Because of this last Theorem, when we want to calculate the Galois group of a polynomial we're aiming to describe a subgroup of S_n according to how it permutes the roots of the polynomial.

We'll also restrict to considering only polynomials with distinct roots, which means the irreducible factors are separable. Let us start with degree two and work our way to higher degrees.

<u>Proposition</u>: Suppose $f \in K[x]$ is irreducible, and $\deg f = 2$. If f is separable then the Galois group of f is $\mathbb{Z}_2$, otherwise it's $\{id\}$.

<u>Proof</u>: Since $f(x) = ax^2 + bx + c$, and $f'(x) = 2ax + b$,
$(a \neq 0)$

the only way $f'(x)$ can be zero is if $2 = 0$ (ie if K has characteristic 2). In this case $f(x)$ is not separable so $f(x) = (x-r)^2$ and the splitting field is $K(r)$. Every element of the Galois group fixes r and so $G = \{id\}$.

On the other hand if $f(x)$ is separable then $\deg f = 2$ divides $|G|$ and $G < S_2 \cong \mathbb{Z}_2$, so $G = \mathbb{Z}_2$.

Next we do degree 3 polynomials. For this we need:

<u>Definition</u>: Let K be a field with $\boxed{\operatorname{char} K \neq 2}$ and $f \in K[x]$ a polynomial of degree n with n distinct roots $u_1, \dots, u_n$ in some splitting field F over K.

Set $\Delta = \prod_{i<j} (u_i - u_j) \in F$, this is related to the quantity $\Delta^2 \in F$ which is typically denoted D and is called the <u>discriminant</u>.

<u>Proposition</u>: With K, f, F, Δ as above:

(i) $\Delta^2 \in K$ (not just in F!)

(ii) If $\sigma \in \mathrm{Aut}_K F$ then σ is an even permutation iff $\sigma(\Delta) = \Delta$ and odd iff $\sigma(\Delta) = -\Delta$.

<u>Proof</u>: It's a bit of a computation to prove (ii), but nothing clever: Remember that σ permutes the u_i in the formula $\prod_{i<j} (u_i - u_j)$ so it's a matter of keeping track of which indices increase under σ and which decrease.

To prove (i), note $\sigma(\Delta^2) = \Delta^2$ $\forall \sigma \in \mathrm{Aut}_K F$, so $\Delta^2 \in K$ since it's a Galois extension.

<u>Corollary</u>: With K, f, F, Δ as above (in particular F is a Galois extension). The correspondence in the fundamental theorem of Galois theory sends $K(\Delta)$ to the subgroup $G \cap A_n$ of $G \leq S_n$. (ie, it's the even permutations). In particular,

$$G \subset A_n \Leftrightarrow \Delta \in K.$$

<u>Proof</u>:

The elements of $K(\Delta)'$ consist of $\sigma : F \longrightarrow F$ with $\sigma(\Delta) = \Delta$, thus they are even permutations of the roots of f by the previous proposition.

On the other hand if $\sigma \in G \cap A_n$ then $\sigma(\Delta) = \Delta$ and so σ fixes $K(\Delta)$; we conclude $(K(\Delta))' = G \cap A_n$. In particular: If $G \subset A_n$ then $\sigma \in (K(\Delta))'$ $\forall \sigma \in G$, so $K(\Delta)' = K$ since F is Galois over K. On the other hand $\Delta \in K \Rightarrow G \subset A_n$ since every $\sigma \in G$ fixes Δ.

Corollary: Suppose $f \in K[x]$ is separable (irreducible) with $\deg f = 3$. Then the Galois group of f is either A_3 or S_3. If char $K \neq 2$ then it's A_3 iff $\Delta \in K$.

Proof: If $\deg f = 3$ and f is separable, then the Galois group is A_3 or S_3 because these are the only subgroups of S_3 that have order divisible by $\deg f = 3$.

Assuming char $K \neq 2$, then $\Delta \in K \Leftrightarrow$ the Galois group is contained in A_3

$\Rightarrow$ it's equal to A_3.

Remark:

Why do we need char $K \neq 2$?

The role of the discriminant is to be a quantity that's fixed by all $\sigma \in A_3$ but not by all $\sigma \in S_3$. Unfortunately if $+1 = -1$ (i.e. char $K = 2$) then the discriminant:

$$\Delta^2 = \left(\prod_{i<j} (u_i + u_j)\right)^2$$

becomes an expression symmetric in the u_i's. Consequently it's fixed by every $\sigma \in S_3$.

Thus: If char $K \neq 2$, finding the Galois group of $f \in K[x]$ means, if $\deg f \leq 3$, finding Δ and determining if $\Delta \in K$.

Proposition: Suppose char $K \neq 2$ or 3. If $f(x) = x^3 + bx^2 + cx + d \in K[x]$ is separable then $g(x) = f(x - b/3) \in K[x]$ is of the form $x^3 + px + q$ and the discriminant of f is $-4p^3 - 27q^2$.

Proof: Note u is a root of f

$\iff u + b/3$ is a root of g.

So a little check shows that g has the same discriminant of f. So write v_1, v_2, v_3 for the roots of g. Then

$$x^3 + px + q = (x - v_1)(x - v_2)(x - v_3),$$

multiplying out and equating coefficients gives

$$v_1 + v_2 + v_3 = 0$$
$$v_1 v_2 + v_1 v_3 + v_2 v_3 = p$$
$$-v_1 v_2 v_3 = q,$$

and $v_i^3 = -pv_i - q$ for $i = 1, 2, 3$. Now use the defintion

$$\Delta^2 = (v_1 - v_2)^2 (v_1 - v_3)^2 (v_2 - v_3)^2$$

and $(v_i - v_j)^2 = (v_i + v_j)^2 - 4v_i v_j$ to reduce to

$$\Delta^2 = -4p^3 - 27q^2.$$

<u>Example</u>: The polynomial x^3+5x+1 is irreducible by the rational root test. As an element of $\mathbb{Q}[x]$ it's separable too since $\operatorname{char}\mathbb{Q}=0$. The discriminant is

$$-4(5)^3-27(1)^2$$

$$= -4(-125)-27 = \overset{500}{\cancel{+425}} - 27 = 473,$$ which is not a square so the Galois group is A_3.

