ALGEBRA QUALIFYING EXAM 2

(1) Let p be an odd prime number, and let $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ be a primitive pth root of unity. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ and recall the isomorphism $\chi : G \to (\mathbb{Z}/p\mathbb{Z})^\times$ determined by $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for $\sigma \in G$. For $i \in (\mathbb{Z}/p\mathbb{Z})^\times$, let $\sigma_i = \chi^{-1}(i) \in G$.

Let $H \subset G$ be the index two subgroup and let $S \subset (\mathbb{Z}/p\mathbb{Z})^\times$ be the set of squares, so that $\chi(H) = S$. Let $N = (\mathbb{Z}/p\mathbb{Z})^\times - S$ be the set of non-squares. Let $\alpha \in \mathbb{Q}(\zeta)$ be the element

$$\alpha = \sum_{\sigma \in H} \sigma(\zeta) = \sum_{i \in S} \zeta^i$$

and let $\beta \in \mathbb{Q}(\zeta)$ be the element

$$\beta = \sum_{j \in N} \zeta^j.$$

(a) Show that $\alpha + \beta = -1$ and that α and β are fixed by H.
(b) Show that, if $\tau \in G - H$, then $\tau(\alpha) = \beta$ and $\tau(\beta) = \alpha$. Deduce that $\alpha\beta \in \mathbb{Q}$.
(c) Show that

$$\alpha\beta = \sum_{j \in N} \sum_{i \in S} \zeta^{i+ij}.$$

(d) Use the previous formula to compute which rational number $\alpha\beta$ is. (Hint: the answer will depend on whether $-1 \in S$ or $-1 \in N$.)
(e) Note that $[\mathbb{Q}(\zeta)^H : \mathbb{Q}] = 2$, so $\mathbb{Q}(\zeta)^H = \mathbb{Q}(\sqrt{d})$ for some squarefree d. What is d?

(2) Let p be a prime number and let $f(x) \in \mathbb{Q}[x]$ be an irreducible polynomial of degree p. Let F_f be the splitting field of f in $\mathbb{C}$. Suppose that $f(x)$ has $p-2$ real roots and 2 non-real roots in $\mathbb{C}$. Show that the Galois group $\mathrm{Gal}(F_f/\mathbb{Q})$ is S_p.

For the next two questions, let R be a Noetherian commutative ring.

(3) Let M be an R-module and assume that there is an isomorphism

$$\phi : R \to M \otimes_R N$$

for some R-module N.
(a) Show that M is finitely generated (Hint: write $\phi(1) = \sum_{i=1}^n x_i \otimes y_i$ with $x_i \in M$ and $y_i \in N$ and show that $x_1, \ldots, x_n$ generate M as an R-module.)
(b) Show that $M_\mathfrak{m} \cong R_\mathfrak{m}$ as $R_\mathfrak{m}$-modules for every maximal ideal $\mathfrak{m} \subset R$.

(4) Assume that R is an integral domain, and let M be an injective R-module.
(a) Show that M is divisible. That is, show that for any $m \in M$ and any $r \in R$, there is an $m' \in M$ such that $m = rm'$.
(b) Now suppose that M is non-zero and finitely generated. Show that R is a field. (Hint: show that $M_\mathfrak{m} = 0$ for all non-zero maximal ideals $\mathfrak{m} \subset R$.)