# Solutions to odd-numbered exercises
# Peter J. Cameron, *Introduction to Algebra*, Chapter 7

7.1 Suppose that (GA1) and (GA2) hold. Then

$$\mu(\mu(x,g),g^{-1}) = \mu(x,gg^{-1}) = \mu(x,1) = x,$$

where the first equality uses (GA1) and the third uses (GA2); the middle inequality uses the group axiom (G3). The other part of (GA3) is proved similarly.

7.3 (a) First we show that an element of $HK$ has $|H \cap K|$ representations of the form $hk$ for $h \in H$ and $k \in K$. For if $x = hk = h'k'$, then $(h')^{-1}h = k'k^{-1} \in H \cap K$; and conversely, for any element $g \in H \cap K$, we have $hk = (hg^{-1})(gk)$, with $hg^{-1} \in H$ and $gk \in K$.

Now there are $|H| \cdot |K|$ pairs $(h,k)$ with $h \in H$ and $k \in K$. For any such pair, $hk \in HK$; and each element of $HK$ has $|H \cap K|$ such representations. So we have $|HK| = |H| \cdot |K|/|H \cap K|$.

(b) Let $X^{-1} = \{x^{-1} : x \in X\}$ for any subset $X$ of $G$. Suppose first that $HK$ is a subgroup. Then

$$HK = (HK)^{-1} = K^{-1}H^{-1} = KH.$$

Conversely, suppose that $HK = KH$. Since, as above, $(HK)^{-1} = KH$, we see that $HK$ is inverse-closed; so, using the First Subgroup Test, we have to show it is product-closed. So take $h_1k_1, h_2k_2 \in HK$. Then $k_1h_2 \in KH = HK$, so $k_1h_2 = hk$ for some $h \in H$ and $k \in K$. Then

$$(h_1k_1)(h_2k_2) = h_1(k_1h_2)k_2 = h_1(hk)k_2 = (h_1h)(kk_2) \in HK,$$

and we are done.

(c) The given equation shows that, for any $h \in H$ and $k \in K$, there exists $k' \in K$ such that $kh = hk'$. We apply the Second Subgroup Test to $HK$. Take $h_1k_1, h_2k_2 \in HK$. Choose $k' \in K$ such that $(k_1k_2^{-1})h_2^{-1} = h_2^{-1}k'$. Then

$$(h_1k_1)(h_2k_2)^{-1} = h_1(k_1k_2^{-1})h_2^{-1} = h_1h_2^{-1}k' \in HK,$$

and we are done.

7.5. For the conjugation action, the fixed point set of an element $g \in G$ is its centraliser $C_G(g)$, while the orbits are the conjugacy classes. So the Orbit-Counting Lemma says that the number of conjugacy classes is equal to

$$\frac{1}{|G|}\sum_{g \in G} |C_G(g)|.$$

To see this directly, note that the size of the conjugacy class containing $g$ is $|G|/|C_G(g)|$, so for any conjugacy class $\mathscr{C}$ we have

$$\frac{1}{|G|}\sum_{g \in \mathscr{C}} |C_G(g)| = 1,$$

from which the result follows. (This is just the proof of the Orbit-Counting Lemma in this special case.)

7.7 Take $g \in N_G(H)$, where $H = N_G(P)$. Then $g^{-1}Pg$ is a Sylow $p$-subgroup of $G$ (since it has the same order as $P$) and is contained in $H$ (since $g$ normalises $H$); so it is a Sylow $p$-subgroup of $H$. By Sylow's Theorem, $g^{-1}Pg$ is conjugate to $P$ in $H$; that is, there exists $h \in H$ such that $g^{-1}Pg = h^{-1}Ph$. This implies that $(gh^{-1})^{-1}P(gh^{-1}) = P$. So $k = gh^{-1}$ belongs to the normaliser of $P$, which of course is $H$. Now $g = kh$, and $k, h \in H$, so $g \in H$.

We conclude that $N_G(H) \leq H$. But trivially the reverse inequality holds; so $N_G(H) = H$, as required.

