Solutions to the Midterm

Problem 1. Let K be a field and let p be a prime number not equal to the characteristic of K. Suppose that K contains primitive $p-$th root of 1 and if $p=2$ also the primitive 4-th root of 1.

1. Suppose that for some k the splitting fields of $x^{p^k}-1$ and of $x^{p^{k+1}}-1$ coincide. Prove that K contains primitive p^{k+1}-th root of 1.

2. Suppose that K contains primitive p^k-th root of 1 for all k. Prove that if for some $a \in K$ the polynomials x^p-a and $x^{p^2}-a$ have the same splitting fields over K then both polynomials have all their roots in K.

Hint: If p is odd and p^{k+1} divides m^p-1 then p^k divides $m-1$.

Solution: 1. Let L be the splitting field of $x^{p^{k+1}}-1$ over K and let m be smallest such that L is the splitting field of $x^{p^m}-1$ over K. Thus $m \leq k$. If $m=1$ then $L=K$, since K contains primitive p-th root of 1. Similarly if $p=2$ and $m=2$ then $L=K$.

Suppose $m>1$ or $p=2$ and $m>2$. Let $M=K(\zeta_{p^{m-1}})$ be the splitting field of $x^{p^{m-1}}-1$ over K, where $\zeta_{p^{m-1}}$ is a primitive p^{m-1}-th root of 1. Thus L is the splitting field of $x^p-\zeta_{p^{m-1}}$ over M. Since M contains primitive $p-$th root of 1 and $L \neq M$, the extension L/M has degree p and is Galois with cyclic Galois group generated by τ. Let $\zeta \in L$ be a root of $x^p-\zeta_{p^{m-1}}$, so ζ is a primitive p^m-th root of 1 and $L=M(\zeta)$. Since L contains all p^{m+1}-th roots of 1, there is $\xi \in L$ such that $\xi^p=\zeta$. Thus ξ is a primitive p^{m+1}-th root of 1 and therefore $\tau(\xi)=\xi^r$ for some r prime to p. It follows that $\xi=\tau^p(\xi)=\xi^{r^p}$, i.e. $\xi^{r^p-1}=1$. This implies that p^{m+1} divides r^p-1.

If p is odd, we conclude that p^m divides $r-1$ and therefore $\zeta^r=\zeta$. Since $\xi^p=\zeta$ and $\tau(\xi)=\xi^r$, we see that

$$\tau(\zeta)=\tau(\xi^p)=\tau(\xi)^p=\xi^{rp}=\zeta^r=\zeta,$$

which implies that $\zeta \in M$, a contradiction.

If $p = 2$, then either 2^m divides $r - 1$ or 2^m divides $r + 1$. In the former case we get a contradiction in exactly same way as for p odd. In the latter case, $\zeta^r = \zeta^{-1}$ so

$$\tau(\zeta) = \tau(\xi^2) = \tau(\xi)^2 = \xi^{2r} = \zeta^r = \zeta^{-1}$$

and

$$\zeta_{2^{m-1}} = \tau(\zeta_{2^{m-1}}) = \tau(\zeta^2) = \tau(\zeta)^2 = \zeta^{-2} = \zeta_{2^{m-1}}^{-1}.$$

Thus $\zeta_{2^{m-1}}^2 = 1$, which is false since $m \geq 3$.

We have seen that the assumption that $m > 1$ or $p = 2$ and $m > 2$ leads to a contradiction. This completes our proof that $L = K$.

2. Let L be the splitting field of $x^p - a$. We need to show that $L = K$. Suppose not. Let $u \in L$ be a root of $x^p - a$. Since K contains primitive p-th root of 1, $L = K(u)$ is a Galois extension of K of degree p with cyclic Galois group generated by τ. Since $x^{p^2} - a$ splits in L, there is $w \in L$ such that $w^p = u$. We have $\tau(w) = \xi w$ for some p^2-th root of 1 ξ. Since $\xi \in K$, it is fixed by τ so $w = \tau^p(w) = \xi^p w$, i.e. $\xi^p = 1$. Thus

$$\tau(u) = \tau(w^p) = \tau(w)^p = (\xi w)^p = w^p = u$$

which implies that $u \in K$, a contradiction. Thus $L = K$.

