BRENDAN WHITAKER
THE OHIO STATE UNIVERSITY
MATHEMATICS

ABSTRACT ALGEBRA II
(MATH 5591H)

Instructor:
Alexander Leibman
Professor
Dept. of Mathematics

January-April, 2018
Lecture Notes

Contents

SECTION 0.1

Review of groups

Theorem 0.1. *(1)*

SECTION 0.2

Review of rings

We note here that $\mathbb{Z}[x]/(x^2-2) \cong \mathbb{Z}[\sqrt{2}]$, but we also have $\mathbb{Z}[x]/(x^2-4) \ncong \mathbb{Z}$. And it is not correct to say $x = \sqrt{2}$ in the former case because these are two distinct elements in the quotient ring.

Definition 0.2. We denote the **group of units** of a ring R as $R^\times$.

Definition 0.3. An **integral domain** is a commutative, unital ring with no zero-divisors.

Definition 0.4. We define the product IJ of ideals I, J as:

$$IJ = \{\, i_1 j_1 + \cdots i_n j_n \mid i_k \in I, j_k \in J \,\}.$$

Definition 0.5. We define the sum $I + J$ of ideals I, J as:

$$I + J = \{\, i + j \mid i \in I, j \in J \,\}.$$

Definition 0.6. A **Noetherian ring** R is a ring in which any collection if ideals in R has a maximal element.

Definition 0.7. A **Noetherian ring** R is a ring in which any ideal is finitely generated.

Theorem 0.8 (**Eisenstein's Criterion**). *Consider $q(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$. If there exists a prime integer p such that the following three conditions all apply:*

- *p divides each a_i for $i \neq n$,*
- *p does not divide a_n,*
- *p^2 does not divide a_0,*

then q is irreducible over the rational numbers.

Part 3

MODULES AND VECTOR SPACES

CHAPTER 10

Introduction to module theory

SECTION 10.1

Basic definitions and examples

Monday, January 8th

Definition 10.1. An **R-module** (left) is a set M with:

(1) Abelian addition operation
(2) Action of R on M s.t.
   (a) $(r+s)m = rm + sm$
   (b) $(rs)m = r(sm)$
   (c) $r(m+n) = rm+rn$ — this says that r acts as a self homomorphism of the ring.
   (d) $1m = m$

   So it's an abelian group with an R-action.

We should think of elements of R as "scalars", and elements of M as "vectors".

Lemma 10.2. *The set Hom(*M, M*)* $= \{$*homomorphisms* $\varphi : M \to M\}$ *is a ring.*

Proof. If you have two homs, you can add them, and the product is a composition. They are associative, under addition, they form a group. And we have the distributive law:

$$\varphi(\xi + \psi) = \varphi\xi + \varphi\psi.$$

You should think of it as similar to the ring of matrices. □

Lemma 10.3. *If* M *is an* R*-module, then we have a ring homomorphism* $\Phi : R \to Hom(M, M)$*. And then mapping is given by* $\Phi : a \to \varphi_a$ *s.t.* $\varphi_a(u) = au$*.*

Note that there may be elements of R that act trivially, i.e. which send every element to zero.

Definition 10.4. Module means left-module.

Definition 10.5. Modules with $1m = m$ are **unital** modules. All modules dealt with are unital.

Definition 10.6. An R**-submodule** is $N \leqslant M$ closed under the ring action ($rn \in N$).

Proposition 10.7 (**The submodule criterion**). *Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if:*

(1) $N \neq \varnothing$,
(2) $x + ry \in N$ for all $r \in R$ and for all $x, y \in N$.

Lemma 10.8. *Every R-module M has two submodules, 0 and M.*

Lemma 10.9. *R is a module over itself, and in this case, the submodules of R are exactly the left ideals of R.*

Definition 10.10. The **free module** of rank n over R is

$$R^n = \{(a_1, ..., a_n) : a_i \in R\}.$$

They are analogous to free groups. The set

$$\{(0, ..., 0, a_i, 0, ..., 0)\}$$

is the i-th component module and is a submodule of the free module.

Lemma 10.11. *If M is an R-module and S is a subring of R with $1_S = 1_R$, then M is automatically an S-module as well.*

Definition 10.12. If M is an R-module and I a two sided ideal of R, we say M is **annihilated** by I when for all $a \in I$, and for all $m \in M$ we have:

$$am = 0.$$

Definition 10.13. We define the **annihilator** of M as $\mathrm{Ann}(M) = \{a \in R : au = 0 \forall u \in M\} = \{a : aM = 0\}$. This is an ideal in R, and it is exactly the kernel of the homomorphism $\Phi : R \to Hom(M, M)$.

Lemma 10.14. *When M is annihilated by I, we can make M into an (R/I)-module by redefining our ring action as:*

$$(r + I)m = rm,$$

which divys the distinct ring actions into cosets of the quotient ring.

Lemma 10.15. *When I is maximal in R and $IM = 0$, M is a vector space over the field R/I.*

Example 10.16. We give some examples of modules:

(1) The 0 module is $\{0\}$, where $a0 = 0\ \forall a$.
(2) R is an R-module.
(3) Free module of rank n, R^n as defined above.
(4) Any abelian group is a $\mathbb{Z}$-module:

$$nu = u + \cdots + u \text{ (n times)}.$$

(5) Any ideal in R is an R-module. $\forall u \in I$, $a \in R$ we have $au \in I$.

(6) (a) Let F be a field, and V an F-vector space. Let T be a linear transfomation of V. Then V is an $F[x]$-module:

$$(a_n x^n + \cdots a_1 x + a_0)u = a_n T^n(u) + \cdots + a_1 T(u) + a_0 u.$$

We have this because we let $xu = Tu$. And we can apply the same construction to any ring, and any modulo over this ring, it doesn't have to be a field.

(b) R-module, $T : M \to M$ is a hom-sm (as R-module, $T(au) = aT(u)$) then M is an $R[x]$-module, $xu = Tu$.

(7) Let R be a ring, X is a set, and $M = \{\text{functions } X \to R\}$.
Then M is an R-module, $(af)(x) = a(f(x))$. In this case we call M an algebra.

Definition 10.17. If A is an R-module, and A is a ring itself with $a(uv) = (au)v = u(av)$ $\forall a \in R$ and $\forall u, v \in A$, then A is called an R**-algebra**.

Lemma 10.18. *If R is a commutative ring, then $\{$functions $X \to R\}$ and R^n are R-algebras.*

Also $M_n = \{n \times n \text{ matrices over } R\}$ is a (noncommutative) R-algebra. (Why?)
If R is a subring of a ring A and $R \subset Z(A)$, then A is an R-algebra. Or: if R, A are rings and $\varphi : R \to A$ is a hom-sm with $\varphi(R) \subset Z(A)$, then again A is an R-algebra, $au = \varphi(a)u$.

Lemma 10.19. *For any ideal I of a ring R, R is an I-algebra.*

Constructions:

(1) Submodule: a subgroup $N \subset M$ s.t. $RN \subset N$.
(2) S is a subring of R and M is an R-module, then $M$is an S-module **(reduction of scalars)**.
(3) M is an R-module, then M is an $R/\mathrm{Ann}(M)$-module.

$$\overline{a}u = au, \overline{a} = a + \mathrm{Ann}(M).$$

Tuesday, January 9th

Recall we noted that if we don't have the condition that $1u = u$. Assume that we don't have this condition. Let M be an R-module without it. Then define:

$$M_0 = \{u \in M : 1u = 0\},$$
$$M_1 = \{u \in M : 1u = u\}.$$

We can check that both of these are submodules of M. $\forall c \in R$, if $u \in M_0$, then $1 \cdot (cu) = c(1u) = 0$, so $cu \in M_0$. And if $u \in M_1$, then $1(cu) = c(1u) = cu$, so $cu \in M_1$. So we have checked that the definition of submodule is satisfied. Also note that $M_0 \cap M_1 = 0$.
And $\forall u \in M$, $u = 1u + (u - 1 \cdot u)$. The stuff on the right side of plus sign is in M_0 and left side is in M_1. So we have $M = M_0 \oplus M_1$.
So $\forall c \in R$, $\forall u \in M_0$, $cu = c \cdot 1u = 0$. So the above statement just says that each element in M can be written as a sum of elements from M_0, M_1.

Keep in mind that what we defined yesterday was a left module. A right module is an abelian group M with mapping $M \times R \to M$ where $(u, a) \to ua$ s.t. we have:

(1) $(u + v)a = ua + va$

(2) $(u(a+b) = ua + ub$
(3) $u(ab) = (ua)b$
(4) $u1 = u$

So note that the first two conditions are unchanged in nature from left modules, since it doesn't matter on which side you multiply the scalar (a). But the third condition is different, because we are now using a right group action. In the left module we first multiplied b by u and then a. Here we do a first, because right group action.

Lemma 10.20. *If R is commutative, then left modules are right modules because we apply commutativity to the difference described above in the third condition.*

Lemma 10.21. *Left ideals in R are left R-modules, and same for right.*

Definition 10.22. A **two-sided R-module** is an abelian group with both left and right module structures.

Note that a two-sided ideal is an example of a two-sided module. We will only deal with commutative rings forever, and we assume that our modules are left modules, except maybe when we discuss tensor products.

Remark 10.23. There are 2 definitions of **annihilators** in module theory. The first is the one used to define $\mathrm{Ann}_R(N)$ where N is a submodule of an R-module M, where we allow $N = M$. This is Definition 10.13. The second is the definition of the annihilator of an ideal in a module, given in Exercise 10 below, which is:

$$Ann_M(I) = \{m \in M : am = 0, \forall a \in I\}.$$

Remark 10.24. If $N \subseteq M$, for some R-module M, then N is always a left-ideal, but not necessarily two sided, this requires N to be a submodule. But if R is commutative, this is unimportant since left ideals are right ideals.

We define the annihilator of a subset $S \subseteq R$.

Definition 10.25.

$$Ann_M(S) = \{u \in M : su = 0, \forall s \in S\}.$$

The annihilator above is an additive subgroup, but not a submodule, we need S to be a **right** ideal in order to get a submodule, since we need $S(cu) = 0$, so we need $Sc \subseteq S$. Also, it is a submodule if R is commutative.

Remark 10.26. If R is commutative, annihilators of subsets of R in M are submodules, and annihilators of subsets of M in R are two-sided ideals.

Now Professor Leibman does Exercise 10.1.11 and several others from this section.

Some particulars on the definitions of an R-algebra:

Definition 10.27 (Leibman's Definition). A is an R-algebra if A is a ring and an R-module so that:

$$a(uv) = (au)v = u(av).$$

Definition 10.28 (Dummit and Foote's Definition). A ring A is an R-algebra if we are given a ring homomorphism $\varphi : R \to A$ s.t. $\varphi(R) \subseteq Z(A)$, where we define the R-action on A by $au = \varphi(a)u$.

Note that if $1 \in A$, then define $\varphi : R \to A$ by $\varphi(a) = a \times 1 \in A$. Hence the two above definitions are equivalent when we have $1 \in A$. So our takeaway is that the top definition (Leibman's) is more general and just better in every way.

10.1 Exercises

1. *Prove that* $0m = 0$ *and* $(-1)m = -m\ \forall m \in M$.

   Proof. Suppose there exists m s.t. $0m = c \neq 0$. Then because of the group structure of our module, we have:

   $$c - c = 0 = 0m - 0m = (0 - 0)m = 0m$$

   which is a contradiction, since we assumed $0m \neq 0$.
   We add:

   $$1m + (-1)m = (1 - 1)m = 0m = 0,$$

   so since $1m = m$, we know $1m + (-1)m = 0 \Rightarrow m + (-1)m = 0 \Rightarrow (-1)m = -m$. □

2. *Prove that* $R^\times$ *and* M *satisfy the two axioms in Section 1.7 for a group action of the multiplicative group* $R^\times$ *on the set* M.

   Proof. Recall that $R^\times$ denotes the group of units of R. The group action properties of a group G acting on a set X are:
   (a) $g_1(g_2x) = (g_1g_2)x$,
   (b) $1x = x\ \forall x \in X$.
   Note that the definition of an R module stipulates that we have $(rs)m = r(sm)\ \forall r, s \in R^\times$ and $\forall m \in M$. And another part of the definition of an R-module gives us that $1m = m\ \forall m \in M$, and since $R^\times$ is a group, we have satisfied the definition of a group action. □

3. *Assume that* $rm = 0$ *for some* $r \in R$ *and some* $m \in M$ *with* $m \neq 0$. *Prove that* r *does not have a left inverse (i.e. there is no such* $s \in R$ *s.t.* $sr = 1$*).*

   Proof. Suppose there were such an s. Then we would have:

   $$srm = 1m = m = s(0) = 0,$$

   which is a contradiction, since we said $m \neq 0$. □

5. *For any left ideal* I *of* R, *define:*

   $$IM = \{ \sum_{finite} a_i m_i : a_i \in I, m_i \in M\}$$

   to be the collection of all finite sums of elements of the form am *where* $a \in I$ *and* $m \in M$. *Prove that* IM *is a submodule of* M.

Proof. We know IM is nonempty since I contains 0, so $0m \in IM$, and by exercise 1, we know $0 \in IM$. So let $x, y \in IM$ such that:

$$x = a_1m_1 + \cdots + a_km_k$$

$$y = b_1n_1 + \cdots + b_ln_l$$

with $a_i, b_i \in I$, $m_i, n_i \in M$, and let $r \in R$. Then we have the following by the distributive property of scalars in the definition of an R-module:

$$\begin{aligned} x + ry &= a_1m_1 + \cdots + a_km_k + r(b_1n_1 + \cdots + b_ln_l) \\ &= a_1m_1 + \cdots + a_km_k + rb_1n_1 + \cdots rb_ln_l. \end{aligned} \tag{10.1}$$

Now since I is a left ideal, we know $rb_i \in I$ since $b_i \in I$, so $x + ry$ is a finite sum of elements of the form a_im_i and so it is in IM. Then by the submodule criterion, IM is a submodule of M. □

6. *Show that the intersection of any nonempty collection of submodules of an R-module M is a submodule.*

   Proof. Let $N = \cap N_i$ be an arbitrary collection of submodules of M. Recall from group theory that an arbitrary intersection of subgroups is a subgroups, so we know $N \leqslant M$. So we need only show that it is closed under the group action of R. So let $r \in R$, and let $n \in N$. Then $n \in N_i$ $\forall i$. So $rn \in N_i$ $\forall i$ since N_i is a submodule of M. But then $rn \in N$ by definition, so N is a submodule. □

7. *Let $N_1 \subset N_2 \subset \cdots$ be an ascending chain of submodules of M. Prove that $N = \cup_{i=1}^{\infty} N_i$ is a submodule of M.*

   Proof. We first prove that N is a subgroup under addition of M. It is a subset of M since it is a union of subsets of M. Since $0 \in N_1$, and $N_1 \subset N_i$ $\forall i$, we know $0 \in N_i$ $\forall i$, so $0 \in N$. Let $n \in N$, then $n \in N_i$ for some i, so we have $-n \in N_i \subset N$, so we have additive inverses. And let $n_1, n_2 \in N$, then $n_1 \in N_i, n_2 \in N_j$ for some i, j, and without loss of generality, we may assume $i \leqslant j$. Then $N_i \subset N_j$, so $n_1 \in N_j$, and by closure of the subgroup N_j, we know $n_1 + n_2 \in N_j \subset N$, so we have additive closure of N, hence it is a subgroup of M. Now we show that N is closed under the ring action of R. So let $r \in R$, and let $n \in N$, then $n \in N_i$ for some i, so $rn \in N_i$ since N_i is a submodule, and since $N_i \subset N$, we know $rn \in N$, so N is a submodule. □

8. *An element m of the R-module M is called a torsion element if $rm = 0$ for some nonzero element $r \in R$. The set of torsion elements is denoted:*

   $$Tor(M) = \{m \in M : rm = 0 \text{ for some nonzero } r \in R\}.$$

   (a) *Prove that if R is an integral domain, then $Tor(M)$ is a submodule of M (called the torsion submodule of M).*

   Proof. We know $\mathrm{Tor}(M)$ is a subset of M by its definition. We first prove it is an additive subgroup. Let $m \in$

Tor(M). Then $\exists r \in R$, $r \neq 0$ s.t. $rm = 0$. Then consider $-m \in M$. From exercise 1 we know $-m = (-1)m$, so we have:

$$r(-m) = r(-1)m = (-1)rm = (-1)0 = 0,$$

since R is commutative. So we have that $-m \in$ Tor(M) as well, hence we have additive inverses. We check that it has additive closure. Let $m, n \in$ Tor(M). Then we have $r, s \in R$, neither being zero, s.t. $rm = 0, sn = 0$. Now consider $m + n$. We have:

$$rs(m+n) = rsm + rsn = srm + rsn = s0 + r0 = 0.$$

Since we have no zero divisors, since R is an integral domain, we know $rs \neq 0$, so $m + n \in$ Tor(M), we have additive closure, and Tor(M) is a subgroup of M. Now we need only check that it is closed under the left action of R. So let $r \in R$ and $m \in$ Tor(M). Then consider rm. We assume $r \neq 0$, since otherwise $rm = 0$ which is in our subgroup. And we know $\exists s \in R$, $s \neq 0$ s.t. $sm = 0$. Now we have $srm = rsm = r0 = 0$, so rm is in Tor(M). So it's a submodule. □

(b) *Give an example of a ring R and an R-module M such that $Tor(M)$ is not a submodule (consider the torsion elements in the R-module R).*
So from the previous exercise, we know we must choose some R which is not an integral domain. We consider the torsion elements in the R-module R, which are:

$$\text{Tor}(R) = \{r \in R : sr = 0 \text{ for some nonzero } s \in R\},$$

but these are exactly the right zero divisors of R. We consider the ring $R = \mathbb{Z}_6 \cong \mathbb{Z}/6\mathbb{Z}$, and the module of R over itself. Note that in R, $2 \cdot 3 = 6 = 0$, $4 \cdot 3 = 12 = 0$, and $1, 5$ are not zero divisors, so we have:

$$\text{Tor}(R) = \{0, 2, 3, 4\}.$$

So note that $2, 3 \in$ Tor(R) and $1 \in R$, but $2 + 1 \cdot 3 = 5 \notin$ Tor(R), so by the submodule criterion, it is not a submodule.

(c) *If R has zero divisors, show that every nonzero R-module has nonzero torsion elements.*
PROOF. Suppose R has zero divisors. So $\exists r, s \in R$ nonzero such that $rs = 0$. Now let M be an R-module. We wish to show that $\exists m \in M$ s.t. $m \neq 0$, $tm = 0$ for some nonzero $t \in R$. Let $n \in M$ s.t. $n \neq 0$. Now consider $sn \in M$ and $r \in R$. Now note that $rsn = 0$ and that r and sn are both nonzero, so sn is a nonzero torsion element. □

9. *If N is a submodule of M, the annihilator of N in R is defined to be:*

$$Ann_R(N) = \{r \in R : rn = 0 \textit{ for all } n \in N\}.$$

Prove that the annihilator of N in R is a two-sided ideal of R.

Proof. Let $A = \text{Ann}_R(N)$. We first show that A is an additive subgroup of R. We know it is nonempty since $0 \in A$, and it is a subset of R by construction. Now let $x, y \in A$. Consider $x(-y) = -xy$. Note $-xyn = -x(yn) = -x0 = 0\ \forall n \in N$, so by the subgroup criterion, A is a subgroup. Let $r \in R$, $n \in N$, and $a \in A$. Observe:

$$ran = r(an) = r0 = 0,$$

$$arn = a(rn) = 0,$$

since a annihilates n, and N is closed under the action of R, so $rn \in N$, and hence a also annihilates (rn). Since our n was arbitrary, this holds for all $n \in N$. Thus $ra \in A$ and $ar \in A$, and thus $RA \subseteq A$ and $AR \subseteq A$, so since it's also an additive subgroup, A is a two-sided ideal. □

10. *If I is a right ideal of R, the annihilator of I in M is defined to be:*

$$Ann_M(I) = \{m \in M : am = 0 \text{ for all } a \in I\}.$$

Prove that the annihilator of I in M is a submodule of M.

