I'll start with restatement and proofs of two result from the last week.

Quotient rings Let A be a commutative ring, $I \subset A$ an ideal. We define an equivalence relation on A by saying $a \equiv b$ if $a - b \in I$ and denote by A/I the corresponding set of equivalence classes. We denote by $a \to \bar{a}$ the map $A \to A/I$ assigning to any $a \in A$ the equivalence class $a + I \in A/I$.

Claim. a)

i) if $a \equiv a', b \equiv b'$ then $a + b \equiv a' + b'$ and $ab \equiv a'b'$,

ii) there exists operations $+ : A/I \times A/I \to A/I$ and $\times : A/I \times A/I \to A/I$ such that for any $a, b \in A$ we have

$$\overline{a+b} = \bar{a} + \bar{b}, \overline{ab} = \bar{a} \times \bar{b}$$

iii) $A/$ with operations $+ : A/I \times A/I \to A/I$ and $\times : A/I \times A/I \to A/I$, unit $= \bar{1}$ and zero $= \bar{0}$ has a structure of a commutative ring.

b) The quotient ring A/I is a field iff I is a maximal proper [that is different from A] ideal of A.

The proof of a) assigned as the Problem 3.8.

Proof of b). Let $\alpha \in A/I$ be a non-zero element. We want to prove the existence of $\beta \in A/I$ such that $\alpha \times \beta = 1$.

Let $\bar{J} \subset A/I$ be the set of elements of the form $\alpha \times \beta, \beta \in A/I$. It is clear that $\bar{J} \subset A/I$ is an ideal. We want to show that $\bar{J} = A/I$.

Let $J =: \{a \in A | \bar{a} \in \bar{J}\}$. It is clear that J is an ideal of A such that $J \supsetneqq I$. Since I is a maximal ideal of A we see that $J = A$. But this implies that $\bar{J} = A/I$.$\square$

Corollary. If $p(t) \in K[t]$ is an irreducible polynomial then the quotient ring is a field. It is sufficient to show that for any irreducible polynomial $p(t) \in K[t]$ the ideal $(p(t)) \subset K[t]$ is maximal.

I'll leave a proof of this result as a homework problem.

Lemma 3.1. Let $L \supset K$ be field extension, $\alpha_1, ..., \alpha_n \in L$ a sequence of elements algebraic over K. Then $[K(\alpha_1, ..., \alpha_n) : K] < \infty$.

Proof. We prove Lemma by the induction in n. We want to show that $[K(\alpha_1, ..., \alpha_n) : K] < \infty$. Let $F := K(\alpha_1, ..., \alpha_{n-1}) \subset L$. By the inductive assumption we know that $[F : K] < \infty$. $G := F(\alpha_n) \subset L$. Since $\alpha_i \in G, 1 \leq i \leq n$ we have $K(\alpha_1, ..., \alpha_n) \subset G$. So it is sufficient to show that $[G : K] < \infty$.

Since $\alpha_n \in G$ is algebraic over K then by Theorem 1.2 there exists a non-zero polynomial $p(t) \in K[t]$ such that $p(\beta) = 0$. Therefore β is also algebraic over F [you can use the same polynomial $p(t)$] and we see that $[G : F] < \infty$. It follows from the Product formula [Theorem 1.1] that $[G : K] < \infty$.□

Remark. It is not difficult to show that $K(\alpha_1, ..., \alpha_n) = G$.

Definition 3.1. Let $L \supset K$ be a field extension and $\alpha \in L$ an element algebraic over K. We denote by $Irr(\alpha, K, t) \in K[t]$ the irreducible monic polynomial $p(t)$ such that $p(\alpha) = 0$ [See Problem 1.2]. We say that $p(t)$ is *the minimal polynomial* of α over K.

The splitting field.

Definition 3.2. Let K be a field, $p(t) \in K[t]$ a monic polynomial. An extension $L \supset K$ is called a *splitting field* of $p(t)$ if
i) $p(t) = (t - a_1)(t - a_2...)(t - a_n), a_i \in L, 1 \leq i \leq n$
and
ii) $L = K(a_1, ..., a_n)$

Lemma 3.2. Any monic polynomial $p(t) \in K[t]$ of positive degree has a splitting field $F \supset K$.