Remark. In our solution to 2. we only used the fact that K contains a primitive p^2-th root of 1. For p odd it is enough to assume only that a primitive p-th root of 1 is in K. Indeed, as in our solution to 2. we have $\tau(w) = \xi w$ for some p^2-th root of 1 $\xi \in L$ (we no longer can assume that $\xi \in K$). Now $\tau(\xi) = \eta\xi$ for some p-th root of 1 (since $\xi^p \in K$). It follows that $\tau^i(w) = \eta^{1+2+\ldots+(i-1)}\xi^i w$ for all i (note that $\tau(\eta) = \eta$). In particular, $w = \tau^p(w) = \eta^{1+2+\ldots+(p-1)}\xi^p w = \xi^p w$. Thus we have $\xi^p = 1$ and therefore $\xi \in K$. The rest of the argument is the same as in our solution to part 2.

Problem 2. Let L/K be a Galois extension. We say that $a \in L$ generates a normal basis of L/K if the set $\{\tau(a) : \tau \in \text{Gal}(L/K)\}$ is a basis of L over K. Let $K \subseteq M \subseteq L$ be a subfield such that M/K is Galois. Prove that if $a \in L$ generates a normal basis of L/K then the trace $Tr_{L/M}(a)$ generates a normal basis of M/K.

Solution: Let G, H be the Galois groups of L/K and L/M respectively. Thus H is normal in G and the Galois group of M/K is isomorphic to G/H. Choose coset representatives $\tau_1, ..., \tau_k$ of H in G. Then the restrictions of τ_i to M constitute the group Gal(M/K). Let $b = Tr_{L/M}(a) = \sum_{\tau \in H} \tau(a)$. Note that

$$\tau_i(b) = \sum_{\tau \in H} \tau_i \tau(a) = \sum_{\tau \in \tau_i H} \tau(a).$$

If the elements $\tau_1(b), ..., \tau_k(b)$ are linearly dependent over K then there are elements $a_1, ..., a_k$ in K, not all equal to 0, such that

$$0 = \sum_{i=1}^{k} a_i \tau_i(b) = \sum_{i=1}^{k} \sum_{\tau \in \tau_i H} a_i \tau(a)$$

But this means that the elements $\tau(a)$, $\tau \in G$, are linearly dependent over K, which contradicts the assumption that a generates a normal basis of L/K.

Problem 3. Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n with roots x_1,..., x_n.

1. Prove that for every integer $k > 0$ there is a monic polynomial $g_k \in \mathbb{Z}[x]$ of degree n whose roots are $x_1^k, x_2^k, ..., x_n^k$ (one way is to use symmetric functions).
2. Suppose that the absolute values $|x_i|$ satisfy $|x_i| \leq 1$ for all i. Prove that the sequence g_1, g_2,... from 1. contains only a finite number of different polynomials (Hint: bound the coefficients of g_k). Conclude that each x_i is a root of unity.

Solution: We have no choice but to define $g_k(x)$ as

$$g_k(x) = \prod_{i=1}^{n} (x - x_i^k).$$

Let s_1,...,s_n be the elementary symmetric functions in n variables. The coefficient of g_k at x^i is $(-1)^i s_i(x_1^k, ..., x_n^k)$. The function $s_i(y_1^k, ..., y_n^k)$ is a symmetric polynomial in the variables $y_1, ..., y_n$ and with integral coefficients. It follows that $s_i(y_1^k, ..., y_n^k) = f_i(s_1(y_1, ..., y_n), ..., s_n(y_1, ..., y_n))$ for some polynomial f_i with integral coefficients. The numbers $(-1)^i s_i(x_1, ..., x_n) = a_i$ are the coefficients of f. Thus $a_i \in \mathbb{Z}$ and $s_i(x_1^k, ..., x_n^k) = f_i((-1)^i a_1, ..., (-1)^i a_n)$ are integers. This proves that g_k has integral coefficients for all k.

