Exam solutions GRK

Fredrik Meyer

May 23, 2016

Exercise 1 (Eksamen 2008, 1)**.**
1. Find three different abelian groups of order 8. Explain why all abelian groups of order 8 are isomorphic to one of these.
2. Find a non-abelian group of order 8.
3. How many subgroups of order 8 does S_4 have? How many of these are abelian?

♠

Solution 1.
1. All finite abelian groups are products of cyclic groups. If the order of the group is 8, then the order of each factor must be 2. Hence there are three possibilities: $\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, and these are all of them.

   Note that we used the theorem about finitely generated abelian groups in the first sentence.
2. Let D_4 be the group of symmetries of the square. It is generated by a rotation of order 4, together with a reflection through one of the diagonals. Explicitly, call these two generators for ρ and σ. They satisify the three relations $\rho^4 = e$, $\sigma^2 = e$, and $\sigma\rho\sigma = \rho^{-1}$. The last one implies that the $\rho\sigma \neq \sigma\rho$, hence the groups is not abelian.

   To see this more explicitly, make a paper square, and mark its corners with the letters $A - D$ on both sides of the paper. Then "compute" what the results of $\rho\sigma$ and $\sigma\rho$ are.
3. S_4 is the symmetric group on 4 letters, hence it has order 24. A subgroup of order 8 is a Sylow 2-subgroup.

   By the Sylow theorem, the number of Sylow 2-subgroups n_2 is divisible by 3 and satisfies $n_2 \equiv 1 \pmod 2$. Hence there are either 1 or 3 such subgroups.

I claim that there cannot be just 1. Here's why. Note that $D_4 \subset S_4$ as a subgroup. It is generated by the permutation $\rho = (1234)$ and $\sigma = (24)$. I claim that D_4 is *not* a normal subgroup of S_4.

Namely, let γ be the permutation (14). Then compute $\gamma^{-1}\rho\gamma$. It turns out to be equal to (1423), which is not in D_4 (it is not a symmetry of the square!). Hence D_4 is not a normal subgroup of S_4, but it is a Sylow 2-subgroup. Since it is not normal, there must be 3 such groups.

Note that all conjugate groups are isomorphic, hence there are no abelian subgroups of order 8.

♡

Exercise 2 (Eksamen 2008, 3)**.** Let $f(x) = x^4 - 2x^2 - 3$.

1. Find the splitting field E of $f(x)$ over $\mathbb{Q}$. What is $[E : \mathbb{Q}]$ and $\mathrm{Gal}(E/\mathbb{Q})$?
2. Find an element $\alpha \in E$ such that $E = \mathbb{Q}(\alpha)$. What is its minimal polynomial over $\mathbb{Q}$?

♠

Solution 2. 1. The splitting field of a polynomial is the smallest extension of $\mathbb{Q}$ that contains all the roots of $f(x)$. By putting $u = x^2$, we can use the abc-formula to find the roots. One fins that $f(x) = (x^2+1)(x^2-3)$. Hence the roots of $f(x)$ are $\pm i$ and $\pm\sqrt{3}$. Then clearly the splitting field must contain $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{3})$. The smallest field containing both is $\mathbb{Q}(i, \sqrt{3})$, which then must be the splitting field of $f(x)$.

Note that we have $[E : \mathbb{Q})] = [\mathbb{Q}(\sqrt{3})(i) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$. The second factor is 2, and since $i \notin \mathbb{Q}(\sqrt{3})$, the first factor is 2 as well. Hence the extension is of degree 4.

To find the Galois group, one looks at how the roots of $f(x)$ can be permuted. There are only two groups of order 4. Either they are $\mathbb{Z}_4$ or $\mathbb{Z}_2 \times \mathbb{Z}_2$. The Galois groups is generated by the permutations of $E/\mathbb{Q}$ sending $\sqrt{3}$ and i to its conjugates. These two permutations are independent (they commute), hence the group must be $\mathbb{Z}_2 \times \mathbb{Z}_2$.