7.9 Let $p^a$ be the exact power of $p$ dividing the order of $G$. We show that a subgroup $P$ of order $p^i$ is contained in a Sylow $p$-subgroup by induction on $a - i$. (Note that $i \leq a$ by Lagrange's Theorem.)

If $a - i = 0$ then there is nothing to prove: $P$ is already a Sylow subgroup.

Suppose that $a - i > 0$ and that the result holds for subgroups of order $i'$ with $a - i' < a - i$, that is, $i' > i$. By Statement $B_i$ in the proof of Theorem 7.7, $P$ is contained (normally) in a subgroup of order $P^{i+1}$, which is contained in a Sylow $p$-subgroup by the induction hypothesis.

7.11 How does the Jordan–Hölder Theorem for finite groups need to be adapted? If we simply ask that any two composition series of finite length for a group have the same length and the same multiset of composition factors, then the proof for finite groups works without any modification. However, more is true: if $G$ has a composition series of finite length then any finite series of subgroups of $G$ with each normal in the next can be refined to a composition series of finite length.

To show this by induction on the length of a composition series, it is enough to show that any normal subgroup of $G$ is contained in a composition series of finite length. Let

$$G = G_0 \geq G_1 \geq \cdots \geq G_r = 1$$

be a composition series for $G$, and $H$ any normal subgroup of $G$. Then we have

$$G = HG_0 \geq HG_1 \geq \cdots HG_r = H.$$

Now $HG_i = (HG_{i+1})G_i$, so

$$HG_i/HG_{i+1} \cong G_i/HG_{i+1} \cap G_i$$

and the right-hand group is a quotient of $G_i/G_{i+1}$, hence is trivial or simple; so deleting repetitions, we have part of a composition series from $G$ to $H$. Similarly we have

$$H = G_0 \cap H \geq G_1 \cap H \geq \cdots \geq G_r \cap H = \{1\}.$$

Here $(G_i \cap H) \cap G_{i+1} = G_{i+1} \cap H$, so

$$(G_i \cap H)/(G_{i+1} \cap H) \cong (G_i \cap H)G_{i+1}/G_{i+1},$$

which is a normal subgroup of $G_i/G_{i+1}$, and again is trivial or simple; dropping repetitions we get the remainder of the composition series.

7.13 Recall two facts:

- the conjugate of $c$ by an element $g$ is obtained by replacing the entries in the cycles of $c$ by their images under $g$;
- two permutations in cycle form are equal if and only if they differ only in the orders of the factors and the chosen starting points of the cycles.

From the second assertion, it is clear that (writing the expression for $c$ with the cycle lengths in decreasing order, say) there are $f$ different expressions for $c$. By first assertion, for each such expression there is a unique element $g$ performing the required substitution; then $g^{-1}cg = c$, so $g$ belongs to the centraliser of $c$. Moreover, every element of the centraliser arises in this way. So $C_G(c)$ has order $f$, as required.

Now suppose that, for some cycle structure, we have $n!/f \leq 2(n-1)$. If there is some collection of cycle lengths such that the union of all cycles of these lengths has length $j$, then $n!/f \geq \binom{n}{j}$. [WHY?] If $1 < j < n-1$, then

$$\binom{n}{j} \geq \binom{n}{2} > 2(n-1) \text{ for } n > 5,$$

so we can assume that this is not the case. This leaves only the cases when $c$ is a product of cycles of the same length, or has a fixed point together with a product of cycles of the same length. In each of these cases the required inequality can be verified directly.

7.15 We show that any simple group of order 60 is isomorphic to $A_5$. Then the assertion follows. So let $G$ be a simple group of order 60. We will show that $G$ has a subgroup of index 5. Then $G$ acts on the cosets of this subgroup, so has a homomorphism to the symmetric group $S_5$. Since $G$ is simple, the kernel of this homomorphism is trivial, so that $G$ is isomorphic to a subgroup of $S_5$. This subgroup has index 2, and so is normal in $S_5$; as we saw in Proposition 3.30, it must be $A_5$.