We can also do all polynomials of degree 4, again it is simply a recipe:

Suppose $f \in K[x]$ has roots u_1, u_2, u_3, u_4. in a splitting field F. Recall that S_4 has a special normal subgroup

$$V = \{(1), (12)(3,4), (13)(24), (14)(23)\} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

So $V \cap G \trianglelefteq G = \operatorname{Aut}_K F \leq S_4$.

Set $\alpha = u_1u_2+u_3u_4$, $\beta = u_1u_3+u_2u_4$, $\gamma = u_1u_4+u_2u_3 \in F$. Then $(x-\alpha)(x-\beta)(x-\gamma)$ is the <u>resolvant cubic of f</u>. If $f(x) = x^4+bx^3+cx^2+dx+e$ then

$$(x-\alpha)(x-\beta)(x-\gamma) = x^3 - cx^2 + (bd-4e)x - b^2e + 4ce - d^2.$$

Use this to compute $m = [K(\alpha,\beta,\gamma):K]$. Then:

(i) $m=6 \iff \operatorname{Aut}_K F \simeq S_4$

(ii) $m=3 \iff \operatorname{Aut}_K F \simeq A_4$

(iii) $m=1 \iff \operatorname{Aut}_K F \simeq V$

(iv) $m=2 \iff \operatorname{Aut}_K F \simeq D_4$ or $\mathbb{Z}_4$. It's D_4 if f is irreducible over $K(\alpha,\beta,\gamma)$ and $\mathbb{Z}_4$ otherwise.

Theorem 4.12: If p is prime and f is irreducible with $\deg f = p$ over $\mathbb{Q}$, and f has exactly two non-real roots then the Galois group of f is S_p. (Let $K = \mathbb{Q}$, $F =$ splitting field)

Proof: Since $p \mid |\mathrm{Aut}_K F|$, $\mathrm{Aut}_K F$ contains an element of order p, call it σ. Since $\sigma \in \mathrm{Aut}_K F \leq S_p$, σ must be a p-cycle.

Now $a+ib \longmapsto a-ib$ is an element of $\mathrm{Aut}_K F$ that must swap the two nonreal roots of $f(x)$ and fix all others, so this element must be a transposition $\tau = (ab)$ in S_p.

Now σ is a p-cycle, so we can write it $\sigma = (a\, j_2 \cdots j_p)$, and some power is $\sigma^k = (a\, b\, j_3 \cdots i_p)$. We can assume $a=1$, $b=2$, and $i_k = k$ for $k \geq 3$ by relabeling if necessary. So $\sigma^k = (1\ 2\ 3 \cdots p) \in \mathrm{Aut}_K F$, as is (12). But these two elements generate S_p, so $\mathrm{Aut}_K F \cong S_p$.

§5.9 Radical extensions.

The goal of this content is to prove the classic result:

There is no formula that involves field operations and extraction of n^{th} roots which allows you to compute the roots of an arbitrary degree 5 polynomial.

First goal: Precisely state the problem in field-theoretic terms.

Intuition: The existence of such a formula would mean there's a finite sequence of steps, each step being either the application of a field operation $(+, \cdot, ^{-1})$ or an n^{th} root $\sqrt[n]{c}$ for c in the field.

The step of finding $\sqrt[n]{c}$ where $c \in E$ amounts to constructing an extension $E(u)$ with $u^n = c \in E$ (i.e. it could be the splitting field of $x^n - c \in E[x]$).

Thus repeatedly extracting roots in the process of solving a degree 5 polynomial $f(x)$ would yield

$$K = E_0 \subset E_1 \subset E_2 \subset \dots \subset E_n$$

where E_n is a splitting field of $f(x)$ and for $i > 0$ $E_i = E_{i-1}(u_i)$ where $u_i^n \in E_{i-1}$.

Thus:

Definition: If $K \subseteq F$ are fields, then F is a radical extension of K if $F = K(u_1, \ldots, u_n)$ and $\exists\, n_1 \in \mathbb{Z}_{>0}$ such that $u_1^{n_1} \in K$ and $n_i \in \mathbb{Z}_{>0}$ such that for $i = 2, \ldots, n$ $u_i^{n_i} \in K(u_1, \ldots, u_{i-1})$.

Remark: For each i, since $u_i^{n_i} \in K(u_1, \ldots, u_{i-1})$ then u_i is a root of $x^{n_i} - u_i^{n_i} \in K(u_1, \ldots, u_{i-1})[x]$, so $K(u_1, \ldots, u_i)$ is algebraic over $K(u_1, \ldots, u_{i-1})$. Thus every radical extension is finite dimensional and algebraic.

Definition: Let $f(x) \in K[x]$. We say $f(x) = 0$ is solvable by radicals over K if there exists a radical extension F of K and a splitting field E of f over K such that $K \subset E \subset F$.

So our goal: Show that there exist polynomials of degree ≥ 5 that are not solvable by radicals. Show that every polynomial of degree ≤ 4 IS solvable by radicals.

To do this, we prep some Lemmas/propositions.

Theorem 3.16: If E is an algebraic extension of K, then there exists an extension F of E such that:

(i) F is normal over K,

(ii) No proper subfield of F containing E is normal over K,

(iii) If E is separable over K then F is Galois over K,

(iv) $[F:K] < \infty$ iff $[E:K] < \infty$.

Moreover, F is unique up to isomorphism

Remark: The extension E may not be normal. The field F is meant to be "the smallest way of extending E to be normal", so is often called the normal closure of E.

Proof: (i) Let $\{u_i\}_{i\in I} \subset E$ be a basis for E over K, and $\forall i \in I$ let $f_i \in K[x]$ be the minimal polynomial of u_i. Set F = splitting field of $\{f_i\}_{i\in I}$ over K. Then F contains E and F is normal over K because splitting fields of sets of polynomials are normal (this is a theorem we skipped for the sake of time, do not worry about the proof).

(iii) If E is separable then each f_i is separable so F is Galois over K.

(iv). If $[E:K] < \infty$ then $\{u_i\}_{i\in I}$ above is finite, so $\{f_i\}_{i\in I}$ is finite and so $[F:K] < \infty$. On the other hand $[F:K] < \infty \Rightarrow [E:K] < \infty$ since $E \subset F$.

