Éléments de correction de l'examen de session 1

Exercice 1.

1. $P(X) = (X^3-5)(X^3+5)$ et $X^3 \pm 5$ est 5-Eisenstein donc irréductible sur $\mathbb{Q}$.
2. Chaque facteur irréductible de $P(X)$ sur $\mathbb{Q}$ convient : K est engendré sur $\mathbb{Q}$ par les racines de $P(X)$, réunion des racines de X^3-5 et de X^3+5, or si α est racine d'un de ces polynômes alors $-\alpha$ est racine de l'autre. En conclusion les racines de l'un ou l'autre des polynômes$X^3 \pm 5$ engendre K sur $\mathbb{Q}$. Ainsi K est corps de décomposition de chaque polynôme $X^3 \pm 5$.
3. Les racines complexes de X^3-5 sont les $\omega^j \sqrt[3]{5}$ ($j = 0, 1, 2$). Donc $K \subset \mathbb{Q}(\omega, \sqrt[3]{5})$. Réciproquement $\sqrt[3]{5}$ est une racine de X^3-5 donc est élément de K, et ω est quotient des racines $\omega^2\sqrt[3]{5}$ et $\omega\sqrt[3]{5}$, donc est élément de K.
4. Comme K est corps de décomposition de X^3-5 à racines simples sur $\mathbb{Q}$, on déduit que $K/\mathbb{Q}$ est une extension galoisienne. Le groupe $G = \mathrm{Gal}(K/\mathbb{Q})$ agit trivialement sur les coefficients de X^3-5 et donc permute les racines de ce polynôme. Cela définit un morphisme
$$\mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Sym}(\{\omega^j \sqrt[3]{5} \colon 0 \leq j \leq 2\}) \simeq \mathcal{S}_3\,,$$
qui est injectif, car $K^G = \mathbb{Q}$.
5. Notons $M = \mathbb{Q}(\sqrt[3]{5})$. On a $\mathbb{Q} \subset M \subset K$ et $[M : \mathbb{Q}] = 3 = \deg\ X^3-5$. Comme $M \subset \mathbb{R}$ et $K \not\subset \mathbb{R}$, on a $M \neq K$. Donc $[K : M] \geq 2$, mais ω est de degré 2 sur $\mathbb{Q}$ donc de degré ≤ 2 sur M. On conclut que $[K : M] = 2$ puis, par multiplicativité des degrés, que $[K : \mathbb{Q}] = 6$. Ainsi $\mathrm{Gal}(K/\mathbb{Q})$ s'injecte dans $\mathcal{S}_3$ et est d'ordre 6, donc $\mathrm{Gal}(K/\mathbb{Q}) \simeq \mathcal{S}_3$.
6. Un $\mathbb{Q}(\sqrt[3]{5})$-automorphisme de K est entièrement déterminé par sa valeur en ω. L'image par ω d'un tel morphisme est une racine de X^2+X+1 (polynôme minimal de ω sur M d'après la question précédente) et tout choix d'une telle racine donne bien lieu à un $\mathbb{Q}(\sqrt[3]{5})$-automorphisme de K. Ainsi il existe un $\mathbb{Q}(\sqrt[3]{5})$-automorphisme de K (en particulier élément de G) vérifiant les deux propriétés demandées pour τ. On fait le même raisonnement pour construire un $\mathbb{Q}(\omega)$-automorphisme de K satisfaisant les propriétés demandées pour σ.
7. Si $\theta \in G$ alors θ fixe les coefficients de X^3-5 donc doit envoyer $\sqrt[3]{5}$ sur une racine de X^3-5, ce qui n'est pas le cas. Il n'y a donc pas d'élément de G vérifiant la propriété demandée.
8. (a) On sait que $[K : K^H] = |H|$. On a $\sigma\tau(\omega) = \sigma(\omega^2) = \omega^2$ donc $\sigma\tau \neq 1$. Comme $\sigma\tau(\omega^2) = \sigma(\omega^4) = \sigma(\omega) = \omega$ et $(\sigma\tau)^2(\sqrt[3]{5}) = \sigma\tau(\omega\sqrt[3]{5}) = \sigma(\omega^2\sqrt[3]{5}) = \sqrt[3]{5}$, on déduit que $|H| = 2$. Ainsi $[K : K^H] = 2$ puis $[K^H : \mathbb{Q}] = 3$. Enfin $\omega^2\sqrt[3]{5}$ est de degré 3 sur $\mathbb{Q}$ de polynôme minimal X^3-5 et :
$$\sigma\tau(\omega^2\sqrt[3]{5}) = \sigma(\omega\sqrt[3]{5}) = \omega^2\sqrt[3]{5}\,.$$
On conclut que $K^H = \mathbb{Q}(\omega^2\sqrt[3]{5})$.
   (b) $K^H/\mathbb{Q}$ n'est pas galoisienne. On le voit soit en remarquant que $\mathbb{Q}(\omega^2\sqrt[3]{5})/\mathbb{Q}$ n'est pas normale (puisque X^3-5 a une unique racine dans $\mathbb{Q}(\omega^2\sqrt[3]{5})$), soit en invoquant la correspondance de Galois et en remarquant qu'il n'y a pas de sous-groupe distingué d'ordre 2 dans $\mathcal{S}_3$.

Exercice 2.

