J(0,3)$ plus one $J(0,1)$ **or** one $J(0,3)$ plus two $J(0,2)$ **or** one $J(0,3)$ plus one $J(0,2)$ plus two $J(0,1)$ **or** one $J(0,3)$ plus four $J(0,1)$

(d) two $J(1,2)$ plus two $J(-1,2)$ **or** two $J(1,2)$ plus one $J(-1,2)$ plus two $J(-1,1)$ **or** one $J(1,2)$ plus two $J(1,1)$ plus two $J(-1,2)$ **or** one $J(1,2)$ plus two $J(1,1)$ plus one $J(-1,2)$ plus two $J(-1,1)$

65) (a) no (b) yes (c) yes

66) Remember that the minimal polynomial divides the characteristic polynomial and has the same roots (possibly with different multiplicity). Then use Exercise 59. Note that if the characteristic polynomial has the form $(X-a)^4$ and the minimal polynomial has the form $(X-a)^2$ then there are two possibilities which we cannot distinguish without more information. In the following list, a, b, c, d are distinct scalars.

characteristic polynomial	minimal polynomial	JNF
$(X-a)(X-b)(X-c)(X-d)$	$(X-a)(X-b)(X-c)(X-d)$	$J(a,1) \oplus J(b,1) \oplus J(c,1) \oplus J(d,1)$
$(X-a)^2(X-b)(X-c)$	$(X-a)(X-b)(X-c)$	$J(a,1) \oplus J(a,1) \oplus J(b,1) \oplus J(c,1)$
	$(X-a)^2(X-b)(X-c)$	$J(a,2) \oplus J(b,1) \oplus J(c,1)$
$(X-a)^2(X-b)^2$	$(X-a)(X-b)$	$J(a,1) \oplus J(a,1) \oplus J(b,1) \oplus J(b,1)$
	$(X-a)^2(X-b)$	$J(a,2) \oplus J(b,1) \oplus J(b,1)$
	$(X-a)(X-b)^2$	$J(a,1) \oplus J(a,1) \oplus J(b,2)$
	$(X-a)^2(X-b)^2$	$J(a,2) \oplus J(b,2)$
$(X-a)^3(X-b)$	$(X-a)(X-b)$	$J(a,1) \oplus J(a,1) \oplus J(a,1) \oplus J(b,1)$
	$(X-a)^2(X-b)$	$J(a,1) \oplus J(a,2) \oplus J(b,1)$
	$(X-a)^3(X-b)$	$J(a,3) \oplus J(b,1)$
$(X-a)^4$	$(X-a)$	$J(a,1) \oplus J(a,1) \oplus J(a,1) \oplus J(a,1)$
	$(X-a)^2$	$J(a,1) \oplus J(a,1) \oplus J(a,2)$ OR $J(a,2) \oplus J(a,2)$
	$(X-a)^3$	$J(a,1) \oplus J(a,3)$
	$(X-a)^4$	$J(a,4)$

67) Set D to be the diagonal part of J and set $N = J - D$. Then Exercise 54 shows that N is nilpotent. For the second part, choose a basis so that f is represented by a JNF matrix J. Write $J = D + N$ as in the first part. Then let d and n be the linear transformations corresponding to the matrices D and N.

68) Show that $JD = DJ$ first (you can easily reduce it to the case where J is just a single Jordan block.) Then $JN = NJ$ follows quickly. The last part is now immediate.

Groups

70)

(a)

$$\begin{aligned} e' &= e * e' && \text{(since } \forall g \in G, e * g = g\text{)} \\ &= e && \text{(since } \forall g \in G, g * e' = g\text{)} \end{aligned}$$

(b)

$$\begin{aligned} h' &= (h * g) * h' && \text{(since } h * g = e\text{)} \\ &= h * (g * h') \\ &= h && \text{(since } g * h' = e\text{)} \end{aligned}$$

(c) Note that

$$(g * h) * (h^{-1} * g^{-1}) = g * (h * h^{-1}) * g^{-1} = g * g^{-1} = e$$
$$(h^{-1} * g^{-1}) * (g * h) = h^{-1} * (g^{-1} * g) * h = h^{-1} * h = e$$

and apply the previous part.

72) Let $I = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, $-I = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$, $A = \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, $-A = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$, $B = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$, and $-B = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]$.

V	I	A	$-I$	$-A$
I	I	A	$-I$	$-A$
A	A	I	$-A$	$-I$
$-I$	$-I$	$-A$	I	A
$-A$	$-A$	$-I$	A	I

C_4	I	B	$-I$	$-B$
I	I	A	$-I$	$-B$
B	B	$-I$	$-B$	I
$-I$	$-I$	$-B$	I	B
$-B$	$-B$	I	B	$-I$

73) For the second part, note that the product of two reflections having the same centre, is a rotation.

74) Use $w = yx^{-1}$ and $z = x^{-1}y$. For uniqueness, suppose that, also, $w_1 x = y$. Then $wx = w_1 x$ and so $wx(x^{-1}) = w_1 x(x^{-1})$. Then $w(xx^{-1}) = w_1(xx^{-1})$ and so $we_G = w_1 e_G$. That is, $w = w_1$. A similar argument works to show the uniqueness of z. For the final sentence, choose x and y which do not commute to show that the answer is no.