(ii) If F_0 is a normal field with $E \subset F_0 \subset F$, then $u_i \in E \subset F_0$ $\forall i$. But then F_0 contains a root of f_i for each i, and so contains all roots of f_i for each i by normality. So all f_i split over F_0 and

Thus $F \subset F_0$, so $F_0 = F$.

Uniqueness is left as an exercise.

Lemma 9.3: If F is a radical extension of K and N is a normal closure of F over K, then N is a radical extension of K

Sketch: For subfields L, M of a field F, their composite is written LM and is defined to be the subfield of F generated by $L \cup M$. The proof of the lemma then proceeds as follows:

Claim 1: If $[F:K] < \infty$, then $N = E_1 E_2 \cdots E_r$ where $E_i \subset N$ is a subfield isomorphic to F. To see this, suppose $\{u_1, \ldots, u_n\}$ are a basis of F over K with min polynomials $\{f_1, \ldots, f_n\}$ over K, then N is the splitting field of $\{f_1, \ldots, f_n\}$. Let v be the root of ~~any~~ some f_j.

Then there's an isomorphism $\sigma : K(u_j) \longrightarrow K(v)$ with $\sigma(u_j) = v$ extending to an automorphism $\sigma : N \to N$. Then $\sigma(F)$ is a subfield of N isomorphic to F containing $\sigma(u_j) = v$. So for every root of every f_j there's a subfield isomorphic to F containing that root, say $\{E_1, \ldots, E_r\}$ is a list of all such subfields. Then $\{f_1, \ldots, f_n\}$ split over $E_1 \cdots E_r$, so $E_1 \cdots E_r = N$.

Claim 2: If $E_1, \ldots, E_r$ are radical extensions of K, then so is $E_1 \cdots E_r$. To see this, we consider $r=2$. Then $E_1 = K(u_1, \ldots, u_k)$, $E_2 = K(v_1, \ldots, v_m)$ and $E_1 E_2 = K(u_1, \ldots, u_k, v_1, \ldots, v_m)$ is a radical extension since $v_1^k \in K \in E_1$ for some k, and all other adjoined elements satisfy the necessary restrictions/conditions from the assumption that E_1 and E_2 are radical extensions.

Theorem 9.4: If F is a radical extension of K and E is an intermediate field, then $\mathrm{Aut}_K E$ is solvable.

Corollary: If $f \in K[x]$ is solvable by radicals, then the Galois group of $f(x)$ is solvable.

Solvability lemma.

Theorem: If N is a normal subgroup of a group G such that N and G/N are solvable, then G is solvable.

Proof: Let $q: G \longrightarrow G/N$ be the quotient. Since G/N is solvable, for some $n > 0$ we have

$$q(G^{(n)}) = (G/N)^{(n)} = \{id\}. \text{ So } G^{(n)} < \ker q.$$

But $G^{(n)}$ is solvable since it's the subgroup of a solvable group. But now $\exists k$ such that $(G^{(n)})^{(k)} = \{id\}$, meaning $G^{(n+k)} = (G^{(n)})^{(k)} = \{id\}$, so G is solvable.

Basic idea:

If $K(u_1, \dots, u_n)$ is a radical extension of K, then the tower of subfields

$$K \subset K(u_1) \subset K(u_1, u_2) \subset \dots \subset K(u_1, \dots, u_n)$$

should give subgroups

$$\mathrm{Aut}_K K(u_1, \dots, u_n) = H_n \geq H_{n-1} \geq \dots \geq \{id\}$$

where H_i/H_{i-1} is cyclic since $K(u_1, \dots, u_i)$ arises from $K(u_1, \dots, u_{i-1})$ by adding roots of $x^{n_i} - u_i^{n_i}$. However This only turns out to work if K contains an n_ith root of unity, so we need to correct for this.

Theorem 9.4: If F is a radical extension of K and E is an intermediate field, then $\mathrm{Aut}_K E$ is a solvable group.

Proof: Set $K_0 = (\mathrm{Aut}_K E)'$, then E is Galois over K_0. Moreover $\mathrm{Aut}_K E = \mathrm{Aut}_{K_0} E$, and F is actually a radical extension of K_0 (c.f. assignment problem). So replacing K by K_0 changes nothing in terms of the structure of the Galois group or the fact that F is radical over the base field; thus we assume E/K is Galois (by replacing K by K_0 if needed).

Let N be the normal closure of F over K. Then by Lemma 9.3, N is radical over K and since E is Galois and algebraic over K, it's stable. Therefore there is a homomorphism

$$\begin{aligned} \theta : \mathrm{Aut}_K N &\longrightarrow \mathrm{Aut}_K E \\ \sigma &\longmapsto \sigma|_E \end{aligned}$$

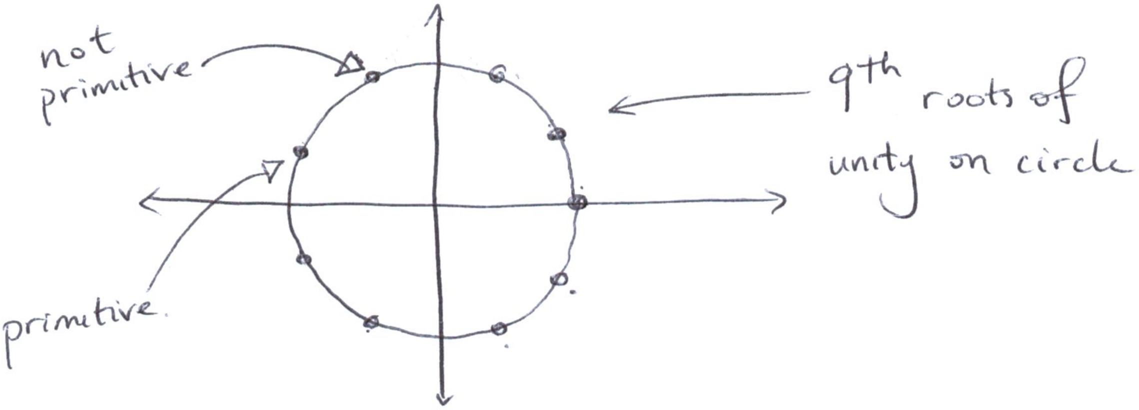
given by restriction.