Proof. As you have shown [problem 2.5] there exists a field $L \supset K$ such that $p(t)$ can be written in the form
$p(t) = (t - a_1)(t - a_2...)(t - a_n), a_i \in L, 1 \leq i \leq n$
So we can take $F = K(a_1, ..., a_n)$□.

Now we show that the splitting field is essentially unique.

Definition 3.2. a) Let K, K' be fields and $\eta : K \to K'$ a map. We say that η is a homomorphism if
$\eta(1) = 1, \eta(a + b) = \eta(a) + \eta(b), \eta(ab) = \eta(a)\eta(b)$,

b) if $p(t) = \sum_{i=0}^n c_i t^i \in K[t]$ is a polynomial we define

$$\eta(p(t)) := \sum_{i=0}^n c'_i t^i \in K'[t], c'_i := \eta(c_i)$$

and say that $\eta(p(t))$ is the image of $p(t)$ in $K'[t]$.

Theorem 3.1. Let $\eta : K \to K'$ be a field isomorphism, $q(t) \in K[t]$ a monic polynomial of positive degree, $q'(t) \in K'[t]$ the image of $q(t)$ and $L \supset K, L' \supset K'$ be splitting fields of $q(t)$ and $q'(t)$ respectively. Then the isomorphism $\eta : K \to K'$ can be extended to an isomorphism from L to L'.

We start with two lemmas.

Lemma 3.3. Let $\eta : K \to K'$ be K, K' be an isomorphism between fields, $L \supset K, L' \supset K'$ be field extensions and $\alpha \in L$ an algebraic element with the minimal polynomial $p(t)$. Then the extensions of η

to a homomorphism $\tilde{\eta} : K(\alpha) \to L'$ are in one-to-one correspondence with roots α' of $p'(t) := \eta(p(t))$ in L'.

Proof of Lemma. a) For any extension $\tilde{\eta} : K(\alpha) \to L'$ we define $\alpha'(\tilde{\eta}) := \tilde{\eta}(\alpha) \in L'$. It is clear that $\alpha'(\tilde{\eta}) \in L'$ is a root of $p'(t)$.

b) Conversely given a root α' of $p'(t)$ in L' consider a ring homomorphism $f' : K[t] \to L'$ such that $f'(t) = \alpha', f'(c) = \eta(c) \in K$.

As we have seen [Lemma 2.4] there exists unique ring epimorphism

$$f : K[t] \to K(\alpha)$$

such that Ker (f)=(p(t)), $f(t) = \alpha$ and $f(c) = c \in K$. Since $p'(\alpha') = 0$ we see that $f'(p(t)) = 0$. So $f'(q(t)) = 0$ for all $q(t) \in (p(t))$. Therefore the homomorphism f' induces a homomorphism $\tilde{\eta}(\alpha') : K(\alpha) \to L'$ which is an extension of η.

It is clear that the maps $\alpha' \to \tilde{\eta}(\alpha')$ and $\tilde{\eta} \to \alpha'(\tilde{\eta})$ define one-to-one correspondence between extensions of η to a homomorphism $\tilde{\eta} : K(\alpha) \to L'$ and roots α' of $p'(t)$ in L'.□

Lemma 3.4. Let $L \subset K$ be a field extension, $p(t) \in K[t]$ an irreducible polynomial of positive degree, $\alpha \in L$ a root of $p(t)$. Then L is a splitting field for $p(t)$ over K iff it is a splitting field for $p(t)$ over $K(\alpha)$.

I'll leave a proof of Lemma 3.4 as a homework problem.

Proof of Theorem. We will prove the theorem by the induction in the degree $[\tilde{L} : \tilde{K}]$ over all splitting fields $\tilde{L} \supset \tilde{K}$.

Consider first the case when $[L : K] = 1$. In this case all roots of $p(t)$ are in K. Therefore

$$p(t) = (t - \alpha_1)^{m_1} \times ... \times (t - \alpha_s)^{m_s}, 1 \leq i \leq s$$

where $\alpha_i \in K$ are roots of $p(t), m_i > 0$. Since η is a homomorphism we have

$$p'(t) = (t - \alpha'_1)^{m_1} \times ... \times (t - \alpha'_s)^{m_s}, 1 \leq i \leq s$$

where $\alpha'_i \in K'$ are roots of $p'(t), m_i > 0$. where $\alpha'_i := \eta(\alpha_i)$. So K' is the splitting field of $p'(t)$ and $\tilde{\eta} = \eta$.

