

### Midterm Exam 2 - Solutions

1. (3 + 3 points)
- a) Give an example of a field extension which is normal but not separable. Explain why your example has the required property.
- b) Give an example of a field extension which is separable but not normal. Explain why your example has the required property.

Solution:

There are many examples.  $\mathbb{Z}_p(u, \alpha) : \mathbb{Z}_p(u)$  is one, where  $u$  is an indeterminate, and  $\alpha$  is a zero of  $t^p - u$ . This polynomial is irreducible over  $\mathbb{Z}_p(u)$  as we have seen in class, and equal to  $(t - \alpha)^p$  over the larger field. So it has multiple zeros, which means that  $\alpha$  is inseparable over  $\mathbb{Z}_p(u)$ , and the field extension is inseparable. On the other hand, the extension is the splitting field extension of  $t^p - u$ , so it is normal.

$\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$  is separable since all extensions in characteristic 0 are separable, and not normal since the polynomial  $t^3 - 2$  is irreducible over  $\mathbb{Q}$ , has a zero in the larger field but does not split.

2. (3 + 5 points)
- a) Let  $G$  be a group of order  $(35)^3$ . Show that it has a normal subgroup of order 125.
- b) Let  $p, q$  be two prime numbers. Show that all groups of order  $p^2q$  are soluble. Consider the cases  $p > q$ ,  $p = q$  and (extra credit since this is more difficult)  $p < q$ .

Solution:

By the Sylow theorems  $G$  has a Sylow 5-subgroup of order  $5^3 = 125$ . The number of these is congruent to 1 modulo 5 and divides  $7^3$ , which has the divisors 1, 7,  $7^2$ ,  $7^3$ . The only possibility is exactly one subgroup of order 125, hence a normal subgroup of order 125.

If  $p > q$ , then a similar application of the Sylow theorems shows that  $G$  has a normal subgroup  $H$  of order  $p^2$ . Then  $1 \leq H \leq G$  is a series as required: the inclusions are inclusions of normal subgroups,  $G/H$  has order  $q$ , so is cyclic and abelian, and  $H/1$  has order  $p^2$ , so it is abelian by a homework problem.

If  $p = q$ , then  $G$  has order  $p^3$ , it is a finite  $p$ -group, which by a theorem from the lecture is soluble.

If  $p < q$ , then by the Sylow theorems the number of subgroups of order  $p^2$  divides  $q$  and is congruent to 1 modulo  $p$ , and the number of subgroups of order  $q$  divides  $p^2$  and is congruent to 1 modulo  $q$ . We are done with a similar reasoning as in the first case if there is a single subgroup of order  $p^2$  or a single subgroup of order  $q$ . What are the other possibilities? The only other divisor of  $q$  is  $q$ , so  $G$  must have  $q$  subgroups of order  $p^2$ , and  $q$  is congruent to 1 modulo  $p$ . The only other divisors of  $p^2$  are  $p$  or  $p^2$ .  $G$  can't have  $p$  subgroups of order  $q$ , since if  $p$  is congruent to 1 modulo  $q$ , we must have  $p > q$ . So we must have that  $p^2$  congruent to 1 modulo  $q$ , which implies that  $p$  is congruent to  $\pm 1$  modulo  $q$ . We have seen that only  $p$  congruent  $-1$  modulo  $q$  could be possible. Since  $p < q$ , we must have  $p = q - 1$ , so  $p = 2, q = 3$  and  $|G| = 12$  with 4 subgroups of order 3 and 3 subgroups of order 4. But looking at the orders of the elements one sees that this would give too many elements.

**3.** (5 + 4 + 4 points) Let  $f = (t^2 - 2)(t^3 - 2) \in \mathbb{Q}[t]$ . Let  $\Sigma$  be the splitting field of  $f$  over  $\mathbb{Q}$ .