The normal closure N is a splitting field by construction, so every $\sigma : E \longrightarrow E$ fixing K extends to an automorphism $\sigma : N \longrightarrow N$, and this means that θ is surjective. Now from one of our earlier assignments we saw that every quotient of a nilpotent group is nilpotent —

it turns out the same is true replacing nilpotent with solvable. So if we show $\text{Aut}_K N$ is solvable, then Θ being surjective proves $\text{Aut}_K E$ is solvable. So we focus on $\text{Aut}_K N$.

Before proceeding, however: observe that if $(\text{Aut}_K N)' = K_1$ then $\text{Aut}_K N = \text{Aut}_{K_1} N$ and N is a radical Galois extension of K_1. Thus by replacing K by K_1 if necessary, we can assume N is a radical Galois extension. So we're in the situation of considering a radical Galois extension and its intermediate fields. Use notation $F \subset E \subset K$ from this point on for consistency. We'lll also assume from here on that $\text{char } K = 0$ to keep things easy, and focus on F/K.

Suppose $F = K(u_1, \dots, u_n)$ with $u_1^{m_1} \in K$ and $u_i^{m_i} \in K(u_1, \dots, u_{i-1})$ for $i \geq 2$. Set $m = m_1 \cdots m_n$. Let γ be a primitive m^{th} root of unity, i.e. a "complex number" with $\gamma^m = 1$ which is a generator of the ~~the~~ subgroup of m^{th} roots of unity in $\mathbb{C}$:



Except in our case, instead of working over $\mathbb{C}$ we're working ~~of~~ over K and these elements are roots of $x^{m-1} - 1$. So we arrive at

$$\begin{tikzcd}
 & F(\gamma) \arrow[dl, dash] \arrow[dr, dash] & \\
F \arrow[dr, dash] & & K(\gamma) \arrow[dl, dash] \\
 & K &
\end{tikzcd}$$

Since powers of γ yield all solutions to x^{m-1}, $F(\gamma)$ is actually a splitting field of $x^m - 1$ and we can conclude that $F(\gamma)$ is Galois over F, and therefore over K (this is an exercise in one of the chapters that we skipped).

The fundamental theorem of Galois theory gives $\operatorname{Aut}_K F \simeq \operatorname{Aut}_K F(\gamma) \big/ \operatorname{Aut}_F F(\gamma)$, so we can focus on showing $\operatorname{Aut}_K F(\gamma)$ is solvable. But now there is a theorem:

Theorem 8.1: Let $n > 0$ and F the splitting field over K of $x^n - 1$. Then $\mathrm{Aut}_K F$ is an abelian group.

In our situation, this means since $K(\gamma)$ is the splitting field of $x^n - 1$ the group $\mathrm{Aut}_K K(\gamma)$ is abelian. Then the fundamental theorem gives:

$$\mathrm{Aut}_K K(\gamma) = \mathrm{Aut}_K F(\gamma) \Big/ \mathrm{Aut}_{K(\gamma)} F(\gamma)$$

So by Lemma (solvability), we need only prove that $\mathrm{Aut}_{K(\gamma)} F(\gamma)$ is solvable. So recall $F = K(u_1, \ldots, u_n)$ and since $F(\gamma)$ is Galois over K it's Galois over all intermediate fields, so we construct

$E_0 = K(\gamma)$, $E_i = K(\gamma_1, u_1, \ldots, u_i)$, $E_n = F(\gamma)$., and set $H_i = \mathrm{Aut}_{E_i} F(\gamma)$, the subgroup of $\mathrm{Aut}_{K(\gamma)} F(\gamma)$ under the correspondence of the fundamental theorem. We have

$$\begin{tikzcd}
E_0 \arrow[r, phantom, "\subset"] \arrow[d, mapsto] & E_1 \arrow[r, phantom, "\subset"] \arrow[d, mapsto] & \cdots \arrow[r, phantom, "\subset"] & E_n \arrow[d, mapsto] \\
H_0 \arrow[r, phantom, "\supset"] \arrow[d, phantom, "\parallel"] & H_1 \arrow[r, phantom, "\supset"] & \cdots \arrow[r, phantom, "\supset"] & H_n = \{id\} \\
\mathrm{Aut}_{K(\gamma)} F(\gamma) & & &
\end{tikzcd}$$

Now $K(\gamma)$ contains all mth roots of unity, so in particular contains an m_i-th root of unity for each i. Then since $u_i^{m_i} \in E_{i-1}$, $E_i = E_{i-1}(u_i)$ and E_{i-1}~~(u_i)~~ contains an m_i-th root of unity, we can compute that the Galois group of the extension E_i/E_{i-1} is (it's Galois) cyclic (hence abelian). (This is basically the content of chapter 7). But now the fundamental theorem gives

$$H_i \lhd H_{i-1} \quad \text{and} \quad H_{i-1}/H_i = \operatorname{Aut}_{E_{i-1}} F(\gamma) \Big/ \operatorname{Aut}_{E_i} F(\gamma)$$

$$\cong \operatorname{Aut}_{E_{i-1}} E_i = \text{cyclic, so}$$

$$1 = H_n < H_{n-1} < \dots < H_0 = \operatorname{Aut}_{K(\gamma)} F(\gamma) \text{ is a}$$

solvable series. So $\operatorname{Aut}_{K(\gamma)} F(\gamma)$ is solvable.

Example: If we graph $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$, we can see that it has only 3 real roots (use calculus to find ~~f~~ maxes/mins, for example). Thus it has exactly two non-real ~~complex~~ roots, and it's irreducible by Eisenstein with $p = 2$. So its Galois group is S_5, which is not solvable since $A_5 < S_5$ is in fact simple (and nonabelian).

To finish off the Galois Theory stuff:

Example: Graph the polynomial $f(x) = x^5 - 4x + 2 \in \mathbb{Q}[x]$. It has exactly 3 real roots, so two non-real roots. It's irreducible by Eisenstein, so its Galois group is S_5. It's not solvable; since (for example) $A_5 < S_5$ and A_5 is simple.

Example: Any polynomial that's irreducible with degree p (p prime) with $p \geq 5$ having exactly $p-2$ real roots cannot be solved by radicals, since the Galois group is S_p ($p \geq 5$) which is not solvable.