Assume now that we know the Theorem for all splitting fields $\tilde{L} \supset \tilde{K}$ such that $[\tilde{L} : \tilde{K}] < N$. Let $\eta : K \to K'$ be an isomorphism, $q(t) \in K[t]$ be a monic polynomial of positive degree, $q'(t) \in K'[t]$ be the image of $q(t)$, $L \supset K, L' \supset K'$ be splitting fields of $q(t)$ and $q'(t)$ respectively and $[L : K] = N$. We want to show that isomorphism $\eta : K \to K'$ can be extended to an isomorphism $\tilde{\eta}$ between L and L'.

Consider the decomposition of $q(t)$

$$q(t) = p_1(t)^{m_1} ... p_n(t)^{m_n}$$

where $p_i(t)$ are irreducible monic polynomials and $m_i > 0$. Since $[L : K] > 1$ there exists $i, 1 \leq i \leq n$ such that deg $p_i(t) > 1$. Since L is a splitting field of $q(t)$ we can find $\alpha \in L$ such that $p_i(\alpha) = 0$. Let $F := K(\alpha) \subset L$. It is clear that $[F : K] =$deg $p_i(t) > 1$.

Since L' is a splitting field of $q'(t)$ any factor of $q'(t)$ decomposes in $L[t]$ in a product of linear factors. Therefore there exists $\alpha' \in L'$ such that $p_i'(\alpha) = 0$ [see Problem 3.1].

By Lemma 3.3 there exists a field homomorphism $\eta_F : F \to L'$ such that $\eta_F(\alpha) = \alpha', \eta_F(c) = c, c \in K$. Let $F' := Im(\eta_F) \subset L'$. By Lemma 3.4 L is a splitting field of $q(t)$ over F and L' is a splitting field of $q'(t)$ over F'. Since $[L : F] = [L : K]/[F : K] < [L : K] = N$ we know [by the inductive assumptions] that the isomorphism $\eta_F : F \to F'$ can be extended to an isomorphism $\tilde{\eta}$ between L and L'.$\square$

Criteria for irreducibility. The first criteria is for some polynomials over fields of characteristic $p > 0$.

Lemma 3.5. Let K be a field of characteristic $p > 0, \alpha \in K$. Then either there exists $\beta \in K$ such that $\alpha = \beta^p$ or the polynomial $p(t) = t^p - \alpha \in K[t]$ is irreducible.

Proof. a) If $\alpha = \beta^p$ then the polynomial $p(t) = t^p - \alpha = t^p - \beta^p = (t - \beta)^p$ is reducible.

b) Assume that $= t^p - \alpha = g(t)r(t)$ where $g(t), r(t) \in K[t]$ are polynomials of positive degree. We want to show the existence of $\beta \in K$ such that $\alpha = \beta^p$.

Let L be the splitting field of $p(t) = t^p - \alpha$ and $\beta \in L$ a root of $p(t)$. Then $\beta^p = \alpha$ and $p(t) = t^p - \alpha = (t - \beta)^p$. So we see that $g(t) = (t - \beta)^n, r(t) = (t - \beta)^m, m, n > 0, m + n = p$. The inclusion $r(t) \in K[t]$ implies that $\beta^m \in K$. Since p is a prime number and m is prime to p there exist integers a, b such that $am + bp = 1$. Therefore $\beta = \beta^{am+bp} = (\beta^m)^a \times (\beta^p)^b \in K$. Since $\beta^m, \beta^p \in K$ we see that $\beta \in K$.$\square$

The second irreducibility criteria is for polynomials over $\mathbb{Q}$. We start with a couple of auxiliary results.

Definition 3.3. A polynomial $q(t) = \sum_{i=0}^n c_i t^i \in \mathbb{Z}[t]$ with integer coefficients c_i is *primitive* if the greatest common divisor of integers $c_i, 0 \leq i \leq n$ is equal to 1.

Lemma 3.6. Any non-zero polynomial $r(t) \in \mathbb{Q}[t]$ can be written uniquely in the form

$r(t) = (u/m)q(t)$

where $q(t) \in \mathbb{Z}[t]$ is a primitive polynomial and u, m are positive integers.

I'll leave a proof of Lemma 3.6 as a homework problem.