75) For example,

$$h\left(g(x)\right) = \frac{1}{\frac{x-1}{x}} = \frac{x}{x-1} = k(x)$$

so that $hg = k$. The simplest way to do this question is to construct a multiplication table:

	f	g	h	i	j	k
f	g	i	k	f	h	j
g	i	f	j	g	k	h
h	j	k	i	h	f	g
i	f	g	h	i	j	k
j	k	h	g	j	i	f
k	h	j	f	k	g	i

The operations is associative because it is composition of functions. The identity is i and it is easy to check from the table that every element has an inverse.

76) Let $g, h \in G$. Then

$$ghgh = g^2h^2 \implies g^{-1}ghghh^{-1} = g^{-1}g^2h^2h^{-1} \implies hg = gh$$

77)

(a) $(264)(35)$ (b) (1356724) (c) (1456)

78) Let $H = \cap_{i \in I} H_i$.

$$\begin{aligned} h, k \in H &\implies \forall i \in I,\ h \in H_i \wedge k \in H_i \\ &\implies \forall i \in I,\ hk^{-1} \in H_i && \text{(since } H_i \text{ is a subgroup)} \\ &\implies hk^{-1} \in H \end{aligned}$$

79) $\{0\}$, $\{0, 6\}$, $\{0, 4, 8\}$, $\{0, 3, 6, 9\}$, $\{0, 2, 4, 6, 8, 10\}$, $\mathbb{Z}/12\mathbb{Z}$.

80)

(a) No (b) No (c) Yes

81) Let $H = \{z \in \mathbb{C} \mid \exists n \in \mathbb{N},\ z^n = 1\}$ and let $h, k \in H$. Note that $H \neq \emptyset$ since $1 \in H$. Let $m, n \in \mathbb{N}$ be such that $h^m = 1$ and $k^n = 1$. Then $hk^{-1} \in H$ since $(hk^{-1})^{mn} = (h^m)^n (k^n)^{-m} = 1^n 1^{-m} = 1$. Apply Lemma 3.12.

84)

(a) 12

(b) 10

(c) 2

(d) infinite order

(e) 10, 5, 20, 10

(f) 12, 2, 4

85) Note that for any $m \in \mathbb{N}$.

$$g^m = e \implies (g^{-1})^m = (g^m)^{-1} = e^{-1} = e$$

Similarly, $(g^{-1})^m = e \implies g^m = e$. That $|g| = |g^{-1}|$ is then immediate from the definition of order.

86) Let $g, h \in G$ and $m, n \in \mathbb{N}$ with $g^m = h^n = e$. Then $(gh)^{mn} = g^{mn}h^{mn} = e^n e^m = e$.

87)

$$\begin{aligned}
&A \neq I \qquad A^2 = \begin{bmatrix} -1 & -1 \\ 1 & 0 \end{bmatrix} \neq I \qquad A^3 = I \\
&B \neq I \qquad B^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \neq I \qquad B^3 = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \neq I \qquad B^4 = I \\
&AB = \begin{bmatrix} -1 & 0 \\ 1 & -1 \end{bmatrix} \neq I \qquad (AB)^2 = \begin{bmatrix} 1 & 0 \\ -2 & 1 \end{bmatrix} \neq I \qquad (AB)^3 = \begin{bmatrix} -1 & 0 \\ 3 & -1 \end{bmatrix} \neq I \\
&(AB)^m = (-1)^m \begin{bmatrix} 1 & 0 \\ -m & 1 \end{bmatrix} \neq I \qquad \text{(for all } m \in \mathbb{N})
\end{aligned}$$

89) $|e| = 1$. For $1 \leqslant i \leqslant n$ we have: $|r^i s| = 2$, $|r^i| = n/\gcd(i, n)$.
To show that $|r^i| = n/\gcd(i, n)$ we can argue as follows. Let $d = \gcd(i, n)$ and let $i', n' \in \mathbb{N}$ be such that $i = di'$ and $n = dn'$. Note that i' and n' are relatively prime since

$$\begin{aligned}
d &= xi + yn && \text{(for some } x, y \in \mathbb{Z}) \\
&= xdi' + ydn' \\
\implies 1 &= xi' + yn'
\end{aligned}$$

Note that

$$(r^i)^{n'} = r^{di'n'} = (r^n)^{i'} = e^{i'} = e$$

and for $m \in \mathbb{N}$

$$\begin{aligned}
(r^i)^m = e &\implies r^{im} = e \implies n \mid im && (|r| = n) \\
&\implies n' \mid i'm \\
&\implies n' \mid m && (i' \text{ and } n' \text{ are relatively prime})
\end{aligned}$$

Therefore $|r^i| = n'$.

90)

(a) See Lemma 3.30.

(b) From Lemma 3.30 we have that $|\varphi(g)| \mid |g|$ and $|g| = |\varphi^{-1}(\varphi(g))| \mid |\varphi(g)|$.