A quick introduction to modules.

(Chapter 10, Dummit and Foote).

Definition: Let R be a ring (maybe not commutative, maybe not with 1). A left R-module is an abelian group $(M,+)$ and a map $R \times M \longrightarrow M$ satisfying:

$$(r,m) \longmapsto rm$$

(i) $(r+s)m = rm + sm$ for all $r,s \in R$ and $m \in M$.

(ii) $(rs)m = r(sm)$ for all $r,s \in R$ and $m \in M$

(iii) $r(m+n) = rm + rn$ for all $r \in R$ and $m,n \in M$.

If the ring also has a multiplicative identity 1, then

(iv) $1m = m$ for all $m \in M$. (We will always assume this holds)

Remark ① We use "left" above to make it clear that ring elements appear on the left hand side of elements $m \in M$. We can analogously define right R-modules. The distinction is very important when working with non-commutative rings.

② An easy way to understand modules is the following observation: When the ring R has an identity 1 and multiplicative inverses + commutativity, then it's a field, and every R-module is just an R-vector space.

So a module is like "a vector space over a ring".

Examples:

① If $M=R$ where R is any ring, then we get a module. I.e. every ring R is both a left and right module over itself.

② Let R be a ring and define

$$R^n = \{(a_1, \dots, a_n) \mid a_i \in R\}$$

define ~~multiplication and~~ addition on R component-wise, and multiplication by $r \in R$ according to

$$r(a_1, \dots, a_n) = (ra_1, ra_2, \dots, ra_n).$$

Then R^n becomes an R-module called the "free R-module of rank n".

③ Let $R = \mathbb{Z}$ and let A be any abelian group. Write the operation of A as $+$. Define the usual notation: Given $a \in A$, set

$$na = \begin{cases} a + a + \dots + a \text{ (n times) if } n>0 \\ 0 \quad \text{if} \quad n=0 \\ -a-a- \dots -a \text{ (n times) if } n<0. \end{cases}$$

This notation makes A into a $\mathbb{Z}$-module. So <u>every</u> abelian group is (an always has been) a $\mathbb{Z}$-module.

Definition: Let R be a ring and M an R-module. An R-submodule of M is a subgroup $N < M$ such that $rn \in N$ whenever $r \in R$ and $n \in N$.

Example: If A is an abeliangroup then it's a $\mathbb{Z}$-module. From our definitions, the submodules of A correspond exactly to the subgroups of A.
(I.e. the submodules are exactly subgroups $B < A$ such that $nb \in B$ for every $n \in \mathbb{Z}$ and $b \in B$ — but this is true of every $b \in B$ and $n \in \mathbb{Z}$ for every $B < A$).

Example: $F[x]$-modules.

Let F be a field, and let $R = F[x]$. Let V be a vector space over F, and $T : V \longrightarrow V$ a linear transformation.

First, V is an F-module: The usual rules of vector addition and scalar multiplication give us this. In fact, V is an $F[x]$-module if we use T for the action of x on V.

Recall that by $T^0, T^1, T^2, \ldots, T^n$ we mean $\mathrm{Id}, T, T\circ T, T\circ T\circ T, \ldots, \underbrace{T\circ T\circ \ldots \circ T}_{n \text{ times}}$, and that if $S, T : V \longrightarrow V$ are linear maps then we can define $S+T : V \longrightarrow V$ by

$$(S+T)(v) = S(v) + T(v),$$ and $S+T$

is also a linear map.

Now, given $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0, = p(x)$, set

$$p(x)v = \left(a_n T^n + a_{n-1} T^{n-1} + \dots + a_1 T + a_0 I\right)(v)$$

$$= a_n T^n(v) + a_{n-1} T^{n-1}(v) + \dots + a_1 T(v) \boxed{+ a_0 v}$$

(ie. plug T into p(x) and then use the new linear transformation to act on v).

Observe that the vector space V with its original F-module structure appears as part of our new F[x]-module, namely the constant polynomials in F[x] and their multiplication by elements of V.

like this

This construction therefore describes <u>all</u> F[x] modules M: There's always an underlying vector space V, which is the abelian group of the module M multiplied by the constant polynomials in F[x]. Then multiplication by x is always some linear transformation from this vector space to itself, because

$$x(fm) \underset{\text{module axiom}}{=} (xf)m \underset{\text{commutativity of } F[x]}{=} (fx)m \underset{\text{module axiom}}{=} f(xm)$$

and $x(m_1 + m_2) = xm_1 + xm_2$, by module axioms.

So we have a bijection

$$\left\{ V \text{ an } F[x]\text{-module} \right\} \Longleftrightarrow \left\{ \begin{array}{c} V \text{ a vector space over } F \\ \text{and} \\ T: V \to V \text{ a linear transformation} \end{array} \right\}$$

The correspondence is stronger than this: Consider an $F[x]$-submodule of V as above with transformation T. First it must be $W \leq V$ must be a subgroup of V as an abelian group, and if it's going to be an $F[x]$-submodule it has to be an F-module, so $W \leq V$ and $fw \in W$ $\forall w \in W$ — ie. it's a subspace of the vector space V. Next we need $xw \in W$ $\forall w \in W$, ie $T(w) \in W$ $\forall w \in W$, and $T^2(w) \in W$, $T^3(w) \in W$, etc. But $T^n(w) \in W$ $\forall w \in W$ follows from $T(W) \subset W$, and $T(W) \subset W$ is necessary if $T(w) \in W$ $\forall w \in W$ is to hold. Such a W is called a T-stable subspace, and we get:

$$\left\{ W \text{ an } F[x]\text{-submodule} \right\} \Longleftrightarrow \left\{ \begin{array}{c} W \leq V \text{ is a} \\ T\text{-stable subspace} \end{array} \right\}.$$

<u>Example</u>: If $V = F^n$ and $T: V \longrightarrow V$ is

$$T(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, 0)$$ then

every

$$W_k = \{ (x_1, \ldots, x_k, 0, \ldots, 0) \mid x_i \in F \} \leq V$$

is T- stable, so each gives a submodule of the $F[x]$-module arising from $T: V^n \longrightarrow V^n$.

Proposition: (Submodule criterion).