Proof. Since I is a right ideal, we know $Ir \subseteq I\ \forall r \in R$. Let $A = \text{Ann}_M(I)$ which we know is nonempty since $0 \in M$ since it is an abelian group, and $a0 = 0\ \forall a \in I$. Let $m, n \in A$, let $a \in I$, and let $r \in R$. Observe:

$$a(m + rn) = am + arn = 0 + arn = (ar)n = 0,$$

since $a \in I \Rightarrow ar \in I$ (I is right ideal), hence n annihilates (ar). Thus $(m + rn) \in A$. Then by the submodule criterion, since this holds for arbitrary $m, n \in A$, $r \in R$, and A is nonempty, we know A is a submodule of M. □

11. *Let M be the abelian group (i.e. $\mathbb{Z}$-module) $\mathbb{Z}/24\mathbb{Z} \times \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/50\mathbb{Z}$.*

(a) *Find the annihilator of M in $\mathbb{Z}$ (i.e. a generator for this principal ideal).*

Recall that $\text{Ann}_{\mathbb{Z}}(M) = \{z \in \mathbb{Z} : zm = 0, \forall m \in M\}$. Observe that the least common multiple of $24, 15, 50$ is 600. We claim that this is a generator for the principal ideal given by $\text{Ann}_{\mathbb{Z}}(M)$. We must only check that it is nonzero, which is obvious, and that $600m = 0$, $\forall m \in M$. So let $m \in M$, then $m = (a, b, c)$ s.t. $a \in \mathbb{Z}/24\mathbb{Z}$, $b \in \mathbb{Z}/15\mathbb{Z}$, and $c \in \mathbb{Z}/60\mathbb{Z}$. Now observe:

$$600m = 600(a, b, c) = (600a, 600b, 600c) \equiv (0, 0, 0) = 0 \in M,$$

since $600 \equiv 0 \mod 24, 15, 50$. So $\text{Ann}_{\mathbb{Z}}(M) = \langle 600 \rangle$.

(b) *Let $I = 2\mathbb{Z}$. Describe the annihilator of I in M as a direct product of cyclic groups.*

Recall that $\text{Ann}_M(I) = \{m \in M : mr = 0, \forall r \in I\}$. Thus we know:

$$Ann_M(I) = \{(a, b, c) \in M : (a, b, c)\},$$

$$Ann_M(2\mathbb{Z}) = \{0, 12\} \times \{0\} \times \{0, 25\}$$

12. (a) *N is a submodule of M, $I = Ann(N)$, and $K = Ann(I)$. Then $N \subseteq K$. Give an example where $N \neq K$. We have notation for annihilator, $AnnN = N^\perp$.*
    Note that $N \subseteq (N^\perp)^\perp$. Also note that for all $a \in I$, $\forall u \in N$, $au = 0$, so $u \in I^\perp$. So take $M = \mathbb{Z}_6 \times \mathbb{Z}_6$, $N = \{0,3\} \times \{0\}$, where we consider these two objects as $\mathbb{Z}$-modules (abelian groups). Note $I = N^\perp = 2\mathbb{Z}$. And $I^\perp = \{0,3\} \times \{0,3\}$.

    (b) *I is an ideal in R. Then $I \subseteq (I^\perp)^\perp$. Give an example where they are not equal.*
    Take $M = \mathbb{Z}_2, I = (4)$, then $I^\perp = M$, but $M^\perp = (2)$.

13. *I - ideal in R. $M' = \{u \in M : I^k u = 0$ for some $k \in \mathbb{N}\}$. Then prove that M' is a submodule.*

    Proof. For any k, let $M_k = Ann(I_k)$. Then note that $M_1 \subseteq M_2 \subseteq \cdots$. If $I \subseteq J$, then $Ann(J) \subseteq Ann(I)$. Then $M' = \bigcup_{k=1}^\infty M_k$ is a submodule (can be easily checked). □

18. *Let $V = \mathbb{R}^2$, and let $R = \mathbb{R}[x]$. Let x be the 2 by 2 matrix with 0,-1,1,0. And let x act on V by counterclockwise rotations by 90 degrees. Then V is an R-module. Prove that V is simple. Note that R is isomorphic to $\mathbb{C}$.*

    Proof. A general rule is that submodules of V are x-invariant subspaces of V as an R-module. □

19. *Let $F = \mathbb{R}$, and $V = \mathbb{R}^2$, and let T be the linear transformation that projects to the y-axis. Show that $V, 0$, the x-axis, and the y-axis are the only $F[x]$-submodule for T.*

    Proof. Note it's obvious that $0, V$ work as subspaces. Note to be a subspace we need $x + ry$ to be in the space for all r. Note our scalars in this case are polynomials in T, and they're going to send this expression to x plus some polynomial function of the y coordinate of y, so it will move up and down in a vertical line in $\mathbb{R}^2$ from where x was. Now in order for this to be in a 1-dimensional subspace, we need to have all points above and below any point in the space also in our space, unless the y coordinates are all zero, so the x-axis and y-axis work, and non others do. Note any potential subspace must go through the origin as well. □

20. *Let $F = \mathbb{R}$, and $V = \mathbb{R}^2$, and let T be the linear transformation that rotates by π. Show that every subspace of V is an $F[x]$-submodule for T.*

    Proof. For the trivial space and the whole space it is obvious. For any subspace of V which is 1-dimensional, it's a line through the origin, and a rotation by π brings us back to the same line. □

SECTION 10.2

Quotient modules and module homomorphisms

Definition 10.29. Let M, N be R-modules, $\varphi : M \to N$ is an R-**homomorphism** if:

(1) $\varphi(u+v) = \varphi(u) + \varphi(v)$
(2) $\varphi(au) = a\varphi(u)$.

So it is a homomorphism of groups, and also preserves scalar mult.

Definition 10.30. If R is a field and M is then a vector space, φ is called a **linear mapping**, or a **linear transformation**.

The set of all R-hom-sms from $M \to N$ is denoted by $\mathrm{Hom}_R(M, N)$.

Definition 10.31. In the case $M = N$, hom-sms $M \to M$ are called **endomorphisms**, and:

$$\mathrm{Hom}_R(M, M) = \mathrm{End}_R(M).$$

Definition 10.32. Injective hom-sms are called **monomorphisms**.

Definition 10.33. Surjective hom-sms are called **epimorphisms**.

Definition 10.34. Bijective hom-sms are called **isomorphisms**.

Definition 10.35. Bijective endomorphisms $(M \to M)$ are called **automorphisms**.

Lemma 10.36. *If R is a commutative ring, $Hom_R(M, N)$ is an R-module, by*

- $\varphi + \psi)(u) = \varphi(u) + \psi(u)$,
- $(a\varphi)(u) = a\varphi(u)$.

So why does it have to be commutative?

Proof. So is $a\varphi$ a hom-sm? So consider:

$$(a\varphi)(bu) = a(\varphi(bu)) = ab\varphi(u) \neq b(a\varphi)(u) = ba\varphi(u),$$

if $ab \neq ba$, so if R is noncommutative, $a\varphi$ may not be a hom-sm. □

If R is commutative, $\mathrm{End}_R(M)$ is an R-algebra, because $(\varphi\psi)(u) = \varphi(\psi(u))$, and you also have to prove that it is a ring. Under an addition it is a group, associativity is clear, and the distributive law:

$$\varphi(\psi + \xi)(u) = \varphi(\psi(u) + \xi(u)) = \varphi(\psi(u)) + \varphi(\xi(u)) = (\varphi\psi)(u) + (\varphi\xi)(u),$$

the first equality is by definition, the second is by def of hom-sm. And we also must check that scalar multiplication is preserved to prove that it is an algebra. We have:

$$((a\varphi)\psi)(u) = (\varphi(a\psi))(u) = a(\varphi\psi)(u)$$
$$((a\varphi)\psi)(u) = (a\varphi)(\psi(u)) - a(\varphi(\psi(u)))$$
$$(\varphi(a\psi))(u) = \varphi((a\psi)(u)) = \varphi(a\psi(u)) = a\varphi(\psi(u))$$

check over these conditions, confusing And $\mathrm{Aut}_R(M)$ is a group under multiplication (compositions), which is exactly the group of units in $\mathrm{End}_R(M)$. We outline some elementary properties of modules:

(1) $0u = 0$

Proof.

$$0u = (0 + 0)u = 0u + 0u,$$

so done. □

(2) $a0 = 0$
(3) $(-a)u = a(-u) = -au$

Example 10.37. We give some examples of R-hom-sms:

(1) $\mathbb{Z}$-modules = abelian groups (written additively). So what are $\mathbb{Z}$-hom-sms of $\mathbb{Z}$-modules? They are of course, the hom-sms of the abelian groups. If $\varphi : G \to H$ is a group hom-sm, then $\varphi(nu) = n\varphi(u)$. For vector spaces, this is not true. Note in this case:

$$\varphi : V \to W, \varphi(u+v) = \varphi(u) + \varphi(v) \not\Rightarrow \varphi(cu) = c\varphi(u),$$

it only works for $\mathbb{Z}$-modules.

(2) If R is commutative, and $c \in R$, then $\varphi(u) = cu$ is an R-endomorphism of M. Note:

$$\varphi(u+v) = c(u+v) = cu + cv = \varphi(u) + \varphi(v),$$

$\forall a \in R$, $\varphi(au) = cau = acu = a\varphi(u)$.

Consider $\varphi : \mathbb{Z} \to \mathbb{Z}$ given by $\varphi(n) = 2n$. It isn't a ring hom-sm since it doesn't respect mult ($\varphi(mn) \neq \varphi(m)\varphi(n)$. **But this is** a hom-sm of $\mathbb{Z}$-modules. Why? Because $\varphi(mn) = m\varphi(n)$. Now consider the ring of polyns $R = F[x,y], \varphi : x \leftrightarrow y$. Then note φ is automorphism of R, but is not a hom-sm of R-modules. Why? because it doesn't respect multiplication by scalars, take

$$yx = \varphi(xy) \neq x\varphi(y) = xx.$$

The **kernel and image** of a hom-sm are submodules. There are no "normal" submodules, we can factorize by any of them.

Wednesday, January 10th

Lemma 10.38. *Let $\varphi : M \to N$ be a hom-sm of R-modules. Then $ker\varphi$ and $\varphi(M)$ are submodules of M and N respectively.*

Proof. Recall K is a submodule of M if K is a subgroup of M and $RK \subseteq K$. So we will show that the two objects in the above remark are submodules. The kernel and the image are groups, if $u \in ker\varphi$, then for any $a \in R$, $\varphi(au) = a\varphi(u) = 0$l, so au is in the kernel. If $v \in \varphi(M)$, $v = \varphi(u)$, then for any $a \in R$,

$$av = \varphi(au),$$

so $av \in \varphi(M)$. □

Definition 10.39. A module M is **simple**, or **irreducible**, if it has no submodules (except 0 and itself).

There are many simple modules. We will discuss Schur's Lemma.

Lemma 10.40 (**Schur's Lemma**). *If M, N are simple R-modules, then any R-hom-sm $\varphi : M \to N$ is either 0 or an isomorphism.*

Proof. The kernel of φ is a submodule of M, so $ker\varphi = 0$ or $\ker\varphi = M$. $\varphi(M)$ is submodule, so it is either 0 or M. If $\ker\varphi = M$, or $\varphi(M) = 0$, then $\varphi = 0$ (obvious).
Otherwise, $\ker\varphi = 0$ and $\varphi(M) = N$, so φ is an isomorphism. □

Corollary 10.41. *If R is commutative, and M is a simple R-module, then $End_R(M) = Hom_R(M, M)$ is a division ring.*

The only example of a **noncommutative division ring** we have is the quaternions:

$$\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}.$$

Now we will discuss **factorization of modules**.

Definition 10.42. Let M be a module, and N a submodule of M, then

$$M/N = \{a + N : a \in M\}$$

has a structure of an R-module.

Recall that you needed a two-sided ideal to get a quotient ring, but we only need a left ideal to get a quotient module.

Example 10.43. If R is a ring, and I is a left ideal in R, then R/I is not a ring, but it is an R-module.

Example 10.44. Consider space R of square matrices with entries in a set S, and the ideal I with zeroes in the first column and arbitrary elements in all other spots. Then R/I is the set of all first columns and is isomorphic to S^n. The ideal is left and the resulting quotient is a module, but not a ring.

Observe that M/N is an abelian group. $\overline{u} = u + N \in M/N$. Let $a \in R$, then:

$$a\overline{u} = au + aN \subset au + N = \overline{au}.$$

Or: if $v = u \mod N$, $v - u \in N$, then $av = au \mod N$, $av - au = a(v - u) \in N$. So multiplication by scalars is well defined on M/N.

Theorem 10.45. ***Isomorphism Theorems:***

1. *If $\varphi : M \to N$ is an R-hom-sm of R-modules, then $\varphi(M) \cong M/ker\varphi$ (isomorphic as modules).*
2. *Let N, K be submodules of an R-module M, then*

$$N + K = \{u + v\}$$

is a submodule and $(N + K)/K \cong N/(N \cap K)$.

3. *If N is a submodule of N and K is a submodule of N, then:*

$$M/N \cong \frac{(M/K)}{(N/K)}.$$

4. *Submodules of M/N are in bijection with submodules of M containing N. The correspondence is:*

$$K \leftrightarrow K/N$$

where $K \subseteq M$ and $K/N \subseteq M/N$.

Remark 10.46. $N + K$ is the smallest module containing both N and K.

10.2 Exercises

4. *A is a $\mathbb{Z}$-module. $H' = Hom(\mathbb{Z}_n, A) = ?$*

Recall $Hom(\mathbb{Z}, A) \cong A$, since from another exercise we have

$$Hom(R, M) \cong M$$

as R-modules, since we map $\varphi \in H$ to $\varphi(1)$. So we do the same thing. We map $\varphi \in H'$ to $\varphi(1)$. So we must have $\varphi(n) = n\varphi(1) = 0$. So $\varphi(1)$ must satisfy $n\varphi(1) = 0$. So we have $\varphi(1) \in \text{Ann}(n)$. And this map is injective, $H' \to A$. On the other hand, if $b \in A$, and $nb = 0$, then define $\varphi(\overline{k}) = bk$, $k \in \mathbb{Z}$, and $\varphi \in H'$, where $\overline{k} = k$ mod n. So, $\text{Hom}(\mathbb{Z}_n, A) \cong \{\, a \in A : na = 0 \,\} = \text{Ann}(n)$.

Generalization: What are $H_1 = \text{Hom}(R, M) \cong M$? And what are $H_2 = \text{Hom}(R/I, M) \cong$? So we must have that $H_2 \subseteq H_1$. We have:

$$H_2 = \{\, u \in M : Iu = 0 \,\} = Ann(I).$$

Then we map $\varphi \mapsto \varphi(1)$, and I is sent to zero.

Now $\text{Hom}(R^n, M) \cong M^n$, since we map $\varphi \mapsto (\varphi(e_1), ..., \varphi(e_n))$. Or we can use the exercise from the last homework:

$$Hom(A \oplus B, M) \cong Hom(A, M) \oplus Hom(B, M),$$

since:

$$Hom(R^n, M) \cong Hom(R, M)^n \cong M^n.$$

Another one: $\text{Hom}(R^n/I, M) \cong Ann(I) \subseteq M^n$, where I is an ideal in R^n.

Another one: $\text{Hom}(A, B^n) \cong Hom(A, B)^n$, since we proved that

$$Hom(A, B \oplus C) \cong Hom(A, B) \oplus Hom(A, C).$$

Another one: $\text{Hom}(R^n, R^m) \cong R^{nm}$. These are $m \times n$ matrices over R. We have a basis $e_1, ..., e_n \in R^n$ and a basis $\{\, b_i \,\} \subseteq R^m$. So for any i, we have:

$$\varphi(e_i) = c_{1,i}b_1 + \cdots + c_{m,i}b_m.$$

And these coefficients $\{\, c_i \,\}$ are just elements of the matrix. We have a standard basis in this module, which are matrices which are zero everywhere except for one entry, and the value of this entry is 1 (typical vector space basis over $\mathbb{R}$). We do get a different isomorphism if we change our basis, so is it canonical? It is canonical because R^n has a standard basis, and so does R^m and given these bases, we have a canonical basis for R^{nm}. If we deal with an abstract free module, we may not have a standard basis.

Another one: $\text{Hom}(R, R) \cong R$ as rings. This is easy. Map $\varphi \mapsto \varphi(1)$. The checking is easy. This is actually the ring $\text{End}_R(R)$. Let's check it:

$$(\varphi\psi)(1) = \varphi(\psi(1)) = \varphi(\psi(1) \cdot 1) = \psi(1)\varphi(1).$$

We have this last equality because $\varphi(1)$ is a scalar element of R and so we can take it out of ψ. And We also know $\text{End}_R(R^n) \cong$

$M_{n\times n}(R)$. Multiplication is defined so that this is a ring isomorphism.

6. *Prove that $Hom_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/m\mathbb{Z}) \cong \mathbb{Z}/(n,m)\mathbb{Z}$.*

   Proof. Let $H = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m)$, and let $K = \mathbb{Z}/(n,m)$. Also, let $l = \gcd(n,m)$. Then $K = \mathbb{Z}_l$. So let $\varphi \in H$. Then $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$. We note here that φ is completely determined by where it sends $1 \in \mathbb{Z}_n$, since we must have $\varphi(n\cdot 1) = \varphi(0) = 0$ by the definition of a group homomorphism, thus we must have that $n\varphi(1) = 0 \in \mathbb{Z}_m$. In order to have $n\varphi(1) = 0$, we need $\varphi(1)$ to be a multiple of m. So we need $\varphi(1)$ to be a multiple of m/l, since every prime factor in l is also in the factorization of n, so we need only the prime factors of m which are not in l, hence $\varphi(1)$ must be a multiple of m/l. Now note there are exactly l multiples of m/l in $\mathbb{Z}_m$. We denote these $a_0, ..., a_{l-1}$. So we have exactly l distinct homomorphisms in H, so we denote these $\varphi_0, ..., \varphi_{l-1}$, where $\varphi_i(1) = a_i = im/l \in \mathbb{Z}_m$. Then let $\Phi : H \to K$ be given by:

$$\Phi(\varphi_i) = i \in \mathbb{Z}_l.$$

   We prove this map is an isomorphism. **Homomorphism:** Observe:

$$\Phi(\varphi_i + \varphi_j) = \Phi(\varphi_{i+j \mod l}) = i + j = \Phi(\varphi_i) + \Phi(\varphi_j) \in \mathbb{Z}_l.$$

   The first equality is by the additive operation on the $\mathbb{Z}$-module H, and the other equalities follow from the definition of Φ and the additive operation on $\mathbb{Z}_l$. Since φ_i is a homomorphism of R-modules, it preserves multiplication by scalars, so we have $z\varphi_i(1) = \varphi_i(z) = za_i$, and since $\{a_i\} \cong \mathbb{Z}_l$ as a group, we know $za_i = a_{zi \mod l}$. So we have:

$$\Phi(z\varphi_i) = zi = z\Phi(\varphi_i) \in \mathbb{Z}_l.$$

   So Φ preserves scalar mult, and hence it is a homomorphism.
   Surjectivity: Let $i \in \mathbb{Z}_l$. Then consider $\psi \in H$ s.t. $\psi(1) = im/l$, but this is exactly how we defined φ_i, so we know $\varphi_i = \psi$, and then $\Phi(\psi) = \Phi(\varphi_i) = i$. So Φ is surjective.
   Injectivity: Let:

$$\Phi(\psi) = \Phi(\xi),$$

   then since we enumerated all the elements of H, we know we must have $\psi = \varphi_i$ and $\xi = \varphi_j$ for some $0 \leqslant i, j \leqslant l - 1$. Then we have:

$$\Phi(\varphi_i) = i = j = \Phi(\varphi_j) \in \mathbb{Z}_l,$$

   so $i \equiv j \mod l$, but since both these numbers are between 0 and $l - 1$, we know $i = j$, so $\psi = \xi$, and Φ is injective. Hence it is an isomorphism. □

9. *Let R be a commutative ring. Prove that $Hom_R(R, M)$ and M are isomorphic as left R-modules. [Show that each element of $Hom_R(R, M)$ is determined by its value on the identity of R.]*

   Proof. Recall:

$$H = \mathrm{Hom}_R(R, M) = \{\varphi : R \to M\},$$

where R and M are R-modules. Let $\varphi \in H$. Recall that from the definition of H, we know:

$$\varphi(rs + t) = r\varphi(s) + \varphi(t),$$

for all $r, s, t \in R$. So note that $\forall r \in R$, we have:

$$\varphi(r) = r\varphi(1_R),$$

hence φ is complete determined by its value on 1_R. Also observe that $\varphi(1_R) \in M$, so define a map $\Phi : M \to H$ by $\Phi(m) = \varphi_m$, where we define $\varphi_m(1_R) = m$. We prove this map is an R-module isomorphism. We first prove it is an R-module homomorphism. So let $m, n \in M$, then we have:

$$\Phi(m) + \Phi(n) = \varphi_m + \varphi_n$$

Now we prove surjectivity. So let $\psi \in H$, then $\psi(1_R) = m$ for some $m \in M$, so we know $\psi = \varphi_m$. Then note that $\Phi(m) = \varphi_m$, so Φ is surjective. □

11. *Let $A_1, A_2, ..., A_n$ be R-modules and let B_i be a submodule of A_i for each $i = 1, 2, ..., n$. Prove that:*

$$(A_1 \times \cdots \times A_n)/(B_1 \times \cdots \times B_n) \cong (A_1/B_1) \times \cdots \times (A_n/B_n).$$

Proof. So let $A = (A_1 \times \cdots \times A_n)$, $B = (B_1 \times \cdots \times B_n)$, and $C = (A_1/B_1) \times \cdots \times (A_n/B_n)$. Note that:

$$A/B = \{ (a_1, ..., a_n) + B \}.$$

We know B is a submodule of A since it is clearly a subset since each component b_i of $(b_1, ..., b_n)$ is also in A_i. Also:

$$(b_1, ..., b_n) + r(d_1, ..., d_n) = (b_1, ..., b_n) + (rd_1, ..., rd_n) = (b_1 + rd_1, ..., b_n + rd_n),$$

because of how we defined add. and mult. by R in the R -module B, and because each B_i is a submodule of A_i. Then we know A/B is an R-module since we may factorize by any submodule of A. , so we let $\varphi : A/B \to C$ be given by

$$\varphi((a_1, a_2, ..., a_n) + B) = (a_1 + B_1, a_2 + B_2, ..., a_n + B_n).$$

We prove that φ is an isomorphism.