The number of Sylow 5-subgroups of $G$ is congruent to 1 mod 5 and divides 12, but is not 1 (else the Slow 5-subgroup is normal in $G$, contrary to assumption). So there are 6 Sylow 5-subgroups of $G$. Since each is cyclic, they intersect pairwise in the identity, and contain between them 24 elements of order 5.

A similar argument shows that there are 10 Sylow 3-subgroups, containing 20 elements of order 3. Hence there are 15 elements of order other than 1, 3 or 5.

The number of Sylow 2-subgroups of $G$ is congruent to 1 mod 2 and divides 15, so must be 1, 3, 5 or 15. If it is 1, the Sylow 2-subgroup is normal, contrary to assumption. If 3, we have a homomorphism from $G$ to $S_3$ whose kernel is trivial, which is impossible since $G$ is larger than $S_3$. If the number if 5, the normaliser is a subgroup of index 5 and we are done. So we can assume that there are 15 Sylow 2-subgroups. Since there are only 15 non-identity elements which can lie in such subgroups, we can find subgroups $P, Q$ of order 4 such that $|P \cap Q| = 2$.

Now $N_G(P \cap Q)$ contains $P$ and $Q$ [WHY?], so has order greater than 4 but dividing 60. So $N_G(P \cap Q)$ has order 12, 20 or 60. As before, 20 and 60 are impossible, while 12 gives the required conclusion.

**Remark:** We have two cases in the above argument (viz., 5 or 15 Sylow 2-subgroups), both leading to the conclusion that $G$ is isomorphic to $A_5$. Since $A_5$ has five Sylow 2-subgroups, it turns out that in fact the second case is impossible.

7.17 If the action $\phi$ is trivial (so that $b\phi$ is the identity automorphism of $A$ for all $b \in B$), then the rule for composition in the semidirect product at the top of p.251 says

$$(b_1, a_1) \circ (b_2, a_2) = (b_1 b_2, b_1 a_2),$$

which is identical to the composition in $B \times A \cong A \times B$.

7.19 In the case $A = B = C_p$, for $p$ prime, the only possible homomorphism from $B$ to $\mathrm{Aut}(A)$ is the identity. We write both $A$ and $B$ as integers mod $p$, at slight risk of confusion. Then $f(0,b) = f(b,0) = 0$ and

$$f(b_1, b_2 + b_3) + f(b_2, b_3) = f(b_1 + b_2, b_3) + f(b_1, b_2).$$

We claim first that $f(1,b) = f(b,1)$ for all $b$. This holds for $b = 1$, and

$$f(1, b+1) + f(b,1) = f(b+1,1) + f(1,b)$$

(putting $b_1 = b_3 = 1$), so it holds for all $b$ by induction.

Next we claim that the values of $f(1,b)$ determine $f$. This is also proved by induction using

$$f(b_1, b_2 + 1) + f(b_2, 1) = f(b_1 + b_2, 1) + f(b_1, b_2).$$

Let $f$ be any factor set. Define a function $d$ on the integers mod $p$ by the rule that $d(0) = d(1) = 0$ and

$$d(b+1) = d(b) - f(1,b)$$

for $1 < b < p-2$. Then the corresponding inner derivation $f'$ given by $f'(b_1, b_2) = d(b_1) + d(b_2) - d(b_1 + b_2)$ agrees with $f$ at $(1,b)$ for $b = 0, \ldots, p-1$, Subtracting $f'$ from $f$, we see that any element of the extension group is represented by a factor set with $f(1,b) = 0$ for $b = 0, \ldots, p-2$. Hence there at most $p$ elements of $E(C_p, C_p)$, corresponding to the possible values of $f(1, p-1)$.

On the other hand, $E(C_p, C_p)$ is not the trivial group, since there exist non-isomorphic extensions; and it is a group of exponent $p$, by the argument in Schur's Theorem. So its order is $p$, as required.

