Homework 6
Solutions

Problem 1 [14.2.23] Let K be a Galois extension of F with cyclic Galois group of order n generated by σ. Suppose $\alpha \in K$ has $N_{K/F}(\alpha) = 1$. Prove that $\alpha = \frac{\beta}{\sigma\beta}$ for some nonzero $\beta \in K$.

Proof. By the linear independence of the characters $1, \sigma, \ldots, \sigma^{n-1}$ (Th 7, Sec 14.2), $\exists\ \theta \in K$ such that

$$\beta := \theta + \alpha\ \sigma(\theta) + (\alpha\ \sigma\alpha)\sigma^2(\theta) + \cdots + (\alpha\sigma\alpha \ldots \sigma^{n-2}\alpha)\sigma^{n-1}(\theta) \neq 0.$$

Considering that $\sigma^n(\theta) = \theta$ and $N(\alpha) = \alpha\ \sigma\alpha\ \ldots\ \sigma^{n-1}\alpha = 1$ we obtain

$$\begin{aligned}\sigma(\beta) &= \sigma(\theta) + \sigma(\alpha)\ \sigma^2(\theta) + \cdots + (\sigma(\alpha) \ldots \sigma^{n-1}(\alpha))\sigma^n(\theta) \\ &= \sigma(\theta) + \sigma(\alpha)\ \sigma^2(\theta) + \cdots + \frac{1}{\alpha} \cdot \theta \\ &= \frac{\alpha\sigma(\theta) + \alpha\sigma(\alpha)\ \sigma^2(\theta) + \cdots + \theta}{\alpha} \\ &= \frac{\beta}{\alpha}, \text{ showing that } \alpha = \frac{\beta}{\sigma\beta}.\end{aligned}$$

□

Problem 2 [14.2.29] Let k be a field and let $k(t)$ be the field of rational functions in the variable t. Define the maps σ and τ of $k(t)$ to itself by $\sigma f(t) = f\left(\frac{1}{1-t}\right)$ and $\tau f(t) = f\left(\frac{1}{t}\right)$ for $f(t) \in k(t)$.

(a) Prove that σ and τ are automorphisms of $k(t)$ and that $G := \langle \sigma, \tau \rangle \cong S_3$.

(b) Prove that the element $s = \frac{(t^2-t+1)^3}{t^2(t-1)^2}$ is fixed by all the elements of G.

(c) Prove that $k(s)$ is precisely the fixed field if G in $k(t)$.

Proof. (a) From HW 4 ([14.1.8])we know that the automorphisms of $k(t)$ are given by the fractional linear transformation $t \mapsto \frac{at+b}{ct+d}$, with $ad - bc \neq 0$. Clearly, the maps $\sigma : t \mapsto \frac{1}{1-t}$ and $\tau : t \mapsto \frac{1}{t}$ satisfy this requirement, so σ and τ are automorphisms of $k(t)$.

Moreover, it's easy to check that $\sigma^3 = \tau^2 = 1$ and $\tau\sigma\tau = \sigma^{-1}$, which is a presentation for the dihedral group of order 6. Thus $G = \langle \sigma, \tau \rangle \cong D_6 \cong S_3$.

(b) It's enough to verify that s is fixed by the two generators of G. Indeed

$$\sigma(s) = \frac{\left(\left(\frac{1}{1-t}\right)^2 - \frac{1}{1-t} + 1\right)^3}{\left(\frac{1}{1-t}\right)^2\left(\frac{1}{1-t} - 1\right)^2} = \frac{(t^2-t+1)^3}{t^2(t-1)^2} = s \text{ and } \tau(s) = \frac{\left(\frac{1}{t^2} - \frac{1}{t} + 1\right)^3}{\frac{1}{t^2}\left(\frac{1}{t} - 1\right)^2} = \frac{(t^2-t+1)^3}{t^2(t-1)^2} = s.$$

(c) If $(k(t))^G$ is the fixed field of G in $k(t)$, then in view of (b): $k(s) \subseteq (k(t))^G \subseteq k(t)$. Now by (a) we find that $[k(t) : (k(t))^G] = |G| = |S_3| = 6$. Moreover, by HW 3 ([13.2.18]) we infer that $[k(t) : k(s)] = \max(\deg{(t^2-t+1)^3}, \deg t^2(t-1)^2) = 6$. By the multiplicativity of degrees $[k(t) : k(s)] = [k(t) : (k(t))^G][(k(t))^G : k(s)]$, which implies that $[(k(t))^G : k(s)] = 1$ and hence $(k(t))^G = k(s)$. □

Problem 3 [14.2.31] Let K be a finite extension of F of degree n. Let α be an element of K.

