ALGEBRA QUAL PREP: FIELDS AND GALOIS THEORY

TONY FENG

These are hints/solutions/commentary on the problems. They are not a model for what to actually write on the quals.

1. Spring 2010 M4

(a) This is equivalent to $x^7 - 12$ being irreducible. (Which can be checked using *Eisenstein's criterion* – look this up if you don't know it.)
(b) Write $\beta = \sum a_j \alpha^j$. This gives two expressions for $\sigma(\beta)$; comparing them using linear independence gives the result.
(c) The Galois conjugates of a root of $x^7 - 11$ are translates by ζ^i; then use (b) to see that it must be a 7th root of 12.

2. Spring 2011 M2

(a) If such a root α existed, then we would have $\mathbf{Q}(\alpha) \subset \mathbf{Q}(\zeta_{25})$. Since $\mathbf{Q}(\zeta_{25})/\mathbf{Q}$ is cyclic, it has only one degree-5 subextension over $\mathbf{Q}$. Since $-1 \in (\mathbf{Z}/25)^*$ becomes trivial in the $\mathbf{Z}/5$-quotient of $(\mathbf{Z}/25)^*$, this subextension is totally real and cannot agree with $\mathbf{Q}(\alpha)$.
(b) As $[\mathbf{Q}(\zeta_{25}, \alpha) : \mathbf{Q}(\zeta_{25})] = 5$, the polynomial $x^5 - 5$ must still be irreducible over $\mathbf{Q}(\zeta_{25})$. So $\mathrm{Nm}_{\mathbf{Q}(\zeta_{25},\alpha)/\mathbf{Q}(\zeta_{25})}(\alpha) = 5$. Therefore $\alpha = \beta^5$ in $\mathbf{Q}(\zeta_{25}, \alpha)$, taking norms gives a 5th root of 5 in $\mathbf{Q}(\zeta_{25}, \alpha)$.

3. Fall 2015 M3

(a) You can take $f(X) = X^{p^n - 1} - 1$. The splitting field for f contains K because every non-zero element of K is a root of f, and is contained in K because f has $p^n - 1$ roots over K.

We claim that the Galois group is generated by the automorphism $\alpha \mapsto \alpha^p$. It is easily checked that this is an automorphism of K with order n, hence generates all of $\mathrm{Gal}(K/\mathbf{F}_p)$ since $[K : \mathbf{F}_p] = n$.
(b) This matrix consists of the elements of $\mathrm{Gal}(K/\mathbf{F}_p)$ applied to the column $v := (x_1, \ldots, x_n)$. The non-vanishing of the determinant amounts to linear independence of characters. Explicitly, suppose that there is a non-trivial linear combination

$$\sum a_i \sigma^i(v) = 0$$

with $a_i \in K$.

We may assume $a_1 \neq 0$. Applying this with $v \mapsto \alpha v$ gives

$$\sum a_i \sigma^i(\alpha) \sigma(v) = 0.$$

On the other hand, multiplying by α gives

$$\sum a_i \alpha \sigma^i(v) = 0.$$

Subtracting these two expressions eliminates the $i=0$ coefficient, creating a shorter expression unless a_i is only non-zero for $i=0$, which however is also impossible.

(c) Since $\mathbf{F}_3[x]/(x^4-x-1) \cong \mathbf{F}_{81}$, every element $\alpha \in \mathbf{F}_3[x]/(x^4-x-1) \cong \mathbf{F}_{81}$ satisfies $\alpha^{80}=1$. In particular we have $x^{40} = \pm 1$. Which is it? Well, $x^{40}=1$ if and only if x is a square in $\mathbf{F}_3[x]/(x^4-x-1)$, since $\mathbf{F}_{81}^\times \cong \mathbf{Z}/80$ is cyclic. If this were the case, then the norm of x (down to $\mathbf{F}_3$) would be a square, but it is -1. So $x^{40}=-1$, and then we know that x^{20} is a square root of -1.

4. Fall 2010 A3

(i) By the Primitive Element Theorem, we may write $L = K[t]/(f)$. Then $L \otimes_K L' \cong L[t]/(f)$. Factoring $f = \prod f_i$ into irreducibles over L, the f_i are coprime because f is separable, hence we get

$$L[t]/(f) = \prod L[t]/(f_i)$$

which is a product of field extension.