7.21. Let $R$ be a unique factorisation domain, and suppose that the polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ satisfies the conditions of Theorem 7.27: that is,

- $f$ is primitive (this means that the gcd of its coefficients is 1, which is meaningful over a UFD);
- $p$ divides $a_0, \ldots, a_{n-1}$ but not $a_n$;
- $p^2$ does not divide $a_0$;

where $p$ is an irreducible. We observe that, if $p$ divides $ab$, then $p$ divides $a$ or $p$ divides $b$; for if not, then we have $ab = pc$, and if we factorise $a, b, c$ into irreducibles we see that $p$ occurs in the factorisation on the left but not in that on the right.

Suppose that $f$ is reducible, say $f = gh$, where

$$\begin{aligned} g(x) &= b_m x^m + \cdots + b_0, \\ h(x) &= c_{n-m} x^{n-m} + \cdots + c_0. \end{aligned}$$

Then $b_0 c_0 = a_0$; so one of $b_0$ and $c_0$ but not the other is divisible by $p$. Say $p \mid b_0$. For $1 \le i \le m$, we have

$$a_i = b_0 c_i + b_1 c_{i-1} + \cdots + b_{i-1} c_1 + b_i c_0.$$

Assuming inductively that $p$ divides $b_0, \ldots, b_{i-1}$, we conclude from this equation that $p$ divides $b_i c_0$, so that $p$ divides $b_i$.

The final conclusion is that $p \mid b_m$. But then $p \mid b_m c_{n-m} = a_n$, contrary to assumption.

7.23. (a) Let $J$ be the radical of $I$. We have first to show that $J$ is an ideal.

- Take $a, b \in J$, and suppose that $a^m, b^n \in I$. Then

$$(a+b)^{m+n-1} = \sum_{i=0}^{m+n-1} \binom{m+n-1}{i} a^i b^{m+n-1-i}.$$

  Now, for each $i$, either $i \le m$, or $i > m$, in which case $m+n-1-i \le n$. So each term in the binomial sum has a factor in $I$; since $I$ is an ideal, the whole term belongs to $I$, and hence so does the sum. So $(a+b) \in J$.

- Suppose that $a \in J$, with, say, $a^n \in I$, and take any $r \in R$. Then $(ra)^n = r^n a^n \in I$; so $ra \in J$.

So $J$ is indeed an ideal.

It is a radical ideal. For, suppose that $r \in R$ with $r^n \in J$. Then $r^{mn} \in I$ for some $m$, by definition of $J$; so $r \in J$.

(b) Suppose first that $f$ belongs to the radical of $\langle g_1, \ldots, g_m \rangle$. Then $f^n \in \langle g_1, \ldots, g_m \rangle$; so, if $x$ is a vector for which $g_1(x) = \cdots = g_m(x) = 0$, then $f(x) = 0$. So $f \in I(A(g_1, \ldots, g_m))$.

Conversely, suppose that $f \in I(A(g_1, \ldots, g_m))$. Then, if $x$ satisfies $g_1(x) = \cdots = g_m(x) = 0$, then $f(x) = 0$. According to the Nullstellensatz, $f^k \in \langle g_1, \ldots, g_m \rangle$ for some $k$; so $f$ belongs to the radical of this ideal.

7.25. Suppose that $f(x) = \sum a_n x^n$ and $g(x) = \sum b_n x^n$ are non-zero formal power series satisfying $f(x)g(x) = 0$. Let $i$ and $j$ be the smallest natural numbers such that $a_i \neq 0$ and $b_j \neq 0$. Then the coefficient of $x^{i+j}$ in $f(x)g(x)$ is $a_i b_j$ (all other terms in the sum are zero); this product is non-zero, a contradiction.

Now let $(a_n)$ and $(b_n)$ be non-zero $p$-adic integers whose product is zero. Let $i$ and $j$ be the smallest natural numbers such that $a_i$ is not zero mod $p^i$, and $b_j$ is not zero mod $p^j$. Now $a_{i+j}$ and $b_{i+j}$ are congruent to $a_i$ and $b_j$ respectively mod $p^{i+j-1}$; so $a_{i+j} b_{i+j}$ is not congruent to zero mod $p^{i+j}$, whence $ab \neq 0$, a contradiction.

