1 Let $F \subseteq K$ be a field extensions, $F[X] \subseteq K[X]$ the corresponding polynomial rings, and $f, g \in F[X]$ nonzero polynomials. Show that $g \mid f$ in $F[X]$ if and only if $g \mid f$ in $K[X]$.

Proof. Since $F[X]$ is a subring of $K[X]$, divisibility in $F[X]$ is simply a special case of divisibility in $K[X]$.

Suppose $g \mid f$ in $K[X]$, i.e., there exists $h \in K[X]$ such that $f = gh$ in $K[X]$. The result is trivial if any of the three polynomials is zero, so we assume all are nonzero. Suppose a, b, c are the leading coefficients of f, g, h, respectively. We know that $a, b \in F$ and $c \in K$. Since the leading coefficient of the product of polynomials is the product of the leading coefficients, we have $a = bc$, which implies $c = b^{-1}a \in F$. That is, the leading coefficient of h is in F.

We prove, by induction on the degree of h, that all the coefficients of h must be in F. For the base case, when $\deg h = 0$, we have $h = c \in F$. For the inductive step, assume that the result holds whenever the degree of h is less than some $n > 0$, i.e., the following holds:

$$f, g \in F[X],\ h \in K[X],\ f = gh \text{ in } K[X],\ \deg h < n \quad \implies \quad h \in F[X].$$

Assume f, g, h are as in the hypothesis, but $\deg h = n$. Write $h = cX^n + h_0$, where cX^n is the leading term of h and h_0 is the sum of the remaining terms. In particular, $h_0 \in K[X]$ with $\deg h_0 < \deg h = n$. We now have

$$f = gh = g(cX^n + h_0) = cX^n g + gh_0,$$

then define

$$\tilde{f} = f - cX^n g = gh_0.$$

We have shown above that $c \in F$, which implies $\tilde{f} \in F[X]$. Applying the inductive hypothesis to $\tilde{f}, g, h_0$, we conclude that $h_0 \in F[X]$. Since the coefficients of h consist of its leading coefficient, c, and the coefficients of h_0, we conclude all the coefficients of h are in F, hence $h \in F[X]$. $\square$

2 Let $a := \sqrt[4]{3} \in \mathbb{R}_{>0}$. Show that

(a) Neither a nor i lies in $\mathbb{Q}(ai)$.

Proof. We first note that it suffices to prove that $a \notin \mathbb{Q}(ai)$, since $i \in \mathbb{Q}(ai)$ implies $a = ai \cdot i^{-1} \in \mathbb{Q}(ai)$.

Denote the polynomial $f = X^4 - 3 \in \mathbb{Q}[X]$, which is irreducible by Eisenstein's criterion. Since f is monic and irreducible with ai as a root, it must be the minimal polynomial of ai over $\mathbb{Q}$. Therefore,

$$[\mathbb{Q}(ai) : \mathbb{Q}] = \deg p_{ai,\mathbb{Q}} = \deg f = 4.$$

By the same argument, $[\mathbb{Q}(a) : \mathbb{Q}] = 4$.

Assume for contradiction that $a \in \mathbb{Q}(ai)$. Then we have a tower $\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq \mathbb{Q}(ai)$, so the tower rule gives us

$$[\mathbb{Q}(ai) : \mathbb{Q}(a)] = \frac{[\mathbb{Q}(ai) : \mathbb{Q}]}{[\mathbb{Q}(a) : \mathbb{Q}]} = \frac{4}{4} = 1.$$

It follows that $\mathbb{Q}(a) = \mathbb{Q}(ai)$, but this is a contradiction since the former consists entirely of real elements, while the latter contains the imaginary element ai. We conclude that a does not lie in $\mathbb{Q}(ai)$.

Note that $i \in \mathbb{Q}(ai)$ implies $a = ai \cdot i^{-1} \in \mathbb{Q}(ai)$, so the contrapositive tells us $i \notin \mathbb{Q}(ai)$. $\square$

(b) The minimal polynomial of a over $\mathbb{Q}(i)$ is $X^4 - 3$.

Proof. Since a is a root of $X^4 - 3$, the minimal polynomial of a over $\mathbb{Q}(i)$ divides $X^4 - 3$, so

$$\deg p_{a,\mathbb{Q}(i)} \leq \deg(X^4 - 3) = 4.$$

It remains to prove that $\deg p_{a,\mathbb{Q}(i)} = 4$.

The complex roots of $X^2 + 1$ are $\pm i$; neither is real, so the polynomial is irreducible over $\mathbb{R}$. In particular, $X^2 + 1$ is irreducible over $\mathbb{Q}(a)$, since $\mathbb{Q}(a)$ is contained in $\mathbb{R}$. Therefore, $X^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(a)$ and we calculate

$$[\mathbb{Q}(a, i) : \mathbb{Q}(a)] = \deg p_{i,\mathbb{Q}(a)} = \deg(X^2 + 1) = 2.$$

By the same argument, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$.