Homomorphism: Let $(x_1, x_2, ..., x_n) + B, (y_1, y_2, ..., y_n) + B \in A/B$, then

$$\begin{aligned}
&\varphi(((x_1, x_2, ..., x_n) + B) + ((y_1, y_2, ..., y_n) + B)) \\
&= \varphi(((x_1, x_2, ..., x_n) + (y_1, y_2, ..., y_n)) + B) \\
&= \varphi((x_1 + y_1, x_2 + y_2, ..., x_n + y_n) + B) \\
&= (x_1 + y_1 + B_1, x_2 + y_2 + B_2, ..., x_n + y_n + B_n) \qquad (10.2)\\
&= (x_1 + B_1, x_2 + B_2, ..., x_n + B_n) \\
&+ (y_1 + B_1, y_2 + B_2, ..., y_n + B_n) \\
&= \varphi((x_1, x_2, ..., x_n) + B) + \varphi((y_1, y_2, ..., y_n) + B),
\end{aligned}$$

by the direct product operation on A/B and C. And for multiplication, we have:

$$\begin{aligned}\varphi(r((x_1,...,x_n)+B)) &= \varphi(r(x_1,...,x_n)+B)\\ &= \varphi(rx_1,...,rx_n)+B)\\ &= (rx_1+B,...,rx_n+B)\\ &= r(x_1+B,...,x_n+B)\\ &= r\varphi((x_1,...,x_n)+B),\end{aligned} \tag{10.3}$$

so φ is a homomorphism.

Injection: Let $(x_1,x_2,...,x_n)+B,(y_1,y_2,...,y_n)+B \in A/B$, and let

$$\begin{aligned} &\varphi((x_1,x_2,...,x_n)+B) = \varphi((y_1,y_2,...,y_n)+B)\\ \Rightarrow\ &(x_1+B_1,x_2+B_2,...,x_n+B_n) = (y_1+B_1,y_2+B_2,...,y_n+B_n).\end{aligned} \tag{10.4}$$

So then we have that $x_i+B_i = y_i+B_i$ for all i, thus

$$\begin{aligned}(y_1,y_2,...,y_n)+B &= (y_1,y_2,...,y_n)+(B_1\times B_2\times\cdots\times B_n)\\ &= (y_1+B_1\times y_2+B_2\times\cdots\times y_n+B_n)\\ &= (x_1+B_1\times x_2+B_2\times\cdots\times x_n+B_n) = (x_1,x_2,...,x_n)+B\end{aligned} \tag{10.5}$$

by the direct product operation, so φ is in injective.

Surjection: Let $(a_1+B_1,a_2+B_2,...,a_n+B_n) \in C$. Then we must have that $a_i \in A_i$ for all i by definition of C and the quotient modules A_i/B_i, so $(a_1,a_2,...,a_n) \in A \Rightarrow (a_1,a_2,...,a_n)+B \in A/B$, and $\varphi((a_1,a_2,...,a_n)+B) = (a_1+B_1,a_2+B_2,...,a_n+B_n)$, so φ is surjective by definition. Hence φ is an isomorphism, and $A/B \cong C$. □

12. *Let I be a left ideal of R and let $n \in \mathbb{N}$. Prove:*

$$R^n/IR^n \cong R/IR\times\cdots\times R/IR$$

.

Proof. So we use the first isomorphism theorem. We map $R^n \to (R/I)^n$ by $(a_1,...,a_n) \mapsto (a_1 \mod I,...,a_n \mod I) = (\overline{a_1},...,\overline{a_n}) \in (R/I)^n$. This is clearly surjective. And the kernel is just $I^= \{ (a_1,...,a_n) : a_i \in I \}$. And $I^n = IR^n$, why?

Proof. Take:

$$IR^n = \left\{ \sum b_i(a_{i,1},...,a_{i,n}) : b_i \in I \right\}.$$

And also take note: $(b_1,...,b_n) \in I$ can be written as:

$$(b_1,...,b_n) = b_1(1,...,0)+\cdots+b_n(0,...,0,1) \in IR^n.$$

So these are the same object. □

□

SECTION 10.3

Generation of modules, direct sums, and free modules

Assume R is a unital ring, i.e. that $1 \in R$.

Definition 10.47. Let M be an R-module and S be a subset of M. We say that M is **generated by** S if for any $u \in M$, there exists $v_1, ..., v_k \in S, a_1, ..., a_k \in R$ such that:

$$u = a_1 v_1 + \cdots + a_k v_k,$$

which is called a **linear combination** of $v_1, ..., v_k$.

We could define it another way.

Definition 10.48. Let $S \subseteq M$. Then

$$RS = \{a_1 v_1 + \cdots + a_k v_k : a_i \in R, v_i \in S\}$$

is the smallest submodule of M containing S. RS is called the **submodule generated by** S**.**

Remark 10.49. M is generated by S iff $M = RS$.

Definition 10.50. The **free module generated by** S is the set of functions $f : S \to R$ s.t. $f(s) = 0$ for all but finitely many $s \in S$.

So consider the case where S is finite to simplify the discussion: If $S = \{s_1, ..., s_n\}$, the free module is $\{a_1 s_1 + \cdots + a_n s_n : a_i \in R, s_i \in S\}$.

It is the direct sum of $|S|$ copies of R. Equivalently, the free module is:

$$\{a_1 s_1 + \cdots + a_n s_n : a_i \in R, s_i \in S\},$$

the set of formal linear combinations of elements in S. Each element in this set corresponds to a function $f : s_i \to a_i$ and maps s to zero if $s \neq s_1, ..., s_n$. You should think of this like a free group.

The difference between the above definitions is the free generated module is the case where S is not a subset of M, it is just some random set.

Let M be an R-module, let S be a subset of M. let F be the free module generated by S, then we have a unique hom-sm $\varphi : F \to M$ s.t. $\varphi(s) = s \ \forall s \in S$.

$$\varphi(a_1 s_1 + \cdots + a_n s_n) = a_1 s_1 + \cdots + a_n s_n \in M.$$

On the left hand side inside φ we see a formal linear combination, the s's are just letters, we forget that they come from a subset of M. They are just symbols. On the right hand side, we are in M, so we remember that $S \subseteq M$.

Example 10.51. Let $S = \{2, 3\} \subseteq \mathbb{Z}$. And let:

$$F = \{n \cdot 2 + m \cdot 3\} \cong \mathbb{Z}^2,$$

where in the above we see $2, 3$ as just symbols, easily replaceable by x, y. Now consider a map $F \to \mathbb{Z}$, where $n \cdot 2 + m \cdot 3 \to 2n + 3m$ and on the left hand side of this map, we then remember that $2, 3$ are numbers.

If M is generated by S, then φ is surjective, and $M \cong F / ker \varphi$.

Definition 10.52. If M has a finite generated set S, then M is **finitely generated**.

Remark 10.53. If $|S| = n$, then M is a factor module of R^n.

Definition 10.54. M is called **cyclic** if it is generated by just one element, $M = Ru$ for some $u \in M$.

In this case, $M \cong R/I$, I is a left ideal in R. We have $\varphi : R \to M$ - surjective, which maps a to au, and $I = ker\varphi$ is a left ideal. Observe:

$$I = \{a : au = 0\} = \text{Ann}(u).$$

And $au = 0 \Rightarrow \forall b \in R, (ba)u = 0$, so $ba \in I$. But $ab(u) =?$

Thursday, January 11th

Remark 10.55. When M is cyclic, we know:

$$M \cong R/I$$

where $I = \text{Ann}(u) = \{a : au = 0\}$, which is a left ideal. Recall that u is the generator of M.

Lemma 10.56. *An abelian group G is cyclic as a $\mathbb{Z}$-module if and only if it is cyclic as a group.*

Proof. $\exists u \in G$ s.t. $G = \mathbb{Z}u = \{nu : n \in \mathbb{Z}\}$. □

Remark 10.57. Let M be an F-vector space, and let T be a linear transformation of M. Then M is an $F[x]$-module by $xu = Tu$, $u \in M$.

$$(a_n x^n + \dots + a_1 x + a_0)u = a_n T^n u + \dots + a_1 Tu + a_0 u.$$

Also, M is cyclic as an $F[x]$-module if $\exists u$ s.t. $\forall v \in M$, $\exists n, a_i$ s.t. $v = a_n T^n u + \dots + a_1 Tu + a_0 u$.

Definition 10.58. That is, if $u, Tu, T^2 u, \ldots$ span M, then u is called a **cyclic vector** for T.

Lemma 10.59. *For any simple module M is cyclic*

Proof. take any nonzero $u \in M$, then Ru is a nonzero submodule, so $Ru = M$. □

Converse is not true: $\mathbb{Z}_6$ as a $\mathbb{Z}$-module is cyclic (generated by 1), but not simple (has a submodule $2\mathbb{Z}_6 = \{0, 2, 4\}$.

Every group is a factor group of a free group.

Friday, January 12th Now we'll do some exercises. Professor Leibman does Exercises 10.1.5,6 which are completed above. He defines the annihilator of a subset of M again, and proves it is a left ideal. This is Exercise 10.1.9.

Tuesday, January 16th

Take $R = F[x_1, x_2, \ldots]$. Consider R as a module over itself. It is generated by 1, since $R = R \cdot 1$.

Note $I = (x_1, x_2, ..)$-submodule of R, all polynomials with zero constant term.

Lemma 10.60. *I as defined above is not finitely generated.*

Proof. Assume that it is finitely generated. So $I = R(f_1, ..., f_k)$, for $f_i \in I$, where we assume f_i has zero constant term. Let $x_1, ..., x_n$ be all variables appearing in $f_1, ..., f_k$, then any nonzero element of $R(f_1, ..., f_k)$ (these are linear combinations of the f's) contains at least one of $x_1, ..., x_n$, since f_i has zero constant term. But I is not such, $x_{n+1} \in I$, so $I \neq R(f_1, ..., f_k)$. □

Example 10.61. Let $R = F[x, y]$, and $I = (x, y)$. Then R is an R module, is generated by 1, and I needs at least two generators. So we can think of this as R being a one "dimensional" module, but I is not one "dimensional". Let

$$f = ax + by + g(x, y),$$

$\forall g \in R$, $gf = c(ax + by) + (\cdots)$. We are assuming $a, b \neq 0$. The linear part of I is two "dimensional". So

$$\{g \in R, gf = c(ax + by) + (\cdots)\} \neq I.$$

If $b \neq 0$, $x \notin Rf$, and if $a \neq 0$, $y \notin Rf$.

Consider $M_1 \oplus M_2 = M_1 \times M_2$ is called direct sum = direct product, for two or finitely many modules. And this direct sum has the universal repelling property (appendix A).

For $M_1, M_2, ...$

Definition 10.62. Direct product $M_1 \times M_2 \times \cdots = \Pi_{i=1}^{\infty} M_i$ is

$$M = \{(u_1, u_2, ...) : u_i \in M_i\},$$

with $(u_1, u_2, ...) + (v_1, v_2, ...) = (u_1 + v_1, u_2 + v_2, ...)$. And scalar mult. is defined as one would expect.

More generally, if M_α $\alpha \in \Lambda$ are modules, then $\Pi_{\alpha\in\Lambda} = \{f : \Lambda \to \cup_{\alpha+\Lambda} M_\alpha : f(\alpha) \in M_\alpha\}$. For any α, choose $u_\alpha \in M_\alpha$.

Elements: $(u_\alpha)_{\alpha\in\Lambda}$.

Direct Sums:

$$M_1 \oplus M_2 \oplus \cdots = \{(u_1, u_2, ...) : u_i \in M_i, u_i = 0, \text{ for all but finitely many } i\}.$$

This is a subset of $M_1 \times M_2 \times \cdots$.

Another way:

$M_1 \oplus M_2 \oplus \cdots = \{u_{i_1} + u_{i_2} + \cdots + u_{i_k} : u_{i_j} \in M_{i_j}\}$. This is a submodule of $M_1 \times M_2 \times$.

For M_α, $\alpha \in \Lambda$,

$$\bigoplus_{\alpha\in\Lambda} M_\alpha = \{f : \Lambda \to \cup M_\alpha : \forall\alpha \in \Lambda, f(\alpha) \in M_\alpha, f(\alpha) = 0 \text{ for all but finitely many } \alpha\}.$$

This is a superset of $\Pi_{\alpha\in\Lambda} M_\alpha$.

Universal Properties:

R-modules M_α, $\alpha \in \Lambda$.

(1) Direct Product: Category: objects are (Module N with hom-sms $\psi_\alpha : N \to M_\alpha$, $\forall\alpha \in \Lambda$.

Morphisms: given two objects $(N_1, \psi_\alpha : N \to M_\alpha)$ $(N_2, \psi_\alpha : n \to M_\alpha)$ a morphism is a hom-sm $\varphi : N_1 \to N_2$ s.t. $\psi_\alpha = \varphi_\alpha\varphi$ $\forall\alpha$.

Direct product is universal attracting object.

Wednesday, January 17th

THEOREM 10.63 (**Chinese Remainder Theorem for Modules**). *Let R be a commutative unital ring, $I_1, ..., I_n$ be pairwise comaximal ideals in R:*

$$(I_i + I_j = (1), \forall i \neq j),$$

and M be a an R-module. Then the homomorphism $M \to M/I_1M \oplus \cdots \oplus M/I_nM$ given by $u \to (u \mod I_1M, ..., u \mod I_nM)$ induces an isomorphism $M/(I_1 \cdots I_n)M \to M/I_1M \oplus \cdots M/I_nM$ and $I_1M \cap \cdots \cap I_nM = (I_1 \cdots I_n)M$.

PROOF. For $n = 2$. $I_1 + I_2 = (1)$.

Define $\varphi : M \to M/I_1M \oplus M/I_2M$, where $\ker\varphi = I_1M \cap I_2M$. And there exists $a_1 \in I_1, a_2 \in I_2$ s.t. $a_1 + a_2 = 1$, since comaximal. And $\forall u \in I_1M \cap I_2M$, we have:

$$u = 1u = a_1u + a_2u.$$

So, $I_1M \cap I_2M \subseteq I_1I_2M$, since the first term in the righthand side above is in $I_1(I_2)M$ and so is the second term, by commutativity. Also, $I_1I_2M \subseteq I_2M \cap I_2M$. So $I_1I_2M = I_1M \cap I_2M = \ker\varphi$.

Surjectivity: $\forall u_1, u_2 \in M$, put $u = a_2u_1 + a_1u_2$. Then:

$$u = (1 - a_1)u_1 + a_1u_2 = u_1 + a_1(u_2 - u_1) = u_1 \mod I_1M,$$

and $u = u_2 \mod I_2M$. So $\varphi(u) = (\overline{u}_1, \overline{u}_2)$.

Now for $n \geqslant 3$, we use induction.

LEMMA 10.64. *I_1 and $I_2 \cdots I_n$ are comaximal.*

PROOF. $\forall i = 2, ..., n$, let $a_i \in I_1, b_i \in I_i$ be s.t. $a_i + b_i = 1$. Then:

$$1 = \prod (a_i + b_i) = (\textit{something}) + b_2 \cdots b_n,$$

where something is in I_1 and $b_2 \cdots b_n \in I_2 \cdots I_n$. □

Then:

$$M/(I_1I_2 \cdots I_n)M \cong M/I_1 \oplus M/(I_2 \cdots I_n)M \cong \cdots \cong M/I_1M \oplus \cdots \oplus M/I_nM$$

by induction, where the last $\cong$ is under the mapping

$$u \to (u \mod I_1M, ..., u \mod I_nM).$$

□

DEFINITION 10.65. M_1, M_2 are submodules of M. M is said to be an internal direct sum $M = M_1 \oplus M_2$ if there exists a $\varphi : M \to M_1 \oplus M_2$ where we also have maps in a diamond up to M_1 and down to M_2 s.t. $\varphi|_{M_1} = Id_{M_1}$ and the same for M_2.

REMARK 10.66. We say that we have an **internal direct sum** if the above map exists. The "internal" means that we are working entirely inside a parent module M.

THEOREM 10.67. *Let M_1, M_2 be submodules of M. Then $M = M_1 \oplus M_2$ (**internal direct sum**) if and only if $\forall u \in M$ is uniquely representable in the form $u = u_1 + u_2$ s.t. $u_1 \in M_1$, $u_2 \in M_2$ if and only if $M = M_1 + M_2$ and $M_1 \cap M_2 = 0$. These are all equivalent definitions.*

Let M_α, $\alpha \in \Lambda$ be submodules of$M$. M is an (internal) direct sum of M_α:

$$M = \bigoplus_{\alpha\in\Lambda} M_\alpha,$$

if there exists an isomorphism $\varphi : M \to \bigoplus_{\alpha\in\Lambda} M_\alpha$ where the target space is the external, formal direct sum, s.t. $\varphi|_{M_\alpha} = Id_{M_\alpha}, \forall\alpha$. This is so if and only if $\forall u \in M$ is uniquely representable as $u = \sum_{i=1}^k u_{\alpha_i}$ for some distinct $\alpha_1, ..., \alpha_k$ where $u_{\alpha_i} \in M_{\alpha_i}, \forall i$ and if and only if $M = \sum M_\alpha$ and $\forall\alpha$, $M_\alpha \cap \sum_{\beta\neq\alpha} M_\beta = 0$.