7.27 For each natural number $a$, let $\overline{a}$ be the $p$-adic integer $(a_n)$, where $a_n \equiv a \bmod p^n$ for all $n$. (We can take $a_n = a$ when $p^n > a$.) It is easy to see that $a \mapsto \overline{a}$ is a one-to-one ring homomorphism.

7.29 This exercise is really just straightforward verification!

7.31 Suppose that $f(x)/g(x)$ is a $p$th root of $x$. Then $f(x)^p = xg(x)^p$ in $F[x]$. Now $F[x]$ is a unique factorisation domain, and the irreducible polynomial $x$ has multiplicity divisible by $p$ in $f(x)^p$, but congruent to 1 mod $p$ in $xg(x)^p$, a contradiction.

The polynomial $y^2 - x$ is irreducible over $F(x)$ since, if it were reducible, it would have a root in $F(x)$, that is, a square root of $x$, contradicting the first paragraph. But, if $\alpha$ is a root of this polynomial in an extension of $F(x)$, we have $(y-\alpha)^2 = y^2 - \alpha^2 = y^2 - x$ (since the characteristic is 2), so $\alpha$ has multiplicity 2 in its minimal polynomial over $F(x)$.

7.33 Since $x-1$ divides $x^q - 1$ (as polynomials) for any positive integer $q$, we see that $p^k - 1$ divides $p^{kq} - 1$. So, if $n = kq + r$, then

$$p^n - 1 = (p^n - p^r) + (p^r - 1) = p^r(p^{kq} - 1) + (p^r - 1) \equiv p^r - 1 \bmod p^k - 1.$$

So, applying Euclid's algorithm to $m$ and $n$, and simultaneously to $p^m - 1$ and $p^n - 1$, we see that it terminates at the same stage and yields the required result. [In the second calculation, every remainder has the form $p^r - 1$, where $r$ is the corresponding remainder in the first calculation.]

7.35 Some of these axioms speak of an identity element, which we regard as a nullary operation (an operation of arity zero). Some speak of inverses; we take the inverse to be a unary operation. With this convention, all the axioms are laws (universally quantified statements). For example, the inverse law for the abelian group with operation $\circ$ and identity 0 would not be written as

$$(\forall x)(\exists y)(x \circ y = 0)$$

but as

$$(\forall x)(x \circ x\iota = 0),$$

where $\iota$ is the inverse operation.

With these conventions, it is just a case of observing that all axioms are laws.

7.37 Let $a_1, \ldots, a_n \in A$; let $a_i$ have length $l_i$ (then the sum of the arities of the operation symbols in $a_i$ is $l_i - 1$. Then $a_1 \ldots a_n \mu$ has length $(\sum l_i) + 1$, and the sum of the arities of its operation symbols is $(\sum(l_i - 1)) + n$; so indeed this string has variability 1.

Any proper non-empty prefix of $a_1 \ldots a_n \mu$ has the form $a_1 \ldots a_i p$; its variability is the sum of those of $a_1, \ldots, a_n, p$, which is certainly positive.

So $a_1, \ldots, a_n \mu \in A$.

If $B$ is an algebra and we choose elements $b_i \in B$, define the map $\phi : A \to B$ by induction on the length of the string by

$$\begin{aligned} x_i\phi &= b_i, \\ (a_1 \ldots a_n \mu)\phi &= (a_1\phi)\ldots(a_n\phi)\mu, \end{aligned}$$

where on the right, the operation $\mu$ is applied in the algebra $B$. It is immediate that $\phi$ is uniquely defined and is a homomorphism. (We use the fact that elements of $A$ can be parsed uniquely, proved in the preceding question.)

7.41 (a) $[x,y] = 1$ means $x^{-1}y^{-1}xy = 1$, or $yx = xy$.