Applying the tower rule to $\mathbb{Q} \subseteq \mathbb{Q}(a) \subseteq \mathbb{Q}(a, i)$, we obtain

$$[\mathbb{Q}(a, i) : \mathbb{Q}] = [\mathbb{Q}(a, i) : \mathbb{Q}(a)][\mathbb{Q}(a) : \mathbb{Q}] = 2 \cdot 4 = 8.$$

Lastly, applying the tower rule to $\mathbb{Q} \subseteq \mathbb{Q}(i) \subseteq \mathbb{Q}(a, i)$ gives

$$\deg p_{a,\mathbb{Q}(i)} = [\mathbb{Q}(a, i) : \mathbb{Q}(i)] = \frac{[\mathbb{Q}(a, i) : \mathbb{Q}]}{[\mathbb{Q}(i) : \mathbb{Q}]} = \frac{8}{2} = 4.$$

We conclude that $X^4 - 3$ is a monic polynomial divisible by and having the same degree as the minimal polynomial $p_{a,\mathbb{Q}(i)}$, so in fact $p_{a,\mathbb{Q}(i)} = X^4 - 3$. $\square$

3 Let $F \subseteq K = F(a)$ be a simple algebraic field extension such that the minimal polynomial of a over F has degree p^m for some odd prime p and some $m > 0$. Show that $F(a^i) = K$ for all $i = 2, \dots, p-1$.

Proof. Fix some $i \in \{2, \dots, p-1\}$. Since $a^i \in K$, we have a tower $F \subseteq F(a^i) \subseteq K$. Then

$$p^m = \deg p_{a,F} = [K : F] = [K : F(a^i)][F(a^i) : F].$$

Since p is prime, it follows that

$$\deg p_{a^i,F} = [F(a^i) : F] = p^n,$$

for some $0 < n \leq m$. Define the polynomial $f = p_{a^i,F}(X^i) \in F[X]$, which has degree ip^n. Then a is a root of f, so $p_{a,F}$ divides f. In particular,

$$p^m = \deg p_{a,F} \leq \deg f = ip^n < p^{n+1},$$

so $m \leq n$, hence $n = m$. We then calculate

$$[K : F(a^i)] = \frac{[K : F]}{[F(a^i) : F]} = \frac{p^m}{p^n} = 1,$$

which implies $F(a^i) = K$.

$\square$

4

Lemma 1. For nonnegative integers M, N, P with $M \leq N$, we have

$$\frac{N!}{M!} \leq \frac{(N+P)!}{(M+P)!}.$$

Proof. We perform induction on P. For the base case, note that $(M+1)/(N+1) \leq 1$, so

$$\frac{N!}{M!} = \frac{(N+1)!/(N+1)}{(M+1)!/(M+1)} = \frac{(N+1)!}{(M+1)!} \cdot \frac{M+1}{N+1} \leq \frac{(N+1)!}{(M+1)!}.$$

Assuming the result holds for $P-1$, we find

$$\frac{N!}{M!} \leq \frac{(N+P-1)!}{(M+P-1)!} \leq \frac{(N+P)!}{(M+P)!},$$

where the second inequality is an application of the base case. $\square$

Let $F \subseteq K$ be a field extension, $f \in F[X]$ a polynomial with degree $n > 0$, and r the number of distinct roots of f in K. Assume that K is a splitting field for f over F. Show that $[K : F] \leq n!/(n-r)!$.

Proof. Write $K = F(a_1, \ldots, a_r)$, where the a_i's are the distinct roots of f in K. Let $m_i \in \mathbb{Z}_{>0}$ be the multiplicity of a_i in f, then in $K[X]$ we can write

$$f = \prod_{i=1}^{r} (X - a_i)^{m_i}.$$

To prove the inequality, we perform induction on r.

When $r = 1$, we have $f = (X-a)^n$ with $a = a_1$. Then a is a root of f, so the minimal polynomial of a over F divides f, thus

$$[K : F] = [F(a) : F] = \deg p_{a,F} \leq \deg f = n = \frac{n!}{(n-1)!}.$$

For the inductive step, assume the result hold in any case that the number of distinct roots is at most than $r-1$. Define the polynomial

$$g = \prod_{i=1}^{r-1} (X - a_i)^{m_i} \in K[X],$$

then $f = (X - a_r)^{m_r} g$ in $K[X]$. Both f and $(X - a_r)^{m_r}$ are in $F(a_r)[X]$, so Problem 1 tells us that g is also in $F(a_r)[X]$. Moreover, g is of degree $n - m_r$ and has $r-1$ distinct roots in K, so the inductive hypothesis gives us

$$[K : F(a_r)] \leq \frac{(n-m_r)!}{(n-m_r-(r-1))!} \leq \frac{(n-1)!}{(n-r)!},$$

where the second inequality is an application of Lemma 1 with $P = m_r - 1$. Similar to the base case, the minimal polynomial of a_r over F divides f, so

$$[F(a_r) : F] = \deg p_{a_r,F} \leq \deg f = n.$$

Combining these inequalities with the tower rule, we obtain

$$[K : F] = [K : F(a_r)][F(a_r) : F] \leq \frac{(n-1)!}{(n-r)!} \cdot n = \frac{n!}{(n-r)!}.$$

$\square$