MATH 7211 Homework 6

Andrea Bourque

May 9, 2023

1 Problem 14.2 From Lecture Notes

Show that a field extension E/F is normal iff for any extension K/E and any $\sigma \in \mathrm{Aut}(K/F)$, we have $\sigma(E) \subseteq E$.

Proof. ($\rightarrow$) Let $\alpha \in E$. Then the irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ has a root in E, and thus it splits in E, by definition of normality. But given $\sigma \in \mathrm{Aut}(K/F)$, we know that $\sigma(\alpha)$ is a root of $m_{\alpha,F}(x)$, since the polynomial's coefficients are fixed by α. Since E contains all the roots of $m_{\alpha,F}(x)$, and $\sigma(\alpha)$ is a root, we must have $\sigma(\alpha) \in E$. Since α is an arbitrary element of E, we must have $\sigma(E) \subseteq E$.

($\leftarrow$) Let $p(x) \in F[x]$ be irreducible with a root $\alpha \in E$. Considering $p(x)$ as an element of $E[x]$, let $K \supseteq E$ be the splitting field of $p(x)$ over E. In particular, K is also a splitting field of $p(x)$ over F; we have just chosen it to contain E. Now, E clearly contains $F(\alpha)$. For any other root $\beta \in K$ of $p(x)$, the proof of Theorem 27 in Chapter 13 of Dummit and Foote shows that there is an automorphism σ of K/F which maps α to β. Since $\alpha \in E$ and $\sigma(E) \subseteq E$, we have $\beta \in E$. Since β is an arbitrary root of $p(x)$, it follows that E contains all roots of $p(x)$, meaning that E/F is normal. $\square$

2 Problem 14.3 From Lecture Notes

Let K/F be a field extension, let H be a subgroup of $G := \mathrm{Aut}(K/F)$, let $E = K^H$ (or $\mathrm{Inv}(H)$), and let $\sigma \in G$. Show that $K^{\sigma H \sigma^{-1}} = \sigma(E)$.

Proof. Let $\tau \in H$ and let $x \in E$. We have $(\sigma\tau\sigma^{-1})(\sigma(x)) = \sigma(\tau(x))$. Since $E = K^H$ and $\tau \in H$, we have $\tau(x) = x$. Thus $(\sigma\tau\sigma^{-1})(\sigma(x)) = \sigma(x)$, so $\sigma\tau\sigma^{-1}$ fixes $\sigma(x)$. Since τ and x are arbitrary, $\sigma H \sigma^{-1}$ fixes $\sigma(E)$, so $\sigma(E) \subseteq K^{\sigma H \sigma^{-1}}$.

Conversely, let $x \in K^{\sigma H \sigma^{-1}}$ and let $\tau \in H$. Then $x = (\sigma\tau\sigma^{-1})(x)$, so $\sigma^{-1}(x) = \tau(\sigma^{-1}(x))$. Thus $\sigma^{-1}(x)$ is fixed by τ. Since τ is arbitrary, $\sigma^{-1}(x)$ is fixed by H. In particular, $\sigma^{-1}(x) \in K^H = E$. Then $x \in \sigma(E)$. Since x is arbitrary, $K^{\sigma H \sigma^{-1}} \subseteq \sigma(E)$ as desired. $\square$

3 Problem 14.3.5

Exhibit an explicit isomorphism between the splitting fields F_1, F_2 of $x^3 - x + 1$ and $x^3 - x - 1$ over $\mathbb{F}_3$.

Proof. As is noted in my solution of Problem 14.3.8, the splitting field of these polynomials is given by adjoining a single root; i.e. they are isomorphic to $\mathbb{F}_3[x]/(x^3 - x + 1)$ and $\mathbb{F}_3[x]/(x^3 - x - 1)$ respectively. Recall that for a ring R and ideals I, J, a homomorphism $R \to R$ which restricts to a function $I \to J$ determines a unique ring homomorphism $R/I \to R/J$ "compatible" (there is a commuting square) with the quotient maps $R \to R/I$ and $R \to R/J$. Therefore, it suffices to give an automorphism of $\mathbb{F}_3[x]$ which restricts to a bijection of ideals $(x^3 - x + 1) \to (x^3 - x - 1)$. For this, we give the map $x \mapsto -x$. This is certainly an automorphism of $\mathbb{F}_3[x]$ (it is its own inverse), and $x^3 - x + 1 \mapsto -x^3 + x + 1 = -(x^3 - x - 1)$, so the ideal $(x^3 - x + 1)$ is mapped bijectively to the ideal $(x^3 - x - 1)$. Thus we have an isomorphism $\mathbb{F}_3[x]/(x^3 - x + 1) \to \mathbb{F}_3[x]/(x^3 - x - 1)$ defined by sending $x + (x^3 - x + 1)$ to $-x + (x^3 - x - 1)$. $\square$

4 Problem 14.3.8

Determine the splitting field of $x^p - x - a$ over $\mathbb{F}_p$, where $a \neq 0$ is an element of $\mathbb{F}_p$. Show explicitly that the Galois group of the extension is cyclic.