(ii) Take $K = \mathbf{F}_p(x)$ and $L = \mathbf{F}_p(x^{1/p}) = K(t)/(t^p - x)$. Then $L \otimes_K L = L[t]/(t-x^{1/p})^p$ is non-reduced, hence certainly not a product of fields.

5. Spring 2012 M3

(a) If E/k is separable, then by the primitive element theorem we may write $E = k(\alpha)$ for some $\alpha \in k$ satisfying a polynomial of degree $[E:k]$. Any automorphism of E over k is completely determined by its effect on α, and must take α to another root of this polynomial, so there are at most $[E:k]$ choices.

In general, there is a maximal separable subextension $k \subset E^s \subset E$. As separable elements go to separable elements, any automorphism of E over k takes E^s to itself, so we may reduce to the case where $k = E^s$, i.e. E/k is totally inseparable. But then there are no non-trivial automorphisms.

(b) In this case, the norm map for $\mathbf{F}_{p^r}/\mathbf{F}_p$ is given by

$$x \mapsto x \cdot x^p \cdot x^{p^2} \cdot \ldots \cdot x^{p^{r-1}} = x^{1+p+\ldots+p^{r-1}} = \frac{x^{p^r}-1}{x-1}.$$

Hence, for any $\alpha \in \mathbf{F}_p$ we want to solve $x^{1+p+\ldots+p^{r-1}} = \alpha$ in $\mathbf{F}_{p^r}$. The map $x \mapsto x^{1+p+\ldots+p^{r-1}}$ sends $(\mathbf{F}_{p^r})^\times \to (\mathbf{F}_p)^\times$ with kernel of size at most p^{r-1}, hence is surjective by looking at the orders of the groups.

(c) $\mathbf{C}/\mathbf{R}$.

6. Fall 2012 A7

(i) If $X^q - b$ is reducible, then a is a root of some factor $f(X)$ that properly divides $X^q - b$, hence $[E':E] < q$. Conversely, if $[E':E] < q$ then $1, a, \ldots, a^{[E':E]}$ satisfy a linear dependence, hence a is the root of a polynomial $f(X)$ properly dividing $X^q - b$.

Suppose $[E' : E] = d < q$, applying $\mathrm{Nm}_{E'/E}$ to the equation $a^q = b$ gives

$$\mathrm{Nm}(a)^q = \mathrm{Nm}(b) = b^d.$$

Since $(d, q) = 1$, we may pick e such that $ed \equiv 1 \pmod q$, so that

$$\mathrm{Nm}(a^e)^q = b^{de} = b \cdot (b^q)^n.$$

Hence b has a qth root in E, say a'. Then $(a/a')^q = 1$ with $a/a' \in E' - E$, so it is a primitive qth roof of 1.

(ii) Since K is Galois over E, every E-embedding $K \hookrightarrow \overline{E}$ lands in K. Hence every E'-embedding $KE' \hookrightarrow \overline{E}$ lands in KE', therefore KE'/E' is Galois. It is obviously non-trivial of degree at most p, so it has degree exactly p. The restriction map $\mathrm{Gal}(KE'/E') \to \mathrm{Gal}(K/E)$ is evidently injective, but since both sides have size p it must be an isomorphism.

(iii) Supposing such an embedding exist, with the radical extension being

$$E \hookrightarrow E_1 \hookrightarrow E_2 \hookrightarrow \ldots \hookrightarrow E_n.$$

We may assume that $[E_i : E_{i-1}]$ is prime, by the structure of radical extensions. If i is maximal such that K cannot be embedded into E_i, then after replacing K/E by KE_i/E_i, we may assume that $[K : E]$ is the qth root of $b \in E_i$, for q a prime. Then we can apply (i), which tells us that since E_{i+1} cannot contain odd order roots of unity (since it's a subfield of $\mathbf{R}$), we must have $[E_{i+1} : E_i] = q$. But then there are no proper subextensions between E_i and E_{i+1}, which forces the embedding $K \hookrightarrow E_{i+1}$ to be an isomorphism, contradicting the fact that the extension $E_i(\sqrt[q]{b})/E_i$ is visibly not Galois.

