## Assignment 4

September 4, 2015

Problem 1. Are the fields

$$
\frac{\mathbb{F}_{2}[X]}{\left(X^{3}+X^{2}+1\right)} \quad \text { and } \quad \frac{\mathbb{F}_{2}[Y]}{\left(Y^{3}+Y+1\right)}
$$

isomorphic? Can you construct such an isomorphism? (hint ${ }^{1}$ )
Problem 2. Find the degree of the splitting field of $\left(X^{2}-2\right)\left(X^{2}-3\right)$ over $\mathbb{Q}$.
Problem 3. Write down a polynomial over $\mathbb{Q}$ whose splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. What can you say about $\operatorname{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) / \mathbb{Q})$ ?

Problem 4. Prove that $\alpha_{1}, \ldots \alpha_{n} \in E$ for some field extension $E / F$. Prove that

$$
F\left(\alpha_{1}, \ldots, \alpha_{n}\right)=\left\{\left.\frac{f\left(\alpha_{1}, \ldots, \alpha_{n}\right)}{g\left(\alpha_{1}, \ldots, \alpha_{n}\right)} \right\rvert\, f, g \in F\left[X_{1}, \ldots, X_{n}\right] \text { and } g\left(\alpha_{1}, \ldots, \alpha_{n}\right) \neq 0 \in E\right\} .
$$

Problem 5. Prove that if $f(X) \in F[X]$ is a polynomial over a field $F$, and $E / F$ is a splitting field of $f$, and if $\alpha_{1}, \ldots, \alpha_{n}$ are the roots of $f$ in $E$, then $E=F\left(\alpha_{1}, \ldots, \alpha_{n}\right)$.

Problem 6. If $R$ is a ring and if $c \in R$, prove that the map

$$
\psi_{c}: R[X] \rightarrow R[X]
$$

given by $\left(\psi_{c}(f)\right)(X)=f(X+c)$ is an isomorphism and conclude that in the case $R$ is a field, $p(X)$ is irreducible iff $\psi_{c}(p)$ is irreducible.

Problem 7. Let $p(X)$ be a monic polynomial in $\mathbb{Z}[X]$. Prove that any rational root of $p$ has to be an integer. (hint ${ }^{2}$ )

Problem 8. Suppose $f(X) \in F[X]$ be an irreducible polynomial of degree $n$. Let $E / F$ be the splitting field of $f(X)$. Prove that $n \mid[E: F]$. If $f$ is separable, prove that $n \mid \operatorname{Gal}(E / F)$.

[^0]
[^0]:    ${ }^{1}$ Hint: $\quad X \mapsto Y+1$.
    ${ }^{2} H$ int: Prove that if $r / s$ is a root of $p(X)=a_{0}+a_{1} X+\cdots+a_{k} X^{k}$, then $r \mid a_{0}$ and $s \mid a_{k}$.