Lemma 3.7 [Gauss lemma]. Let $q(t) \in \mathbb{Z}[t]$ be a monic polynomial with integer coefficients and $q(t) = f(t)g(t)$ where $f(t), g(t) \in \mathbb{Q}[t]$. Then we can find $c \in \mathbb{Q}, c \neq 0$ such that $cf(t), c^{-1}g(t)$ are monic polynomials with integer coefficients.

Proof. By Lemma 3.6 we can write $f(t) = u'/m'a(t), g(t) = u''/m''b(t)$ where $a(t), b(t)$ are primitive polynomials with integral coefficients and u', u'', m', m'' are positive integers. Then

$$q(t) = f(t)g(t) = u'u''/m'm''a(t)b(t)$$

We can write the fraction $u'u''/m'm''$ in the form $u'u''/m'm'' = u/m$ where u, m are relatively prime positive integers. We see that

$$mq(t) = ua(t)b(t)$$

Claim. $m = 1$

Proof of Claim. We show that an assumption that $m > 1$ leads to a contradiction. So assume $m > 1$ and choose a prime divisor p of m. We denote by $c \to \bar{c}$ the reduction $\mathbb{Z} \to \mathbb{F}_p$ mod p and denote by $\bar{a}(t), \bar{b}(t) \in \mathbb{F}_p[t]$ the reduction of polynomials $a(t), b(t)$ mod p.

Since the numbers u, m are relatively prime we have $\bar{u} \neq 0$. On the other hand since polynomials $a(t), b(t) \in \mathbb{Z}[t]$ are primitive we have $\bar{a}(t) \neq 0, \bar{b}(t) \neq 0$. The ring $\mathbb{F}_p[t]$ is integral and therefore $\bar{u}\bar{a}(t)\bar{b}(t) \neq 0$. On the other hand since $p|m$ we have $\bar{m} = 0$. This contradiction proves the Claim.

Now we can finish the proof of the Gauss lemma. We have

$$q(t) = ua(t)b(t)$$

Let $a, b \in \mathbb{Z}$ be the leading coefficients of polynomials $a(t), b(t) \in \mathbb{Z}[t]$. Since $q(t) \in \mathbb{Z}[t]$ is a monic polynomial we have $1 = uab$. But this is possible only if either when $a = b = 1$ and the polynomials $a(t), b(t) \in \mathbb{Z}[t]$ are monic or when $a = b = -1$ and the polynomials $-a(t), -b(t) \in \mathbb{Z}[t]$ are monic.

By the construction the polynomials $a(t), b(t) \in \mathbb{Z}[t]$ are multiples of $f(t), g(t), a(t) = cf(t), b(t) = dg(t)$. Since $a(t) \times b(t) = cf(t) \times dg(t)$ we have $cd = 1\square$.

Theorem 3.2 (Eisenstein's criteria). Let

$$q(t) = t^n + a_{n-1}t^{n-1} + ... + a_0 \in \mathbb{Z}[t]$$

be a monic polynomial with integer coefficients. Suppose that for some prime p we have $p|a_i, 0 \leq i \leq n-1$ but a_0 is not divisible by p^2. Then the polynomial $q(t)$ in $\mathbb{Q}[t]$ is irreducible.

Proof. Suppose that $q(t) = a(t)b(t)$ where $a(t), b(t) \in \mathbb{Q}[t]$ are polynomials of positive degree. By the Gauss lemma we can assume that $a(t), b(t)$ are monic polynomials with integral coefficients. Let $\bar{q}(t), \bar{a}(t), \bar{b}(t) \in \mathbb{F}_p[t]$ be the reductions of polynomials $q(t), a(t), b(t)$. The condition of the Theorem imply that $\bar{q}(t) = t^n$. Therefore all the roots of $q(t), a(t), b(t)$ are equal to $0 \in \mathbb{F}_p$. So

$$\bar{a}(t) = t^u, \bar{b}(t) = t^v, u + v = n$$

Since $\bar{a}(t) = t^c$ and the polynomial $a(t) \in \mathbb{Z}[t]$ is monic we have $a(t) = t^u + pc(t), c(t) = \sum_{i=0}^{u-1} c_i t^i \in \mathbb{Z}[t]$. Analogously $ba(t) = t^v + pd(t), d(t) = \sum_{j=0}^{v-1} d_j t^j \in \mathbb{Z}[t]$. But then we have $a_0 = p^2 c_0 d_0$. This contradicts the assumption that a_0 is not divisible by $p^2\square$.