Let R be a ring and M an R-module. Then $N \subset M$ is a submodule iff

(i) $N \neq \emptyset$

(ii) $x + ry \in N$ for all $r \in R$ and $x, y \in N$.

Proof: If N is a submodule, then $0 \in N$ so $N \neq \emptyset$, also $ry \in N$ $\forall r \in R$ and $y \in N$; and N is closed under addition so $x + ry \in N$.

On the other hand, with $r = -1$ we see that (ii) is the subgroup criterion, so N is a subgroup. In particular, $0 \in N$ so we can let $x = 0$ and get that $ry \in N$ $\forall r \in R$ and $y \in N$, meaning it is a submodule.

§ 10.2 Quotient modules and module homomorphisms

§10.2 : Quotient Modules and module homomorphisms.

Definitions: Let R be a ring and suppose M, N are R-modules.

A map $\varphi : M \longrightarrow N$ is an R-module homomorphism if $\varphi(m_1 + m_2) = \varphi(m_1) + \varphi(m_2)$ and $\varphi(rm) = r\varphi(m)$. $\forall\, r \in R,\ m, m_1, m_2 \in M$.

It's an R-module isomorphism if it's onto and oneto one. The kernel of φ is the set

$$\ker \varphi = \{ m \in M \mid \varphi(m) = 0 \}.$$

Example: ① If U, V are vector spaces over a field F, then they're also modules over F and every linear transformation $L : U \longrightarrow V$ is an F-module homomorphism

② Recall if $M = R$ then M is an R-module by left multiplication in the ring. Then R-module homomorphisms $M \longrightarrow M$ are not necessarily ring homomorphisms $R \longrightarrow R$. E.g If $R = \mathbb{Z}$ then

$\varphi(z) = 2z$ is an R-module homomorphism $\mathbb{Z} \to \mathbb{Z}$ but not a ring homomorphism since $\varphi(1) = 2$.

However we do have the following fact:

If A, B are abelian groups (thinking of them also as $\mathbb{Z}$-modules) then $\mathbb{Z}$-module homomorphisms are the same as abelian group homomorphisms.

③ Making R^n into an R-module as last day, the map $\pi_i : R^n \to R$ given by $(a_1, \dots, a_n) \mapsto a_i$ is an R-module homomorphism. It is projection onto the ith factor.

Proposition : A map $\varphi: M \to N$ (where M, N are R-modules) is an R-module homomorphism iff $\varphi(rm_1 + m_2)$

$$= r\varphi(m_1) + \varphi(m_2)$$

$$\forall r \in R, \ m_1, m_2 \in M.$$

Proof : Straightforward.

Next steps : Recall that for groups, we had to define "normal" subgroups $N \trianglelefteq G$ as the groups for which the set of cosets inherit a group structure.

In a module, every submodule is normal in this sense: If N is a submodule of M, M/N always naturally inherits the structure of an R-module, so we get a quotient homomorphism $M \xrightarrow{\pi} M/N$ with kernel N.

Proposition: Let R be a ring, M an R-module and N a submodule. Then M/N is an abelian group that can naturally be made into an R-module by setting:

$$r(x+N) = rx+N \quad \forall r\in R,\ x+N \in M/N.$$

Moreover the natural projection $\pi : M \to M/N$ defined by $\pi(x) = x+N$ is an R-module homomorphism with kernel N.

Proof:

First, M is an abelian group and N is a subgroup, so M/N is an abelian group. We need only check that the definition $r(x+N) = rx+N$ is well-defined, ie if $x+N = y+N$ then does $r(x+N) = r(y+N)$?

If $x+N = y+N$ then $x-y \in N$, so $r(x-y) = rx-ry \in N$ since N is an R-submodule. But $rx-ry \in N$ $\Rightarrow rx+N = ry+N$, so it's well-defined.

So since everything (addition, mult by elements of R) is well-defined, checking the R-module axioms is easy.

E.g. to see that 2(b) $(rs)m = r(sm)$ holds:

Let $r_1, r_2 \in R$ and $x+N \in M/N$. Then

$$\begin{aligned}(r_1r_2)(x+N) &= (r_1r_2)x+N \\ &= r_1(r_2x)+N \\ &= r_1(r_2x+N) = r_1(r_2(x+N)).\end{aligned}$$

Checking the other axioms similarly boils down to an application of the definition.

Now the map $\pi : M \to M/N$ exists as a homomorphism of abelian groups defined by $\pi(x) = x+N$, we need only check that is is naturally an R-module homomorphism, ie $\pi(rm) = r(\pi(m))$. We calculate.

$$\begin{aligned}\pi(rm) &= rm+N \\ &= r(m+N) \\ &= r(\pi(m)).\end{aligned}$$

So it all works.

Definition: Let A, B be submodules of M, and set

$$A+B = \{a+b \mid a \in A, b \in B\}.$$

Then $A+B$ is a submodule of M.

Using this notion in place of products of subgroups, one can prove that all the expected isomorphism theorems hold.

Theorem:

① First isomorphism theorem:
Suppose M, N are R-modules and $\varphi: M \to N$ an R-module homomorphism. Then $\ker\varphi$ is a submodule of M and $M/_{\ker\varphi} \simeq \varphi(M)$.

② Second isomorphism theorem:

If A and B are submodules of an R-module M, then $(A+B)/B \cong A/(A \cap B)$.

③ Third isomorphism theorem:

Let A, B be submodules ~~with~~ of M with $A \subseteq B$. Then $(M/A)/(B/A) \cong M/B$.

④ Fourth/Lattice isomorphism theorem:

Let N be a submodule of M. Then there is a bijection between submodules of M containing N and submodules of M/N

$$A \longleftrightarrow A/N,$$

and it commutes with taking sums and intersections. (ie it gives an isomorphism of lattices of submodules).

§10.4: Tensor products of modules.

Let us first analyze a special case in detail to motivate the general definition.

Suppose $R < S$ are rings and N is a left S-module. Then N is also a left R-module, because the elements of R can be multiplied by all $n \in N$ in a way consistent with the module axioms.

How can we reverse this process? Given $R < S$ and N a left R-module, is there some way of making a "bigger" S-module out of N, such that restricting to R gives back our original module? In general: No, we can't simply take our original N and put an S-multiplication on it.