Proof. Let $f(x) = x^p - x - a$. For any $b \in \mathbb{F}_p$, we have $f(b) = b^p - b - a = -a \neq 0$, since elements of $\mathbb{F}_p$ satisfy $x^p = x$. Thus $f(x)$ has no linear factors in $\mathbb{F}_p[x]$. If α, β are two roots of $f(x)$ in a splitting field, then

$$\begin{aligned}(\alpha - \beta)^p - (\alpha - \beta) \\ = (\alpha^p - \alpha) - (\beta^p - \beta) \\ = (\alpha^p - \alpha - a) - (\beta^p - \beta - a) = f(\alpha) - f(\beta) = 0.\end{aligned}$$

We know that the roots of $x^p - x$ in $\mathbb{F}_p$ are exactly the elements of $\mathbb{F}_p$, so this shows that two roots of $f(x)$ differ by an element of $\mathbb{F}_p$. Conversely, if $f(\alpha) = 0$ and $b \in \mathbb{F}_p$, then $\alpha + b$ is a root:

$$\begin{aligned}f(\alpha + b) = (\alpha + b)^p - (\alpha + b) - a \\ = \alpha^p + b^p - \alpha - b - a \\ = (\alpha^p - \alpha - a) + (b^p - b) \\ = f(\alpha) - 0 = 0.\end{aligned}$$

It follows that for a fixed root α of $f(x)$, the other roots are given by $\alpha + 1, ..., \alpha + p - 1$. Then the splitting field of $f(x)$ is $\mathbb{F}_p(\alpha)$. We would like to show that $f(x)$ is irreducible, so that $F_p(\alpha) = F_p[x]/(f(x))$ and any two roots of $f(x)$ are Galois conjugates. Suppose that none of the other roots are conjugate to α. Then the minimal polynomial of α over $\mathbb{F}_p$ is $x - \alpha$; in other words, $\alpha \in \mathbb{F}_p$. But this is a contradiction, as we showed that elements of $\mathbb{F}_p$ are not roots of $f(x)$. Thus α is conjugate to some $\alpha + b$ for non-zero $b \in \mathbb{F}_p$. Then there is an automorphism of $\mathbb{F}_p(b)$ sending α to $\alpha + b$. Applying this automorphism b^{-1} times gives an automorphism $\alpha \mapsto \alpha + 1$, and applying this automorphism c times gives an automorphism $\alpha \mapsto \alpha + c$ for any $c \in \mathbb{F}_p$. Thus, all the roots of $f(x)$ are conjugate. In particular, the minimal polynomial of α has degree p, whence it equals $f(x)$, so $f(x)$ is irreducible. As mentioned above, we now know that $\mathbb{F}_p[x]/(f(x))$ is the splitting field of $f(x)$ over $\mathbb{F}_p$.

Now let $F = \mathbb{F}_p[x]/(x^p - x - a)$ Note that since $[F : \mathbb{F}_p] = \deg f(x) = p$, the field F is the (up to isomorphism) finite field of order p^p. Also, $F/\mathbb{F}_p$ is Galois, since $f(x)$ is separable (the roots were shown to be distinct).

We have already seen that $m \in \{0, 1, ..., p-1\}$, there is always an automorphism of $F/\mathbb{F}_p$ which sends α to $\alpha + m$. By counting the values of m, we see that this gives p automorphisms. But as $[F : \mathbb{F}_p] = p$, these are all of the automorphisms. Furthermore, the automorphism $\alpha \mapsto \alpha + m$ is given by σ^m where $\sigma : \alpha \mapsto \alpha + 1$, so σ generates the Galois group, and we are done. $\square$

5 Problem 14.3.10

Prove that n divides $\varphi(p^n - 1)$.

Proof. A note before the proof: The usage of p certainly indicates that it should be prime, but I found two solutions to this exercise which do not require p to be prime. I will of course assume $p > 1$, since $\varphi(0)$ is not defined. Furthermore, the problem statement is trivial for $n = 1$, so I will assume $n > 1$ as well.

Recall the Fermat-Euler theorem, which states that if $\gcd(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \mod m$. Certainly $\gcd(p, p^n - 1) = 1$ by the Euclidean algorithm, so $p^{\varphi(p^n-1)} \equiv 1 \mod p^n - 1$. It is certainly true that $p^n = 1 + p^n - 1 \equiv 1 \mod p^n - 1$. Furthermore, for $0 < m < n$, we have $0 < p^m - 1 < p^n - 1$, so it is impossible for $p^m \equiv 1 \mod p^n - 1$ to hold. It follows that $n \leq \varphi(p^n - 1)$. For convenience, write $m = \varphi(p^n - 1)$. Then $0 = 1 - 1 \equiv p^m - p^n = p^n(p^{m-n} - 1) \equiv p^{m-n} - 1 \mod p^n - 1$. If $m - n < n$, then we must have $m - n = 0$, since we observed that no integer strictly between 0 and n satisfies this congruence. If $m - n \geq n$, then we can do the same analysis to show that $p^{m-2n} \equiv 1 \mod p^n - 1$, and we can repeat our casework on $m - 2n$; either $m = 2n$ or $m - 2n \geq n$. Since m is finite, this process will eventually terminate, so we will find that $m = kn$ for some integer k, as desired.

An alternative proof, following the hint in the textbook, is sketched as follows: $\varphi(p^n - 1) = |\mathrm{Aut}(\mathbb{Z}/(p^n - 1)\mathbb{Z})|$, and multiplication by p is an order n element of $\mathrm{Aut}(\mathbb{Z}/(p^n - 1)\mathbb{Z})$, so Lagrange's theorem concludes the proof. $\square$