Free Modules.

Definition 10.68. A **free module** is a direct sum of finitely or infinitely many copies of R,

$$F_\Lambda = \bigoplus_{\alpha\in\Lambda} R = \{a_{\alpha_1} + \cdots + a_{\alpha_k} : k \in \mathbb{N}, \alpha_i \in \Lambda, a_{\alpha_i} \in R\},$$

where the sum of u's above is a formal sum. We can also define it as:

$$F_\Lambda = \{(a_\alpha)_{\alpha\in\Lambda} : a_\alpha \in R, \forall\alpha, a_\alpha = 0 \text{ for all but finitely many } \alpha\}.$$

Note R is unital here.

If M is an R-module, $v_\alpha \in M, \alpha \in \Lambda$. Then there exists a unique hom-sm $\varphi : F \to M$ s.t. $\varphi(e_\alpha) = v_\alpha, \forall\alpha$ where $e_\alpha = (a_\beta)_{\beta\in\Lambda}, a_\alpha = 1, a_\beta = 0$ for $\beta \neq \alpha$. As an example, if $\Lambda = \{1, ..., k\}$, we have:

$$e_1 = (1, 0, ..., 0),$$

$$e_k = (0, ..., 0, 1).$$

Also, we say that a module M is free if $M \cong$ a free module F. This is so if any only if M has a **basis**: elements $u_\alpha, \alpha \in \Lambda$.

Thursday, January 18th

Let R be a unital ring. Recall that a **free module** is $\bigoplus_{\alpha\in\Lambda} R$. If Λ is finite, $\Lambda = k$, then this is just R^k.

Definition 10.69. Our **standard basis** in R^k is

$$e_1 = (1, 0, ..., 0),$$

$$e_k = (0, ..., 0, 1).$$

Definition 10.70. The **rank** of the free module is k.

In $F = \oplus_{\alpha\in\Lambda} R$, the standard basis is $e_\alpha = (a_\beta)_{\beta\in\Lambda}, a_\alpha = 1, a_\beta = 0$ for $\beta \neq \alpha$.

Definition 10.71. For any $u \in F$, $u = \sum_{\alpha\in\Lambda} a_\alpha e_\alpha$, $a_\alpha \in R$ uniquely, where $a_\alpha = 0$ for all but finitely many α. (Namely, $u = (a_\alpha)_{\alpha\in\Lambda}$).

Remark 10.72. For a basis the representation must be unique, for generators, it does not.

Definition 10.73. Also, if $M \cong F$ for some Λ, M is called **free of rank** $|\Lambda|$.

REMARK 10.74. *M is free if and only if it has a basis:* a set$\{u_\alpha, \alpha \in \Lambda\} \subseteq M$ s.t. every u in M is uniquely representable in the form:

$$u = \sum_{\alpha \in \Lambda} a_\alpha u_\alpha,$$

where the a's are zero for all but finitely many of them.

DEFINITION 10.75. A set $\{u_\alpha, \alpha \in \Lambda\}$ in a module M is **linearly independent** if $\sum_{\alpha \in \Lambda} a_\alpha u_\alpha = 0$ only if $a_{\alpha_i} = 0$ for all i. In other words, a linear combination is zero if and only if all the coefficients are zero.

REMARK 10.76. A set $\{u_\alpha, \alpha \in \Lambda\}$ is a basis in M if and only if it is linearly independent and generates M. (It is unique since if we have two representations $u = \sum_{\alpha \in \Lambda} a_\alpha u_\alpha = \sum_{\alpha \in \Lambda} b_\alpha u_\alpha$, then $\sum_{\alpha \in \Lambda} (a_\alpha - b_\alpha) u_\alpha = 0$ so by linear independence, all the differences of coefficients are zero.)

THEOREM 10.77. *Any vector space is a free module. More generally, if R is a division ring, the any R module is free.*

PROOF. Let M be a nonzero R-module. Take the maximum linearly independent set B in M. It exists by Zorn Lemma. Indeed, take a nonzero element $u \in M$, then $\{u\}$ is linearly independent (proof is elementary, requires that R is a division ring). If you have a chain/subset tower of linearly independent sets, then their union is linearly independent, by Zorn Lemma. If $\mathcal{B}$ is a chain of linearly independent sets in M, the n $\bigcup \mathcal{B}$ is linearly independent. If

$$u_1, ..., u_n \in \bigcup \mathcal{B},$$

$$\sum_{i=1}^{n} a_i u_i = 0,$$

find $C \in \mathcal{B}$ s.t. these u's are all in C, C is linearly independent, so $a_i = 0$ for all i. So Zorn applies, and B exists. Now we claim that B generates M so B is a basis by Remark 10.76.

PROOF. Let $u \notin RB$. Then $B \cup \{u\}$ is linearly independent, contradiction, since then it would be bigger than B but B is maximal. Indeed, if:

$$au + \sum_{i=1}^{k} a_i u_i = 0,$$

for some $u_{\alpha_i} \in B$ for all i. If $a = 0$, then all a's are zero, since B is linearly independent. If a is note zero, then $u = -a^{-1} \sum_{i=1}^{k} a_i u_i \in RB$, which is impossible, since we said $u \notin RB$ at beginning of claim. □

□

REMARK 10.78. It is impossible for all of M to be linearly independent since we have u and $2u$ which are clearly dependent.

EXAMPLE 10.79. $\mathbb{R}$ is a vector space over $\mathbb{Q}$. We need Hamel basis. We start with $\{1, \alpha_1, \alpha_2, ...\}$, you need to get more than countably many. This has something to do with Zorn Lemma. The process cannot be defined with an algorithm.

DEFINITION 10.80. The rank of a vector space is called the **dimension**.

THEOREM 10.81. *The dimension of a vector space is uniquely defined: If R is a field, or a division ring, then $R^n \ncong R^m$ for $n \neq m$. This is for finite dimension, but for infinite dimensions it is also true.*

PROOF. **Finite Case:** Let R be a division ring, let M be an R-module, let $\{u_1, ..., u_n\}$, and $\{v_1, ..., v_m\}$ be two bases in M. We claim $m = n$.

PROOF. Assume that $n \geqslant m$. We have $v_1 = a_1 u_1 + \cdots a_n u_n$ for some coefficients not all zero. Without loss of generality, assume that the first a_1 is nonzero. Then:

$$u_1 = a_1^{-1} v_1 - a_1^{-1} a_2 u_2 - \cdots - a_1^{-1} a_n u_n.$$

Then $R\{v_1, u_2, ..., u_m\} = M$: if

$$v = \sum_{i=1}^{n} b_i u_i = b_1 u_1 + \sum_{i=2}^{n} b_i u_i = b_1(a_1^{-1} v_1 - a_1^{-1} a_2 u_2 - \cdots) + \sum b_i u_i = c v_1 + \sum_{i=2}^{n} c_i = u_i.$$

And $\{v_1, u_2, ..., u_n\}$ is linearly independent: if

$$cv_1 + c_2 u_2 + \cdots + c_n u_n = 0 = c(a_1 u_1 + \cdots a_n u_n) + c_2 u_2 + \cdots + c_n u_n = c a_1 u_1 + \sum i = 2^n d_i u_i,$$

then $ca_1 = 0$, so $c = 0$, so all c's are zero. Hence $\{v_1, u_2, ..., u_n\}$ is a basis. Next, replace one of $u_2, ..., u_n$ by v_2, and without loss of generality, replace u_2 with v_2. And after m steps, we see that $\{v_1, ..., v_m, u_{m+1}, ..., u_n\}$ is a basis. But $\{v_1, ..., v_m\}$ is a basis, so by definition those extra u's don't exist, and $n = m$. □

REMARK 10.82. If R is commutative and unital, then the rank of a free R-module is well defined:

$$R^n \ncong R^m,$$

where $n \neq m$.

PROOF. Let I be a maximal ideal in R, exists by Zorn Lemma. The R/I is a field. Then $R^n/(IR^n) \cong (R/I)^n = F^n$, where R^n is the free module of rank n. And $R^m/(IR^m) \cong F^m$. And $F^n \ncong F^m$ since dimension is well defined, so $R^n \ncong R^m$. □

□

Friday, January 19th We do exercises from Section 10.2,3.

DEFINITION 10.83. An R-module is called a **torsion module** if for each $m \in M$, there exists a nonzero $r \in R$ s.t. $rm = 0$.

Monday, January 22th

REMARK 10.84. Any module M has a maximal linearly independent set B of elements, by Zorn Lemma.

LEMMA 10.85. *If M is a torsion module, this set is empty.*

PROOF. Any element is not linearly independent if you take it alone. $\forall u \ \exists a \neq 0$, s.t. $au = 0$. □

However, B doesn't have to generate M. So what can we say about the submodule generated by B. The submodule RB has as basis (B), a linearly independent system which generates this module. **So, it's free.** And in fact:

Remark 10.86. It is the maximal free submodule: when you factorize by this submodule, you get a torsion ring.

Lemma 10.87. *M/RB is a torsion module if and only if B is a **maximal linearly independent set**.*

Proof. We assume R is unital, since otherwise, B may not be in RB. Or we could define RB as $RB \cup B$. Indeed, if $\exists u \in M$ s.t. $\overline{u} \equiv u \mod RB$ is not a torsion element, this means that $au \notin RB\ \forall a \neq 0 \in R$. This is because "0" in the quotient module is the kernel, RB so au cannot be in RB. Then if:

$$au + c_1v_1 = \cdots c_kv_k = 0,$$

with $v_i \in B, c_i \in R, a \in R$, then $a = 0$, since if a was nonzero, then $au = -c_1v_1 - \cdots - c_kv_k \in RB$. so $c_1v_1 + \cdots c_kv_k = 0$, so $c_i = 0$ for all i, so $\{u\} \cup B$ is linearly independent, contradiction, since B was the largest linearly independent set in M.

For any u, there exists a nonzero a s.t. $a\overline{u} \in RB$, so $au + c_1v_1 + \cdots c_kv_k = 0$ for some $c_i \in R, v_i \in B$. □

Example 10.88. Let $R = F[x,y], M = (x,y)$. The lines represent the ideals $(x),(y)$, and the empty box in the bottom left corner are just the constants.

$B = \{ x \}$. $RB = (x)$. And $M/RB = M/(x)$.

10.3 Exercises

7. *Let N be a submodule of M. Prove that if both M/N and N are finitely generated, then so is M.*

   Proof. Suppose M is not finitely generated. Then we have:

   $$M/N = RA,$$

   where $A = \{x_1 + N, \dots, x_n + N\}$. And since N is also finitely generated, we know $N = RA_N$, and $M - N$ is not finitely generated. Now we know $x_i \in M - N$ since otherwise we would have $x_i + N = N$. So then since M is not finitely generated, we know $\exists y \in M - N$ s.t. $y \notin R\{x_i\}$, hence $y + N \notin RA = \{(rx_1) + N, \dots, (rx_n) + N\}$, but since $y \in M - N$ we know $y + N \neq N$, hence $y + N \in M/N$. But we said $M/N = RA$, so this is a contradiction, so we must have that M is finitely generated. □

12. *Let R be a commutative ring and let A, B, and M be R-modules. Prove the following isomorphisms of R-modules:*

(a) $Hom_R(A \times B, M) \cong Hom_R(A, M) \times Hom_R(B, M)$.

PROOF. Let $H = \operatorname{Hom}_R(A \times B, M)$, $H_A = \operatorname{Hom}_R(A, M)$, and $H_B = \operatorname{Hom}_R(B, M)$. Let $\Phi : H_A \times H_B \to H$ be given by $\Phi((\varphi, \psi)) = \varphi + \psi$, where $\varphi \in H_A, \psi \in H_B$. We prove this is an isomorphism of R-modules.

Homomorphism: Observe:

$$\begin{aligned}\Phi((\varphi_1, \psi_1) + (\varphi_2, \psi_2)) &= \Phi((\varphi_1 + \varphi_2, \psi_1 + \psi_2)) = \varphi_1 + \psi_1 + \varphi_2 + \psi_2 \\ &= \Phi((\varphi_1, \psi_1)) + \Phi((\varphi_2, \psi_2)).\end{aligned} \tag{10.6}$$

In the above expression, the first equality comes from the definition of addition in $H_A \times H_B$. The second and third equalities comes from the definition of Φ. And we also know:

$$\Phi(r(\varphi, \psi)) = \Phi((r\varphi, r\psi)) = r\varphi + r\psi = r(\varphi + \psi) = r\Phi((\varphi, \psi)),$$

hence Φ preserves mult. by R, by the definition of scalar multiplication on the R-module $H_A \times H_B$, and the definition of Φ.

Surjectivity: Let $\varphi \in H$. Then $\varphi : A \times B \to M$. So let $\varphi \in H_A$ be given by $\varphi(a) = \varphi(a, 0)$, and let $\psi \in H_B$ be given by $\varphi(b) = \varphi(0, b)$. Then we have: $\Phi((\varphi, \psi)) = \varphi$. Then Φ is surjective.

Injectivity: Let $\Phi((\varphi_1, \psi_1)) = \varphi_1 + \psi_1 = \varphi_2 + \psi_2 = \Phi((\varphi_2, \psi_2)) \in H_A \times H_B$. Then note that

$$(\varphi_1 + \psi_1)(a, 0) = \varphi_1(a) = \varphi_2(a) = (\varphi_2 + \psi_2)(a, 0),$$

and the same holds when we let $a = 0$, and use an arbitrary b value, so we get that $\psi_1 = \psi_2$ as well. Hence Φ is injective. And thus it is an isomorphism. □

(b) $Hom_R(M, A \times B) \cong Hom_R(M, A) \times Hom_R(M, B)$.

PROOF. Let $H = \operatorname{Hom}_R(M, A \times B)$, $H_A = \operatorname{Hom}_R(M, A)$, and $H_B = \operatorname{Hom}_R(M, B)$. Let $\Phi : H_A \times H_B \to H$ be given by $\Phi((\varphi, \psi)) = (\varphi, \psi) \in H$, where $\varphi \in H_A$, and $\psi \in H_B$. We prove this map is an isomorphism.

Homormorphism: Observe:

$$\begin{aligned}\Phi((\varphi_1, \psi_1) + (\varphi_2, \psi_2)) &= \Phi((\varphi_1 + \varphi_2, \psi_1 + \psi_2)) = (\varphi_1 + \varphi_2, \psi_1 + \psi_2) \\ &= (\varphi_1, \psi_1) + (\varphi_2, \psi_2) = \Phi((\varphi_1, \psi_1)) + \Phi((\varphi_2, \psi_2)).\end{aligned} \tag{10.7}$$

The first equality follows from addition in the R-module $H_A \times H_B$, the second comes from the definition of Φ, the third comes from addition in H, and the last again comes from the definition of Φ. And we also know:

$$\Phi(r(\varphi, \psi)) = \Phi((r\varphi, r\psi)) = (r\varphi, r\psi) = r(\varphi, \psi) = r\Phi((\varphi, \psi)),$$

by the definition of scalar mult. in H, hence since Φ preserves addition and scalar multiplication, we know it is a homomorphism.

Surjectivity: Let $\varphi \in H$, then we know $\varphi : M \to A \times B$. Then the image of any element of M under φ is a two dimensional vector whose first component lives in A, and whose second

component lives in B. So let $\varphi : M \to A$ be given by $\varphi(m) = \varphi(m)_1$, the first component of $\varphi(m)$. and let $\psi(m) = \varphi(m)_2$. Then $\Phi((\varphi,\psi)) = (\varphi,\psi) = \varphi$. Hence Φ is surjective.
Injectivity: Let $\Phi((\varphi_1,\psi_1)) = (\varphi_1,\psi_1) = (\varphi_2,\psi_2) = \Phi((\varphi_2,\psi_2))$. Then we must have $\varphi_1 = \varphi_2$, and $\psi_1 = \psi_2$, since otherwise we do not have equality of these ordered pairs of hom-sms in H. But then we have shown that the arguments of Φ are equal in this case, so Φ must be injective. □

15. *An element $e \in R$ is called a **central idempotent** if $e^2 = e$ and $er = re$ for all $r \in R$. If e is a central idempotent in R, prove that $M = eM \oplus (1-e)M$.*

Proof. So we wish to show that M is the direct sum of the two specified submodules. Note that we know that these sets are both submodules by Exercise 14 of Section 1, which tells us that zM is a submodule for any z in the center of R. We know e is in the center since it is a central idempotent. And $(1-e)r = r - er = r - re = r(1-e)$. So it is also in the center. Now we need only show that $M = eM + (1-e)M$, and that $eM \cap (1-e)M = 0$.

Let $m \in M$. Then $m = em + (1-e)m = em + m - em$, where $em \in eM$, and $(1-e)m \in (1-e)M$, so $m \in eM + (1-e)M$. Now let $em + (1-e)n \in eM + (1-e)M$. Then we have $em + n - en = n + e(m-n)$. So we know $M = eM + (1-e)M$. So let $m \in eM \cap (1-e)M$. Then $m = en_1 = (1-e)n_2$ for some $n_1, n_2 \in M$. Then we have:

$$m = en_1 = (1-e)n_2 = e^2 n_1 = e(1-e)n_2 = (e-e^2)n_2 = (e-e)n_2 = 0,$$

so we have shown that if $m \in eM \cap (1-e)M$, $m = 0$, so $eM \cap (1-e)M = 0$. And thus $M = eM \oplus (1-e)M$ by definition. □

18. *Let R be a PID, let M be an R-module, and assume that $aM = 0$ for some $a \neq 0$ where $a \in R$. Let:*

$$a = p_1^{r_1} \cdots p_k^{r_k},$$

distinct primes in R $\forall i$, and let:

$$M_i = Ann(p_i^{r_i}) = \{u \in M : p_i^{r_i} u = 0\}.$$

Then $M = M_1 \oplus \cdots \oplus M_k$.

Proof. $\forall i$, let $a_i = a/p_i^{r_i} (= \prod_{j \neq i} p_j^{r_j})$. Then $a_i M \subseteq M_i$, since

$$p_i^{r_i}(a_i M) = aM = 0$$

(by assumptions of theorem). Then:

$$gcd(a_1, ..., a_k) = 1,$$

so there exists $c_1, ..., c_k \in R$ s.t. $c_1 a_1 + \cdots + c_k a_k = 1$. So $\forall u \in M$,

$$u = c_1 a_1 u + \cdots + c_k a_k u \in M_1 + \cdots M_k.$$

Now let $u \in M_i \cap (\sum_{j \neq i} M_j)$. Then $p_i^{r_i}, a_i \in Ann(u)$. So, $(p_i^{r_i}) = (1) \subseteq Ann(u)$, so $u = 0$. So $\forall i, M_i \cap (\sum_{j \neq i} M_j) = 0$. □

22. *Let R be a Principal Ideal Domain, let M be a torsion R-module, and let p be a prime in R (do not assume M is finitely generated, hence it need not have a nonzero annihilator). The **p-primary***

component of *M is the set of all elements of M that are annihilated by some positive power of p.*

(a) *Prove that the p-primary component is a submodule.*

PROOF. Let N denote the p-primary component of M. Note that:

$$N = \left\{ m \in M : \exists k \in \mathbb{N}, p^k m = 0 \right\}.$$

We apply the submodule criterion. Note that $N \neq \varnothing$ since $0 \in N$. Let $x, y \in N$, and let $r \in R$. Then we know $\exists k, l \in \mathbb{N}$ s.t. $p^k x = p^l y = 0$. Observe:

$$p^k p^l (x + ry) = p^l p^k x + rp^k p^l y = p^l 0 + rp^k 0 = 0,$$

so we know $x + ry \in N$, hence by the submodule criterion, N is a submodule of M. □

(b) *Prove that this definition of p-primary component agrees with the one given in Exercise 18 when M has a nonzero annihilator.*

PROOF. Assume M has a nonzero annihilator a, and this is the minimal such element. Then let p^α be a prime power factor in the prime factorization of a. Let:

$$N = \left\{ m \in M : \exists k \in \mathbb{N}, p^k m = 0 \right\}.$$

In Exercise 18, the definition given for the annihilator of p^α is:

$$A = Ann_M(p^\alpha) = \{m \in M : p^\alpha m = 0\}.$$

So clearly any element of A is in N; just let $k = \alpha$. So let $m \in N$. Then $\exists k \in \mathbb{N}$ s.t. $p^k m = 0$. Suppose $k > \alpha$. Then since $am = 0$, we must have some other product of primes $r = r_1 \cdots r_l \mid a$ s.t. $r \nmid p^\alpha$. But since we proved that N is a submodule in part (a), we know $Ann(N) = \left\{ r \in R : rm = 0, \forall m \in N \right\}$ is an ideal in R. Note then that $r, p^k \in Ann(N)$. But since $p^k \nmid r$ since otherwise we would have $p^k \mid a$, which is impossible since we said $r > \alpha$. So then $r \notin Rp^k$, hence $Ann(N)$ is not a principal ideal, but this is impossible, since we are in a PID, so we must have $k \leqslant \alpha$. Hence $m \in A$, and thus $N \subseteq A$, and the definitions are equivalent, because the sets are equal.

