Solutions to odd-numbered exercises
Peter J. Cameron, *Introduction to Algebra*, Chapter 8

8.1 This code is non-linear, so we have to look at the distances between all pairs of words.

The first three words are mutually at distance 6, as are the last three. Symmetry between the symbols $1,2,3$ shows that we need only consider the distances from the first three words to the fourth, which all turn out to be 4. So the minumum distance is 4.

8.3 (a) The code has dimension 2 over $\mathbb{Z}_3$ (since the generator matrix has rank 2), so there are $3^2 = 9$ codewords These are 0000, 1011, 2022, 0112, 1120, 2101, 0221, 1202, 2210.

(c) By inspection the minimum weight is 3: all non-zero words have weight 3.

(b) Since C is linear, its minimum distance is equal to its minimum weight (which is 3).

(d) The generator matrix is $G = (I \quad A)$, where $A = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$. By Theorem 8.8 on p.308, a check matrix is

$$H = (-A^\top \quad I) = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}.$$

(e) 12 is encoded as

$$(1 \quad 2)\begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix} = (1 \quad 2 \quad 0 \quad 2).$$

For decoding, we note that C has minimum weight 3 and so is 1-error-correcting. Now the syndrome of $(1 \quad 0 \quad 2 \quad 1)$ is

$$(1 \quad 0 \quad 2 \quad 1)\begin{pmatrix} 2 & 2 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}^\top = (1 \quad 0),$$

which is the transpose of the third column of H; so the error is 0010, and the transmitted word is 1011. This is the first row of G, so the message is 10. (We could simply observe that, since G is in standard form, the first two digits of the codeword are information digits.)

8.5 Let $n = 2m+1$. Then, by the symmetry of the binomial coefficients,

$$\sum_{i=0}^{m} \binom{n}{i} = \sum_{i=m+1}^{n} \binom{n}{i},$$

and hence

$$\sum_{i=0}^{m} \binom{n}{i} = 2^{n-1}.$$

The repetition code $C|$ has minimum weight n and so is m-error-correcting; the Hamming bound gives

$$|C| \leq 2^n \Big/ \left(\sum_{i=0}^{m} \binom{n}{i} \right) = 2.$$

Since $|C| = 2$, the bound is attained.

8.7 We note that, over $\mathbb{Z}_2$, $\mathrm{wt}(v)$ is congruent to $v \cdot v$ mod 2, where $\cdot$ is the standard inner product. Hence

$$\mathrm{wt}(v+w) \equiv_2 (v+w)\cdot(v+w) \equiv_2 v\cdot v + w\cdot w \equiv_2 \mathrm{wt}(v) + \mathrm{wt}(w).$$

So, if $\mathrm{wt}(v)$ and $\mathrm{wt}(w)$ are even, then also $\mathrm{wt}(v+w)$ is even. This shows that the set of words of even weight in C is closed under addition, and hence forms a linear subcode.

8.9 (a) See p.103.

(b) We claim that the minimum weight of C is 4. Clearly it cannot be larger, since the rows of the generator matrix all have weight 4. Could some non-zero linear combination of the rows have weight 3 or less? Let v be such a word, and i the number of non-zero elements among the first three coordinates of v.

If $i = 0$, then clearly $v = 0$, contrary to assumption.

If $i = 1$, then v is a multiple of a row of G; but then v has weight 4.

If $i = 2$, then v has at least two zero entries among the last three coordinates. Suppose for example, that $v = av_1 + bv_2$, where v_1 and v_2 are the first two rows of G. Then two of $a+b$, $a+b\omega$, $a+b\bar{\omega}$ are zero, which is impossible since this would imply that two of $1, \omega, \bar{\omega}$ are equal to $-b/a$ and hence to one another. A similar argument holds if $v = av_1 + cv_3$ or $v = bv_2 + cv_3$.

If $i = 3$, and $v = av_1 + bv_2 + cv_3$, then $(a,b,c)^\top$ is in the kernel of the matrix formed by the last three columns of G; but this matrix is a Vandermonde, and so is invertible (p.177), a contradiction.

The code C has dimension 3 and so contains 64 codewords. The Singleton bound (Theorem 8.3(b), p.302) shows that a code with length 6 and minimum distance 4 over an alphabet of size 4 has at most $4^{6-4+1} = 64$ codewords.

8.11 This code has the rows $(1, a^j, a^{2j}, \ldots)$ in its check matrix for $j = 1,2,3,4$. However, the rows for $j = 2$ and $j = 4$ can be omitted, by Proposition 8.16 (p.314). So the check matrix has 10 rows over $\mathbb{Z}_2$, and the dimension of the code is at least $31 - 10 = 21$.