2. By an educated guess, let $\alpha = \sqrt{3} + i$. Then clearly $\alpha \in E$. We have:

$$\begin{aligned} \alpha^2 &= 3 + 2i\sqrt{3} - 1 = 2 + 2i\sqrt{3} \\ &\Rightarrow (\alpha^2 - 2)^2 = -12. \end{aligned}$$

Multiplying out gives $\alpha^4 - 4\alpha^2 + 16 = 0$. Then let $g(x) = x^4 - 4x^2 + 16$. I claim that $g(x)$ is irreducible. It cannot have any linear factors, because its roots are $\pm\sqrt{3} \pm i$. What could potentially happen, is that $g(x) = h_1(x)h_2(x)$, for two quadratic polynomials h_1, h_2. Let $h_1(x) = x^2 + bx + c$ and $h_2(x) = x^2 + dx + e$. Then $h_1(x)h_2(x) = x^4 + (d+b)x^3 + (e + bd + c)x^2 + (be + cd)x + ce$. Then $b + d = 0$, så $d = -b$. Putting this into the equation $e + bd + c = 4$, we get $e+c = b^2-4 = (b-2)(b+2)$. But we also have that $ec = 16$. Hence (e, c) must be one of $(1, 16)$, $(2, 8)$ or $(4, 4)$. This gives us three possibilities: the first one gives $b^2 - 4 = 17$, the second one gives $b^2 - 4 = 10$, and the third one gives $b^2 - 4 = 8$. None of these equations have solutions, and we have reached a contradiction. Hence $g(x)$ is irreducible.

This means that α is an element contained in E of degree 4 over $\mathbb{Q}$. But E also had degree 4, so $E = \mathbb{Q}(\alpha)$.

♡

Exercise 3 (Eksamen 2010, 3)**.** Let $f(x) = x^3 - 3$ and $g(x) = x^4 - 2x^2 - 3$ be polynomials in $\mathbb{Q}[x]$.

1. Show that $f(x)$ is irreducible over $\mathbb{Q}$ and that $g(x)$ is reducible.

2. Find the splitting field of $g(x)$. Compute $[E : \mathbb{Q}]$ and find the Galois group.

3. Find the splitting field K of the family $\{f(x), g(x)\}$. Show that $[K : \mathbb{Q}] = 12$.

♠

Solution 3.

1. That $f(x)$ is irreducible follows for example by Eisenstein's criterium by setting $p = 3$. Another way to see this is the following: if $f(x)$ was reducible, it would have a linear factor. But none of the roots of $f(x)$ are integers, hence there can be no linear factor. The other polynomial was computed with in the previous exercise.

2. See the above.

3. K is the smallest field containing all the roots of $f(x)$ and $g(x)$. Hence it is equal to $\mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3}e^{2\pi i/3})$.

   Let $\zeta = e^{2\pi i/3}$. This is a solution of $z^3 - 1 = 0$, but this polynomial is reducible. The minimal polynomial of ζ is $x^2 + x + 1$, which have solutions $(-1 \pm \sqrt{-3})/2$. But these elements are already in E (since $\sqrt{3}$ and $\sqrt{-1}$ are)! Hence

$$K = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3}e^{2\pi i/3}) = \mathbb{Q}(i, \sqrt{3}, \sqrt[3]{3}).$$

I claim that this extension has degree 12. To see this, consider the tower of extensions

$$\begin{array}{c} K \\ | \\ \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) \\ | \\ \mathbb{Q}(\sqrt{3}) \\ | \\ \mathbb{Q} \end{array}$$

Then the order of K over $\mathbb{Q}$ is the product of the orders of each intermediate extension. The first extension has order 2, since $\sqrt{3} \notin \mathbb{Q}$. I claim that the second extension has order 3.

First we make the following observation. We have that

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2a,$$

but also

$$[\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}, \sqrt[3]{3}) : \mathbb{Q}(\sqrt[3]{3})][\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = 3b.$$

Hence the degree of the first two extensions must be divisible by 6, since 2 and 3 are coprime.

The element $\sqrt[3]{3}$ has order 3 over $\mathbb{Q}$. Hence its degree over $\mathbb{Q}(\sqrt{3})$ is either $1, 2$ or 3. It cannot be 1, because that would imply that $\sqrt[3]{3} \in \mathbb{Q}(\sqrt{3})$, which is not the case since its minimal polynomial is irreducible over $\mathbb{Q}$. If the degree were 2, that would imply that the degree of the first two extensions were 4, which is not divisible by 6! Hence the degree must be 3, so the degree of the first two extensions is 6.

Finally, since i is complex, and the two other generators are real, the last extension must be of degree 2. In total, the degree is $2 \times 3 \times 2 = 12$.
♡