□

(c) *Prove that M is the (possibly infinite) direct sum of its p-primary components $\{ M_i \}$, as p runs over all primes of R.*

PROOF. Let $\{ p_i \}$ be all the primes in R. $\forall i$, let $a_i = \prod_{j \neq i} p_j^{r_j}$. Then $a_i M \subseteq M_i$, since $p_i^{r_i}(a_i M) = \prod_{j=1}^{\infty} p_j^{r_j} M = 0$ (since M is a torsion module, and hence $\forall m \in M$ there exists a nonzero $r \in R$ s.t. $rm = 0$, and the prime decomposition of r is in $\prod_{j=1}^{\infty} p_j^{r_j}$). Then:

$$gcd(a_1, a_2, \ldots) = 1,$$

so there exists $c_1, c_2, \ldots \in R$ not necessarily all nonzero s.t. $c_1 a_1 + \cdots = 1$. So $\forall u \in M$,

$$u = \sum_{i=1}^{\infty} c_i a_i \in M_1 + M_2 + \cdots.$$

Now let $u \in M_i \cap (\sum_{j \neq i} M_j)$. Then $p_i^{r_i}, a_i \in Ann(u)$. So, $(p_i^{r_i}) = (1) \subseteq Ann(u)$, so $u = 0$. So $\forall i, M_i \cap (\sum_{j \neq i} M_j) = 0$. So since we know $M = M_1 + M_2 + \cdots$, and the pairwise intersection of each of these is 0, we know that $M = M_1 \oplus M_2 \oplus \cdots$. □

27. *We show that* ***free modules over noncommutative rings need not have a unique rank.*** *Let:*

$$M = \mathbb{Z}^n = \{ (a_1, \ldots, a_n) : a_i \in \mathbb{Z} \}.$$

Let $R = End_{\mathbb{Z}}(M)$. Consider R as a module over itself. It is a free module of rank 1. We claim $R \cong R^2$. And so we would have $R \cong R^n$ for any n.

Proof. Consider $\varphi_1, \varphi_2, \psi_1, \psi_2 \in R$. Define:

$$\begin{aligned} \varphi_1(a_1, a_2, \ldots) &= (a_1, a_3, a_5, \ldots) \\ \varphi_2(\ldots\ldots\ldots..) &= (a_2, a_4, \ldots) \\ \psi_1(\ldots\ldots\ldots..) &= (a_1, 0, a_2, 0, \ldots) \\ \psi_2(\ldots\ldots\ldots..) &= (0, a_1, 0, a_2, \ldots) \end{aligned} \tag{10.8}$$

We claim that $\{ \varphi_1, \varphi_2 \}$ is a basis of R as an R-module, so $R \cong R^2$ as R-modules. **Why this implication!! Ask after class.** The general situation: M is R module, $u_1, \ldots, u_n$ is basis in M. Then every element of M is a linear combination uniquely. Then $M \cong R^n$ under isomorphism $u \mapsto (a_1, \ldots, a_n)$, the coefficients of the unique linear combination representing u. We have:

$$\varphi_1\psi_1 = \varphi_2\psi_2 = 1,$$
$$\varphi_1\psi_2 = \varphi_2\psi_1 = 0,$$
$$\psi_1\varphi_1 + \psi_2\varphi_2 = 1.$$

These can be checked easily. Any $\varphi = \varphi 1 = (\varphi\psi_1)\varphi_1 + (\varphi\psi_2)\varphi_2)$. So φ_1, φ_2 generate φ. If $\beta_1\varphi_1 + \beta_2\varphi_2 = 0$, then $\beta_1\varphi_1\psi_1 + \beta_2\varphi_2\psi_1 = 0$. So we get $\beta_1 = 0$. And to get $\beta_2 = 0$, we multiply on the right by ψ_2 instead of ψ_1. And they are linearly independent. And thus a basis, so the claim is fulfilled. □

0. *Let M be an R-module and let I, J be ideals in R.*
   (a) *Prove that $Ann(I + J) = Ann(I) \cap Ann(J)$.*

   Proof. Let $m \in Ann(I + J)$. Then $(i + j)m = 0$ for all $i \in I, j \in J$. Then letting $i = 0$, we know $m \in Ann(J)$, and letting $j = 0$, we know $m \in Ann(I)$. So $Ann(I + J) \subseteq Ann(I) \cap Ann(J)$. Now let $m \in Ann(I) \cap Ann(J)$. Then $im = 0, \forall i \in I$, and $jm = 0, \forall j \in J$. Then we have:

   $$(i + j)m = im + jm = 0 + 0 = 0,$$

   by he definition of an R-module. So $Ann(I) \cap Ann(J) \subseteq Ann(I + J)$. Hence they are equal. □

   (b) *Prove that $Ann(I) + Ann(J) \subseteq Ann(I \cap J)$.*

Proof. Let $m \in Ann(I) + Ann(J)$. Then $m = n + k$ for some $n \in Ann(I), k \in Ann(J)$. Let $i \in I \cap J$. Then we know:

$$im = i(n+k) = in + ik = 0 + 0 = 0,$$

by the distributivity of the action of R on M, and since $i \in I$, and $i \in J$, and since n, k are in the respective annihilators. Thus $m \in Ann(I \cap J) \Rightarrow Ann(I) + Ann(J) \subseteq Ann(I \cap J)$. □

(c) *Give an example where the inclusion in part (b) is strict.*
Let R be the ring of continuous functions $f : [0,1] \to \mathbb{R}$. Note this is not an integral domain since we can construct zero divisors in the form of a pair piecewise functions, one of which is zero on half the interval, and the other being zero on the other half. We consider the R-module of R over itself. Then let I be the ideal of functions which are zero on $[0, 1/2]$, and J be the ideal of functions which are zero on $[1/2, 1]$. Now note that $I + J \neq R$ since $f(x) = 1$ is in R, but not in $I + J$, since all functions in $I + J$ are zero at $1/2$. But $I \cap J = 0$, since these functions must be zero across both halves, and so $Ann(I \cap J) = R$, and so $Ann(J) + Ann(I) = I + J \subsetneq R = Ann(I \cap J)$.
We give another example. Consider $R = F[x,y]$,

$$M = R/(xy) = \{ a_0 + b_1x + \cdots b_nx^n + c_1y + \cdots + c_ny^n \}.$$

$I = (x), J = (y)$, and $I \cap J = (xy)$. Then we have:

$$\begin{gathered} Ann(I) = \{ c_1y + \cdots + c_ny^n \} \subseteq M, \\ Ann(J) = \{ b_1x + \cdots + b_nx^n \}. \end{gathered} \tag{10.9}$$

And $Ann(I \cap J) = Ann(xy) = M$. And $F \subseteq Ann(I \cap J) \subsetneq Ann(I) + Ann(J)$.

(d) *If R is commutative and unital and I, J are comaximal, prove that $Ann(I \cap J) = Ann(I) + Ann(J)$.*

Proof. Assume R is commutative and unital, and I, J are comaximal. Let $m \in Ann(I + J) = Ann((1)) = Ann(R)$ since I, J are comaximal, and R is commutative and unital. So $rm = 0$ for all $r \in R$. So then $m \in Ann(I)$, and since $0 \in Ann(J)$, we may write $m = m + 0$, so $m \in Ann(I) + Ann(J)$. And thus $Ann(I + J) \subseteq Ann(I) + Ann(J)$. So they are equal by the result of part (b). **This is just very wrong, I think.** □

SECTION 10.4

Tensor products of modules

Monday, January, 22nd
Let R be a unital, commutative ring. Let M, N be R-modules. We have:

$$M \times N = M \oplus N.$$

i.e. $(u,v) = u + v = (u,0) + (0,v)$. If we want to actually multiply M, N, multiply elements of M and elements of N: uv. Then the first thing we need is for it to be distributive. Then we want:

$$\begin{aligned}(u_1 + u_2)v &= u_1 v + u_2 v,\\ u(v_1 + v_2) &= uv_1 + uv_2.\end{aligned} \tag{10.10}$$

Definition 10.89. A mapping $\beta : M \times N \to K$ is said to be **bilinear** if for all $v \in N$, $\beta : (\cdot, v) : M \to K$ is a hom-sm, and for any $u \in M$, $\beta(u, \cdot) : N \to K$ is a hom-sm, that is, $\forall v \in N, \forall u_1, u_2 \in M$:

$$\beta(u_1 + u_2, v) = \beta(u_1, v) + \beta(u_2, v).$$

And $\forall u \in M, a \in R$:

$$\beta(au, v) = a\beta(u, v).$$

And $\forall u \in M, \forall v_1, v_2 \in N$:

$$\beta(u, v_1 + v_2) = \beta(u, v_1) + \beta(u, v_2).$$

Where above, we put $\beta_v(u) = \beta(u, v)$ for all $u \in M$. $\beta_v : M \to K$.

Definition 10.90. The **tensor product** $M \otimes_R N$ is an R-module with a bilinear mapping $\beta : M \times N \to M \otimes N$ such that for any module K, and any bilinear mapping $\gamma : M \times N \to K$, there is a unique homomorphism $\varphi : M \otimes N \to K$ such that $\gamma = \varphi \circ \beta$, i.e.:

$$\begin{tikzcd} & M \times N \arrow[dl, "\beta"'] \arrow[dr, "\gamma"] & \\ M \otimes N \arrow[rr, "\varphi"] & & K \end{tikzcd}$$

is commutative.

In the above diagram, the top and left nodes together are the universal object. And the morphism is φ.

We need to prove this because the above definition is not constructive. We just said it's a module with certain properties. Now we construct it explicitly. If such a module exists, then it is unique up to isomorphism.

Proposition 10.91. *$M \otimes N$ exists.*

Proof. Let $\mathcal{M}$ be the free R-module generated by $M \times N$ - as a set. That is, the set of formal linear combinations of pairs $(u, v) \in M \times N$. So:

$$\mathcal{M} = \{\, a_1(u_1, v_1) + \cdots + a_n(u_n, v_n) : a_i \in R, (u_i, v_i) \in M \times N \,\}.$$

Let $\mathcal{L}$ be the submodule of $\mathcal{M}$ generated by elements of the form:

$$\begin{aligned}(u_1 + u_2, v) - (u_1, v) - (u_2, v),\\ (u, v_1 + v_2) - (u, v_1) - (u, v_2),\\ (au, v) - a(u, v),\\ (u, av) - (a(u, v)).\end{aligned} \tag{10.11}$$

We want the bilinearity relations to be satisfied, so we declare all these elements to be zero. Claim: $\mathcal{M}/\mathcal{L} = M \otimes N$. So what are elements of this module? These are classes of linear combinations of pairs. Elements of $\mathcal{M}/\mathcal{L}$ are classes (module $\mathcal{L}$) of linear combinations of (u, v). The class of (u, v) is denoted by $u \otimes b$. So

$$\mathcal{M}/\mathcal{L} = \left\{ \textstyle\sum a_i(u_i \otimes v_i) : a_i \in R, u_i \in M, v_i \in N \right\}.$$

Definition 10.92. The elements of of the set above are called **tensors**, and $u \otimes v$ is called a **simple tensor**.

So:

$$\mathcal{M}/\mathcal{L} = \left\{ \sum a_i \overline{(u_i, v_i)} \right\}.$$

And:

$$\begin{aligned} \overline{(u,v)} &= u \otimes v, \\ \overline{(u_1+u_2, v)} &= \overline{(u_1,v)} + \overline{(u_2,v)}, \\ (u_1+u_2) \otimes v &= u_1 \otimes v + u_2 \otimes v. \end{aligned} \tag{10.12}$$

The mapping $M \times N \to \mathcal{M}/\mathcal{L}$ given by $(u,v) \mapsto u \otimes v$ is bilinear: in $\mathcal{M}/\mathcal{L}$, we have:

$$\begin{aligned} (u_1+u_2) \otimes v &= u_1 \otimes v + u_2 \otimes v, \\ \beta(u_1+u_2, v) &= \beta(u_1,v) + \beta(u_2,v), \end{aligned} \tag{10.13}$$

where the stuff in the bottom line is equal to the stuff it lines up with in the top line. Also:

$$\begin{aligned} (au) \otimes v &= a(u \otimes v), \\ u \otimes (v_1+v_2) &= u \otimes v_1 + u \otimes v_2, \\ u \otimes (av) &= a(u \otimes v). \end{aligned} \tag{10.14}$$

if $\gamma : M \times N \to K$ is bilinear, we have a unique homomorphism $\Phi : M \to K$ with $\Phi(u,v) = \gamma(u,v)$ for all u, v.

Since γ is bilinear, $\Phi(\mathcal{L}) = 0$,

$$\begin{aligned} (\Phi(u_1+u_2,v) - (u_1,v) - (u_2,v)) &= \Phi(u_1+u_2,v) - \Phi(u_1,v) - \Phi(u_2,v) \\ &= \gamma(u_1+u_2,v) - \gamma(u_1,v) - \gamma(u_2,v). \end{aligned} \tag{10.15}$$

and the same holds for all other relations. So Φ is factorized to a hom-sm $\varphi : \mathcal{M}/\mathcal{K} \to K$. It is unique since $\mathcal{M}$ is generated by $M \times N$ s.t. $\varphi(u \otimes v) = \gamma(u,v)$. □

Tuesday, January 23rd

Let R be commutative, unital. And M, N be R-modules. Then: $M \otimes N = M \otimes_R N$ is an R-module consisting of **tensors:**

$$a_1(u_1 \otimes v_1) + \cdots + a_n(u_n \otimes v_n),$$

with $a_i \in R, u_i \in M, v_i \in N$. It is generated by **simple tensors** $u \otimes v$, with relations:

$$\begin{aligned} (u_1+u_2) \otimes v &= u_1 \otimes v + u_2 \otimes v, \\ (au) \otimes v &= a(u \otimes v), \\ u \otimes (v_1+v_2) &= u \otimes v_1 + u \otimes v_2, \\ u \otimes (av) &= a(u \otimes v). \end{aligned} \tag{10.16}$$

And it has no other relations! It has a universal property: for any R-module K and a bilinear mapping $\gamma : M \times N \to K$ there exists a unique hom-sm $\varphi : M \otimes N \to K$ such that $\varphi(u \otimes v) = \gamma(u,v)$ for each $u \in M, v \in N$.

Lemma 10.93. *We list some properties.*

(1) *If $M = RB$, $N = RC$, then $M \otimes N = R(B \otimes C)$, where:*

$$B \otimes C = \{ u \otimes v : u \in B, v \in C \}.$$

Proof. $\forall u \in M$, $u = \sum a_i u_i, u_i \in B$. And $\forall v \in N, v = \sum b_j v_j, v_j \in C$. Then:

$$u \otimes v = \sum_{i,j} a_i b_j (u_i \otimes v_j).$$

i.e. any tensor in $M \otimes N$ is a linear combinations of such simple tensors. □

(2) *$\forall u \in M$, $u \otimes 0 = 0$, and $\forall v \in N$, $0 \otimes v = 0$.*

Proof. $u \otimes 0 = u \otimes (0 + 0) = u \otimes 0 + u \otimes 0$, so we must have that it is zero. □

(3) *$\forall$ module M, $M \otimes 0 = 0 \otimes M = 0$.*

(4) *$\forall$ module M, $M \otimes R \cong R \otimes M \cong M$.*

R plays the role of the identity in this algebra of modules.

Proof. Take any tensor, it is of the form:

$$\begin{aligned} a_1(u_1 \otimes b_1) + \cdots + a_n(u_n \otimes b_n) &= a_1 b_1 (u_1 \otimes 1) + \cdots + a_n b_n (u_n \otimes 1) \\ &= (a_1 b_1 u_1) \otimes 1 + \cdots + (a_n b_n u_n) \otimes 1 \qquad (10.17) \\ &= (a_1 b_1 u_1 + \cdots + a_n b_n u_n) \otimes 1 = v \otimes 1. \end{aligned}$$

Note in the above, $b_i \in R$, so we can take them out: $u \otimes b = u \otimes (b \cdot 1) = b(u \otimes 1)$.

So define a hom-sm $\varphi : M \otimes R \to M$ by:

$$\sum_{i=1}^{n} b_i (u_i \otimes a_i) \mapsto \sum_{i=1}^{n} a_i b_i u_i.$$

Why is φ defined, and why is it a homomorphism? First, define $\gamma : M \times R \to M$, $\gamma(u, a) = au$. This γ is bilinear. If u is fixed, it is linear with respect to a, if a is fixed, it is linear with respect to u. So there exists a unique hom-sm $\varphi : M \otimes R$ s.t. $\varphi(u \otimes a) = au$ $\forall u \in M, a \in R$. This is our φ. Why is it an isomorphism. Construct the inverse mapping. Take $u \mapsto u \otimes 1$. And why do we need to prove that it is defined? There are relations in the module.

Example 10.94. The same tensor can be written in several ways as a sum of simple tensors, in $\mathbb{Z} \otimes \mathbb{Z}$:

$$5 \otimes 6 = 2 \otimes 6 + 3 \otimes 6.$$

The left hand side is sent to 30, but we need it to be bilinear or something.

So the inverse is a homomorphism, $M \to M \otimes R$. It is an inverse, since if we start with a tensor, send it to the $v \otimes 1$ in Equation 10.17, we get:

$$\sum a_i (u_i \otimes b_i) \mapsto^{\varphi} \sum a_i b_i u_i \mapsto^{\varphi^{-1}} \left(\sum a_i b_i u_i\right) \otimes 1.$$

□

(5) *$M \otimes N \cong N \otimes M$ by the map $u \otimes v \mapsto v \otimes u$. We send $(u, v) \mapsto v \otimes u$ - linear, so φ exists. And $v \otimes u \mapsto u \otimes v$ is its inverse.*

(6) $M \otimes N) \otimes K \cong M \otimes (N \otimes K)$ *by the map:*

$$(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w).$$

(7) $M \otimes (M \oplus K) \cong (M \otimes K) \oplus (M \otimes K)$.

So in naive set theory, any collection of objects is a set, but this leads to immediate crap. So we use ZFC, axiomatic. Modules don't form a set because there are too many of them, lmao.