91) By definition $SO(2) = \{A \in M_2(\mathbb{R}) \mid A^T A = I\}$. Each element of $SO(2)$ is of the form $A = \left[\begin{smallmatrix} \cos(\theta_A) & -\sin(\theta_A) \\ \sin(\theta_A) & \cos(\theta_A) \end{smallmatrix}\right]$ for some $\theta_A \in (-\pi, \pi]$. Show that the map $\varphi : SO(2) \to S^1$, $\varphi(A) = \theta_A$ is an isomorphism.

92) If $n = mk$, then we can draw a regular m-gon inside the regular n-gon. Use this to show that a subgroup of D_n can be identified with (i.e., is isomorphic to) the symmetries of a regular m-gon.

93)

(a) The element $-1 \in \mathbb{R}^\times$ has order 2. No element in $(\mathbb{R}, +)$ has order 2.

(b) Suppose that $\varphi : \mathbb{Z} \to \mathbb{Q}$ is an isomorphism. Consider the element $z = \varphi^{-1}(\varphi(1)/2) \in \mathbb{Z}$. Then $\varphi(z + z) = \varphi(z) + \varphi(z) = \varphi(1)$, which implies that $2z = 1$. Contradiction.

(c) Suppose that $\varphi : (\mathbb{Q}, +) \to (\mathbb{Q}^+, \times)$ is an isomorphism. Consider the element $q = \varphi(\varphi^{-1}(2)/2) \in (\mathbb{Q}^+, \times)$. Then $q^2 = \varphi(\varphi^{-1}(2)/2)\varphi(\varphi^{-1}(2)/2) = \varphi(\varphi^{-1}(2)/2 + \varphi^{-1}(2)/2) = \varphi(\varphi^{-1}(2)) = 2$. Contradiction.

95) The order of $H \cap K$ must divide both 7 and 29.

96) Each right coset

$$H \begin{bmatrix} x_0 & y_0 \\ 0 & 1 \end{bmatrix} = \left\{ \begin{bmatrix} zx_0 & zy_0 \\ 0 & 1 \end{bmatrix} \mid z > 0 \right\}$$

can be identified with a half-line through a point (x_0, y_0) with $x_0 > 0$ and the origin (that is, with a non-vertical half-line through the origin). Each left coset

$$\begin{bmatrix} x_0 & y_0 \\ 0 & 1 \end{bmatrix} H = \left\{ \begin{bmatrix} x_0 z & y_0 \\ 0 & 1 \end{bmatrix} \mid z > 0 \right\}$$

can be identified with a horizontal half-line.

97) This is exactly the argument that each solution of the inhomogeneous set of equations is the sum of a solution of the corresponding homogeneous set and a fixed solution of the inhomogeneous set (a coset representative).

98)

(a) The cosets of H are H and Hb. Now show that if $ab \in Hb$, then $a \in H$.

(b) Consider cosets H, Hx, Hy with $H \neq Hx$ and $H \neq Hy$. So $x, y \notin H$ and therefore $x, y^{-1} \notin H$. Thus $xy^{-1} \in H$ and so $Hx = Hy$. Thus there can be at most one coset different from H.

99) Suppose that r is a rotation through $2\pi/5$ and s is a reflection. Then the subgroups are

$$\{e\}, \langle r\rangle, \langle s\rangle, \langle rs\rangle, \langle r^2 s\rangle, \langle r^3 s\rangle, \langle r^4 s\rangle, D_5$$

100)

(a) $D_4 = \{e, r, r^2, r^3, s, rs, r^2 s, r^3 s\}$. The cyclic subgroups are: $\langle e\rangle, \langle r\rangle = \langle r^3\rangle, \langle r^2\rangle, \langle s\rangle, \langle rs\rangle, \langle r^2 s\rangle, \langle r^3 s\rangle$.

(b) The idea is to find two reflections that commute.

One such pair is s and $r^2 s$. This subgroup is $\langle s, r^2 s\rangle = \{e, s, r^2 s, r^2\}$. Observe that no element has order 4.

Another pair of reflections that commute is rs and $r^3 s$. This subgroup is $\langle rs, r^3 s\rangle = \{e, rs, r^3 s, r^2\}$. Observe that no element has order 4.

(c) The subgroup of all rotations is cyclic and so any non-cylic subgroup must contain at least one reflection. Since groups of order 2 are cyclic, it must also contain at least one more non-identity element. If this is another reflection then the product of these two different reflections is a non-identity rotation. Thus the subgroup must contain a non-identity rotation. A little checking should now convince you that the subgroup is either one of the two subgroups above or the whole group.

101) For the subgroups of orders 2,3, take cyclic subgroups generated by rotations about the midpoint of an edge and a vertex (respectively). For the subgroup of order 4, consider the set of all rotations about axes connecting the midpoints of opposite sides (you need to show it gives a subgroup). For the last part, first establish that there is no element of order 6 and so no cyclic subgroup of order 6.

102) Let $p = 29$ and note that p is prime. An element of G must have order dividing p^2 and so must have order 1, p or p^2. If there is an element of order p^2, then G is cyclic.