(a) Prove that α acting by left multiplication on K is an F-linear transformation T_α of K.

(b) Prove that the minimal polynomial for α over F is the same as the minimal polynomial for the linear transformation T_α.

(c) Prove that the trace $Tr_{K/F}(\alpha)$ is the trace of the $n \times n$ matrix defined by T_α. Prove that the norm is the determinant of T_α.

Proof. (a) Let $T_\alpha : K \to K$ be defined as $T_\alpha(x) = \alpha x$, for all $x \in K$. Pick any $x, y \in K$ and $a \in F$, then $T_\alpha(ax+y) = \alpha(ax+y) = a\alpha x + \alpha y = aT_\alpha(x) + T_\alpha(y)$, showing that T_α is F-linear.

(b) Let $m(x) = x^d + \ldots + a_1x + a_0$ be the minimal polynomial of α over F, and let $f(x)$ be the minimal polynomial of T_α. Since $m(\alpha) = 0$ and $T_\alpha^m(x) = \alpha^m x$ (for all integers m) we get that

$$(m(T_\alpha))(x) = (T_\alpha^d + \ldots + a_1T_\alpha + a_0)(x) = (\alpha^d + \ldots + a_1\alpha + a_0)x = 0.$$

Hence $m(T_\alpha) = 0$, which implies that $f(x)|m(x)$. Since $m(x)$ is irreducible, we should necessarily have $m(x) = f(x)$.

(c) Let $p(x) = x^n + \ldots + b_1x + b_0$ be the characteristic polynomial of T_α. From Ma 1b (or Prop 20, Sec. 12.2), we know that $p(x)$ and $m(x)$ have the same roots (not counting multiplicities) and $m(x)|p(x)$. As $m(x)$ is irreducible, all irreducible factors of $p(x)$ should be equal to $m(x)$ and thus $p(x)$ is a power of $m(x)$, i.e. $d|n$ and $p(x) = (m(x))^{n/d}$. Then by [14.2.17] and [14.2.18] we obtain that $Tr_{K/F}(\alpha) = -\frac{n}{d}a_{d-1} = -b_{n-1} = Tr(T_\alpha)$ and $N_{K/F}(\alpha) = (-1)^n a_0^{n/d} = (-1)^n b_0 = \det(T_\alpha)$. □

Problem 4 [14.3.7] Prove that one of $2, 3$ or 6 is a square in $\mathbb{F}_p$ for every prime p. Conclude that the polynomial

$$f(x) = x^6 - 11x^4 + 36x^2 - 36 = (x^2-2)(x^2-3)(x^2-6)$$

has a root modulo p for every prime p but has no root in $\mathbb{Z}$.

Proof. Let y be a generator of the cyclic group $\mathbb{F}_p^\times$. Then $n \in \mathbb{F}_p^\times$ is a square iff it is an even power of y. Consequently, if 2 and 3 are not squares in F_p, it follows that $2 \equiv y^{2k+1} (\mod p)$ and $3 \equiv y^{2l+1} (\mod p)$, for some $k, l \in \mathbb{Z}$. Hence $6 \equiv y^{2(k+l+1)} (\mod p)$ is a square in $\mathbb{F}_p$.

Now $f(x)$ clearly doesn't have any integer roots. However, by the above analysis we know that there exists $\gamma \in \{2, 3, 6\}$ such that $\gamma = \alpha^2$, for some $\alpha \in \mathbb{F}_p$. Then $x - \alpha \mid x^2 - \gamma \mid f(x)$ so α is a root of f in $\mathbb{F}_p$. □

Remark. *Alternatively, a group-theoretic approach is also possible: Consider the group homomorphism $\phi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times$, given by $x \mapsto x^2$. If $H := Im(\phi)$ then $H \cong \mathbb{F}_p^\times / \ker(\phi)$, and since $\ker(\phi) = \{\pm 1\}$ it follows that H has index $[\mathbb{F}_p^\times : H] = 2$ in $\mathbb{F}_p^\times$. This means that H has precisely 2 cosets in $\mathbb{F}_p^\times$. If 2 and 3 are not squares in $\mathbb{F}_p$ then $2, 3 \notin H$, so they belong to the same coset, i.e.*

$2H = 3H$. Therefore $H = (2H)(2H) = (2H)(3H) = 6H$, which shows that $6 \in H$ and thus 6 is a square in $\mathbb{F}_p^\times$. This proves that one of $2, 3$ or 6 is a square in $\mathbb{F}_p$.

