HOMEWORK #9
SOLUTIONS TO SELECTED PROBLEMS

Problem 9.5. Let K be of prime characteristic p, and let L/K be Galois extension of degree p. Since $[L : K] = p$, the Galois group of L/K is cyclic of order p. Let σ be a generator.

First reduction. Suppose that there exists $\alpha \in L$ such that $\sigma(\alpha) = \alpha - 1$. Then obviously $\alpha \notin K$ and $\sigma^i(\alpha) = \alpha - i$ for $0 \le i < p$. Therefore $N_{L/K}(\alpha) = \alpha \cdot \sigma(\alpha) \cdot \sigma^2(\alpha) \cdot \ldots \cdot \sigma^{p-1}(\alpha) = \alpha(\alpha-1)(\alpha-2) \cdot \ldots \cdot (\alpha - (p-1)) = \alpha^p - \alpha$ is an element of K.

Note that the last equality follows from the factorization $t^p - t = t(t-1) \cdot \ldots \cdot (t - (p-1))$ that holds in $\mathbb{F}_p$ hence in any field of characteristic p.

Second reduction. Now suppose that there exists $\beta \in L$ with $Tr_{L/K}(\beta) = 1$. Let $\alpha \in L$ be the element

$$\alpha = \sigma(\beta) + 2\sigma^2(\beta) + \cdots + (p-1)\sigma^{p-1}(\beta)$$

Then

$$\sigma(\alpha) = \sigma^2(\beta) + 2\sigma^3(\beta) + \cdots + (p-2)\sigma^{p-1}(\beta) + (p-1)\sigma^p(\beta)$$

hence

$$\alpha - \sigma(\alpha) = \sigma(\beta) + \sigma^2(\beta) + \cdots + \sigma^{p-1}(\beta) + \sigma^p(\beta) = Tr_{L/K}(\beta) = 1$$

and we found $\alpha \in L$ with $\sigma(\alpha) = \alpha - 1$.

Finding β with $Tr_{L/K}(\beta) = 1$. This follows from the non-degeneracy of the trace form. To prove this directly, we use the Dedekind theorem on the linear dependence of automorphisms to deduce the existence of $\gamma \in L$ such that $c = \gamma + \sigma(\gamma) + \cdots + \sigma^{p-1}(\gamma) \neq 0$. But $c = Tr_{L/K}(\gamma)$, so taking $\beta = \gamma/c$ we have $Tr_{L/K}(\beta) = Tr_{L/K}(\gamma)/c = 1$.

Problem 9.6. Consider the polynomial $f(t) = t^4 + 30t^2 + 45$ over $\mathbb{Q}$. It is irreducible by Eisenstein criterion with the prime 5. Let $\alpha \in \mathbb{C}$ be a root of t and let $L = \mathbb{Q}(\alpha)$.

We first show that $[L : \mathbb{Q}] = 4$. Let $\beta = \alpha^2$. Then β is a root of the polynomial $u^2 + 30u + 45$. The roots of this polynomial are $-15 \pm 6\sqrt{5}$ so $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{5})$ hence $[\mathbb{Q}(\beta) : \mathbb{Q}] = 2$. Since $\alpha^2 = \beta$ we have $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta)] \le 2$. To show that the degree equals 2 and not 1, it is enough to show $\alpha \notin \mathbb{Q}(\sqrt{5})$.

Indeed, solving the equation $(a + b\sqrt{5})^2 = -15 + 6\sqrt{5}$ with $a, b \in \mathbb{Q}$, we see that $a^2 + 5b^2 = -15$ and $2ab = 6$. Substituting back $b = 3/a$ we get $a^4 + 15a^2 + 45 = 0$ which has no solutions in $\mathbb{Q}$ (the polynomial is even irreducible!). By multiplicity of degrees, $[L : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2 \cdot 2 = 4$.

We now show that the other roots of f lie in L. By the previous computation, the roots are $\pm\sqrt{-15 \pm 6\sqrt{5}}$, and $\alpha = \sqrt{-15 + 6\sqrt{5}}$ (arbitrary choice).

But $(-15+6\sqrt{5})(-15-6\sqrt{5}) = 225-36\cdot 5 = 45$ hence $-15-6\sqrt{5} = 45/\alpha^2$, so the four roots of f are $\alpha, -\alpha, 3\sqrt{5}/\alpha, -3\sqrt{5}/\alpha$ and since $\sqrt{5} \in L$, they all lie in L. Therefore L is a splitting field for the separable polynomial f hence $L/\mathbb{Q}$ is Galois.