104) Check explicitly that $\forall \sigma \in S_4\ \forall h \in H,\ \sigma h \sigma^{-1} \in H$. Alternatively, show that for $a, b, c, d \in \{1, 2, 3, 4\}$ distinct, we have

$$\sigma(a, b)(c, d)\sigma^{-1} = (\sigma(a), \sigma(b))(\sigma(c), \sigma(d))$$

105) Let $g \in G \backslash H$. The two left cosets are $\{H, gH\}$. The two right cosets are $\{H, Hg\}$. Since the left cosets partition G and the right cosets partition G, it must be the case that $gH = Hg$. Therefore H is normal.

109) Let $H \leqslant G$ have order n. Show that, for any $g \in G$, gHg^{-1} has the same order as H by showing that the map $H \to gHg^{-1}$ given by $h \mapsto ghg^{-1}$ is a bijection. So, by assumption $gHg^{-1} = H$.

110) The normal subgroups of D_4 are:

$$\{e\}, \langle r^2\rangle, \langle r\rangle, \langle s, r^2 s\rangle, \langle rs, r^3 s\rangle, D_4$$

111)

(a) This is essentially straight calculation.

(b) There are five cyclic subgroups. They are

$$\langle U\rangle, \langle -U\rangle, \langle I\rangle = \langle -I\rangle, \langle J\rangle = \langle -J\rangle, \langle K\rangle = \langle -K\rangle.$$

(c) If we are to find a non-cyclic subgroup of Q_8 then we must include at least two elements out of $\pm I, \pm J, \pm K$ and not two of the form $\{I, -I\}$ etc. But then it is not too hard to check that we can generate every element and so the subgroup is the whole group.

(d) From the pervious parts we know that all subgroups aside from $\langle U\rangle$, $\langle -U\rangle$ and Q_8 have size 4. They are therefore of index 2 and hence normal. The subgroups $\langle U\rangle$ and Q_8 are obviously normal. That $\langle -U\rangle$ is normal is an easy check.

(e) No. *All* proper subgroups of Q_8 are cyclic but this is not true for D_4. (Alternatively, all subgroups of Q_8 are normal but this is not true for D_4.)

113)

$$\mathbb{Q}/\mathbb{Z} = \{a + \mathbb{Z} : a \in \mathbb{Q}\} \leqslant \{a + \mathbb{Z} : a \in \mathbb{R}\} = \mathbb{R}/\mathbb{Z}.$$

For the second part, $a + \mathbb{Z}$ has finite order if and only if $n(a + \mathbb{Z}) = 0 + \mathbb{Z}$ if and only if $na \in \mathbb{Z}$. That is, if and only if $a \in \mathbb{Q}$.

114)

(a) It's enough to note that $sr^4s^{-1} = sr^4s = r^4 \in H$ and $rr^4r^{-1} = r^4 \in H$.

(b)

	H	Hr	Hr^2	Hr^3	Hs	Hrs	Hr^2s	Hr^3s
H	H	Hr	Hr^2	Hr^3	Hs	Hrs	Hr^2s	Hr^3s
Hr	Hr	Hr^2	Hr^3	H	Hrs	Hr^2s	Hr^3s	Hs
Hr^2	Hr^2	Hr^3	H	Hr	Hr^2s	Hr^3s	Hs	Hrs
Hr^3	Hr^3	H	Hr	Hr^2	Hr^3s	Hs	Hrs	Hr^2s
Hs	Hs	Hr^3s	Hr^2s	Hrs	H	Hr^3	Hr^2	Hr
Hrs	Hrs	Hs	Hr^3s	Hr^2s	Hr	H	Hr^3	Hr^2
Hr^2s	Hr^2s	Hrs	Hs	Hr^3s	Hr^2	Hr	H	Hr^3
Hr^3s	Hr^3s	Hr^2s	Hrs	Hs	Hr^3	Hr^2	Hr	H

116) From the first isomorphism theorem, we know that $\mathrm{im}(\varphi) \cong (\mathbb{Z}/8\mathbb{Z})/\ker(\varphi)$. The possibilities for $\ker(\varphi)$ are:

$$\{e\}, \langle 4\rangle, \langle 2\rangle, \langle 1\rangle$$

(These are the only subgroups. All subgroups are normal because the group is abelian.) Then note that $(\mathbb{Z}/8\mathbb{Z})/\{e\} \cong (\mathbb{Z}/8\mathbb{Z})$, $(\mathbb{Z}/8\mathbb{Z})/\langle 4\rangle \cong (\mathbb{Z}/4\mathbb{Z})$, $(\mathbb{Z}/8\mathbb{Z})/\langle 2\rangle \cong (\mathbb{Z}/4\mathbb{Z})$, and $(\mathbb{Z}/8\mathbb{Z})/\langle 1\rangle \cong \{e\}$.

Linear algebra II

119)

(a) $\sqrt{19}$

(b) $\sqrt{\frac{11}{30}}$

(c) $\sqrt{30}$

120) If $u = v$ then the claim gives $\|2u\| = 4\|u\|$, which is false if $u \neq 0$. Try proving $\|u + v\|^2 + \|u - v\|^2 = 2\|u\|^2 + 2\|v\|^2$ by expanding into inner products.

