

Homework 5

Proofs and explanations should always be written using complete English sentences. You should always explain and justify each of the steps in your solution, unless otherwise noted. Write your name and "Math 114" on the top right of the first page.

1. Stewart, exercise 7.4.

Solution:

The extension $P \subseteq K$ is (isomorphic to) $\mathbb{Z}_2 \subseteq \mathbb{Z}_2(\alpha)$, where α has minimal polynomial $t^2 + t + 1$. Also $\beta = \alpha + 1$ has minimal polynomial $t^2 + t + 1$. So there are exactly two P -automorphisms of K : the identity and there is one which maps α to β (and β to α). So $\Gamma(K : P) \cong \mathbb{Z}_2$. The intermediate fields are exactly K and P : since the dimension of K over P is prime, there cannot be other intermediate fields. The identity map fixes K , and K is only fixed by the identity map. Both P -automorphisms fix P , and no other elements are fixed by both P -automorphism. So the Galois correspondence is a bijection.

2. Stewart, exercise 7.5.

Solution:

Let $p \in K[t]$ such that $p(\alpha) = 0$. By the homomorphism property, applied to γ in the Galois group, it follows that $p(\gamma(\alpha)) = 0$. If you apply the homomorphism property to γ^{-1} you see that on the other hand $p(\gamma(\alpha)) = 0$ implies $p(\alpha) = 0$. Thus it follows that α is a zero of a polynomial in $K[t]$ if and only if $\gamma(\alpha)$ is a zero. Hence the minimal polynomials are the same. So γ restricts to a map from the zeros of the minimal polynomial of α to the zeros of the minimal polynomial of α . But since γ is bijective, so is the restriction. So we get a permutation of the zeros of the minimal polynomial of α .

3. Stewart, exercise 7.7.

Solution:

a) True b) True c) False, see e.g. the example on p. 75 of Stewart. d) True, it is cyclic of order 2. e) False, see Ex. 2 on page 73 f) False, they reverse inclusions. g) False, see Ex. 2 on page 73 h) True i) False, sending e.g. t to $t + 1$ will define another one. j) True.

4. Stewart, exercise 8.1.

Solution:

see Stewart, p.192

5. Stewart, exercise 8.3 and 8.4.

Solution:

$t^3 + 2t + 1$ is irreducible over \mathbb{Z}_3 . So in a first step, we take the field extension

$$\mathbb{Z}_3 \rightarrow \mathbb{Z}_3[t]/\langle t^3 + 2t + 1 \rangle,$$

i.e. $\mathbb{Z}_3 \subseteq \mathbb{Z}_3(\alpha)$, where α has minimal polynomial $t^3 + 2t + 1$ over \mathbb{Z}_3 . Then we divide (in $\mathbb{Z}_3(\alpha)[t]$) the polynomial $t^3 + 2t + 1$ by $t - \alpha$. We get $t^2 + \alpha t + (\alpha^2 + 2)$. We have to check again whether this polynomial is irreducible: it is not. We find that $t^2 + \alpha t + (\alpha^2 + 2) = (t - (\alpha + 1))(t - (\alpha - 1))$. So $t^3 + 2t + 1 = (t - \alpha)(t - (\alpha + 1))(t - (\alpha - 1))$ in $\mathbb{Z}_3(\alpha)[t]$, and $\mathbb{Z}_3(\alpha)$ is a splitting field for $t^3 + 2t + 1$.

$t^3 + t^2 + t + 2$ is irreducible over \mathbb{Z}_3 . So in a first step, we take the field extension

$$\mathbb{Z}_3 \rightarrow \mathbb{Z}_3[t]/\langle t^3 + t^2 + t + 2 \rangle,$$

i.e. $\mathbb{Z}_3 \subseteq \mathbb{Z}_3(\beta)$, where β has minimal polynomial $t^3 + t^2 + t + 2$ over \mathbb{Z}_3 . Then we divide (in $\mathbb{Z}_3(\beta)[t]$) the polynomial $t^3 + t^2 + t + 2$ by $t - \beta$. We get $t^2 + (\beta + 1)t + (\beta^2 + \beta + 1)$. We have to check again whether this polynomial is irreducible: it is not. We find that $t^2 + (\beta + 1)t + (\beta^2 + \beta + 1) = (t - (\beta^2 + 1))(t - (-\beta^2 - \beta + 1))$. So $t^3 + t^2 + t + 2 = (t - \beta)(t - (\beta^2 + 1))(t - (-\beta^2 - \beta + 1))$ in $\mathbb{Z}_3(\beta)[t]$, and $\mathbb{Z}_3(\beta)$ is a splitting field for $t^3 + t^2 + t + 2$.

Now both fields have degree 3 over \mathbb{Z}_3 , i.e. 27 elements, and maybe you remember having heard somewhere that finite fields with the same number of elements are isomorphic. A trick is to show that both fields are splitting fields for $t^{26} - 1$ over \mathbb{Z}_3 : Since the multiplicative group of non-zero elements of each of the fields $\mathbb{Z}_3(\alpha)$, $\mathbb{Z}_3(\beta)$ has 26 elements, we get that each non-zero element's 26-th power is 1. So in both cases $t^{26} - 1$ decomposes as a product of 26 linear factors, and it is also clear that there is no subfield over which the polynomial splits. But since splitting fields are "unique", we get an isomorphism of field extensions from $\mathbb{Z}_3 \subseteq \mathbb{Z}_3(\alpha)$ to $\mathbb{Z}_3 \subseteq \mathbb{Z}_3(\beta)$ by Theorem 8.3 of Stewart.