Suppose now that $|x_i| \leq 1$ for all i. Note that the polynomial $s_i(y_1, ..., y_n)$ is a sum of $\binom{n}{i}$ monomials of the form $y_{j_1} y_{j_2} ... y_{j_i}$, each occurring with coefficient 1. It follows that

$$|s_i(z_1, ..., z_n)| \leq \binom{n}{i} B^i$$

for any complex numbers $z_1, ..., z_n$ such that $|z_i| \leq B$ for all i. In particular, $|s_i(x_1^k, ..., x_n^k)| \leq \binom{n}{i} \leq 2^n$ for all i (since $|x_i^k| \leq 1$). Thus all coefficients of each polynomial g_k are bounded by 2^n. But these coefficients are integers. There is only a finite number of distinct polynomials with integral coefficients bounded by 2^n. Given i, the numbers $x_i, x_i^2, x_i^3, ...$ are roots of this finite collection of polynomials, hence they form a finite set. It follows that $x_i^k = x_i^m$ for some $k < m$, so $x_i^{m-k} = 1$, i.e. x_i is a root of 1.

Problem 4. Consider the polynomial $p(x) = x^4 + 5x^2 + 12x + 13$.

1. Prove that p is irreducible over $\mathbb{Q}$.
2. Find the Galois group of the splitting field of p. Provide all details of your solution.
3. Express the roots of p in radicals.

Solution: The only candidates for rational roots of p are $\pm 1, \pm 13$, and direct computation shows that none is a root. Thus if p factors over $\mathbb{Q}$ then the factors must be of degree 2. By Gauss Lemma, if p is reducible then

$$p = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd$$

for some integers a, b, c, d. Thus $a + c = 0$, $b + d + ac = 5$, $ad + bc = 12$ and $bd = 13$. From $bd = 13$ we conclude that either $\{b, d\} = \{1, 13\}$ or $\{b, d\} = \{-1, -13\}$. Thus $b + d = \pm 14$ and $d - b = \pm 12$. Note that $12 = ad + bc = a(d - b)$ so $a = \pm 1$. Hence $5 = b + d + ac = \pm 14 - a^2 = \pm 14 - 1$, a contradiction. It follows that p is irreducible over $\mathbb{Q}$.

Let x_1, x_2, x_3, x_4 be the roots of p. Consider $z_1 = x_1x_2 + x_3x_4$, $z_2 = x_1x_3 + x_2x_4$, $z_3 = x_1x_4 + x_2x_3$. The cubic resolvent of p is the polynomial $q(x) = (x - z_1)(x - z_2)(x - z_3)$. Recall that $z_1 + z_2 + z_3 = s_2$, $z_1z_2 + z_1z_3 + z_2z_3 = s_1s_3 - 4s_4$ and $z_1z_2z_3 = s_1^2s_4 + s_3^2 - 4s_2s_4$, where s_1, s_2, s_3, s_4 are the elementary symmetric functions in x_1, x_2, x_3, x_4. In our case, $s_1 = 0$, $s_2 = 5$, $s_3 = -12$, $s_4 = 13$. Thus $q(x) = x^3 - 5x^2 - 52x + 116$. Looking for rational roots of q we find that $q(2) = 0$ and therefore $q = (x - 2)(x^2 - 3x - 58)$. Since q has exactly one rational root, the