121) For the third part, note that

$$\begin{aligned}\|x + y\|^2 &= \langle x + y, x + y\rangle = \langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle = \langle x + y, x + y\rangle = \langle x, x\rangle + \langle x, y\rangle + \overline{\langle x, y\rangle} + \langle y, y\rangle \\ &= \|x\|^2 + 2\Re(\langle x, y\rangle) + \|y\|^2 \leqslant \|x\|^2 + 2|\langle x, y\rangle| + \|y\|^2 \leqslant \|x\|^2 + 2\|x\|\|y\| + \|y\|^2 = (\|x\| + \|y\|)^2\end{aligned}$$

The required inequality then follows by taking $x = u - w$ and $y = w - v$.

123) We know from Exercise 122 that $W \subseteq (W^\perp)^\perp$ and that $\dim V = \dim W + \dim W^\perp = \dim W^\perp + \dim (W^\perp)^\perp$. Therefore $\dim W = \dim(W^\perp)^\perp$ and $W \subseteq (W^\perp)^\perp$. It follows that $W = (W^\perp)^\perp$.

125) Suppose that $A = [\mathrm{Id}]_{\mathcal{C},\mathcal{B}}$ for orthonormal bases $\mathcal{C}$ and $\mathcal{B} = \{b_1, \dots, b_n\}$. The j-th column of A is equal to $[b_j]_\mathcal{C}$. The i-th row of A^* is equal to $([b_i]_\mathcal{C})^*$. Therefore the ij-th entry of A^*A is equal to $([b_i]_\mathcal{C})^*[b_j]_\mathcal{C}$. Then note that $([b_i]_\mathcal{C})^*[b_j]_\mathcal{C} = \overline{\langle b_i, b_j\rangle}$ because $\mathcal{C}$ is orthonormal.

126) Let $\lambda \in \mathbb{C}$ and $v \in V \setminus \{0\}$ be such that $f(v) = \lambda v$.

(a) If $f^* = f$, then
$$\lambda\langle v, v\rangle = \langle \lambda v, v\rangle = \langle f(v), v\rangle = \langle v, f(v)\rangle = \langle v, \lambda v\rangle = \overline{\lambda}\langle v, v\rangle$$
Therefore $\lambda = \overline{\lambda}$.

(b) If $f^*f = \mathrm{Id}$, then
$$\lambda\overline{\lambda}\langle v, v\rangle = \langle \lambda v, \lambda v\rangle = \langle f(v), f(v)\rangle = \langle v, f^*f(v)\rangle = \langle v, v\rangle$$
Therefore $\lambda\overline{\lambda} = 1$.

127) Let $K = \ker(f)$. Let $k \in \ker(f)$ and $u \in V$. Then $\langle f^*(u), k\rangle = \langle u, (f^*)^*(k)\rangle = \langle u, f(k)\rangle = \langle u, 0\rangle = 0$. Therefore $\mathrm{im}(f^*) \subseteq K^\perp$. Further, $(\mathrm{im}(f^*))^\perp \subseteq K$ since
$$\begin{aligned} w \in \mathrm{im}(f^*)^\perp &\implies \forall v \in V, \quad \langle w, f^*(v)\rangle = 0 \\ &\implies \forall v \in V, \quad \langle f(w), v\rangle = 0 \\ &\implies \langle f(w), f(w)\rangle = 0 \\ &\implies f(w) = 0 \end{aligned}$$
It follows that $\mathrm{im}(f^*) = (\mathrm{im}(f^*)^\perp)^\perp \supseteq K^\perp$.
$$\mathrm{rank}(f^*) = \dim(\mathrm{im}(f^*)) = \dim(K^\perp) = V - \dim(K) = \dim(\mathrm{im}(f)) = \mathrm{rank}(f)$$

130) Suppose that $\{v_1, \dots, v_n\}$ is an orthonormal basis of V. Suppose that $w = \sum_i a_i v_i$ and that $f(v_j) = \sum_i b_{ij} v_i$. Then $\langle f(v_j), w\rangle = \sum_i b_{ij} a_i$. Set $w_1 = \sum_k c_k v_k$ where $c_k = \sum_i b_{ik} a_i$. Note that $\langle v_j, w_1\rangle = c_j = \langle f(v_j), w\rangle$.
For the uniqueness, note that if w_2 also satisfies the conditions, then $\langle v, w_1\rangle = \langle v, w_2\rangle$ for all $v \in V$.

131)

(a) $\langle g(u+w), u+w\rangle = 0 \implies \langle g(u) + g(w), u+w\rangle = 0 \implies \langle g(u), w\rangle + \langle g(w), u\rangle = 0$

(b) Observe that $\langle g(w), u\rangle = \langle w, g^*(u)\rangle = \langle w, g(u)\rangle = \overline{\langle g(u), w\rangle} = \langle g(u), w\rangle$ to show that $2\langle g(u), w\rangle = 0$. Now deduce that g is zero.

(c) As in the previous part but deduce that the real part of $\langle g(u), w\rangle$ is 0.