Finally, we compute the Galois group $\mathrm{Gal}(L/\mathbb{Q})$. Since f is irreducible over $\mathbb{Q}$, one can find automorphisms of L taking α to any of the other roots. Let σ be the automorphism taking α to $3\sqrt{5}/\alpha$. Then σ is of order 4. To see this, we first compute $\sigma(\sqrt{5})$. We know that

$$\sigma(-15+6\sqrt{5}) = \sigma(\alpha^2) = \sigma(\alpha)^2 = (3\sqrt{5}/\alpha)^2 = 45/(-15+6\sqrt{5}) = -15-6\sqrt{5}$$

thus $\sigma(\sqrt{5}) = -\sqrt{5}$. We therefore have

$$\begin{aligned}
\sigma(\alpha) &= 3\sqrt{5}/\alpha \\
\sigma^2(\alpha) &= \sigma(3\sqrt{5}/\alpha) = -3\sqrt{5}/\sigma(\alpha) = -\alpha \\
\sigma^3(\alpha) &= \sigma(-\alpha) = -3\sqrt{5}/\alpha \\
\sigma^4(\alpha) &= \sigma(-3\sqrt{5}/\alpha) = \alpha
\end{aligned}$$

so σ is of order 4. Since $|\mathrm{Gal}(L/\mathbb{Q})| = [L:\mathbb{Q}] = 4$ we deduce that the Galois group is cyclic of order 4.

Problem 9.7. Let L/K be an extension of prime degree p, and let $\alpha \in L\backslash K$. Denote by $f(t) \in K[t]$ the minimal polynomial of α over K, and assume that f has another root $\beta \neq \alpha$ in L.

We will show that L/K is Galois by showing that f is a separable polynomial over K and L is its splitting field over K.

Step 1: Construction of $\sigma \in \mathrm{Gal}(L/K)$ *with* $\sigma(\alpha) = \beta$. We have $[L:K] = [L:K(\alpha)][K(\alpha):K]$ and since $[L:K] = p$ is prime and $\alpha \notin K$, we deduce that $L = K(\alpha)$. Note also that $\beta \notin K$ (otherwise f would have a root in K, contradicting its irreducibility) so the same argument yields $L = K(\beta)$.

Now, α and β are two roots of the same irreducible polynomial $f(t) \in K[t]$, hence there exists a K-isomorphism $\sigma : K(\alpha) \to K(\beta)$ such that $\sigma(\alpha) = \beta$. By the preceding paragraph, $L = K(\alpha) = K(\beta)$, so that $\sigma \in \mathrm{Gal}(L/K)$.

Step 2: Producing more roots of f *in* L. We know that since α is a root of $f \in K[t]$, so is $\sigma(\alpha)$. Applying this again and again, we see that $\sigma^i(\alpha)$ are also roots of f for any $i \geq 0$. Since the number of roots is finite (bounded by $\deg f$), there exist i, j such that $\sigma^i(\alpha) = \sigma^j(\alpha)$ and since σ is invertible, we have $\sigma^{j-i}(\alpha) = \alpha$, so σ has a finite order, denote it by $d \geq 1$.

Step 3: Showing that $d = p$. Consider the field $F = L^{\langle\sigma\rangle}$, the field fixed by the subgroup generated by σ. This is an intermediate field $K \subseteq L^{\langle\sigma\rangle} \subseteq L$. But since $[L:K]$ is prime, again by multiplicity of degrees, either $F = K$ or $F = L$. But $F = L$ is impossible since $\sigma(\alpha) = \beta \neq \alpha$, so $F = K$. Now one can argue in several ways, for example to use (a version of) Galois theorem that asserts what L/F is Galois with Galois group of order $d = |\langle\sigma\rangle|$, hence $d = p$. Alternatively, one can consider the polynomial $F(t) = \prod_{i=0}^{d-1}(t - \sigma^i(\alpha))$ which is invariant under the action of σ on coefficients hence has its coefficients in $F = K$. We get a polynomial in $K[t]$ of degree d which has α as a root, and by minimality of f, we must have $d = p$ and $F = f$ (up to a scalar). We also see that f has p distinct roots (the images of α) hence it is separable.