- a) Find the Galois group  $\Gamma(\Sigma : \mathbb{Q})$ .
- b) Find all intermediate fields of degree 4 over  $\mathbb{Q}$ . For which of these is the extension  $M : \mathbb{Q}$  finite, normal and separable? Find the Galois groups of these extensions.
- c) Find all intermediate fields  $M$  of degree 3 over  $\mathbb{Q}$ . For which of these is the extension  $\Sigma : M$  finite, normal and separable? Find the Galois groups of these extensions.

Solution:

$\Sigma = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \zeta_3)$  has degree 12 over  $\mathbb{Q}$ , as one sees by the tower law. So  $\Gamma$  has order 12. An element  $\gamma \in \Gamma$  permutes  $\pm\sqrt{2}$ , and permutes the three zeros of  $t^3 - 2$ . Since one knows the element if one knows the values on all zeros of  $f$ , and the above gives exactly 12 possibilities, we get a group isomorphic to  $S_2 \times S_3 \cong \mathbb{Z}_2 \times S_3$ .

Intermediate fields of degree 4 over  $\mathbb{Q}$  correspond by the fundamental theorem of Galois theory to subgroups of  $\Gamma$  of index 4, i.e. of order 3. So we should look for elements of order 3. We get exactly one subgroup of order 3, generated by a 3-cycle in the  $S_3$ -part. This fixes  $\sqrt{2}$  and  $\zeta_3$ . So  $\mathbb{Q}(\sqrt{2}, \zeta_3)$  is the unique intermediate field of degree 4 over  $\mathbb{Q}$ . Since this unique subgroup of order 3 must be normal, the field extension  $\mathbb{Q}(\sqrt{2}, \zeta_3) : \mathbb{Q}$  is finite normal and separable, again e.g. by the fundamental theorem. The Galois group is the quotient group of  $\Gamma$  by the subgroup of order 3; it is isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

Intermediate fields of degree 3 over  $\mathbb{Q}$  correspond to subgroups of order 4. One easily finds 3 subgroups of order 4 given by  $\mathbb{Z}_2 \times H_i \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ , where  $H_i$  is generated by one of the three transpositions of  $S_3$ . By the Sylow theorems, there are exactly 3 subgroups of order 4. The subgroups correspond to the fixed fields  $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\zeta_3 \sqrt[3]{2}), \mathbb{Q}(\zeta_3^2 \sqrt[3]{2})$ . By the fundamental theorem, all these extensions  $\Sigma : M$  are finite, normal and separable, and have Galois group isomorphic to the corresponding subgroup, so isomorphic to  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .

4.

(4 + 2 points)

- a) Let  $f \in \mathbb{Q}[t]$  be an irreducible polynomial which over  $\mathbb{C}$  has both real and non-real roots. Show that the Galois group of  $f$  is non-abelian.
- b) Does this still hold true if  $f$  is not irreducible?

Solution:

Let  $a$  be a real root of  $f$  and  $b$  be a non-real root of  $f$ . Then  $\bar{b}$  is another root of  $f$ , and the splitting field of  $f$  is closed under complex conjugation, which makes the restriction of the complex conjugation an element  $\gamma_1$  of  $\Gamma$  such that  $\gamma_1(a) = a$  and  $\gamma_1(b) = \bar{b}$ . Since  $f$  is irreducible,  $\Gamma$  acts transitively on the set of roots, so there is an element  $\gamma_2$  of  $\Gamma$  such that  $\gamma_2(a) = b$ . Then  $\gamma_1\gamma_2(a) = \bar{b}$ , and  $\gamma_2\gamma_1(a) = b$ , so  $\gamma_1\gamma_2 \neq \gamma_2\gamma_1$  and  $\Gamma$  is non-abelian. If  $f$  is not irreducible, the Galois group can be abelian. The Galois group of  $(t^2 - 2)(t^2 + 1)$  is for example  $\mathbb{Z}_2 \times \mathbb{Z}_2$ , or the Galois group of  $(t - 1)(t^2 + 1)$  is  $\mathbb{Z}_2$ .