(d) If $\langle g(iu), w\rangle$ is imaginary for all $u, w \in V$, then $\langle g(u), w\rangle = i\langle g(u), w\rangle$ is both real and imaginary and so zero.

(e) Take $w = g(u)$.

134) You can solve this by writing the matrix as $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$. Then multiply this by its transpose and equate the result to the identity. It will be useful to observe that if $x^2 + y^2 = 1$, then there is an angle θ so that $x = \cos\theta$ and $y = \sin\theta$.

135) Show that $AA^* = UDD^*U^* = UD^*DU^* = A^*A$.

136)
$$\begin{aligned} ff^* = f^*f &\iff \forall v \in V, \quad ff^*(v) - f^*f(v) = 0 \\ &\iff \forall u, v \in V, \quad \langle u, ff^*(v) - f^*f(v)\rangle = 0 \\ &\iff \forall u, v \in V, \quad \langle u, ff^*(v)\rangle - \langle u, f^*f(v)\rangle = 0 \\ &\iff \forall u, v \in V, \quad \langle f^*(u), f^*(v)\rangle - \langle f(u), f(v)\rangle = 0 \end{aligned}$$

137) Find a diagonal matrix similar to A, take the square root of that and use that to find a square root of A.
The matrix $\left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$ (which is not normal) has no square root.

138)

(a) No; different eigenvalues (b) No; different eigenvalues (c) Yes

139) No; they may have different eigenvalues.

141) Choose a diagonal matrix A to represent f. Find a polynomial $p(X)$ so that $p(\lambda) = \overline{\lambda}$ for each eigenvalue λ of A. Then $p(A) = A^*$ and so $p(f) = f^*$.

142) If f, g are normal, they can be simultaneously diagonalised to two matrices A and B say. Then the matrix of f^* is A^* and A^* is diagonal. Thus $A^*B = BA^*$ and so $f^*g = gf^*$.

143)

(a) $(f^*f)(f^*f)^* = (f^*f)(f^*f)$ and $(f^*f)^*(f^*f) = (f^*f)(f^*f)$.

(b) Use the Spectral Theorem and group together equal eigenvalues.

(c) Let B denote the matrix for f with respect to the basis used in the previous part. Write B as an $m \times m$ block matrix and then use the fact that this matrix commutes with the matrix found in the previous part.

(d) The first part is immediate. For the second part, firstly recall that $A_i = \lambda_i I_{m_i}$. Thus, if $\lambda_i \neq 0$ then $B_i^* = \lambda_i B_i^{-1}$ and the result follows. If $\lambda_i = 0$, then $B_i^* B_i$ is the zero matrix. Check that this implies that $B_i = 0$ and so again the result follows.

(e) The matrix of f has the required property and hence so also does f.

Groups II

144)

(a) (i) For injectivity:

$$\varphi_g(x) = \varphi_g(y) \implies g{\cdot}x = g{\cdot}y \implies g^{-1}{\cdot}(g{\cdot}x) = g^{-1}{\cdot}(g{\cdot}y) \implies (g^{-1}g){\cdot}x = (g^{-1}g){\cdot}y \implies e{\cdot}x = e{\cdot}y \implies x = y$$

For surjectivity: given $y \in X$ let $x = g^{-1} \cdot x$. Then $\varphi_g(x) = g \cdot (g^{-1} \cdot y) = (gg^{-1}) \cdot y = e \cdot y = y$

(ii) Let $g, h \in G$. For all $x \in X$ we have

$$\varphi_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot \varphi_h(x) = \varphi_g(\varphi_h(x)) = \varphi_g \circ \varphi_h(x)$$

Since this holds for all $x \in X$, we have $\Phi(gh) = \varphi_{gh} = \varphi_g \circ \varphi_h = \Phi(g)\Phi(h)$

(b) Since Ψ is a homomorphism, $\Psi(e_G) = e_{S_X} = \mathrm{Id}_X$. Therefore, for all $x \in X$ we have

$$e_G \cdot x = \Psi(e_G)(x) = \mathrm{Id}_X(x) = x$$

Let $g, h \in G$. Then

$$(gh) \cdot x = \Psi(gh)(x) = \Psi(g)\Psi(h)(x) = \Psi(g)(h \cdot x) = g \cdot (h \cdot x)$$

146)

(a) Orbits: $\{1,2,3\}, \{4\}$; stabilisers, $\mathrm{Stab}(1) = \mathrm{Stab}(2) = \mathrm{Stab}(3) = \{e\}, \mathrm{Stab}(4) = G$

(b) Orbits: $\{1,2,3,4\}$; stabilisers, $\mathrm{Stab}(1) = \mathrm{Stab}(2) = \mathrm{Stab}(3) = \mathrm{Stab}(4) = \{e\}$

(c) Orbits: $\{1,2\}, \{3,4\}$; stabilisers, $\mathrm{Stab}(1) = \mathrm{Stab}(2) = \langle(34)\rangle, \mathrm{Stab}(3) = \mathrm{Stab}(4) = \langle(12)\rangle$

(d) Orbits: $\{1,2,3,4\}$; stabilisers, $\mathrm{Stab}(i)$ is the set of all permutations not involving i (which is isomorphic to S_3)

(e) Orbits: $\{1,2,3,4\}$; stabilisers, $\mathrm{Stab}(1) = \mathrm{Stab}(3) = \langle(24)\rangle, \mathrm{Stab}(2) = \mathrm{Stab}(4) = \langle(13)\rangle$. (It's convenient to think of $\{1,2,3,4\}$ as the vertices of a square.)

