Applied Algebra: Practice problems for the final exam.

The actual exam problems will be similar to the problems below. Make sure you understand how to solve all of them.

Number theory.

1. Find the greatest common divisor of 26, 91 and 14. Express it in the form $26x+91y+14z$ for some integers x, y and z.

2. Solve the system of simultaneous linear congruences:

$$1) \quad x \equiv 4 \pmod{24} \text{ and } x \equiv 7 \pmod{11};$$

$$2) \quad 3x \equiv 1 \pmod{5} \text{ and } 2x \equiv 6 \pmod{8};$$

$$3) \quad x \equiv \pmod{5}, \quad 2x \equiv 1 \pmod{7} \text{ and } x \equiv 3 \pmod{8}.$$

3. Does there exist an integer x such that $x \equiv 5 \pmod{15}$ and $x \equiv 3 \pmod{15}$. Explain why or why not.

4. Find the last two digits of the number $1 + 7^{162} + 5^{121} \cdot 3^{312}$.

Symmetric groups.

5. Write the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 7 & 2 & 8 & 4 & 11 & 3 & 9 & 5 & 1 & 6 & 10 \end{pmatrix}$$

1) as a product of disjoint cycles;
2) as a product of 3-cycles (not necessarily disjoint).

6. Is it possible to write the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 12 & 7 & 2 & 8 & 4 & 6 & 3 & 9 & 5 & 1 & 11 & 10 \end{pmatrix}$$

as a product of 3-cycles (not necessarily disjoint). Explain why or why not.

Group theory.

7. Let k be any integer. Show that $\varphi(k^3 - 1)$ is divisible by 3.

Hint: k is an element of order 3 in G_n (=the group of invertible congruence classes modulo n) for $n = k^3 - 1$.

8. Let G be the group G_{23}. Find $a \in G_{23}$ such that every element of G_{23} is a power of a: that is, show that G is a cyclic group by finding a generator for it. Similarly show that G_{26} is cyclic by finding a generator for it. Is every group of the form G_n cyclic?

9. Let g and x be elements of a group G. Show that for all positive integers k,

$$(g^{-1}xg)^k = g^{-1}x^k g.$$

10. Prove that for any elements a and b of a group G, we have $ab = ba$ if and only if $(ab)^{-1} = a^{-1}b^{-1}$.

11. Give an example of a group of order 8, that is not cyclic.

Error-correcting/detecting codes:

12. Let the code function $f : B^4 \to B^7$ be given by the generating matrix

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

1) Find the number of the codewords of f. Find the minimal distance between the codewords.

2) How many errors does f detect and how many errors does it correct?

3) Find the parity-check matrix of f. Use it to write down the two-column decoding table for f.

4) Use this table to correct the message

1100111 1011000 1010110 0011001 1101010 1111111 1010101.