1. (a) Comme $k \subset k'$, on peut voir k' comme un k espace vectoriel. L'extension k'/k est par hypothèse finie donc $r := \dim_k k' < \infty$. On déduit immédiatement (en fixant une k-base de k' par exemple) que $|k'| = |k|^r = q^r$.
   (b) Le polynôme $f(X) = X^{q^r} - X \in k[X]$ est scindé sur k' (d'après Lagrange dans le groupe $(k')^\times$) et les racines de f (qui constituent le corps k') engendrent k'/k. Aussi $f'(X) = -1$ (car q est une puissance de la caractéristique de k) de sorte que f est premier à son poynôme dérivé dans $k[X]$ et donc à racines simples dans l'extension k' de k.

(c) Soit α un générateur du groupe $(k')^\times$. L'ordre de α est q^r-1 donc $\alpha^s \neq 1$ si $s < q^r-1$. Comme $\alpha \neq 0$, cela implique $\sigma^{s'}(\alpha) = \alpha^{q^{s'}} \neq \alpha$ si $s' < r$. Ainsi σ est d'ordre au moins r ; il est donc d'ordre exactement r d'après la question (b).

(d) k' est corps de décomposition d'un polynôme à racines simples sur le corps fini k, donc k'/k est galoisienne. Son groupe de Galois G est d'ordre $[k' : k] = r$. Or $\sigma \in G$ (c'est un automorphisme du corps fini k' qui fixe k) est également d'ordre r. On déduit que $G = \langle\sigma\rangle$ est cyclique.

2. (a) Par définition $\sigma(\alpha) = \alpha^q$; or $f(\alpha) = 0$ donc $\sigma(\alpha) = \alpha + 1$. Plus généralement $\sigma^i(\alpha) = \alpha + i$: soit $i \geq 2$, alors $\sigma^i(\alpha) = \sigma(\alpha + i) = \sigma(\alpha) + \sigma(i) = \alpha + (i-1) + 1$, par hypothèse de récurrence et puisque $\mathbb{Z}/p\mathbb{Z}$, sous-corps de k est fixé par σ. En particulier $\sigma^p(\alpha) = \alpha$, puisque k est de caractéristique p. Comme α est une racine arbitraire de f et que k_f est engendré par les racines de f sur k, on conclut $\sigma^p = \mathrm{Id}$. (Plus précisément, σ est d'ordre p.)

(b) Soit α une racine de f dans k_f et g_α son polynôme minimal sur k. On sait que le degré de g_α est égal au cardinal de l'orbite de α sous l'action de $\mathrm{Gal}(k_f/k) = \langle\sigma\rangle$ (cf. question 1, pour le fait que σ engendre le groupe de Galois). D'après la question précédente cette orbite est $\{\alpha + i \colon 0 \leq i \leq p-1\}$. Comme $\alpha + i \neq \alpha + j$ si $i \neq j$ dans $\mathbb{Z}/p\mathbb{Z}$, on conclut que l'orbite considérée est de cardinal p. Ce raisonnement vaut pour toute racine de f dans k_f, et donc tout facteur irréductible de f dans $k[X]$ est de degré p.

(c) D'après (b), chaque facteur irréductible de f sur k est de degré p. Fixons un tel facteur irréductible ; son corps de rupture L est de degré p sur k et s'injecte dans k_f. Or, on a vu en (a) que $[k_f : k] = p$. Donc L est isomorphe à k_f.

Exercice 3.

1. (a) L'action de G sur Y étant transitive, il existe $g_0 \in G$ tel que $y' = g_0 y$. Alors l'application

$$f^{-1}(y) \to f^{-1}(y')\,, \qquad x \mapsto g_0 x$$

est bien définie d'après $(\star)$ et est clairement bijective.

(b) Il suffit de remarquer que X est réunion disjointe des parties $f^{-1}(y)$, où y parcourt Y. D'après (a), on déduit que $|X| = k|Y|$ où k est le cardinal commun aux $f^{-1}(y)$, $y \in Y$.

2. (a) C'est une propriété du cours : $P \cap N$ est un p-sous-groupe de N. Aussi PN est un sous-groupe de G car $N \triangleleft G$ et (par application du 2nd théorème d'isomorphisme) $|PN| = |P| \cdot |N|/|P \cap N|$ donc $(N : P \cap N) = (PN : P)$ qui est premier à P. Donc $P \cap N$ est un p-Sylow de N.

(b) Comme $N \triangleleft G$, le groupe G agit bien par conjugaison sur les p-Sylow de N. Pour tout $g \in G$, on a, avec les mêmes notations qu'en (a), $g(P \cap N)g^{-1} = (gPg^{-1}) \cap N$, car $N \triangleleft G$.

(c) Par Sylow, l'action par conjugaison de N (*a fortiori* celle de G) sur l'ensemble des p-Sylow de N est transitive. On peut donc appliquer la question 1 et conclure que $n_p(N) \mid n_p(G)$.

Pour $\mathcal{A}_4$, comme pour $\mathcal{A}_5$, les 3-Sylow sont engendrés par les 3-cycles. En prenant garde qu'un 3-cycle et son inverse engendrent le même 3-Sylow, on obtient $n_3(\mathcal{A}_5) = ((5 \times 4 \times 3)/3)/2 = 10$ et $n_3(\mathcal{A}_4) = ((4 \times 3 \times 2)/3)/2 = 4$. Bien que $\mathcal{A}_4$ s'injecte dans $\mathcal{A}_5$ (de manière non-unique), on a $n_3(\mathcal{A}_4) \nmid n_3(\mathcal{A}_5)$. Cela illustre la simplicité de $\mathcal{A}_5$: aucune copie de $\mathcal{A}_4$ ne peut être distinguée dans $\mathcal{A}_5$.