Algebra II Assignment 5
Due Friday 22nd April 2022

Please attempt all problems in this assignment and submit your answers (before midnight on Friday 22nd April 2022) by uploading your work to the Moodle page. If you have any questions, feel free to email me at adsg@hku.hk.

Problem 1 (Normal extensions)**.** . (We did this in class. The purpose of this problem is for you to review this part of the material. You should try it first to get as far as you can before consulting the lecture/class notes).

1. State the definition of normal field extensions,
2. Show that a finite extension is normal if and only if it is a splitting field.

Solution. See lecture notes ■

Problem 2. Factorize $x^9 - x$ and $x^{27} - x$ over $\mathbb{F}_3$ into irreducible factors.

Solution. It is straightforward to calculate them by computer searching.

$$x^9 - x = x(x+1)(x+2)(x^2+1)(x^2+x+2)(x^2+2x+2),$$
$$x^{27} - x = x(x+1)(x+2)(x^3+2x+1)(x^3+2x+2)(x^3+x^2+2)(x^3+x^2+x+2)$$
$$(x^3+x^2+2x+1)(x^3+2x^2+1)(x^3+2x^2+x+1)(x^3+2x^2+2x+2)$$

■

Problem 3 (Splitting fields over finite fields)**.** Construct a splitting field L of $f(x) = x^5 + x + 1 \in \mathbb{F}_2[x]$. What is $|L\colon \mathbb{F}_2|$? How many elements does L have?

Solution. First, we prove a fact. Suppose that K is a finite field of characteristic p and $f(x) \in K[x]$ is irreducible and α is a root of $f(x)$ in an algebraic closure of K. Then, we show that $L = K(\alpha)$ is a splitting field of f over K. Since L is a finite field, L is a splitting field of some polynomial over $\mathbb{F}_p$. Thus, L is a splitting field over K. Hence, L is normal over K. Then, because $f(x)$ is irreducible and $f(x)$ has a root α in L, $f(x)$ splits over L. By construction of L, it is a splitting field of $f(x)$ over K.
First we factor $f(x)$. Since $f(x)$ has no roots in $\mathbb{F}_2$, the only possible factorization is $x^5 + x + 1 = (x^3 + ax^2 + bx + c)(x^2 + dx + e)$. Solving this, you see that $x^5 + x + 1 = (x^3 + x^2 + 1)(x^2 + x + 1)$ is a factorization into irreducible polynomials over $\mathbb{F}_2$. Let α be a root of $x^2 + x + 1$ in an algebraic closure of $\mathbb{F}_2$. Let β be a root of $x^3 + x^2 + 1$ in the same algebraic closure of $\mathbb{F}_2$. Then, by the previous fact, $\mathbb{F}_2(\alpha), \mathbb{F}_2(\beta)$ are splitting fields of $x^2 + x + 1$ and $x^3 + x^2 + 1$ over $\mathbb{F}_2$. Hence $L = \mathbb{F}_2(\alpha, \beta)$ is a splitting field of $f(x)$ over $\mathbb{F}_2$. Since $x^2 + x + 1$ is quadratic and $x^3 + x^2 + 1$ is cubic, one has $[L\colon \mathbb{F}_2] = 6$ and L has 64 elements. ■

Problem 4. Let $\mathbb{F}_{11}$ be the field with 11 elements, and let $\mathbb{F}_{11}^*$ denote the group of units of $\mathbb{F}_{11}$.

1. Find all the generators of $\mathbb{F}_{11}^*$ as a multiplicative group.
2. Compute the product of all elements in $\mathbb{F}_{11}^*$.
3. State and prove a generalisation of 2. in the case where $\mathbb{F}_{11}$ is replaced by any finite field $\mathbb{F}_p$ for p prime.

Solution. 1. By direct calculation, they are $2, 6, 7, 8$.
2. The product is equal to 10, or equivalently -1.
3. Claim: For any prime number p, we have $\prod_{x \in \mathbb{F}_p^*} x = -1$.
PROOF: For $p = 2$, this is obvious. Hence, suppose that $p > 2$. By definition, $\mathbb{F}_p^*$ is abelian. Reorder the product so that x is multiplied by its inverse in the product; this is possible whenever x and x^{-1} are distinct. In other words, $\prod_{x \in \mathbb{F}_p^*} x = \prod_{x^2=1} x$. Note that, over any field, the equation $X^2 = 1$ has at most two roots, $X = 1$ and $X = -1$ (inside K, they may be the same). Here, $p > 2$, so $1 \neq -1$, and so $\prod_{x^2=1} x = -1$, proving our claim. ■

Problem 5. Prove that in a finite field of even order, every element is a square.

Solution. A finite field of even order is a splitting field of the polynomial $x^{2^r} - x$ over $\mathbb{F}_2$ for $r \geq 1$ and any element α is a root of the polynomial $x^{2^r} - x$. Thus, $\alpha = (\alpha^{2^{r-1}})^2$ is a square. ■

Problem 6. For any field L, show that $\mathrm{Aut}(L) = \mathrm{Aut}_K(L)$, where K is the prime subfield of L.

Solution. Clearly $\mathrm{Aut}_K(L) \subset \mathrm{Aut}(L)$. For the reversed containment, you notice that for any $\sigma \in \mathrm{Aut}(L)$, $\sigma(1) = 1$ by definition. Then, by additivity and bijectivity of σ, σ fixes $R = \mathbb{Z}$ if $\mathrm{char}(K) = 0$, fixes $R = \mathbb{Z}/p\mathbb{Z}$ if $\mathrm{char}(K) = p$. Finally, by multiplicity and bijectivity of σ, σ fixes the field of fractions of R, i.e., $K = \mathrm{Q}$ if $\mathrm{char}(K) = 0$, or $K = \mathbb{F}_p$ if $\mathrm{char}(K) = p$. ■

Problem 7. Let $K \subset L$ be a finite Galois extension and let $G = \mathrm{Aut}_K(L)$. Prove that for any $\alpha \in L$, if $p(x) \in K[x]$ is the minimal polynomial of α over K, then $|G| \geq \deg(p)$.

Solution. This is trivial by the characterization of finite Galois extensions, i.e., $|G| = [L\colon K]$. ■