MAT2200
Solutions of the problems for the exam June 5. 2013

Problem 1.

Let G be a finite group and let $\phi\colon G \to G$ be the mapping $x \mapsto x^n$ where n is a natural number.

a) Show that if G is abelian, then the mapping ϕ is a group homomorphism. Show that if $n = 2$, and ϕ is a group homomorphism, then G is abelian.

Solution Let x og y be elements in G. We have since G is abelian $\phi(x)\phi(y) = \mathrm{x}^n y^n = (xy)^n = \phi(xy)$. If $n = 2$ and ϕ is a homomorphism, we get $x^2y^2 = \phi(x)\phi(y) = \phi(xy) = xyxy$. Cancelling x from the left and y from the right, we get $xy = yx$.

b) Assume that G is cyclic and of even order, and let $n = 2$. Show that $\operatorname{Im}\phi$ is of index two. Show by giving an example, that the condition G be cyclic, is necessary.

Solution We appeal to the theorem that describes the subgroups of cyclic groups. It says that if $d|n$, then the subgroup $\langle\, \sigma^d \,\rangle$ is of order n/d, hence of index d. Use this for $H = \operatorname{Im}\phi = \langle\, \sigma^2 \,\rangle$ to see that the order of $\operatorname{Im}\phi$ is $n/2$, and thus its index is 2.

In the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ every non-trivial element is of order 2, so $\operatorname{Im}\phi = \{e\}$, and hence it is of index 4.

c) Assume that G is cyclic and of even order, and let $n = 6$. What is the index of $\operatorname{Im}\phi$?

Solution We have that $\operatorname{Im}\phi = \langle\, \sigma^6 \,\rangle$ in this case. If $|G|$ is divisible by 6, then $\langle\, \sigma^6 \,\rangle$ is of order $n/6$ by the theorem describing subgroups of cyclic groups, hence the index is 6. If 6 is not a factor in $|G|$, then 3 is not a factor since $|G|$ is even. Hence σ^3 is a generator for G, and $\operatorname{Im}\phi = \langle\, \sigma^6 \,\rangle = \langle\, \sigma^2 \,\rangle$ and the index is two.

Problem 2.

a) Let A be an integer and let $f(X)$ be the polynomial $f(X) = X^4 + AX + 1$. Show that $f(X)$ is irreducible in $\mathbb{Z}[X]$ if and only if $A \neq \pm 2$. Find a factorization of $f(X)$ into irreducible polynomials when $A = \pm 2$.

Solution We first examine the roots of $f(X)$. If α is an integral root of $f(X)$, then α divides the constant term 1, *i.e.,* $\alpha = \pm 1$. If $A = 2$ one checks that -1 is a root and if $A = -2$ one checks that 1 is a root. I all other cases, *i.e.,* if $A \neq \pm 2$, the polynomial $f(X)$ has no integral roots.

It follows that $f(X)$ is reducible when $A = \pm 2$. Polynomial division gives $X^4 + 2X + 1 = (X + 1)(x^3 - X^2 + X + 1)$ and $X^4 - 2X + 1 = (X - 1)(x^3 + X^2 + X - 1)$.

Assume now that $A \neq \pm 1$. Then $f(X)$ is without integral roots, and if it is reducible, it splits as the product of two quadratic polynomials which are monic and have coefficients in $\mathbb{Z}$:

$$X^4 + AX + 1 = (X^2 + aX + b)(X^2 + cX + d).$$

Equating coefficients, we obtain the following four relations

1. $bc = 1$
2. $ad + bc = A$
3. $b + d + ac = 0$
4. $a + c = 0$

The first gives $b = d = \pm 1$, and the fourth $c = -a$. Substituting this in the third, we find $a^2 = b + d = \pm 2$. This is impossible since $\sqrt{\pm 2}$ is not integral. Hence $f(X)$ is irreducible when $A \pm 2$.

b) Suppose that F a field where the equation $x^2 + 1 = 0$ does not have a solution, but where there is an element $a \in F$ such that $a^2 = -2$. Let $g(X) = X^4 + 1$. Show that $g(X)$ is reducible in the polynomial ring $F[X]$, and write $g(X)$ as a product of polynomials irreducible in $F[X]$.