148) $\{U\}, \{-U\}, \{I, -I\}, \{J, -J\}, \{K, -K\}$

149)

(a) $(123), (132)$

(b) $(123), (132), (124), (142), (134), (143), (234), (243)$

(c) $(1234), (1243), (1324), (1342), (1423), (1432)$

(d) all 4-cycles

(e) all m-cycles

150) Suppose that $\sigma(i) = j$. Then

$$\tau\sigma\tau^{-1}\left(\tau(i)\right) = \tau\sigma(i) = \tau(j).$$

Thus if j follows i in the cycle decomposition of σ then $\tau(j)$ follows $\tau(i)$ in the cycle decomposition of $\tau\sigma\tau^{-1}$. With suitable adaptations for the elements preceding a right parenthesis, this gives the general answer.

151) Show that if $g = khk^{-1}$, then $C_G(g) = kC_G(h)k^{-1}$. In more detail,

$$x \in C_G(g) \iff xg = gx \iff xkhk^{-1} = khk^{-1}x \iff k^{-1}xkh = hk^{-1}xk \iff k^{-1}xk \in C_G(h)$$

152) This can be done by direct computation. We do the first one as an example. Suppose that a matrix

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

commutes with the matrix of part (a). Then we have

$$\begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix} \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 3 \end{bmatrix} \begin{bmatrix} a & b & c \\ d & e & f \\ g & h & i \end{bmatrix}$$

Thus

$$\begin{bmatrix} a & 2b & 3c \\ d & 2e & 3f \\ g & 2h & 3i \end{bmatrix} = \begin{bmatrix} a & b & c \\ 2d & 2e & 2f \\ 3g & 3h & 3i \end{bmatrix}$$

and so,comparing coefficients, we obtain $b = c = f = d = g = h = 0$; that is, the centraliser of the given matrix consists only of (invertible) diagonal matrices.

(a) $\{A \in GL(3, \mathbb{R}) \mid A$ is diagonal$\}$

(b) $\{A \in GL(3, \mathbb{R}) \mid \exists B \in GL(2, \mathbb{R})\, \exists C \in GL(1, \mathbb{R}),\ A = B \oplus C\}$

(c) $\{A \in GL(3, \mathbb{R}) \mid \exists a, b, e \in \mathbb{R}, A = \left[\begin{smallmatrix} a & b & 0 \\ 0 & a & 0 \\ 0 & 0 & e \end{smallmatrix}\right]\}$

(d) $\{A \in GL(3, \mathbb{R}) \mid \exists a, b, c, d, e \in \mathbb{R}, A = \left[\begin{smallmatrix} a & b & c \\ 0 & a & 0 \\ 0 & d & e \end{smallmatrix}\right]\}$

(e) $\{A \in GL(3, \mathbb{R}) \mid \exists a, b, c \in \mathbb{R}, A = \left[\begin{smallmatrix} a & b & c \\ 0 & a & b \\ 0 & 0 & a \end{smallmatrix}\right]\}$

153) The orbits are $\{1, 2, 7, 12\}, \{3, 6, 10\}, \{4, 8, 14\}, \{5, 9, 11, 13, 15\}$. The orbit-stabiliser relation implies that the order of the group is divisible by the size of the orbits. Thus $|G|$ is a multiple of 3 and 4 and 5 and so of 60.

154) Since G has order 5, each orbit has size 1 or 5. The size of X is the sum of the sizes of these orbits. So at least one orbit has size one; that is, some point of X is fixed by every element of G.

For the second part, consider $G = \langle (123)(45678) \rangle \leqslant S_8$ acting on $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$. There is no element of X fixed by every element of G (the orbits have size 5 and 3).

156) Choose h so that G/Z is generated by hZ. Then each element of G can be written in the form $h^i z$ for some $z \in Z$ and some $i \in \mathbb{Z}$.

157) Note that $\{e_G\}$ is always a conjugacy class. So if there is only one class, then G is the identity group.

If there are two classes $\{e_G\}$ and C, say, then $|G| = 1 + |C|$ and $|C|$ divides $|G|$ by the orbit-stabiliser relation. Therefore $|C| = 1$ and $|G| = 2$. Thus G is (isomorphic to) the cyclic group of order 2.

If there are three classes, $\{e_G\}$, C and D say with $|C| \leqslant |D|$, then $|G| = 1 + |C| + |D|$ and both $|C|$ and $|D|$ divide $|G|$. Show that the only solutions to this equation are $|C| = |D| = 1$ or $|C| = 1, |D| = 2$ or $|C| = 2, |D| = 3$. The first possibility corresponds to the cyclic group of order 3. The third possibility corresponds to S_3. The second possibility does not occur because if $|G| = 4$, then G is abelian and therefore the number of conjugacy classes if $|G| = 4$.