Proof. Let $\varphi : u \otimes (v, w) \mapsto (u \otimes v, u \otimes w)$. We only define φ on simple tensors, then by linearity, it is extended to all tensors. Is it well defined? Yes, φ is a well-defined hom-sm if:

$$(u, (v, w)) \mapsto (u \otimes v, u \otimes w),$$

is bilinear. The stuff on the left side, domain, is in $M \times (N \oplus K)$. So we check it:

$$\begin{aligned} (u_1 + u_2, (v, w)) &\mapsto ((u_1, u_2) \otimes v, (u_1, u_2) \otimes w) \\ ((u_1, u_2) \otimes v, (u_1, u_2) \otimes w) &= (u_1 \otimes v + u_2 \otimes v, u_1 \otimes w + u_2 \otimes w) \\ &= (u_1 \otimes v, u_1 \otimes w) + (u_2 \otimes v, u_2 \otimes v). \end{aligned} \tag{10.18}$$

To prove that this is an ismorphism, we need its inverse. Define $\psi : (M \otimes N) \oplus (M \otimes K) \to M \otimes (N \oplus K)$. The direct sum is also a universal object. Define $\psi_1 : M \otimes N \to M \otimes (N \oplus K), \psi_2 : M \otimes K \to M \otimes (N \oplus K)$ by:

$$\begin{aligned} \psi_1(u \otimes v) &= u \otimes (v, 0), \\ \psi_2(u \otimes w) &= u \otimes (0, w). \end{aligned} \tag{10.19}$$

There is a unique hom-sm ψ s.t. $\psi|_{M \otimes N} = \psi_1$, and $\psi|_{M \otimes K} = \psi_2$. So we have:

$$(\psi(\alpha, \beta) = \psi_1(\alpha) + \psi_2(\beta)).$$

So we check that they are inverses of each other. We have:

$$\varphi : u \otimes (v, w) \mapsto (u \otimes v, u \otimes w) \mapsto_\psi u \otimes (v, 0) + u \otimes (0, w) = u \otimes (v, w). \tag{10.20}$$

□

Wednesday, January 24th

Tensors come from physics, from algebra, from topology. Linear transformations, bilinear forms, ... There are many objects that can be interpreted as tensors. In algebra, they can be used to extend scalars.

Example 10.95. It can be shown that:

$$C(x \times y) = \overline{C(x) \otimes C(y)}.$$

For any R-module M, $M \otimes R \cong M$, and $M \otimes (N \oplus K) \cong (M \otimes N) \oplus (M \otimes K)$.

Remark 10.96. $M \otimes R^n \cong M^n = M \oplus \cdots \oplus M$.

Remark 10.97. $R^n \otimes R^m \cong R^{nm}$-free of rank nm.

Example 10.98. (1) *Prove that* $M \otimes R/I \cong M/(IM)$. *What number is this????*

PROOF. The mapping $\gamma : (u, \overline{a}) = a \mod I \mapsto \overline{au} = au \mod (IM)$. This is well-defined, and is bilinear, so it satisfies the properties required for a tensor product. $a + c \mapsto \overline{au + cu} \in IM, c \in I$. So hom-sm $\varphi : M \otimes (R/I) \to M/(IM)$ is defined. And we have: $u \otimes \overline{a} \mapsto \overline{au}$. And it has the inverse: $\psi : \overline{u} \mapsto (u \otimes \overline{1}$, defined from $M/IM \to M \otimes R/I$. You should understand that γ is not an isomorphism itself. Now why is this new map well defined, first? If you replace u by $\overline{u} + \overline{\sum b_i v_i}$, where $b_i \in I$. Then under our new map we have:

$$\psi : \overline{u} = \overline{\sum b_i v_i} \mapsto (u + b_i v_i) \otimes \overline{1} = (u \otimes \overline{1} + \sum (v_i \otimes \overline{b_i},$$

where $\sum (v_i \otimes \overline{b_i} = 0 \mod (M \otimes I)$. So ψ is well-defined, and $\psi = \varphi^{-1}$. □

(2) *Consider $\mathbb{Z}_3 \otimes \mathbb{Z}_2$.*

We may write

$$\begin{aligned} 1 \otimes 1 &= (3 - 2) \otimes 1 \\ &= 3 \otimes 1 - 2 \otimes 1 \\ &= 3 \otimes 1 - 2(1 \otimes 1) \\ &= 3 \otimes 1 - 1 \otimes 2 \\ &= 0 \otimes 1 - 1 \otimes 0 \\ &= 0 - 0 = 0. \end{aligned} \tag{10.21}$$

And for any $n \otimes k = nk(1 \otimes 1) = 0$. So $\mathbb{Z}_3 \otimes \mathbb{Z}_2 = 0$.

LEMMA 10.99. *If $(n, m) = 1$, then $\mathbb{Z}_n \otimes \mathbb{Z}_m = 0$.*

PROOF. There exists k, l s.t. $kn + lm = 1$. Then:

$$1 \otimes 1 = (kn + lm) \otimes 1 = k(n \otimes 1) + l(1 \otimes m) = 0.$$

And $\forall (a \otimes b) = ab(1 \otimes 1) = 0$. □

LEMMA 10.100. *Let $(n, m) = d$. Then $\mathbb{Z}_n \otimes \mathbb{Z}_m \cong \mathbb{Z}_d$.*

PROOF. Define $\varphi : \mathbb{Z}_n \otimes \mathbb{Z}_m \to \mathbb{Z}_d$ by $\varphi(\overline{k} \otimes \overline{l}) = kl \mod d$. If you add a multiple of n to k, the result will be the same because $d|n$, and same for m ($(\overline{k}, \overline{l}) \mapsto kl \mod d$ is bilinear). Why is it a homomorphism? Let's check that it is surjective. Note that $1 \otimes 1 \mapsto 1$, and 1 generates $\mathbb{Z}_d$. So done: $\varphi(1 \otimes a) = a \mod d$, so φ is surjective. Or maybe better to just define an inverse, since injectivity looks hard to prove.

$$\varphi(k(1 \otimes 1)) = k \mod d,$$

for any k, so it's injective or something because the kernel is 0 maybe. □

REMARK 10.101. If G is a finite abelian group, then

$$G \cong \mathbb{Z}_{p_1^{r_{1,1}}} \oplus \cdots \oplus \mathbb{Z}_{p_1^{r_{1,k_1}}} \oplus (..p_2..) \oplus \cdots \oplus (..p_l..).$$

So we have $G \otimes_{\mathbb{Z}} \mathbb{Z}_{p_1} \cong \mathbb{Z}{p_1}^{k_1}$. We get this by multiplying by each component and using the previous result, that since the $\mathbb{Z}$'s are relatively prime, they go to zero. So $\forall p \mid |G|$, $G \otimes \mathbb{Z}_p \cong \mathbb{Z}_p^k$ where k is the number of p-elementary divisors of G.

Remark 10.102. Let R be an integral domain, let F be the field of quotients of R.

$$F \otimes_R M = ?$$

Lemma 10.103. *If M is a torsion module, then $F \otimes_R M = 0$.*

Proof. Let $u \in M$. Find $a \neq 0$ s.t. $au = 0$. Then:

$$1 \otimes u = (aa^{-1}) \otimes u = a^{-1} \otimes (au) = 0.$$

But this is not enough. Moreover, for any $b \in F$, we know:

$$b \otimes u = (aa^{-1}b) \otimes u = (a^{-1}b) \otimes (au) = 0.$$

□

Example 10.104. Consider $F^2 \otimes F^2 \cong F^4$, where $\{ e_1, e_2 \}$ is a basis. So basis of $F^2 \otimes F^2$ is:

$$\{ e_1 \otimes e_1, e_1 \otimes e_2, e_2 \otimes e_1, e_2 \otimes e_2 \}.$$

So $F^2 = e_1 F \oplus e_2 F$. Any tensor from $F^2 \otimes F^2$ is of the form:

$$a_{1,1}(e_1 \otimes e_1) + a_{1,2}(e_1 \otimes e_2) + a_{2,1}(e_2 \otimes e_1) + a_{2,2}(e_2 \otimes e_2),$$

its coordinates form:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

So tensors are in bijection with 2 × 2 matrices. A simple tensor:

$$(a_1 e_1 + a_2 e_2) \otimes (b_1 e_1 + b_2 e_2) \leftrightarrow \begin{pmatrix} a_1 b_1 & a_1 b_2 \\ a_2 b_1 & a_2 b_2 \end{pmatrix},$$

which is degenerate of rank 1. So simple tensors correspond to matrices of rank 1, determinant 0. So note that $(e_1 \otimes e_2) + (e_2 \otimes e_1)$ is not simple.

Remark 10.105. For an R-algebra S, we have $S \otimes_R$ is an S-module.

Thursday, January 25th

Example 10.106. We give an example of when M, N are R-modules but the tensor product of submodules of these are not a submodule of the tensor product of M, N. Note $\mathbb{Z} \subseteq \mathbb{Q}$ as $\mathbb{Z}$-modules. But $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \cong \mathbb{Z}_2$, and $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}_2 = 0$.

Lemma 10.107. *Let S be an R-algebra, M be an R-module then $S \otimes_R M$ has a structure of an S-module by $\alpha(\beta \otimes u) = \alpha\beta \otimes u, \alpha, \beta \in S, u \in M$.*

Proof. Note we have:

$$\alpha \left(\sum a_i(\beta_i \otimes u_i) \right) = \sum a_i(\alpha\beta_i \otimes u_i). \tag{10.22}$$

The line in the above expression, we are checking if the same thing works for arbitrary tensors, since we defined it in the statement of the problem for just simple tensors. We have to check that elements of the kernel... when we convert the stuff in the left to the right, we have to factorize by a submodule. Is the operation well defined? The operation is: $S \otimes M \to S \otimes M$ where $\beta \otimes u \mapsto \alpha\beta \otimes u$. It is well-defined because it is a bilinear operation: $(\beta, u) \mapsto \alpha\beta \otimes u$. This is our universal approach: first we defined some mapping on simple tensors: $\beta\otimes u \mapsto \alpha\beta\otimes u$, which should be a homomorphism of R-modules. Then to check that it is well-defined, we need to check that it is bilinear on the set $StimesM$. Checking bilinearity:

$$(\alpha\beta, u) \mapsto \alpha a\beta \otimes u = a\alpha\beta \otimes u = a(\alpha\beta \otimes u).$$

Checking conditions, we have:

$$\begin{aligned}(\alpha_1 + \alpha_2)(\beta \otimes u) = \alpha_1\beta \otimes u + \alpha_2\beta \otimes u = \alpha_1(\beta \otimes u) + \alpha_2(\beta \otimes u),\\ \alpha(w_1 + w_2) = \alpha w_1 + \alpha w_2, w_i \in S \otimes_R M,\\ \alpha_1(\alpha_2 w) = (\alpha_1\alpha_2)w.\end{aligned} \tag{10.23}$$

The second line is because $w \mapsto \alpha w$ is a homomorphism. This is called **extension of scalars.** □

Example 10.108. We give some examples of **extension of scalars.**

(1) Let F be the field of quotients of an integral domain R. Then $F\otimes_R M$ is an F-module, that is, a vector space. This operation kills all torsion, but preserves the free part. In the case $M = M_1 \oplus M_2$, where M_1 is free, M_2 is torsion. Not always the case, but it is in PID, or in finitely generated abelian groups. So $F\otimes M = F\otimes M \oplus 0$. It has the same rank as M_1. If $M_1 = R^n$, then $F \otimes M_1 \cong F^n$, and it is a vector space.

(2) Let V be an R-vector space. Consider $\mathbb{C} \otimes_{\mathbb{R}} V$ - this is a $\mathbb{C}$-vector space, called **the complexification of V.** We have:

$$\begin{aligned}\mathbb{C} = \mathbb{R} \oplus i\mathbb{R} = R\{1, i\},\\ \mathbb{C} \otimes V = (\mathbb{R} \otimes V) \oplus (i\mathbb{R} \otimes V) = (1 \otimes V) \oplus (i \otimes V).\end{aligned} \tag{10.24}$$

So we have: $a \otimes u = 1 \otimes au$, and $ib \otimes u = i \otimes bu$. So $\forall w \in \mathbb{C} \otimes V$, $w = 1 \otimes u + i \otimes v = u + iv$. Also,

$$(a + ib)(u + iv) = (au - bv) + i(av + bu),$$

$u + iv \in V + iV$. So this is similar to how we get new elements when we extend from $\mathbb{R}$ to $\mathbb{C}$. If V is n-dimensional, with basis $\{e_1, ..., e_n\}$, then $\mathbb{C} \otimes V$ is n-dimensional $\mathbb{C}$-vector space with basis $\{e_1, ..., e_n\}$ and $2n$-dimensional $\mathbb{R}$-vector space with basis $\{e_1, ..., e_n, ie_1, ..., ie_n\}$. Now let T be a linear transformation of V. Then V is an $\mathbb{R}[x]$-module by $xu = Tu$. We have:

$$\left(\sum_{k=0}^{n} a_k x^k\right) u = \sum_{k=0}^{n} a_k T^k u.$$

So $\mathbb{C}[x] \otimes_{\mathbb{R}[x]} V$ is a $\mathbb{C}[x]$-module, that is, we have a $\mathbb{C}$-vector space $\mathbb{C} \otimes_{\mathbb{R}} V$ on which T acts as a linear transformation.

(3) Let A_1, A_2 be R-algebras. Then $A_1 \otimes_R A_2$ has a structure of an R-algebra by

$$\alpha_1 \otimes \beta_1) \cdot (\alpha_2 \otimes \beta_2) = (\alpha_1\alpha_2) \otimes (\beta_1 \otimes \beta_2).$$

Shit should be checked, but it works. The **subscript below the tensor product symbol** represents where the scalars are from.

(4) *This is a problem from the book. If S is an R-algebra, prove that $S \otimes_R R[x] \cong S[x]$.*

Proof. You need to check something like this:

$$(\alpha_1 \otimes (a_1 x^n + \cdots + a_1 x + a_0)) \cdot (\alpha_2 \otimes (\ldots)).$$

The map would be given by:

$$\alpha_1 \otimes (a_1 x^n + \cdots + a_1 x + a_0) \mapsto a_n \alpha x^n + \cdots a_1 \alpha x + a_0 \alpha.$$

Here it is just defined for simple tensors. So any polynomial of S is the image of some tensor, since we have:

$$\alpha_n \otimes x^n + \cdots + \alpha_1 \otimes x + \alpha_0 \otimes 1 \mapsto \alpha_n x^n + \cdots + \alpha_1 x + \alpha_0.$$

□

(5) Prove $R[x] \otimes_R R[y] \cong R[x,y]$.

Proof.

$$(a_n x^n + \cdots a_1 x + a_0) \otimes (b_m y^m + \cdots + b_1 y + b_0) \mapsto a_n b_m x^n y^n + \cdots + a_0 b_0 = p(x) q(x).$$

We map $x^n \otimes y^m \mapsto x^n y^m$. Again this is an exercise from the book. □

Definition 10.109. Let $\varphi_1 \in Hom(M_1, N_1)$ and $\varphi_2 \in Hom(M_2, N_2)$. Then $\varphi_1 \otimes \varphi_2 : M_1 \otimes M_2 \to N_1 \otimes N_2$. is defined by $\varphi_1 \otimes \varphi_2(u_1 \otimes u_2) = \varphi_1(u_1) \otimes \varphi_i(u_2)$. This is the **tensor product of two homomorphisms.**

We prove it is a homomorphism.

Proof. It is well defined since the mapping $(u_1, u_2) \mapsto \varphi_1(u_1) \otimes \varphi_2(u_2)$ is bilinear. So we get a mapping $Hom(M_1, N_1) \times Hom(M_2, N_2) \to Hom(M_1 \otimes M_2, N_1 \otimes N_2)$. This mapping is also bilinear. We have to check four identities. So it defines a homomorphism:

$$Hom(M_1, N_1) \otimes Hom(M_2, N_2) \to Hom(M_1 \otimes M_2, N_1 \otimes N_2),$$

as we have seen from the definition/construction of a tensor product. □

Definition 10.110. Assume that M is an R-module. We want to convert it to an algebra. If we take $M \otimes M$, then we multiply two vectors, but we cannot multiply these tensors. To have an algebra you must be able to multiply any elements. So if we want an algebra, we take $R \oplus M \oplus (M \otimes M) \oplus (M \otimes M \otimes M) \oplus (\ldots) \oplus \cdots$. This is called the **tensor algebra of M.**

Definition 10.111. An **graded algebra**:

$$A = A_0 \oplus A_1 \oplus A_2 \oplus \cdots,$$

such that $\forall i, j,\ A_i \cdot A_j \subseteq A_{i+j}$.

Example 10.112. We give a neat example that demonstrates why the location of the scalars is important:

$$\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{R}^4,$$
$$\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C} \cong \mathbb{C} \cong \mathbb{R}^2.$$

Remark 10.113. In the case $M = M_1 \oplus M_2$, where M_1 is free, M_2 is torsion. Not always the case, but it is in PID, or in finitely generated abelian groups. So $F \otimes M = F \otimes M \oplus 0$. It has the same rank as M_1. If $M_1 = R^n$, then $F \otimes M_1 \cong F^n$, and it is a vector space. So this operation **kills all torsion.**

REMARK 10.114. Recall that an R-**algebra** is basically an R-module which is also a ring. So it is an R-module with multiplication.

Friday, January 26th
We do some exercises from the book starting with 10.4.8.
Monday, January 29th
We go to Section 10.5.

10.4 EXERCISES

8. *Let R be an integral domain, Q-field of quotients, N an R-module, and $U = R^* = R - \{ 0 \}$. We define: $U^{-1}N = U \times N/\sim$. Where:*

$$(u,n) \sim (u',n') \text{ if } v(u'n - un') = 0,$$

for some v. Denote $(u,n) = \frac{n}{u}$. We define addition:

$$\frac{n}{u} + \frac{m}{v} = \frac{vn + um}{uv}.$$

And we define multiplication by scalars:

$$r\frac{n}{u} = \frac{rn}{u}.$$

And we claim that $U^{-1}N$ becomes an R-module.

(a) PROOF. We have:

$$\begin{aligned}(u,n) \sim (u',n') \sim (u'',n'') &\Rightarrow^? (u,n) \sim (u'',n''),\\ u'n = un', u''n' = u'n'' &\Rightarrow^? un'' = u''n.\end{aligned} \tag{10.25}$$

But we have $u''u'n = u''un' = uu'n''$, so $u'(u''n - un'') = 0$. So the relation given by the book, $u'n - un'$ must be the wrong one, so we now switch to using the relation stated above. So we have:

$$\begin{aligned}(u,n) \sim (u',n') \sim (u'',n'') &\Rightarrow^? (u,n) \sim (u'',n''),\\ nu'n = nun', n'u''n' = v'u'n'' &\Rightarrow^? .\end{aligned} \tag{10.26}$$

So we have $vv'u''u'n = vv'u''un' = vv'uu'n''$, so $vv'u'(u''n - un'') = 0$. So $(u,n) \sim (u'',n'')$. If $(n,u) \sim (n',u'), (m,v) \sim (m',v')$ is $(uv, vn + um) \sim (u'v', v'n' + u'm')$. Is this true? Leibman thinks so. Let's believe that this is true. Or not. Let's check. So we have $w(mv' - m'v) = 0$ for some $w \neq 0$. And $w'(nu' - n'u) = 0$ for some $w' \neq 0$. Now we take:

$$\begin{aligned}&ww'(uv(v'n' + u'm') - u'v'(un + um))\\ =&ww'[vv'(un' - u'n) + uu'(vm' - v'm)]\\ =&0.\end{aligned} \tag{10.27}$$

And then we have to check something else, which we will skip. So $U^{-1}N$ is an R-module, $U^{-1}N = \{ \frac{n}{u}, n \in N, u \in R - \{ 0 \} \}$. Up until this point, we only needed that R is commutative, and that U is multiplicatively closed, we did not need that R was integral domain yet.