E.g. If $\mathbb{Z}$ is a $\mathbb{Z}$-module over itself, we can't make $\mathbb{Z}$ into a $\mathbb{Q}$-module by some clever definition of how to multiply each $q \in \mathbb{Q}$ by $z \in \mathbb{Z}$. (If we could, then $\frac{1}{2} \cdot 1 = z \in \mathbb{Z}$ would have to be an element with $z + z = 1$).

So the best "reverse" to this process we can hope for is:

Given an R-module N, can we construct an S-module M such that, thinking of M as an R-module we find our original 'N' as a submodule? Yes.

Here is how: Starting with $R \subset S$,
We want to be able to multiply each $n \in N$ by $s \in S$, and the product will be some element in a larger ~~R~~ module M. So let us proceed as follows:

Start with the set $S \times N$, and think of each pair (s,n) as the "product" sn. This, at the moment, makes no sense and so we impose the things necessary for it to start making sense:

First, $S \times N$ is not a module in any sense, because a module is first and foremost an abelian group. So turn $S \times N$ into an abelian group by adding what we must: all sums.

$$\text{Set } A(S\times N) = \left\{ \sum_{i=1}^{n} \pm (s_i, n_i) \;\middle|\; s_i \in S,\ n_i \in N,\ n \in \mathbb{Z} \right\}$$

I.e. $A(S\times N)$ is the set of all finite formal sums of pairs of elements in S and N. We add them now in the obvious way:

$$\underbrace{(s_1,n_1) + (s_2,n_2)}_{\substack{\text{one element} \\ \text{of } A(S\times N)}} + \underbrace{\left[-(s_3,n_3) + (s_4,n_4)\right]}_{\substack{\text{another element} \\ \text{of } A(S\times N)}}$$

$$= (s_1, n_1) + (s_2, n_2) - (s_3, n_3) + (s_4, n_4).$$

So now we have an abelian group built out of "formal products" of elements of S and elements of N. But the "products" (s,n) don't obey the module axioms. E.g. Axioms 2(a) and 2(c) (we will deal with 2(b) soon) say:

$$(a)\ (s_1 + s_2)m = s_1 m + s_2 m$$

and $$(b)\ (s)(m_1 + m_2) = sm_1 + sm_2.$$

So our formal products need to satisfy:

$$(s_1 + s_2, n) = (s_1, n) + (s_2, n) \qquad ①$$

and $$(s, n_1 + n_2) = (s, n_1) + (s, n_2). \qquad ②$$

We also want these formal products to "extend" our original module structure, ie. when $r \in R$ we want (r,n) to be the original element rn. So we ask for:

$$(r, n) = (1, rn). \qquad ③.$$

So let $K \triangleleft A(S \times N)$ be the subgroup generated by all elements of the form

$$(s_1 + s_2, n) - (s_1, n) - (s_2, n)$$
$$(s, n_1 + n_2) - (s, n_1) - (s, n_2)$$
$$(r, n) - (1, rn).$$

Then take the quotient $A(S \times N)/K$. Denote the coset $(s,n) + K$ by $s \otimes n$, and denote the group $A(S \times N)/K$ by $S \otimes_R N$.

By definition of $S \otimes_R N$, the following relationships hold between cosets:

$$(s_1+s_2)\otimes n = s_1 \otimes n + s_2 \otimes n$$

$$s\otimes(n_1+n_2) = s\otimes n_1 + s\otimes n_2$$

$$r\otimes n = 1\otimes rn.$$

Finally, we make $S\otimes_R N$ into an S-module by defining

$$s\Big(\sum_{\substack{i \\ \text{finite}}} s_i \otimes n_i\Big) = \sum_{\substack{i \\ \text{finite}}} (ss_i)\otimes n_i \quad \Big(\text{this takes care of module axiom } 2(b)\Big).$$

<u>Remark</u>: To be certain this works is a big exercise in definition checking. The first step is to verify it's well-defined meaning that if $\sum s_i \otimes n_i = \sum_i s_i' \otimes n_i'$ (as cosets) then

$$\sum ss_i \otimes n_i = \sum ss_i' \otimes n_i' \text{ (as cosets).}$$

The next is to verify the axioms, e.g.

$$(s+s')\Big(\sum s_i \otimes n_i\Big) = s\Big(\sum_i s_i\otimes n_i\Big) + s'\Big(\sum_i s_i \otimes n_i\Big),$$

which we do by checking that for each i:

$$(s+s')(s_i\otimes n_i) = \big((s+s')s_i \otimes n_i\big) \quad \text{(definition of mult)}$$

$$= \big((ss_i + s's_i)\otimes n_i\big) \quad \text{(ring mult. distributes)}$$

$$= ss_i \otimes n_i + s's_i\otimes n_i$$

(apply relation $\textcircled{1}$)

$$= s(s_i\otimes n_i) + s'(s_i \otimes n_i) \quad \text{(by definition)}$$

In the end, it all works. The elements $s\otimes n$ are called <u>simple tensors</u>.

The module $S \otimes_R N$ is called the left-S-module obtained from N by *extension of scalars*.

There is one aspect of this construction that I'd like to check in full: Our original goal was to take an R-module N and build a bigger S-module that contained N. So... did we succeed?

In $S\otimes_R N$, the elements $r\otimes n = 1\otimes rn$ are suppose to be our original submodule. Let's check: Define $\varphi : N \longrightarrow S\otimes_R N$ by $\varphi(n) = 1\otimes n$. Then:

$$\varphi(n_1+n_2) = 1\otimes(n_1+n_2) = 1\otimes n_1 + 1\otimes n_2 \quad \text{(we imposed this condition)}$$

and $\varphi(n_1)+\varphi(n_2) = 1\otimes n_1 + 1\otimes n_2$, so φ respects addition.

$$\text{Also } \varphi(rn) = 1\otimes rn \underset{\text{by construction}}{=} r\otimes n \underset{\text{by definition of } S\otimes_R N}{=} r(1\otimes n) = r\varphi(n).$$

So φ is an R-module homomorphism. Also note that φ is surjective onto the collection of elements $\{1\otimes n \mid n\in N\}$. Is it injective?

Example: Let $N=\mathbb{Z}_n$, $R=\mathbb{Z}$ and $S=\mathbb{Q}$.