158) Use Cauchy's Theorem to show that the group has an element of order p and so a subgroup of order p. Since this subgroup has index $2p/p = 2$, it is normal.

159) Use the previous exercise to show that there is a normal subgroup of order p, generated by x say. By Cauchy's themorem there is an elment of order 2. Let y be an element of order 2. Since $\langle x \rangle$ is normal, $yxy^{-1} \in \langle x \rangle$. Show that $yxy^{-1} = x$ or $yxy^{-1} = x^{-1}$. Then show that the former case corresponds to the cyclic group of order $2p$ and the latter to D_p.

160)

$g \in D_8$	e	r, r^3, r^5, r^7	r^2, r^6	r^4	s, r^2s, r^4s, r^6s	rs, r^3s, r^5s, r^7s
$\lvert X^g \rvert$	70	0	2	6	6	6

There are $\frac{1}{16}(70 + 2 \times 2 + 6 + 4 \times 6 + 4 \times 6) = 8$ orbits.

161) Consider the homomorphism $\varphi : L \to K$ given by $\varphi(g) = \pi(g)$. Then $\operatorname{im}(\varphi) = K$ and $\ker(\varphi) = N$. By the first isomorphism theorem we have that $K \cong L/N$ and therefore, using Lagrange, $|L| = |K| \times |N| = p^{s-1}p$.

162) If $|G| = p^n$, then it follows from Lagrange's theorem that for all $g \in G$ $|g|$ divides p^n and is therefore a power of p.

For the converse, suppose that all elements of G have order that is a power of p. If G were not a p-group then there is a prime $q \in \mathbb{N}$ such that $q \mid |G|$ and $q \neq p$. But then by Cauchy's theorem (or the first Sylow theorem), there would be an element $g \in G$ of order q.

163)

(a) This follows from the fact that gHg^{-1} is a subgroup of G and has the same size as H.

(b) If H is the only Sylow p-subgroup, then from the previous part we have that $gHg^{-1} = H$ for all $g \in G$.

164) Let H be a Sylow q-subgroup of G. Then $|H| = p$. By the third Sylow theorem we have that $n_q \mid pq$ and $n_q \equiv 1 \pmod{q}$. The only divisors of pq are 1, p, q, and pq. Since $p < q$, $p \not\equiv 1 \pmod{q}$. Also, $pq \equiv q \equiv 0 \not\equiv 1 \pmod{q}$. The only possibility is therefore that $n_q = 1$.

165) This is very similar to the previous exercise. We have that $n_{17} \mid (3 \times 5 \times 17)$ and $n_{17} \equiv 1 \pmod{17}$. The divisors of 255 that are not divisible by 17 are: 1,3,5, and 15. Of these, the only value that is congruent to 1 modulo 17 is 1. Since $n_{17} = 1$, the Sylow 17-subgroup is normal (see Exercise 163).

Linear algebra revision

A.1) A typical element of $U+W$ has the form u_1+w_1 where $u_1 \in U$ and $w_1 \in W$. If α is a scalar, then $\alpha(u_1+w_1) = \alpha u_1 + \alpha w_1$. Since U and W are subspaces, $\alpha u_1 \in U$ and $\alpha w_1 \in W$. Hence $\alpha(u_1 + w_1) \in U + W$. We have shown that $U + W$ is closed under scalar multiplication. The argument that it is closed under addition is similar.

A.2) Use the definition of subspace, as in the previous question.

A.3) If neither U_1 nor U_2 is V, then neither can lie inside the other. Consider an element of V of the form $u_1 + u_2$ with $u_1 \in U_1$ but $u_1 \notin U_2$ and $u_2 \in U_2$ but $u_2 \notin U_1$. Does it lie in U_1 or in U_2?.

A.4)

(a) linearly independent, not a basis;

(b) linearly independent, not a basis;

(c) linearly dependent, not a basis.

A.5) (a) yes (b) yes (c) no

A.8) $\{1, X, X^2, X^3, \dots\}$ is an infinite linearly independent set in $F[X]$. In a finite dimensional vector space every linearly independent set is finite.

A.9) 9

A.10) Given $A_1, A_2 \in M_{2\times 2}$ and $\alpha \in \mathbb{R}$ we have

$$\begin{aligned} g(A_1 + A_2) &= (A_1 + A_2)B = A_1B + A_2B = g(A_1) + g(A_2) \\ g(\alpha A_1) &= (\alpha A_1)B = \alpha(A_1B) = \alpha g(A_1) \end{aligned}$$

(Notice that it doesn't matter what matrix B is.)

A.11) $\begin{bmatrix} 2 & 3 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 1 & -1 \end{bmatrix}$

A.12) The matrix is $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. The matrix with respect to the new basis is

$$\frac{1}{ad-bc} \begin{bmatrix} ad+bc & 2cd \\ -2ab & -(ad+bc) \end{bmatrix}$$

A.13) The nullity is 1; the rank is 2.

A.14) The nullity is 1; the rank is 2.

A.15) Briefly, f is surjective if and only if the range of f equals V if and only if the rank of f equals the dimension of V if and only if the nullity of f is zero.