MAT2200 Eksamen 1. juni 2011

LØSNINGSFORSLAG

Problem 1

Let G be a group. If x and y are two elements in G, we let $[x, y] = xyx^{-1}y^{-1}$.
a) Show that if $N \subseteq G$ is a normal subgroup and $x \in N$ is an element, then $[x, y] \in N$ for every element $y \in G$.

SOLUTION: Since N is a normal subgroup and $x^{-1} \in N$ (because $x \in N$ and N is a subgroup), we know that $yx^{-1}y^{-1} \in N$ for all $y \in G$. Hence $[x, y] = x \cdot yx^{-1}y^{-1} \in N$.

b) If N_1 og N_2 are two normal subgroups of G with $N_1 \cap N_2 = \{e\}$, then every element in N_1 commutes with every element in N_2.

SOLUTION: Let $x \in N_1$ and $y \in N_2$. By a) we have $[x, y] \in N_1 \cap N_2$ since both N_1 and N_2 are normal subgroups. It follows that $[x, y] = e$ and therefore $xy = yx$.

Problem 2

a) Which abelian groups of order 99 are there (up to isomorphism)? And which of order 999?

SOLUTION: Any abelian group is isomorphic to a product $\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_r^{n_r}}$ where the p_i's are primes and the n_i's natural numbers. The order of the abelian group equals the product $p_1^{n_1} \cdot \cdots \cdot p_r^{n_r}$. The prime factorisation of 99 is $99 = 9 \cdot 11 = 3^2 \cdot 11$. The abelian groups of order 99 are therefore $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{11}$ and $\mathbb{Z}_9 \times \mathbb{Z}_{11}$. The prime factorisation of 999 is $999 = 37 \times 27 = 37 \times 3^3$. So the possible abelian groups of order 999 are $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_{37}$, $\mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_{37}$ and $\mathbb{Z}_{27} \times \mathbb{Z}_{37}$

b) If G is a finite group, and p a prime. What is ment by a Sylow p-subgroup of G? What can one say about the number of Sylow p-subgroups in G?

SOLUTION: If $|G| = p^e m$ where m does not have p as a factor, then a Sylow p-subgroup of G is a subgroup of order p^e. In other words, it is a subgroup which is a p-group of maximal possible order. If N denotes the number of Sylow p-subgroups, then $N \equiv 1 \mod p$ and N divides $|G|$.

c) Let G be a group of order 99. Show that all Sylow-subgroups of G are normal. Show that G is abelian.

SOLUTION: G has Sylow 3-subgroups and Sylow 11-subgroups. We know that the number of Sylow p-subgroups are congruent to 1 mod p and that it divides the order of the group. In the case $p = 3$ this gives that there is only one Sylow 3-subgroup since the number of such either is 1 or 11 (it divides 99 and has not 3 as a factor) and 11 is congruent to 2 mod 3 (which is not congruent to 1 mod 3). Similarily, there is also only one Sylow 11-subgroup since the number of such divides 9 and neither 3 or 9 are congruent to 1 mod 11. Finally, if a group has a unique Sylow p-subgroup, that subgroup is normal since a conjugate of a Sylow p-subgroup is a Sylow p-subgroup. If S_3 and S_{11} are the two Sylow-subgroups, they are both abelian since groups of order p and p^2 are known to be abelian when p is a prime. Their orders being relatively prime, the intersection of S_3 and S_{11} is reduced to $\{e\}$. Hence they commute. This gives an injective homorphism from the direct product $S_3 \times S_{11}$ to G which must be an isomorphism since $S_3 \times S_{11}$ and G have the same number of elements.

Problem 3

a) Let $\rho = e^{2\pi i/3}$ be a third root of unity. Find the minimal polynomial $\mathrm{Irr}(\rho, \mathbb{Q})$ of ρ over $\mathbb{Q}$. What is the degree $[\mathbb{Q}(\rho) : \mathbb{Q}]$?

SOLUTION: Vi know that $x^3 - 1 = (x-1)(x^2+x+1)$, hence ρ is a root of x^2+x+1. Since ρ is not in $\mathbb{Q}$, the polynomial $x^2 + x + 1$ does not factor as a product of two linaer polynomials in $\mathbb{Q}[x]$, hence it is irreducible, and $\mathrm{Irr}(\rho, \mathbb{Q}) = x^2 + x + 1$. The degree $[\mathbb{Q}(\rho) : \mathbb{Q}]$ being equal to the degree of $\mathrm{Irr}(\rho, \mathbb{Q})$, is two.

b) Show that $x^2 + x + 1$ is reducible over the field $\mathbb{Z}_{13}$ with 13 elements. (It may be usefull that $6^2 \equiv -3 \mod 13$).

SOLUTION: $3^2 + 3 + 1 = 13 = 0$ in $\mathbb{Z}_{13}$. Hence $x^2 + x + 1$ is not irreducibel.

c) Show that $x^2 + x + 2$ is irreducible in $\mathbb{Z}_5[x]$. Let $a = \bar{x}$ be the class of x in $\mathbb{Z}_5[x]/(x^2 + x + 2)$. The elements $1, a$ constitute a basis for $\mathbb{Z}_5[x]/(x^2 + x + 2)$ as a vector space over $\mathbb{Z}_5$. Express a^4 and $1/(a + 1)$ in that basis.

SOLUTION: We have that $a^2 = -(a+2)$. Hence we obtain by squaring $a^2 = (a+2)^2 = a^2 + 4a + 4 = -(a + 2) + 4a + 4 = 3a + 2$. (Alternative ways of writing this are $2(1 - a)$ and $3(a - 1)$). We have $a(a + 1) = -2$. Hence $(a + 1)^{-1} = -a/2 = 2a$ since $-1/2 = 2$ in $\mathbb{Z}_5$. $(2 \times 2 = 4 = -1)$.

Problem 4

Let A be a cyclic group with generator a and written multiplicatively.

a) Show that every subgroup of A is cyclic.

SOLUTION: Let $B \subseteq A$ be a subgroup, and let m be the minimal, natural number (*i.e.*, the minimal, positive integer) such that $a^m \in B$. Then a^m generates B. Indeed, assume $b \in B$. Since a generates A, we may write $b = a^k$. By dividing k by m we get $k = qm + r$ where the remainder r satisfies $0 \leq r < m$. Then $a^r = a^{k-qm} = a^k(a^m)^{-q} \in B$ since both a^k and a^m are in B. By the minimality of m it follows that $r = 0$ and hence $b = a^k = (a^m)^q$.

b) Let A be a cyclic group of even order $2m$ with generator a and written multiplicativily. Let $b \in A$. Show that there is an $x \in A$ with $x^2 = b$ if and only if $b^m = 1$.

SOLUTION: If $b = x^2$, then $b^m = x^{2m} = 1$ since A is of order $2m$. Assume that $b^m = 1$ and write $b = a^k$. We get $1 = b^m = a^{km}$. Hence $2m$ divides km, the order of a being $2m$. It follows that k is even, say $k = 2n$. Then $x = a^n$ will do.