In fact, the dimension is exactly 21. This is a bit harder and is left to you as a starred exercise.

8.13 Suppose that $\gcd(n, q-1) = 1$, where $n = (q^e - 1)/(q-1)$. The multiplicative group G of $\mathrm{GF}(q^e)$ is cyclic of order $q^e - 1$ (Theorem 7.44(b), p.274). Our assumption shows that G is a direct product $G = G_1 \times G_2$ of cyclic groups of orders $q-1$ and n. The cyclic group of order $q-1$ is the multiplicative group of $\mathrm{GF}(q)$. Now any element of $\mathrm{GF}(q^e)$ which fixes a 1-dimensional $\mathrm{GF}(q)$-subspace must belong to $\mathrm{GF}(q)$; so the stabiliser of a 1-dimensional subspace in the group G_2 is the identity.

Now the non-zero vectors in $\mathrm{GF}(q)^e$ can be identified with the non-zero elements of the field $\mathrm{GF}(q^e)$, and multiplication by an element of this field induces a linear map of the vector space, which permutes among themselves the 1-dimensional subspaces (the columns of the check matrix of the Hamming code). The subgroup G_2 then permutes these columns cyclically: the stabiliser of a column is the identity, and so the Orbit–Stabiliser theorem shows that the orbit length is n. Writing the columns in the order given by applying powers of a generator of G_2 shows that the code is cyclic.

8.15 (a) The polynomial x^3-2 is irreducible over $\mathbb{Q}$, by Eisenstein's criterion. So the order of the Galois group G is divisible by 3. Also, one root is real and the other two non-real, so complex conjugation is an automorphism of order 2. Thus $|G|$ is a multiple of 6, and so $G \cong S_3$. The splitting field is $\mathbb{Q}(\sqrt[3]{2}, \omega)$, where $\omega = (-1+\sqrt{3})/2$ is a primitive cube root of unity.

The subgroups of S_3 are $\{1\}$, three subgroups of order 2, the alternating group A_3 of order 3, and S_3. If symbols $1,2,3$ correspond to the roots a, $a\omega$, $a\omega^2$ respectively, where $a = \sqrt[3]{2}$, then the Galois correspondence is as follows:

- $\{1\}$ corresponds to $\mathbb{Q}(a,\omega)$;
- $\{1,(2,3)\}$ (the stabiliser of a) corresponds to $\mathbb{Q}(a)$;
- $\{1,(1,3)\}$ corresponds to $\mathbb{Q}(a\omega)$;
- $\{1,(1,2)\}$ corresponds to $\mathbb{Q}(a\omega^2)$;
- $A_3 = \{1,(1,2,3),(1,3,2)\}$ corresponds to $\mathbb{Q}(\omega)$;
- S_3 corresponds to $\mathbb{Q}$.

(b) Again the polynomial is irreducible. (By Gauss' Lemma, the only possible roots are ± 1.) Now let a be a root, so that $a^3+a^2-2a-1=0$. Let $b=a^2-2$. Then

$$\begin{aligned} b^3+b^2-2b-1 &= a^6-6a^4+12a^2-8+a^4-4a^2+4-2a^2+4-1 \\ &= a^6-5a^4+6a^2-1 \\ &= (a^3+a^2-2a-1)(a^3-a^2-2a+1) \\ &= 0, \end{aligned}$$

so b is also a root; and clearly $b \neq a$, else a satisfies a polynomial of degree 2. Similarly $c=b^2-2$ is a root different from a and b. So $\mathbb{Q}(a)$ contains all three roots, and is a splitting field; and the Galois group is cyclic of order 3.

Remark Where does this come from? If you put $a = w+w^{-1}$, then calculation shows that

$$0 = a^3+a^2-2a-1 = w^3+w^2+w+1+w^{-1}+w^{-2}+w^{-3}.$$

So w is a primitive cube root of unity, say $w = \mathrm{e}^{2\pi \mathrm{i}/7}$, and $a = 2\cos(2\pi/7)$. Then $b = 2\cos(4\pi/7) = a^2-2$.

8.17 Let G be a subgroup of S_5 containing $(1,2,3,4,5)$ and an arbitrary transposition. Since all the powers of $(1,2,3,4,5)$ except the identity are 5-cycles, and any two symbols occur consecutively in one such power, we may assume without loss of generality that the transposition is in fact $(1,2)$. Then transpositions of adjacent elements (mod 5) are conjugates of $(1,2)$ by powers of the 5-cycle. From these we can obtain transpositions of non-adjacent elements: for example,

$$(1,3) = (2,3)(1,2)(2,3).$$

So G contains all transpositions, and $G = S_5$.