(b) Clear.

(c) If $N$ is a normal subgroup of $G$, then $[xN,yN] = [x,y]N$ (in $G/N$). If $G/N$ is abelian, then $[xN,yN] = N$, that is, $[x,y] \in N$. Clearly, if also $N$ is abelian, then any two commutators commute, so $G$ satisfies the stated law.

(d) For any $g \in G$, we have $[x^g,y^g] = [x,y]^g$, where $x^g$ is the conjugate $g^{-1}xg$. So the conjugate of a commutator is a commutator. Moreover, $[x,y]^{-1} = [y,x]$, so the inverse of a commutator is a commutator. So the subgroup $H$ (consisting of all products of commutators and their inverses) is fixed by conjugation, that is, is normal. Now, since all commutators belong to $H$, reversing the argument in (c) gives $[xH,yH] = [x,y]H = H$, so $G/H$ is abelian.

(e) If $G$ satisfies this law, then any two commutators commute. So any two products of commutators and their inverses commute, that is, the derived group $H$ is abelian, as required.

(f) Groups of derived length at mpst $d$ satisfy the law $c_d = 1$, where $c_d(x_1,\ldots,x_{2^d})$ is defined inductively by the rule that $c_0 = x_1$ and

$$c_d(x_1,\ldots,x_{2^d}) = [c_{d-1}(x_1,\ldots,x_{2^{d-1}}, c_{d-1}[x_{2^{d-1}+1},\ldots,x_{2^d}].$$

7.43 The question is slightly mis-stated: a Boolean ring should be defined as a ring *with identity* satisfying $x^2 = x$.

Let $X$ be a Boolean lattice, and define addition and multiplication by the rules given. We have to verify the ring axioms and the condition $x^2 = x$. The closure laws are clear.

First, observe that, for any elements $x,y$,

$$\begin{aligned}(x\vee y)\vee(x'\wedge y') &= (x\vee y\vee x')\wedge(x\vee y\vee y') = 1\wedge 1 = 1,\\ (x\vee y)\wedge(x'\wedge y') &= (x\wedge x'\wedge y')\vee(y\wedge x'\wedge y') = 0\vee 0 = 0;\end{aligned}$$

by the uniqueness of complement, $(x\vee y)' = x'\wedge y'$. Similarly, $(x\wedge y)' = x'\vee y'$. Thus,

$$x+y = (x\vee y)\wedge(x'\vee y').$$

Then we find after a short calculation that

$$(x+y)+z = (x\vee y\vee z)\wedge(x'\vee y'\vee z)\wedge(x'\vee y\vee z')\wedge(x\vee y'\vee z').$$

Similarly, $x+(y+z)$ works out to the same expression. So addition is associative. Clearly addition is also commutative.

We have

$$x+0 = (x\vee 0)\wedge(x'\vee 1) = x\wedge 1 = x,$$

and

$$x+x = (x\vee x)\wedge(x'\vee x') = x\wedge x' = 0.$$

So the identity and inverse laws hold for addition. Moreover,

$$x \cdot 1 = x \wedge 1 = x,$$

so 1 is the identity.

The associative law for multiplication is immediate from the corresponding lattice law. Furthermore, $x^2 = x \wedge x = x$. So we are done.

Conversely, let $R$ be a Boolean ring. We know that $R$ is commutative and satisfies $x + x = 0$. (For reference, here are the proofs. Consider

$$x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y.$$

By the cancellation law, $xy + yx = 0$ for any $x, y$. Putting $y = x$ gives $x + x = x^2 + x^2 = 0$. Now $xy + yx = 0 = xy + xy$, so $xy = yx$ by the cancellation law.)