Problem 5 [14.3.8] Determine the splitting field of the polynomial $f(x) = x^p - x - a$ over $\mathbb{F}_p$ where $a \neq 0$, $a \in \mathbb{F}_p$. Show explicitly that the Galois group is cyclic.

Proof. Let α be a root of f, then $f(\alpha+1) = (\alpha+1)^p - (\alpha+1) - a = \alpha^p - \alpha - a = 0$ showing that $\alpha + 1$ is also a root. Hence the p roots of f are just $\mathcal{R} := \{\alpha + k \mid 1 \leq k \leq p\}$ (in particular f is separable). Moreover $\alpha \notin \mathbb{F}_p$, for otherwise $\alpha^p = \alpha$ and so $a = \alpha^p - \alpha = 0$, which is a contradiction. Therefore $\mathbb{F}_p(\alpha)$ is the splitting field of the separable polynomial f over $\mathbb{F}_p$, hence $\mathbb{F}_p(\alpha)/\mathbb{F}_p$ is a Galois extension.

Consider the endomorphism $\sigma : \mathbb{F}_p(\alpha) \to \mathbb{F}_p(\alpha)$, which sends $\alpha \mapsto \alpha + 1$ and fixes $\mathbb{F}_p$. Note that σ has a two-sided inverse defined by a map that sends $\alpha \mapsto \alpha - 1$ and fixes $\mathbb{F}_p$. This shows that $\sigma \in Gal(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$.

Any other element $\tau \in Gal(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ must fix $\mathbb{F}_p$ and it must send α to a root of f, so τ is of the form $\tau : \alpha \mapsto \alpha + k$ for some $k \in \mathbb{F}_p$ (recall that $\mathcal{R}$ is the set of all the roots of f). We obtain that $\sigma^k(\alpha) = \alpha + k = \tau(\alpha)$, while σ^k and τ fix $\mathbb{F}_p$, hence $\sigma^k = \tau$. Therefore, every element of $Gal(\mathbb{F}_p(\alpha)/\mathbb{F}_p)$ is a power of σ, and since $\sigma^p = 1$ we conclude that the Galois group is cyclic, of order p, generated by σ.

$\square$

Remark. *The minimal polynomial $m_{\alpha,\mathbb{F}_p}$ of α over $\mathbb{F}_p$ divides $x^p - x - \alpha$ (since α is a root of f), implying that*

$$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg m_{\alpha,\mathbb{F}_p} \leq \deg f = p.$$

Here are two ways you can notice that f is irreducible over $\mathbb{F}_p$ (and hence the equality holds above):

(i) Suppose

$$f(x) = \prod_{i=1}^{p} (x - (\alpha + i)) = g(x)h(x) \text{ in } \mathbb{F}_p[x].$$

Then the roots of g form a subset of $\mathcal{R}$. If $d := \deg(g) \geq 1$ then the of the coefficient a_{d-1} of x^{d-1} in $g(x)$ is the sum of d elements of the form $-(\alpha+k)$, so it is equal to $-d\alpha + N$ for some integer N. However $a_{d-1} \in \mathbb{F}_p$ implies that $d\alpha \in \mathbb{F}_p$, which contradicts the fact that $\alpha \notin \mathbb{F}_p$. Consequently, $f(x)$ is irreducible over $\mathbb{F}_p$ and thus it's the minimal polynomial of α over $\mathbb{F}_p$.

(ii) Let $p_1(x), \ldots, p_t(x)$ be the irreducible factors of f. By adjoining any root of f to $\mathbb{F}_p$ we obtain a splitting field of f, thus each quotient $F_p[x]/(p_i(x))$ is a splitting field of f, implying that all these fields are isomorphic. In particular, this means that $\deg p_1 = \ldots \deg p_t = d$. But then $d \cdot t = p$, which is possible only when $d = p$ and $t = 1$ (note that $d = 1$ and $t = p$ is impossible because f doesn't have linear factors). So f has only one irreducible factor, i.e. it's irreducible.