Galois group of p is either C_4 or D_8. The other two roots of q are $(3 \pm \sqrt{241})/2$. In particular, $\mathbb{Q}(\sqrt{241})$ is a quadratic subfield of the splitting field of p. We may order the roots of p so that $z_1 = 2$, $z_2 = (3+\sqrt{241})/2$, $z_3 = (3 \pm \sqrt{241})/2$. Note that $z_1 = x_1x_2 + x_3x_4 = 2$ and $(x_1x_2)(x_3x_4) = s_4 = 13$. It follows that x_1x_2, x_3x_4 are the roots of $x^2 - 2x + 13$. These roots are $1 \pm 2\sqrt{-3}$. Consequently $\mathbb{Q}(\sqrt{-3})$ is a quadratic subfield of the splitting field of p. We see that the splitting field of p has two different quadratic subfields, hence its Galois group cannot be cyclic. It follows that the Galois group of p is the dihedral group D_8.

Remark. In general, if the cubic resolvent has exactly one rational root, say $z_1 = x_1x_2 + x_3x_4$, then we look at x_1x_2 and x_3x_4. These two numbers are roots of a quadratic polynomial over $\mathbb{Q}$. If this quadratic polynomial is irreducible over $\mathbb{Q}$ then it defines a quadratic extension. If this quadratic extension coincides with the quadratic extension corresponding to the irreducible quadratic factor of q then the Galois group is cyclic of order 4. If it is a different quadratic extension then the Galois group is D_8. It could happen however that both x_1x_2 and x_3x_4 are rational. Then we look instead at $x_1 + x_2$ and $x_3 + x_4$. Note that both $x_1 + x_2 + x_3 + x_4 = s_1$ and $(x_1 + x_2)(x_3 + x_4) = z_2 + z_3$ are rational so $x_1 + x_2$ and $x_3 + x_4$ are roots of a quadratic polynomial over $\mathbb{Q}$. It cannot happen that both x_1x_2 and x_3x_4 are rational and x_1+x_2 and x_3+x_4 are rational, so $\mathbb{Q}(x_1+x_2)$ is a quadratic extension of $\mathbb{Q}$ and the Galois group is cyclic iff this extension coincides with the quadratic extension corresponding to the irreducible quadratic factor of q. Note finally that if neither x_1x_2 nor $x_1 + x_2$ is rational, then they define the same quadratic extension of $\mathbb{Q}$.

In order to find the roots of p recall that we found that x_1x_2 and x_3x_4 are the roots of $x^2 - 2x + 13$. Thus $\{x_1x_2, x_3x_4\} = \{1 + 2\sqrt{-3}, 1 - 2\sqrt{-3}\}$. Similarly, since $x_1+x_2+x_3+x_4 = 0$ and $(x_1+x_2)(x_3+x_4) = z_2+z_3 = 3$, we see that x_1+x_2 and x_3+x_4 are roots of x^2+3. Hence $\{x_1+x_2, x_3+x_4\} = \{\sqrt{-3}, -\sqrt{-3}\}$. We may assume that $x_1x_2 = 1 + 2\sqrt{-3}$ and $x_3x_4 = 1 - 2\sqrt{-3}$. But then $x_1 + x_2 = \pm\sqrt{-3}$ and we must determine if it is plus or minus. Note that $-12 = s_3 = x_1x_2(x_3+x_4)+x_3x_4(x_1+x_2) = (x_1 + x_2)(x_3x_4 - x_1x_2) = (x_1 + x + 2)(-4\sqrt{-3})$. Thus $x_1 + x_2 = -\sqrt{-3}$. We showed that $x_1 + x_2 = -\sqrt{-3}$ and $x_1x_2 = 1 + 2\sqrt{-3}$. It follows that x_1, x_2 are roots of the polynomial $x^2 + \sqrt{-3}x + (1 + 2\sqrt{-3})$. These roots are $(\sqrt{-3} \pm \sqrt{-7 - 8\sqrt{-3}})/2$.

Similarly, x_3, x_4 are roots of the polynomial $x^2 - \sqrt{-3}x + (1 - 2\sqrt{-3})$. These roots are $(-\sqrt{-3} \pm \sqrt{-7 + 8\sqrt{-3}})/2$.