Now defining $x \vee y = x + y + xy$ and $x \wedge y = xy$, we have to prove the lattice axioms, the distributive laws, and the existence of complements. All of this is straightforward. For example, the idempotent law for $\vee$:

$$x \vee x = x^2 + x + x = x,$$

using $x^2 = x$ and $x + x = 0$. The absorptive laws:

$$x \wedge (x \vee y) = x(x + y + xy) = x + xy + xy = x, \quad x \vee (x \wedge y) = x + xy + x^2 y = x.$$

The first distributive law:

$$x \wedge (y \vee z) = x(y + z + yz) = xy + xz + x^2 yz = xy \vee xz = (x \wedge y) \vee (x \wedge z).$$

The complement of $x$ is $1 + x$, since

$$x \vee (1 + x) = x + 1 + x + x + x^2 = 1, \quad x \wedge (1 + x) = x(1 + x) = x + x^2 = 0.$$

Now implicitly we have a bijective map between Boolean lattices and Boolean rings; this is the "map on objects" of the required isomorphism. Moreover, if $\theta : R \to S$ is a Boolean lattice homomorphism, then exactly the same map between the same sets with different operations is a Boolean ring homomorphism, and *vice versa*.

7.45 In a distributive lattice,

$$\begin{array}{rcll} x \vee (y \wedge (x \vee u)) & = & x \vee ((y \wedge x) \vee (y \wedge u)) & \text{(distributive law)} \\ & = & (x \vee (y \wedge x)) \vee (y \wedge u) & \text{(associative law)} \\ & = & x \vee (y \wedge u) & \text{(absorptive law)} \\ & = & (x \vee y) \wedge (x \vee u) & \text{(distributive law)}, \end{array}$$

so the modular law holds.

7.47 We begin by showing directly that the equivalence classes of a congruence $\equiv$ on a group $G$ are the cosets of a normal subgroup. Let $N$ be the equivalence class of the identity.

- If $a, b \in N$ then $a \equiv 1$ and $b \equiv 1$, so $ab \equiv 1$, or $ab \in N$.
- If $a \in N$, then $a \equiv 1$ and $a^{-1} \equiv a^{-1}$, so $1 \equiv a^{-1}$, and $a^{-1} \in N$.
- If $a \in N$ and $g$ is arbitrary, then $a \equiv 1$ and $g \equiv g$, so $ag \equiv a$ and $ga \equiv a$. Thus $ag \equiv ga$. Also, $g^{-1} \equiv g^{-1}$, so $g^{-1}ag \equiv a \equiv 1$, and $g^{-1}ag \in N$.

So indeed $N$ is a normal subgroup, and the equivalence classes are its cosets.

Thus, the congruence lattice is isomorphic to the lattice of normal subgroups. (Under this isomorphism, meet and join correspond to intersection and product.)

Now, if $X, Y, Z$ are normal subgroups with $X \leq Z$, then $X(Y \cap Z) \leq XY \cap Z$, since this holds in any lattice. Take $z \in XY \cap Z$. Then $z \in Z$; and $z = xy$ with $x \in X \leq Z$ and $y \in Y$; so $y \in Z$, and $z \in X(Y \cap Z)$. Thus, $X(Y \cap Z) = XY \cap Z$, and the lattice is modular.

7.49 We prove (b) first. Suppose that $f \in V_{\pi_1} \wedge V_{\pi_2}$. Then $f$ is constant on the parts of $\pi_1$, and also on the parts of $\pi_2$; hence by definition it is constant on the parts of $\pi_1 \vee \pi_2$. (For by definition, if $x, y$ lie in the same part of $\pi_1 \vee \pi_2$, then there is a chain from $x$ to $y$ where successive steps in the chain are alternately in the same part of $\pi_1$ or of $\pi_2$, and the value of $f$ does not change. Conversely, suppose that $f \in V_{\pi_1 \vee \pi_2}$. Then $f$ is constant on parts of $\pi_1$ and of $\pi_2$ (since these two partitions both refine $\pi_1 \vee \pi_2$); so $f \in V_{\pi_1} \wedge V_{\pi_2}$. So we have equality.