Then what is $\mathbb{Q}\otimes_{\mathbb{Z}} N$?

First, note that in any tensor product we always have:

$$\cancel{s\otimes 0} = s\otimes(0+0) = \cancel{s\otimes 0} + s\otimes 0$$

$$\text{cancel} \quad \Rightarrow s\otimes 0 = 0$$

Now let $q \in \mathbb{Q}$ be given. Note that $\left(\frac{q}{n}\right)n = q$, so the simple tensor $q \otimes x$ can be rewritten:

$$q \otimes x = \left(\frac{q}{n}\right)n \otimes x = \left(\frac{q}{n}\right) \otimes nx = \left(\frac{q}{n}\right) \otimes 0 = 0$$

we can move elements of $\mathbb{Z}$ across

(since $nx = 0$ $\forall\, x \in \mathbb{Z}_n$)

So every simple tensor $q \otimes x$ in $\mathbb{Q} \otimes_{\mathbb{Z}} N$ is zero. Then as every element in $\mathbb{Q} \otimes_{\mathbb{Z}} N$ is a sum of simple tensors, <u>every</u> element of $\mathbb{Q} \otimes_{\mathbb{Z}} N$ is zero. So $\mathbb{Q} \otimes_{\mathbb{Z}} N \simeq \{0\}$.

What did we succeed in doing, then?

<u>Theorem</u>: Suppose $R \subset S$ are rings and N is a left R-module. Let $\varphi : N \longrightarrow S \otimes_R N$ be the map $\varphi(n) = 1 \otimes n$. Let M be any left S-module and $\psi : N \longrightarrow M$ any R-module homomorphism. Then there is a unique S-module homomorphism $\overline{\psi} : S \otimes_R N \longrightarrow M$ such that

$$\begin{tikzcd}
N \arrow[r, "\varphi"] \arrow[dr, "\psi"'] & S \otimes_R N \arrow[d, "\overline{\psi}"] \\
& M
\end{tikzcd}$$

commutes.

Remark: • So $S \otimes_R N$ contains a homomorphic image of N, namely $\varphi(N)$, but not N itself.

• In some sense, $\varphi(N)$ is the "biggest" homomorphic image of N that an S-module can contain; because any other homomorphic image (called $\psi(N)$ in our theorem statement) in any other module M arises as a quotient of the image in $S \otimes_R N$ via the map $\overline{\Phi}$.

So, E.G: Returning to $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_n \cong \{0\}$. While arriving at a zero module here is disappointing, every other construction of a $\mathbb{Q}$ module containing a homomorphic image of $\mathbb{Z}_n$ would also give $\{0\}$.

Example: Sometimes $\varphi : N \longrightarrow S \otimes_R N$ is injective. Suppose $N = \mathbb{Z}^n$, considered as a $\mathbb{Z}$-module. Again we use $R = \mathbb{Z}$, $S = \mathbb{Q}$ and consider $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n$. Define a map $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \longrightarrow \mathbb{Q}^n$ by invoking the universal property:

Let $\psi : \mathbb{Z}^n \longrightarrow \mathbb{Q}^n$ be the obvious map

$$(m_1, \dots, m_n) \longmapsto (m_1, \dots, m_n)$$

Then $\overline{\psi} : \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \longrightarrow \mathbb{Q}^n$ exists and satisfies

$$\overline{\psi}(1 \otimes (m_1, \dots, m_n)) = (m_1, \dots, m_n)$$

$$\Rightarrow \overline{\psi}\left(\frac{p}{q} \otimes (m_1, \dots, m_n)\right) = \frac{p}{q}\left(\overline{\psi}(1 \otimes (m_1, \dots, m_n))\right)$$

$$= \frac{p}{q}(m_1, \dots, m_n).$$

This map is injective, thus an isomorphism of S-modules!

To see injectivity, let $\sum_i \frac{p_i}{q_i} \otimes r_i \in \mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n$ be given (so r_i is some vector for each i). Then set

$q = \prod q_i$, and $t_i = \prod_{i \neq j} q_j$, so $\frac{p_i}{q_i} = \frac{p_i t_i}{q}$. Then

$$\sum_i \frac{p_i}{q_i} \otimes r_i = \sum_i \frac{p_i t_i}{q} \otimes r_i = \sum \frac{1}{q} \otimes p_i t_i r_i = \frac{1}{q} \otimes \sum p_i t_i r_i.$$

Now suppose ~~$\overline{\psi}(\frac{p_i}{q_i}$~~ $\overline{\psi}\left(\sum \frac{p_i}{q_i} \otimes r_i\right) = 0$. Then

$$\overline{\psi}\left(\frac{1}{q} \otimes \sum p_i t_i r_i\right) = 0$$

$$\Rightarrow \underbrace{\frac{1}{q}\left(\sum_i p_i t_i r_i\right)}_{\substack{\cap \\ \mathbb{Q}^n}} = 0, \Rightarrow \sum p_i t_i r_i = 0. \text{ But}$$

then $\frac{1}{q} \otimes \sum p_i t_i r_i = \frac{1}{q} \otimes 0 = 0$, so $\overline{\psi}$ is injective.

We can define a tensor product more generally as follows:

Suppose R is a commutative ring with 1 and M, N are R-modules. Construct $A(M \times N)$ as formal sums of pairs:

$$A(M\times N) = \left\{ \sum_{\text{finite}} (m_i, n_i) \;\middle|\; m_i \in M,\ n_i \in N \right\}.$$

Quotient by elements:

$$(m_1+m_2, n) - (m_1, n) - (m_2, n)$$

$$(m, n_1+n_2) - (m, n_1) - (m, n_2)$$

$$(rm, n) - (m, rn),$$ call the quotien $M \otimes_R N$.

Define $r\left(\sum_{\text{finite}} m_i \otimes n_i\right) = \sum_{\text{finite}} rm_i \otimes n_i$, this makes $M \otimes_R N$ a left R-module. There is a similar universal property that characterizes this construction:

$$\begin{tikzcd} M \times N \arrow[r, "\varphi"] \arrow[dr, "\psi"'] & M \otimes_R N \arrow[d, "\bar{\psi}"] \\ & L \end{tikzcd},$$

to be learned in a future course.