□

(b) *Prove that $U'N \cong Q \otimes_R N$.*

PROOF. Define $\varphi : Q \otimes_R N \to U^{-1}N$ by $\frac{a}{b} \otimes n \mapsto \frac{an}{b}$. Of course it is a well-defined homomorphism, it can be easily checked. Can we construct an inverse? Define $\psi : U^{-1}N \to Q \otimes_R N$ by $\frac{n}{u} \mapsto \frac{1}{u} \otimes n$. And check that $\psi = \varphi^{-1}$. Well, is it well-defined? We don't have to check that it is a homomorphism, since if it is the inverse of one, then it is one itself. If $(n', u') \sim (n, u)$, is $\frac{1}{u} \otimes n' = \frac{1}{u} \otimes n$? Let $v(un' - u'n) = 0$. Then:

$$\begin{aligned} \frac{1}{u'} \otimes n' &= uv \cdot \left(\frac{1}{uvu'} \otimes n'\right) \\ &= \frac{1}{uvu'} \otimes uvn' \\ &= \frac{1}{uvu'} \otimes u'vn \\ &= \frac{1}{u} \otimes n. \end{aligned} \tag{10.28}$$

So it's well defined. Now why is it the inverse of φ. Observe:

$$\begin{gathered} \frac{n}{u} \overset{\psi}{\mapsto} \frac{1}{u} \otimes n \overset{\varphi}{\mapsto} \frac{n}{u}, \\ \frac{v}{u} \otimes n = v(\frac{1}{u} \otimes n) \overset{\varphi}{\mapsto} v \cdot \frac{n}{u} \overset{\psi}{\mapsto} \frac{1}{u} \otimes vn = \frac{v}{u} \otimes n. \end{gathered} \tag{10.29}$$

□

(c) *Prove that $\frac{1}{d} \otimes n = 0$ if and only if $rn = 0$ for some $r \in R^*$.*

PROOF. Under the isomorphism from part (b) we have:

$$\frac{1}{d} \otimes n \overset{\varphi}{\mapsto} \frac{n}{d} \in U^{-1}N.$$

And $\frac{n}{d} = 0 = \frac{0}{1}$ if and only if $r(n - 0) = 0$ for some $r \neq 0$. And we make use of this result in Exercise 10.4.9. □

(d) *Let A be an abelian group. Then prove $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$ if and only if A is a torsion group, $|a| < \infty$ $\forall a \in A$.*

PROOF. We claim that $\mathbb{Q} \otimes N = 0$ if and only if $N = Tor(N)$. If $N = Tor(N)$, then $Q \otimes N = 0$. Recall that A being abelian is equivalent to saying it is a $\mathbb{Z}$-module. So $R = \mathbb{Z}$ in this case, so $\mathbb{Q} = Q$, the field of fractions of the ring. If $N = Tor(N)$, then $Q \otimes N = 0$. If $Q \otimes N = 0$, then $\forall n \in N$, $1 \otimes n = 0<$ so $\exists r \neq 0$, s.t. $rn = 0$ by part (c). So $n \in Tor(N)$ for all n. □

9. *Suppose R is an integral domain with quotient field Q and let N be any R-module. Let $Q \otimes_R N$ be the module obtained from N by extension of scalars from R to Q. Prove that the kernel of the R-module homomorphism $\iota : N \to Q \otimes_R N$ is the torsion submodule of N. [Exercise 10.1.8.,Exercise 10.4.8]*

PROOF. Recall that the torsion submodule is defined as:

$$Tor(N) = \{n \in N : rn = 0 \text{ for some nonzero } r \in R\}.$$

And recall that $\iota(n) = 1 \otimes n$. Let $n \in Tor(N)$. Then $\iota(n) = 1 \otimes n$. Since $n \in Tor(N)$, there exists $r \neq 0$ such that $rn = 0$, and we also have $1/r \in Q$. So we have:

$$1 \otimes n = 1(1 \otimes n) = \frac{1}{r} r(1 \otimes n) = \frac{1}{r}(1 \otimes rn) = \frac{1}{r}(1 \otimes 0) = 0.$$

Thus $n \in ker \iota$, and $Tor(N) \subseteq ker \iota$. Now let $n \in ker \iota$. Then

$$\iota(n) = 1 \otimes n = 0 = 1 \otimes 0.$$

So we must have that there exists $r \neq 0$ s.t. $rn = 0$. And by the result of Exercise 10.4.8(c), we know that $(1/d) \otimes n = 0$ if and only if there exists $r \in R$ s.t. $rn = 0$. Hence we know $n \in Tor(N)$. □

10. *Suppose R is commutative and $N \cong R^n$ is a free R-module of rank n with R-module basis $e_1, ..., e_n$.*

Recall the definition of a free module of rank n:

Definition 10.115. A **free module** is a direct sum of finitely or infinitely many copies of R,

$$F_\Lambda = \bigoplus_{\alpha \in \Lambda} R = \{a_{\alpha_1} + \cdots + a_{\alpha_k} : k \in \mathbb{N}, \alpha_i \in \Lambda, a_{\alpha_i} \in R\},$$

where the sum of u's above is a formal sum. We can also define it as:

$$F_\Lambda = \{(a_\alpha)_{\alpha \in \Lambda} : a_\alpha \in R, \forall \alpha, a_\alpha = 0 \text{ for all but finitely many } \alpha\}.$$

Note R is unital here.

(a) *For any nonzero R-module M show that every element of $M \otimes N$ can be written uniquely in the form $\sum_{i=1}^n m_i \otimes e_i$ where $m_i \in M$. Deduce that if $\sum_{i=1}^n m_i \otimes e_i = 0$ in $M \otimes N$, then $m_i = 0$ for $i = 1, ..., n$.*

Proof. Let $t = a_1(u_1 \otimes v_1) + \cdots + a_l(u_l \otimes v_l) \in M \otimes N$. And for each $v_i \in N$ we have:

$$v_i = r_1 e_1 + \cdots + r_n e_n,$$

with $r_j \in R$ uniquely by the definition of our standard basis. Then we may write:

$$\begin{aligned}
t &= a_1(u_1 \otimes (r_{1,1}e_1 + \cdots + r_{1,n}e_n)) + \cdots + a_l(u_l \otimes (r_{l,1}e_1 + \cdots + r_{l,n}e_n)) \\
&= (a_1 u_1 \otimes (r_{1,1}e_1 + \cdots + r_{1,n}e_n)) + \cdots + (a_l u_l \otimes (r_{l,1}e_1 + \cdots + r_{l,n}e_n)) \\
&= ((a_1 u_1 \otimes r_{1,1}e_1) + \cdots + (a_1 u_1 \otimes r_{1,n}e_n)) + \cdots + ((a_l u_l \otimes r_{l,1}e_1) + \cdots + (a_l u_l \otimes r_{l,n}e_n)) \\
&= ((a_1 r_{1,1} u_1 \otimes e_1) + \cdots + (a_1 r_{1,n} u_1 \otimes e_n)) + \cdots + ((a_l r_{l,1} u_l \otimes e_1) + \cdots + (a_l r_{l,n} u_l \otimes e_n)) \\
&= ((a_1 r_{1,1} u_1 \otimes e_1) + \cdots + (a_l r_{l,1} u_l \otimes e_1)) + \cdots + ((a_1 r_{1,n} u_1 \otimes e_n) + \cdots + (a_l r_{l,n} u_l \otimes e_n)) \\
&= ((a_1 r_{1,1} u_1 \cdots + a_l r_{l,1} u_l) \otimes e_1) + \cdots + ((a_1 r_{1,n} u_1 + \cdots + a_l r_{l,n} u_l) \otimes e_n).
\end{aligned} \tag{10.30}$$

So letting $m_i = (a_l r_{1,i} u_1 \cdots + a_l r_{l,i} u_l)$, we have:

$$t = \sum_{i=1}^n m_i \otimes e_i,$$

where $m_i \in M$. Assume that $\sum_{i=1}^n m_i \otimes e_i = 0$. If each term in the sum is identically zero, then the result is proved, all $m_i = 0$. So without loss of generality, assume $m_1, ..., m_k \neq 0$

for some $k \leqslant n$. If the m_i's are linearly independent, then since the e_i's are also linearly independent:

$$\sum_{i=1}^{n} m_i \otimes e_i = 0 \Rightarrow m_i = 0, \forall i,$$

which is a contradiction. So then we must have that the m_i's are linearly dependent. So we can write:

$$\sum_{i=1}^{k} m_i \otimes e_i = \sum_{i=1}^{k} r_i m \otimes e_i = \sum_{i=1}^{k} m \otimes r_i e_i = 0.$$

If $m = 0$ we are done, contradiction, since then $m_i = 0$ for all i. If $\sum r_i e_i = 0$ we have a contradiction, since then the basis wouldn't be linearly independent. So we must have that all $m_i = 0$. □

(b) *Show that if $\sum m_i \otimes n_i = 0$ in $M \otimes N$ where the n_i are merely assumed to be R-linearly independent, then it is not necessarily true that all the m_i are 0. [Consider $R = \mathbb{Z}, n = 1, M = \mathbb{Z}/2\mathbb{Z}$, and the element $1 \otimes 2$.]*

Proof. Note that now we relax the assumption that our elements from R^n generate R^n. So now they are only linearly independent. We have:

$$1 \otimes 2 = 2 \otimes 1 = 0 \otimes 1 = 0,$$

but $1 \neq 0 \in \mathbb{Z}/2\mathbb{Z}$, and 2 is just a single element of some R module over R, so it is linearly independent. So we have found a counterexample. □

15. *Prove that $M \otimes (N \oplus K) \cong (M \otimes N) \oplus (M \otimes K)$. The same is true for:*

$$M \otimes \left(\bigoplus_{\alpha \in \Lambda} N_\alpha \right) \cong \bigoplus_{\alpha \in \Lambda} (M \otimes N_\alpha),$$

which uses the same proof. But:

$$M \otimes \left(\prod_{\alpha \in \Lambda} N_\alpha \right) \ncong \prod_{\alpha \in \Lambda} (M \otimes N_\alpha).$$

Example: $R = \mathbb{Z}, M = \mathbb{Q}, N_i = \mathbb{Z}_{2^i}, i = 1, 2, \ldots$ Consider:

$$\mathbb{Q} \otimes \left(\prod_{i=1}^{\infty} \mathbb{Z}_{2^i} \right) \neq 0,$$

by 8. But note:

$$\prod_{i=1}^{\infty} (\mathbb{Q} \otimes \mathbb{Z}_{2^i}) = 0.$$

16. *Suppose R is commutative and let I and J be ideals of R, so $R/I, R/J$ are naturally R-modules .*

(a) *Prove that every element of $R/I \otimes_R R/J$ can be written as a simple tensor of the form $(1 \mod I) \otimes (r \mod J)$.*

Proof. Let:

$$t = a_1(b_1 \mod I \otimes c_1 \mod J) + \cdots + a_l(b_l \mod I \otimes c_l \mod J) \in R/I \otimes_R R/J,$$

with $a_i, b_i, c_i \in R$. Then we have:

$$\begin{aligned}t &= a_1b_1(1 \mod I \otimes c_1 \mod J) + \cdots + a_lb_l(1 \mod I \otimes c_l \mod J)\\ &= (1 \mod I \otimes a_1b_1c_1 \mod J) + \cdots + (1 \mod I \otimes a_lb_lc_l \mod J)\\ &= 1 \mod I \otimes (a_1b_1c_1 + \cdots + a_lb_lc_l) \mod J,\end{aligned} \tag{10.31}$$

so since $(a_1b_1c_1 + \cdots + a_lb_lc_l) \in R$, we have written t as a simple tensor. □

(b) *Prove that there is an R module isomorphism $R/I \otimes_R R/J \cong R/(I+J)$ mapping $(r \mod I) \otimes (r' \mod J)$ to $rr' \mod (I+J)$.*

PROOF. Let $\varphi : R/I \otimes_R R/J \to R/(I+J)$ be given by $\varphi((r \mod I) \otimes (r' \mod J)) = rr' \mod (I+J)$. We prove this is an isomorphism. Since we proved that every element of $R/I \otimes_R R/J$ can be written as a simple tensor of the form $(1 \mod I) \otimes (r \mod J)$, we need only to check elements of this form.

Homomorphism: We have:

$$\begin{aligned}&\varphi((1 \mod I) \otimes (r \mod J) + (1 \mod I) \otimes (s \mod J))\\ =&\varphi((1 \mod I) \otimes (r + s \mod J))\\ =&r + s \mod (I+J)\\ =&r \mod (I+J) + s \mod (I+J)\\ =&\varphi((1 \mod I) \otimes (r \mod J)) + \varphi((1 \mod I) \otimes (s \mod J)).\end{aligned} \tag{10.32}$$

So addition is preserved, and for $a \in R$, we also have:

$$\begin{aligned}\varphi(a((1 \mod I) \otimes (r \mod J))) &= \varphi(((a \mod I) \otimes (r \mod J)))\\ &= ar \mod (I+J)\\ &= a(r \mod (I+J))\\ &= a\varphi((1 \mod I) \otimes (r \mod J)).\end{aligned} \tag{10.33}$$

So φ is an R-module homomorphism.

Injectivity: Observe:

$$\varphi((1 \mod I) \otimes (r \mod J)) = \varphi((1 \mod I) \otimes (s \mod J)), \tag{10.34}$$

which gives us:

$$r \mod (I+J) = s \mod (I+J), \tag{10.35}$$

thus we know $r - s \in (I+J)$. So $r - s = j \mod I$ for some $j \in J$. So we have:

$$\begin{aligned}&(1 \mod I) \otimes (r \mod J) - (1 \mod I) \otimes (s \mod J)\\ =&(1 \mod I) \otimes (r - s \mod J)\\ =&(r - s \mod I) \otimes (1 \mod J)\\ =&(j \mod I) \otimes (1 \mod J)\\ =&(1 \mod I) \otimes (j \mod J)\\ =&0.\end{aligned} \tag{10.36}$$

So φ must be injective.

Surjectivity: Let $r \mod (I+J) \in R/(I+J)$. Then $\varphi((1 \mod I) \otimes (r \mod J)) = r \mod (I+J)$, so φ is surjective. Hence φ is an isomorphism. □

20. *Let $I = (2, x)$ be the ideal generated by 2 and x in the ring $R = \mathbb{Z}[x]$. Show that the element $2 \otimes 2 + x \otimes x$ in $I \otimes_R I$ is not a simple tensor, i.e., cannot be written as $a \otimes b$ for some $a, b \in I$.*

Proof. Define $t = 2 \otimes 2 + x \otimes x$. We first express t as a simple tensor in R. We define $\beta : \mathbb{Z}[x] \times \mathbb{Z}[x] \to \mathbb{Z}[x] \otimes \mathbb{Z}[x]$ given by $\beta((p(x), q(x)) = p(x) \otimes q(x)$. We also define $\gamma : \mathbb{Z}[x] \times \mathbb{Z}[x] \to \mathbb{Z}[x]$ given by $\gamma((p(x), q(x)) = p(x)q(x)$. This map is bilinear, so we have an induced homomorphism $\varphi : \mathbb{Z}[x] \otimes \mathbb{Z}[x] \to \mathbb{Z}[x]$, so altogether, we have:

$$\begin{tikzcd}
& \mathbb{Z}[x] \times \mathbb{Z}[x] \arrow[dl, "\beta"'] \arrow[dr, "\gamma"] & \\
\mathbb{Z}[x] \otimes \mathbb{Z}[x] \arrow[rr, "\varphi"] & & \mathbb{Z}[x]
\end{tikzcd}.$$

Then we would have:

$$p \otimes q = 2 \otimes 2 + x \otimes x,$$

for some $p, q \in \mathbb{Z}[x]$. But we also know:

$$2 \otimes 2 + x \otimes x = 4(1 \otimes 1) + x \otimes x = 4(1 \otimes 1) + x^2(1 \otimes 1) = (4 + x^2)(1 \otimes 1) \in \mathbb{Z}[x]$$

But $(4 + x^2)$ is a prime in $\mathbb{Z}[x]$. To write t as a simple tensor in $\mathbb{Z}[x]$, we must have $4 + x^2 = ab$ for some $a, b \in \mathbb{Z}[x]$, so that we may write:

$$ab(1 \otimes 1) = a \otimes b \in \mathbb{Z}[x].$$

So let $4 + x^2 = ab$, and since it is a prime and we are in $\mathbb{Z}[x]$, without loss of generality, we must have $b = 1$, but note that $1 \notin I$, so it is impossible to write t as a simple tensor in $I \otimes_R I$, since under the same bilinear map γ, we have:

$$\begin{tikzcd}
& I \times I \arrow[dl, "\beta"'] \arrow[dr, "\gamma"] & \\
I \otimes I \arrow[rr, "\varphi"] & & I^2
\end{tikzcd},$$

from which we see that the image $u \otimes v \mapsto uv$ of any simple tensor is reducible. □

21. *Suppose R is commutative, and let I and J be ideals of R.*
    (a) *Show that there is a surjective R-module homomorphism from $I \otimes_R J$ to the product ideal IJ mapping $i \otimes j$ to the element ij.*

Proof. Let $\varphi : I \otimes_R J \to IJ$ be given by:

$$\varphi(r_1(i_1 \otimes j_1) + \cdots + r_n(i_n \otimes j_n)) = r_1 i_1 j_1 + \cdots + r_n i_n j_n.$$

We show that φ is a surjective homomorphism of R-modules. Observe:

$$\begin{aligned}&\varphi((r_1(i_1\otimes j_1)+\cdots r_n(i_n\otimes j_n))+(s_1(i_1'\otimes j_1')+\cdots s_m(i_m'\otimes j_m')))\\=&\varphi(r_1(i_1\otimes j_1)+\cdots r_n(i_n\otimes j_n)+s_1(i_1'\otimes j_1')+\cdots s_m(i_m'\otimes j_m'))\\=&r_1i_1j_1+\cdots+r_ni_nj_n+s_1i_1'j_1'+\cdots+s_mi_m'j_m'\\=&\varphi((r_1(i_1\otimes j_1)+\cdots r_n(i_n\otimes j_n))+\varphi((s_1(i_1'\otimes j_1')+\cdots s_m(i_m'\otimes j_m'))).\end{aligned}\tag{10.37}$$

So φ preserves addition. Additionally:

$$\begin{aligned}\varphi(r(i\otimes j))&=\varphi((ri\otimes j))\\&=rij\\&=r\varphi((i\otimes j)).\end{aligned}\tag{10.38}$$

So φ also preserves scalar multiplication for simple tensors and thus for general tensors as well. Now we show that φ is surjective. Let $r\in IJ$. Then

$$r=\sum_{k=1}^{n}i_kj_k,$$

for $i_k\in I, j_k\in J$. Then $\varphi(i_1\otimes j_1+\cdots+i_n\otimes j_n)=r$, because we already proved φ is a homomorphism and hence preserves addition, so φ is surjective. □

(b) *Give an example to show that the map in (a) need not be injective [Exercise 10.4.17].*
Consider $I=(2,x)$ and $R=\mathbb{Z}[x]$. We define a map: $\varphi: I\otimes_R I\to II=I$ given by $\varphi(i\otimes j)=ij$. By part (a), we know it is a surjective homomorphism. Note:

$$\varphi(2\otimes x)=\varphi(x\otimes 2)=2x.$$

But from Exercise 10.4.17(c), we know that $2\otimes x\neq x\otimes 2$ in $I\otimes_R I$.

SECTION 10.5

Exact sequences and tensor algebras

Monday, January 29th

Definition 10.116. Let M be an R-module. $\forall k\in\mathbb{N}$ let $\tau_k(M)=M\otimes\cdots\otimes M$ (k-times). These are called the set of k-tensors. Note that $\tau_0(M)=R$ and $\tau_1(M)=M$. We have:

$$\tau(M)=\bigoplus_{K=0}^{\infty}\tau_k(M),$$

called the **tensor algebra of** M.