Now we prove (a). Suppose that $V_{\pi_1} = V_{\pi_2}$, and let $\pi_1 \vee \pi_2 = \pi_3$. By (b), $V_{\pi_1} = V_{\pi_3}$. Without loss of generality, $\pi_1 < \pi_3$; so $\pi_1$ strictly refines $\pi_3$, and there are two points $x, y$ in the same part of $\pi_3$ but not of $\pi_1$. Define

$$f(z) = \begin{cases} 1 & \text{if } z \text{ is in the same part of } \pi_1 \text{ as } x, \\ 0 & \text{otherwise.} \end{cases}.$$

Then $f \in V_{\pi_1}$ but $f \notin V_{\pi_3}$, a contradiction.

The map just defined turns out not to be an embedding of the dual of the partition lattice into the subspace lattice. For it to be so, we would require that

$$V_{\pi_1 \wedge \pi_2} = V_{\pi_1} \vee V_{\pi_2}.$$

To see that this is false, let $S = \{1,2,3,4\}$ and let $\pi_1 = \{\{1,2\},\{3,4\}\}$ and $\pi_2 = \{\{1,3\},\{2,4\}\}$. Then $\pi_1 \wedge \pi_2$ is the partition into singletons, so $V_{\pi_1 \wedge \pi_2}$ is the whole of $F^4$. But $V_{\pi_1}$ and $V_{\pi_2}$ have dimension 2 and intersect in the space of constant functions, so their sum has dimension 3.

In fact, there cannot be an isomorphism. The subspace lattice of a vector space satisfies the modular law by Theorem 7.55, while the dual partition lattice of a set of size at least 4 is not modular [Exercise!]

7.51. $\{0,1\}$ is a Boolean lattice, and Boolean lattices form a variety so are closed under Cartesian product (p.282). Alternatively, this is easily proved directly.

Conversely, a finite Boolean lattice is the lattice of subsets of a finite set $X$ (Exercise 7.44 or 7.53). Now take a family $(I_x : x \in X)$ of copies of $I = \{0,1\}$ indexed by $X$; there is an isomorphism $\theta$ between $\mathscr{P}(X)$ and $\prod_{x \in X} I_x$ given by $Y\theta = f_Y$, where $f_Y$ is the characteristic function of $Y$ (that is, $f_Y(x) = 1$ if $x \in Y$, $f_Y(x) = 0$ if $x \notin Y$).

7.53. (a) We have to show that an atom $a$ satisfies $a \leq x \wedge y$ if and only if $a \leq x$ and $a \leq y$. The forward implication is clear. Conversely, if $a$ is an atom satisfying $a \leq x$ and $a \leq y$, then $a \wedge x = a \wedge y = a$, whence $a \wedge (x \wedge y) = a$ by the associative law, so that $a \leq x \wedge y$ as required.

(b) We show first that a finite Boolean lattice $L$ is atomic. Take $x \in L$ and let $S(x)$ be the set of atoms below $x$. (By finiteness, $x \neq 0$ implies $S(x) \neq \emptyset$.) Let $x^*$ be the join of the atoms in $S(x)$. Clearly $x^* \leq x$. If equality does not hold, then $y = x \wedge (x^*)' \neq 0$. Let $a$ be an atom below $y$; then $a \leq x$, so $a \in S(x)$, so $a \leq x^*$, a contradiction.

We also claim that, if $A$ is the set of atoms, then $S(x') = A \setminus S(x)$. These sets are disjoint, since $x \wedge x' = 0$. Also $1 = x \vee x' = \bigvee(S(x) \cup S(x'))$, so $A = S(1) = S(x) \cup S(x')$. So the claim is proved.

Now, given $x$ and $y$, we have $x \vee y = (x' \wedge y')'$ by De Morgan's Law, so

$$S(x \vee y) = A \setminus S(x' \wedge y') = A \setminus (S(x') \cap S(y')) = A \setminus ((A \setminus S(x)) \cap (A \setminus S(y)) = S(x) \cup S(y).$$

Finally, the isomorphism from $L$ to $\mathscr{P}(A)$ required for the proof of Theorem 7.54 is simply $x \mapsto S(x)$.