7. Spring 2014 A3

(i) The identification is via $\mathrm{Aut}(\mu_p) \cong \mathrm{Aut}(\mathbf{Z}/p) \cong (\mathbf{Z}/p)^*$.

For $k = \mathbf{Q}$, we have to show that $[\mathbf{Q}(\zeta_p) : \mathbf{Q}] = p - 1$. This follows from the irreducibility of the cyclotomic polynomial $\frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \ldots + 1$. [Why is this true?]

8. Spring 2010 A1

As a general fact about finding Galois extensions, recall that if E/F is Galois with Galois group G, then for any normal subgroup $H \subset G$, E^H/F is Galois with Galois group G/H.

Now, we want to find $\mathbf{Z}/3$ as a quotient of $\mathrm{Gal}(\mathbf{Q}(\zeta_n)/\mathbf{Q}) \cong (\mathbf{Z}/n)^*$. The first place to look is at $n = 7$, and we want $K = \mathbf{Q}(\zeta_n)^{\mathbf{Z}/2\mathbf{Z}}$. The nontrivial element of $\mathbf{Z}/2\mathbf{Z}$-action takes $\zeta_n \mapsto \zeta_n^{-1}$, so K is generated by

$$\zeta_7^1 + \zeta_7^6, \zeta_7^2 + \zeta_7^5, \zeta_7^3 + \zeta_7^4.$$

The element $\zeta_7^1 + \zeta_7^6$ generates [why?] so we have to find a minimal polynomial for it. Expand out $1, (\zeta_7^1 + \zeta_7^6), (\zeta_7^1 + \zeta_7^6)^2$ and find a linear combination using the minimal polynomial for ζ_7.

9. Fall 2010 M4

(i) For the irreducibility use Eisenstein's criterion. The Galois group is a subgroup of S_3, so we just have to see that it is large enough. Adjoining the real cube root of 2 makes a cubic extension $L/\mathbf{Q}$ that can be embedded into $\mathbf{R}$, hence it cannot be the full splitting field (since that contains 3rd roots of unity, for example). So the splitting field has degree at least 6, hence must be all of S_3.

(ii) The non-trivial subgroups of S_3 are the three copies of $\mathbf{Z}/2\mathbf{Z}$ generated by the three transpositions, and the copy of $\mathbf{Z}/3\mathbf{Z}$ generated by a 3-cycle.

Let the three roots of f be called $\alpha, \beta, \overline{\beta}$. The cubic extensions corresponding to the three transpositions correspond to adjoining one of the these roots.

For the quadratic extension, adjoin the square root of the discriminant, i.e.

$$(\alpha-\beta)(\alpha-\overline{\beta})(\beta-\overline{\beta}).$$

(iii) Find the smallest power of Frobenius which is trivial on $k[X]/(X^3-2)$.

10. Fall 2011 A5

(1) Since f is an irreducible quartic, we have $4 \mid |G|$. On the other hand, f is evidently split by a degree 8 extension, obtained by adjoining the roots of $Y^2 + aY + b$, and then the square roots of each of those roots.

If $|G| = 4$, then any non-identity element fixing a root must be a transposition. So then $G \cong \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. But one cannot add another transposition to make a group of order 4 that acts transitively.

For future use, we note that the other possibilities for G are a cyclic group of order 4, and the dihedral group of order 8.

(2) Label the roots $\alpha, \beta, \gamma, \delta$ such that G is generated by transpositions $(\alpha\, {-\alpha})(\beta\, {-\beta})$ and $(\alpha\ \beta)(-\alpha\ -\beta)$. Then $b = \alpha^2\beta^2$, and by inspection $\alpha\beta$ is preserved by the Galois group, hence lies in $\mathbf{Q}$.

Conversely, since the other possibilities for G contain a 4-cycle, they do not preserve $\alpha\beta$ so b is not a square in $\mathbf{Q}$.

(3) Note that $a = \alpha^2 + \beta^2$ and $b = \alpha^2\beta^2$, so

$$\frac{a^2-4b}{b} = \frac{(\alpha^2-\beta^2)^2}{\alpha^2\beta^2}.$$

One can check that $\frac{\alpha-\beta}{\alpha\beta}$ is preserved by 4-cycles, but not by the swap $(\alpha\ \beta)(-\alpha - \beta)$ which exists in the other possibilities.