Solutions of the exam problems

PROBLEM 1.

a) Define a permutation ρ by setting $\rho(i) = a_i$ for $1 \leq i \leq n$. Since $(a_1, \ldots, a_n)$ is a cycle, the a_i's are different, so ρ is indeed a permutation. From the formula given in the problem, it follows that

$$\rho(1, 2, \ldots, n)\rho^{-1} = (\rho(1), \ldots, \rho(n)) = (a_1, \ldots, a_n).$$

The number on the first place in a cycle can always be normalized to be 1, and the remaining $n-1$ places can be filled by any choice among the numbers $2, \ldots, n$ as long as they are different. Different choices give different permutations, and there are $(n-1)!$ choices.

b) The symmetric group S_n acts on it self by conjugation. The stabilizer of σ consists of permutations ρ such that $\rho\sigma\rho^{-1} = \sigma$, that is $\rho\sigma = \sigma\rho$. Hence the stabilizer equals $C(\sigma)$. By subproblem a), the orbit of σ consists of all n-cycles, hence has $(n-1)!$ elements. As the order of the group S_n is $n!$, the orbit-stabilizer formula gives

$$|C(\sigma)| = |S_n||S_n\sigma|^{-1} = n!/(n-1)! = n.$$

Clearly $\langle \sigma \rangle \subseteq C(\sigma)$, but as σ is an n-cycle, $|\langle \sigma \rangle| = n$ and therefore $\langle \sigma \rangle = C(\sigma)$.

✸

PROBLEM 2.

a) Disjoint transpositions commute, so the product of $(1, 5)$ and $(2, 4)$ has square equal to the identity. The number 3 does not appear in any of the two transpositions, hence is left fixed. By the formula given in problem one, or by a direct calculation, one finds

$$\tau\sigma\tau = (5, 4, 3, 2, 1) = \sigma^{-1}.$$

b) One has

$$\rho_1\rho_2\sigma\rho_2^{-1}\rho_1^{-1} = \rho_1\sigma^{\epsilon(\rho_2)}\rho_1^{-1} = (\rho_1\sigma\rho_1^{-1})^{\epsilon(\rho_2)} = \sigma^{\epsilon(\rho_2)\epsilon(\rho_1)}$$

and $\epsilon(\rho_2)\epsilon(\rho_1)$ lies in $\{\pm 1\}$ since each of the factors does. It follows that $\rho_1\rho_2 \in N$, and N is a subgroup.

Clearly $\sigma\sigma\sigma^{-1} = \sigma$, so $\sigma \in N$, and therefore the subgroup $\langle \sigma \rangle$ generated by σ is contained in N. One has $\rho\sigma\rho^{-1} = \sigma^{\epsilon(\rho)}$ which clearly is an element in $\langle \sigma \rangle$, and hence $\langle \sigma \rangle$ is normal.

c) One has

$$\sigma^{\epsilon(\rho_1\rho_2)} = \rho_1\rho_2\sigma\rho_2^{-1}\rho_1^{-1} = \rho_1\sigma^{\epsilon(\rho_2)}\rho_1^{-1} = (\rho_1\sigma\rho_1^{-1})^{\epsilon(\rho_2)} = \sigma^{\epsilon(\rho_1)\epsilon(\rho_2)}$$

Since $\epsilon(\rho)$ is ± 1 for any ρ and σ is of order five (which is relatively prime to two), it follows that $\epsilon(\rho_1\rho_2) = \epsilon(\rho_1)\epsilon(\rho_2)$, and ϵ is a group homomorphism. By subproblem a) it is surjective. Clearly the kernel of σ equals $C(\sigma)$, which by problem one equals $\langle \sigma \rangle$. It has order 5 and since $\{\pm 1\}$ has order 2, one finds that $|N| = 2 \cdot 5 = 10$.

✸

PROBLEM 3.

a) Since A and B are of relatively prime orders, one has $A \cap B = \{e\}$. Indeed, and $\alpha = |A|$ and $\beta = |B|$, one may write $1 = c\alpha + d\beta$ with $c, d \in \mathbb{Z}$. Hence if if $x \in A \cap B$, $x = (x^\alpha)^c(x^\beta)^d = e$ since $x^\alpha = x^\beta = e$. Since A and B are normal, it follows that they commute and that AB is a subgroup. It is abelian since A and B commute and both are abelian. The order of AB is equal to $|A||B|/|A \cap B| = |A||B|$.

b) Assume that $A = \langle\, a \,\rangle$ and that $B = \langle\, b \,\rangle$. Then ab generates AB, indeed if $(ab)^n = a^n b^n = e$, we see that $a^n = b^{-n} \in A \cap B = \{e\}$. Hence $\alpha | n$ and $\beta | n$, so $\alpha\beta | n$ since α and β are relatively prime. The order of ab is therefore $\alpha\beta = |AB|$.

c) The orders of the Sylow p-groups of G are 7, 11 and 13. They are all prime, so the Sylow groups are all cyclic. The number of Sylow p-groups must divide 1001 and be congruent 1 mod p. The congruence classes of the divisors of 1001 mod the actual primes p, are listed below. One sees that in all cases, that is for 7, 11 and 13, there is just one Sylow p-group. As the Sylow p-groups are conjugate, they must be normal. It follows by subproblem one, that G is abelian, and since all prime factors in $|G|$ occur with multiplicity one, G is cyclic.

$p = 7$	$p = 11$	$p = 13$
1	1	1
$11 \equiv 4 \mod 7$	7	7
$13 \equiv 5 \mod 7$	$13 \equiv 2 \mod 11$	$11 \equiv -2 \mod 13$
$11 \cdot 13 \equiv 6 \mod 7$	$7 \cdot 13 \equiv 3 \mod 11$	$7 \cdot 11 \equiv -1 \mod 13$

✸

PROBLEM 4.

a) One has $a^4 = i^2 = -1$. One has $((1 \pm i)^2 a^2) = \pm 2i \cdot i = \mp 2$.

b) Clearly $\pm a$ are roots of $x^4 + 1$, and since $i^4 = 1$, one sees that $\pm ia$ are roots as well. As K is not of characteristic 2, it holds that $-1 \neq 1$ and $i \neq \pm 1$, and the four are different. The factorization follows.

c) The polynomial $x^4 + 1$ has a root in K if and only if one of the $\pm a$ or $\pm ia$ is in K. But then, $i = a^2 \in K$.

By grouping the four linear factors two by two in the three different possible ways, one obtains the following possible factorizations of $x^4 + 1$ into two quadratic factors:

$$(x^2 - i)(x^2 + 1) =$$
$$(x^2 - \sqrt{-2}x - 1)(x^2 + \sqrt{-2}x - 1) =$$
$$(x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$

Hence x^4+1 factors in a product of two quadratic factors if an only if either i, $\sqrt{2}$ or $\sqrt{-2}$ lies in K.

d) In $\mathbb{Z}_5$, one has $2^2=-1$, so $i=2$. Hence $x^4+1=(x^2-2)(x^2+2)$. The two factors are irreducible, since 2 is not a square in $\mathbb{Z}_5$ (the squares are just ± 1).

In $\mathbb{Z}_7$ one has $3^2=2$. Hence $x^4+1=(x^2-3x+1)(x^2+3x+1)$. The two factors are irreducible, since their common discriminant equals 5 which is not a square (the squares are 1, 2 and 4).