SOLUTION Referring to the four relations above, we find the factorization

$$X^4 + 1 = (X^2 + aX - 1)(X^2 - aX - 1)$$

of $g(X)$ in $F[X]$. It remains to check that each of the two quadratic factors are irreducible. Their common discriminant equals $a^2 + 4$, and $a^2 + 4 = -2 + 4 = 2$. We claim that this is not a square in F: Since if $b^2 = 2$, then $(a/b)^2 = -2/2 = -1$, and by assumption our field F does not contain a square root of -1. Hence none of the two quadratic factors has roots in F, and therefore they are irreducible in $F[X]$.

c) Show that $X^4 + 1$ is not irreducible over $\mathbb{Z}_{11}$.

SOLUTION We compute the squares in $\mathbb{Z}_{11}$:

n	0	± 1	± 2	± 3	± 4	± 5
n^2	0	1	4	9	5	3

and since $-2 = 9$ i $\mathbb{Z}_{11}$, $g(X)$ is reducible after b). Indeed

$$X^4 + 1 = (X^2 + 3X - 1)(X^2 - 3X - 1).$$

PROBLEM 3. Assume that p is a prime such that $p+2$ is a prime as well. Let G be a group of order $p^2(p+2)$. Show that all the Sylow subgroups of G are abelian and normal.

SOLUTION We first treat the prime p. The number N of Sylow p-subgroups divides the order of G and is congruent one mod p. Hence there are two possibilities for N, either $N = 1$ or $N = p+2$. But $p+2 \equiv 2 \mod p$ and $2 \not\equiv 1 \mod p$ (this holds for all primes p). Thus there is only one Sylow p-subgroup, and it must be normal (any conjugate group is a Sylow p-subgroup).

The Sylow p-subgroup is of order p^2, and any group whose order is the square of a prime, is abelian.

Then we treat the Sylow $p+2$-subgroups, and we denote their number by N. There are three possibilities for N. Either $N = 1$, or $N = p$ or $N = p^2$. The case $N = p$ does not occure since $p \equiv -2 \mod (p+2)$, and $-2 \not\equiv 1 \mod p+2$ because $p+2 \geq 5$. Now $p^2 \equiv (-2)^2 = 4 \mod (p+2)$, and $4 \not\equiv 1 \mod p+2$ since $p+2 > 3$, so N is not equalt to p^2. It follows that there is only one Sylow $p+2$-subgroup in G, and it must be normal.

The Sylow $p+2$-subgroup is of prime order (namely $p+2$) and is therefore abelian.

PROBLEM 4.

Let S_6 denote the symmetric group on 6 letters.

a) Show that the cycles $\sigma = (1,2,3)$ and $\tau = (4,5,6)$ generate an abelian subgroup of order 9 of S_6 which is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$.

SOLUTION The two cycles σ and τ commute since they are disjoint. Hence $H = \langle \sigma \rangle \langle \tau \rangle$ is a subgroup. Since $\langle \sigma \rangle \cap \langle \tau \rangle = \{e\}$ (elements in $\langle \sigma \rangle$ have 4, 5 and 6 as fixed points, and those in $\langle \tau \rangle$ have the fixed points 1, 2 and 3), we know that $H \simeq \langle \sigma \rangle \times \langle \tau \rangle \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$.

b) Show that all the Sylow 3-subgroups of S_6 are isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$.

SOLUTION The order of S_6 is $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 = 5 \cdot 3^2 \cdot 2^4$. Hence the order of a Sylow 3-subgroup equals 9. It follows that the subgroup H from a) is a Sylow 3-subgroup, and it is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. Any other Sylow 3-subgroup is conjugate to H, in particular isomomorphic to H.

c) How many Sylow 3-subgroups are there in S_6? HINT: In how many ways can one write $\{1,2,3,4,5,6\}$ as a disjoint union of two subsets each having three elements?

SOLUTION One can pick a subset A of $\{1,2,3,4,5,6\}$ with three elements in $\binom{6}{3} = 20$ ways. Then the subset A and its complement A^c give a partition of $\{1,2,3,4,5,6\}$ into two sets with three elements. However, chosing A^c in stead of A gives the same partition, so the number of partions is 10. This gives ten different subgroups of the type discribed in a).

If S is any Sylow 3-subgroup, it is conjugate to H by say ρ. If $\rho(i) = a_i$, one finds $\rho(1,2,3)\rho^{-1} = (a_1, a_2, a_3)$ and $\rho(4,5,6)\rho^{-1} = (a_4, a_5, a_6)$, and S is of the type above.