Elements look like sums:

$$a+u_1+b_2(u_2\otimes u_3)+b_3(u_5\otimes u_6\otimes u_7)+\cdots+d_8(u_9\otimes u_{10}).$$

Definition 10.117. **Universal Property:** if A is an R=algebra and $\varphi : M \to A$ is a hom-sm of R-modules, then $\exists$ a unique hom-sm $\Phi : \tau(M) \to A$ of R-algebras such that:

$$\Phi|_{M=\tau_1(M)} = \varphi, \Phi(u_1 \otimes \cdots \otimes u_k) \quad = \varphi(u_1) \cdots \varphi(u_k) \in A. \tag{10.39}$$

Example 10.118. (1) Let $M = R$. Then we have $\tau(R) = R \oplus R \oplus R \cdots$. The elements are finite multiplications. Let's artificially introduce basis vector. Let $M = Rx$, $(x = 1)$. Where x is the basis vector. Then

$$\begin{aligned} \tau_1(R) &= Rx, \\ \tau_2(R) &= R \otimes R = R(x \otimes x), \\ \tau_3(R) &= R(x \otimes x \otimes x), \\ \tau(R) &= R \oplus R \otimes R \oplus R \otimes R \otimes R \oplus \cdots \cong R[x]. \end{aligned} \tag{10.40}$$

(2) $M = R^2 = R\{x, y\}$. Then:

$$\tau(R) \cong \{ \text{polynomials in non-commutative variables x and y.} \} = RG,$$

since $x \otimes y \neq y \otimes x$. where G is the free semigroup generated by x, y:

$$G = \left\{ 1, x, y, x^2, xy, yx, y^2, xyx, \ldots \right\}.$$

Definition 10.119. **Symmetric algebra of M.** Let $\mathcal{C}(M)$ be the ideal in $\tau(M)$ generated by $u \otimes v - v\ tensu, u, v \in M$. The algebra $\mathcal{S}(M) = \tau(M)/\mathcal{C}(M)$ is called the **symmetric algebra of M.**

So in the above definition, we just declare that $x \otimes y = y \otimes x$, and you can switch them along any chain of tensor products:

$$u_1 \otimes u_2 \otimes u_3 \otimes u_4 = u_4 \otimes u_2 \otimes u_3 \otimes u_1 \in \mathcal{S}(M).$$

The ability to do it on more than two tensors follows from the structure of transpositions in symmetric groups. What even is a higher degree tensor? We prove something:

Proof. $\forall k$ S_k acts of $\tau_k(M)$ by $\sigma(u_1 \otimes \cdots u_k) = u_{\sigma(1)} \otimes \cdots \otimes u_{\sigma(k)}$. The action of any transposition is trivial module $\mathcal{C}(M)$ or something like that. □

Definition 10.120. **Universal Property:** If A is a commutative R-algebra, and $\varphi : M \to A$ is a hom-sm of R-modules, then there is a unique hom-sm $\Phi : \mathcal{S}(M) \to A$ such that $\Phi|_M = \varphi$. Also $\mathcal{S}(M)$ is still a **graded algebra** (Definition 10.4):

$$\mathcal{S}(M) = R \oplus \mathcal{S}_1(M) \oplus \mathcal{S}_2(M) \oplus \cdots$$

where the second term is $\cong M$. Why is it unique? Because we have no choice as to send $\Phi(u_1 \otimes \cdots u_k) = \varphi(u_1) \cdots \varphi(u_k)$.

Example 10.121. Take M to be the free module generated by two elements $M = R\{x, y\}$. And then $\mathcal{S}(M) \cong R[x, y]$ (now we have commutativity!).

Definition 10.122. **Exterior Algebra:** let $A(M)$ be the ideal in $\tau(M)$ generated by tensors $u \otimes u$, $u \in M$. The algebra:

$$\Lambda(M) = \tau(M)/A(M),$$

is called the exterior algebra of M.

In $\Lambda(M)$, instead of $\otimes$, we write "$\wedge$" - wedge. So we have:

$$\Lambda(M) = \{ a + u_1 + u_2 \wedge u_3 + u_4 \wedge u_5 \wedge u_6 + \cdots () \}.$$

In $\Lambda(M)$, $u \wedge u = 0$ for all u, and:

$$u \wedge v = -v \wedge u.$$

Proof.

$$(u+v) \wedge (u+v) = u \wedge u + u \wedge v + v \wedge u + v \wedge v.$$

□

$\int f dx \neq \int f(\varphi(t))dt$. But we do have:

$$\int f dx = \int f(\varphi(t))\varphi'(t)dt.$$

fdx is called the **differential form**. And we have $\int f(x,y)dx \wedge dy$, where $f(x,y)dx \wedge dy$ is called a differential form of second order. Recall:

$$\int f(x,y)dx \wedge dy = \int f(x(u,v), y(u,v)) \cdot |J| du \wedge dv.$$

Where $|J|$ is the Jacobian of $(u,v) \mapsto (x,y)$ as vertical vectors.

Bonus Problem: If $x = au + bv$ and $y = cu + dv$ prove that $x \wedge y = \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} u \wedge v$.

Now what the hell is going on when our ring is **noncommutative**. Let M, N be a left R-module. Can you have:

$$(au) \otimes v = u \otimes av?$$

But then we have the following:

$$(abu) \otimes v = (bu) \otimes (av) = u \otimes (bav) = (bau) \otimes v.$$

So we have some weird new hidden relations. So now:

$$ab(u \otimes v) = ba(u \otimes v),$$

R acts on $M \otimes N$ as a commutative ring.

Remark 10.123. If M is a right R-module and N is a left R-module, product $M \otimes_R N$ where:

$$(ua) \otimes v = u \otimes (av),$$

and this will be okay, no problem like this. But you cannot take scalars out. So it is not equal to $a(u \otimes v)$. It is an abelian group only, not an R-module. Mappings with this property are called **balanced maps** since they are missing one of the four bilinearity properties.

Tuesday, January 30th

Definition 10.124. A diagram of sets and mappings is a **commutative diagram** if for all paths with common starting and ending points, the composition of mappings along these paths is the the same.

Definition 10.125. A sequence $A_{i-1} \to^{\varphi_{i-1}} A_i \to^{\varphi_i} A_{i+1} \to^{\varphi_{i+1}} A_{i+2} \to$ of hom-sms of groups, rings, or modules is **exact** if $\forall i \; Image(\varphi_i) = ker(\varphi_{i+1})$.

Remark 10.126. $0 \to A \to_{\varphi} B$ is exact if and only if φ is injective. $(ker(\varphi) = Image(0))$

Remark 10.127. $B \to_{\psi} C \to 0$ is exact if and only if φ is surjective. $(\psi(B) = ker(C \to 0) = C)$

Remark 10.128. The sequence $0 \to A \to_{\varphi} B \to_{\psi} C \to 0$ is exact (a **short exact sequence**) if and only if φ is injective (monomorphism),ψ is surjective (epimorphism), and $\varphi(A) = ker(\psi)$. So we have $C \cong B/\varphi(A)$, $\varphi(A) \cong A$.

For groups: $1 \to A \to B \to C \to 1$, $C \cong B/A$.

Definition 10.129. The short exact sequence **splits** if there exists a hom-sm $\sigma : C \to B$ called a **section**, such that $\psi \circ \sigma = Id_C$. So we have:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\varphi"'] & B \arrow[r, "\psi"'] & C \arrow[l, bend right, "\sigma"'] \arrow[r] & 0 \end{tikzcd}$$

In this case, then $B \cong A \oplus C$,

$$B = \varphi(A) \oplus \sigma(C),$$

with an internal direct product.

Proof. $\forall b \in B$:

$$\begin{aligned} \psi(b - \sigma(\psi(b))) &= \psi(b) - \psi \circ \sigma(\psi(b)) \\ &= \psi(b) - \psi(b) = 0. \end{aligned} \tag{10.41}$$

So $b - \sigma(\psi(b)) \in \varphi(A)$, so $b = \sigma(c) + \varphi(a)$ for $c = \psi(b)$ and some $a \in A$. If $\varphi(a) = \sigma(c)$, then:

$$0 = \psi(\varphi(a)) = \psi(\sigma(c)) = c,$$

so $\sigma(c) = 0$, and $\varphi(a) = 0$, so $\sigma(C) \cap \varphi(A) = 0$. □

Definition 10.130. A homomorphism of two short exact sequences is a commutative diagram of the sort:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r] \arrow[d, "\alpha"] & B \arrow[r] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r] & B' \arrow[r] & C' \arrow[r] & 0 \end{tikzcd},$$

with exact rows.

Lemma 10.131 (**SHORT FIVE LEMMA**). *Let:*

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\varphi"] \arrow[d, "\alpha"] & B \arrow[r, "\psi"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "\varphi'"] & B' \arrow[r, "\psi'"] & C' \arrow[r] & 0 \end{tikzcd},$$

be a homomorphism of short exact sequences.

(a) *If α and γ are surjective, then β is surjective.*
(b) *If α and γ are injective, then β is injective.*
(c) *If α and γ are isomorphisms, then β is an isomorphism.*

Proof. **(b)** We make use of the diagram! Let α,γ be injective. Let $b \in B$, and assume that $\beta(b) = 0$. Consider:

$$\gamma(\psi(b)) = \psi'(\beta(b)) = \psi'(0) = 0. \tag{10.42}$$

But γ is injective, so $\psi(b) = 0$. But the first row is exact, so $b = \varphi(a)$ for some $a \in A$. Then:

$$\varphi'(\alpha(a)) = \beta(\varphi(a)) = \beta(b) = 0, \tag{10.43}$$

But φ', α are injective, so $a = 0$, so $b = \alpha(a) = 0$. □

PROOF. **(a)** Let α, γ be surjective. Let $b' \in B'$ (we need tos how that $b' = \beta(b)$ for some $b \in B$). So take $\psi'(b')$ but then since this is in C' and γ is surjective, so there exists $c \in C$ such that $\gamma(c) = \psi'(b')$. Next, ψ is surjective, so we have $\hat{b} \in B$ such that $\psi(\hat{b}) = c$. So we have:

$$\gamma(c) = \gamma(\psi(\hat{b})) = \psi'(b').$$

Consider:

$$\psi'(b' - \beta(\hat{b})) = \psi'(b') - \psi'(\beta(\hat{b})) = \gamma(c) - \gamma(\psi(\hat{b})) = 0.$$

The second row is exact, so $\exists a' \in A'$ such that:

$$\varphi'(a') = b' - \beta(\hat{b}),$$

α is surjective, so $\exists a \in A$ such that $a' = \alpha(a)$. **If a row is exact, this means the image of first map is the kernel of the second map.** Take $b = \hat{b} + \varphi(a)$. Then:

$$\beta(b) = \beta(\hat{b}) + \beta(\varphi(a)) = \beta(\hat{b}) + \varphi'(\alpha(a)) = \beta(\hat{b}) + b' - \beta(\hat{b}) = b'. \tag{10.44}$$

Part (c) is a corollary of the others. □

LEMMA 10.132 (**SNAKE LEMMA**). $\text{coker}(\alpha) = A'/\alpha(A)$. *We have a commutative diagram with exact rows and columns.*

$$\begin{tikzcd}
 & \ker(\alpha) \arrow[r] \arrow[d] & \ker(\beta) \arrow[r] \arrow[d] & \ker(\gamma) \arrow[d] \arrow[dddll, rounded corners] & \\
 & A \arrow[r, "\psi"] \arrow[d, "a"] & B \arrow[r, "\varphi"] \arrow[d, "b"] & C \arrow[r] \arrow[d, "c"] & 0 \\
0 \arrow[r] & A' \arrow[r, "\psi'"] \arrow[d] & B' \arrow[r, "\varphi'"] \arrow[d] & C' \arrow[d] & \\
 & \text{coker}(\alpha) \arrow[r] & \text{coker}(\beta) \arrow[r] & \text{coker}(\gamma) &
\end{tikzcd}$$

Then there exists a homomorphism $\delta : ker\gamma \to ker\alpha$ such that the snake is exact.

Wednesday, January 31st

REMARK 10.133. Let M be an R-module. Let A be a submodule of module B. Then it may be that $A \otimes M$ is not a submodule of $B \otimes M$!

Consider:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\varphi"] & B \end{tikzcd}$$

which is exact! Then we have:

$$\begin{tikzcd} 0 \arrow[r] & A \otimes M \arrow[r, "\varphi\otimes Id_M"] & B \otimes M \end{tikzcd} ,$$

which may not be exact.

EXAMPLE 10.134. In $\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2$ we have:

$$\forall n \in \mathbb{Z}, 2n \otimes 1 = n \otimes 2 = 0.$$

So observe:

$$\begin{tikzcd} 2\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \arrow[r, "\varphi"'] & \mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}_2 \end{tikzcd} ,$$

where we have $\varphi \otimes Id = 0$. Before we had an embedding:

$$\begin{tikzcd} 0 \arrow[r] & 2\mathbb{Z} \arrow[r, hook, "\varphi"'] & \mathbb{Z} \end{tikzcd} ,$$

but it is no longer an embedding when we take the tensor product with $\mathbb{Z}_2$.

We have a similar example:

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \arrow[r, hook, "\varphi"'] & \mathbb{Q} \end{tikzcd}$$

EXAMPLE 10.135.

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z} \otimes \mathbb{Z}_2 \arrow[r] & \mathbb{Q} \otimes \mathbb{Z}_2 \end{tikzcd}$$

where taking the tensor product with $\mathbb{Z}_2$, we have $\mathbb{Z} \otimes \mathbb{Z}_2 \cong \mathbb{Z}_2$, but $\mathbb{Q} \otimes \mathbb{Z}_2 = 0$. So it isn't injective.

REMARK 10.136. The tensor product preserves surjectivity, but not injectivity.

LEMMA 10.137. *If:*

$$\begin{tikzcd} B \arrow[r, "\psi"'] & C \arrow[r] & 0 \end{tikzcd}$$

is exact (ψ is surjective), then:

$$\begin{tikzcd} B \otimes M \arrow[r, "\psi\otimes Id"'] & C \otimes M \arrow[r] & 0 \end{tikzcd}$$

is exact ($\psi \otimes Id$ is surjective).

PROOF. $\forall c \in C, u \in M$, find $b \in B$ s.t. $\psi(b) = c$, then

$$(\psi \otimes Id)(b \otimes u) = c \otimes u.$$

And simple tensors generate $C \otimes M$, so $\psi \otimes Id(B \otimes M) = C \otimes M$. □

THEOREM 10.138. *If:*

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\varphi"'] & B \arrow[r, "\psi"'] & C \arrow[r] & 0 \end{tikzcd}$$

is exact ($\Rightarrow \psi \circ \varphi = 0$, then:

$$\begin{tikzcd} A \otimes M \arrow[r, "\varphi\otimes Id"'] & B \otimes M \arrow[r, "\psi\otimes Id"'] & C \otimes M \arrow[r] & 0 \end{tikzcd}$$

is exact. (Note that it is still exact on the right, but not on the left, since the zero is dropped)

Proof. First, $(\psi \otimes Id) \cdot (\varphi \otimes Id) = 0$.

$$(\psi \otimes Id)((\varphi \otimes Id)(a \otimes u)) = (\psi \otimes Id)(\varphi(a) \otimes u) = \psi(\varphi(a)) \otimes u = 0 \otimes u = 0.$$

So we have a hom-sm: $\gamma : B \otimes M/((\psi \otimes Id)(A \otimes M)) \to C \otimes M$. We claim this is an isomorphism, so $ker(\psi \otimes Id) = (\varphi \otimes Id)(A \otimes M)$.

Proof. Define a hom-sm $C \otimes M \to MB \otimes M/((\psi \otimes Id)(A \otimes M))$ by:

$$c \otimes u \mapsto b \otimes u \mod ((\psi \otimes Id)(A \otimes M)),$$

where b is s.t. $\psi(b) = c$. Why is it well defined? If b' is another element in B s.t. $\psi(b') = c$, then:

$$b' = b \mod \varphi(A),$$

so $b' \otimes u = b \otimes u \mod (\varphi(A) \otimes M)$. So it's well defined. Next we check that it's bilinear, it's obvious. Claim is that this is inverse of γ and it is, we skip the details. □

□

Remark 10.139. Recall that if we have $\varphi : M \to N$, $K \subseteq M$, and $\varphi(K) = 0$ then we must have a hom-sm $M/K \to N$.

Remark 10.140. $\otimes M$ is a **functor** from the category of R-modules to itself: $A \Rightarrow A \otimes M$, and $A \to B \Rightarrow A \otimes M \to B \otimes M$.

Definition 10.141. A **functor** from category $\mathcal{C}_1$ to category $\mathcal{C}_2$ is a ”mapping” that maps objects to objects and morphisms to morphisms, and preserves compositions of morphisms:

$$\begin{tikzcd} & B \arrow[rr, "F"] & & F(B) \\ A \arrow[ur, "\varphi"] \arrow[rr, "F"] & & F(A) \arrow[ur, "F(\varphi)"] & \end{tikzcd} .$$

Definition 10.142. A functor is **exact** if it maps short exact sequences to short exact sequences.

Remark 10.143. $\otimes M$ is a **right-exact** functor (loses exactness at the left term).

Definition 10.144. A functor is **right-exact** if for any short exact sequence:

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "\varphi"'] & B \arrow[r, "\psi"'] & C \arrow[r] & 0 \end{tikzcd} ,$$

the sequence:

$$\begin{tikzcd} F(A) \arrow[r, "F(\varphi)"'] & F(B) \arrow[r, "F(\psi)"'] & F(C) \arrow[r] & 0 \end{tikzcd}$$

is exact.

Remark 10.145. If R is non-commutative, M is a left R-module, then $\otimes m$ is a functor from category of right R-modules to the category of abelian groups.

There are good modules that preserve exact sequences. They are called flat modules.

Definition 10.146. M is **flat** if whenever:

$$0 \longrightarrow A \xrightarrow[\varphi]{} B$$

is exact, the sequence:

$$0 \longrightarrow A \otimes M \xrightarrow[\varphi \otimes Id]{} B \otimes M$$

is exact. In this case, $\otimes M$ is an exact functor.

Now what modules are flat? The ring R itself is flat.

Remark 10.147. We state some results concerning flat modules.

(1) R is flat:

$$0 \longrightarrow A \longrightarrow B$$

$\Rightarrow$

$$0 \longrightarrow A \otimes R \xrightarrow[\varphi \otimes Id]{} B \otimes R$$

$=$

$$0 \longrightarrow A \longrightarrow B$$

is exact.

(2) If $M = M_1 \oplus M_2$, then M is flat if and only if both M_1, M_2 are flat.

Proof. Let $0 \to A \to_{\varphi} B$ be exact. Then:

$$0 \to A \otimes M \to_{\varphi \otimes Id} B \otimes M$$

is isomorphic to

$$0 \to (A \otimes M_1) \oplus (A \otimes M_2) \to_{\tilde{\varphi}} (B \otimes M_1) \oplus (B \otimes M_2).$$

The things on the left hand side of the $\oplus$ are connected by $\varphi \otimes Id_{M_1}$ and RHS by $\varphi \otimes Id_{M_2}$. And $\tilde{\varphi} = (\varphi_1, \varphi_2)$ and $\tilde{\varphi}$ is injective if and only if φ_1, φ_2 are. □

(3) So R^n (free module of finite rank) is flat. The finiteness is not necessary, it's an exercise in the book.

(4) If M is a direct summand of a free module, i.e. there exists M s.t. $M \oplus N$ is free, then M is flat.

(5) If M_1, M_2 are flat, then $M_1 \otimes M_2$ is flat.

Proof. $\otimes M_1$ is exact as a functor, and $\otimes M_2$ is exact, so $\otimes(M_1 \otimes M_2) = (\otimes M_1) \otimes M_2$ is exact. So if we have:

$$0 \to A \to B$$

then

$$0 \to A \otimes M_2 \to B \otimes M_2$$

then

$$0 \to A \otimes (M_1 \otimes M_2) \to B \otimes M_1 \otimes M_2.$$

□

(6) If M is flat and I is an ideal in R, then $I \otimes M \to IM$ is an isomorphism. This is standard mapping which maps $a \otimes u \mapsto au$.

Proof. $0 \to I \to R$ is exact, so:

$$0 \to I \otimes M \to R \otimes M \cong M$$

is exact. And this is a mapping that maps $a \otimes u \mapsto a \otimes u \mapsto au$. So $I \otimes M \to M$ is injective. The inverse of this mapping is just IM. So actually this is an isomorphism of modules. □

(7) Assume R is an integral domain. Then if $Tor(M) \neq 0$, then M is not flat.

PROOF. $0 \to R \to Q$-the field of fractions. □

Thursday, February 1st

LEMMA 10.148. *If R is an integral domain and M is a flat R-module, then $Tor(M) = 0$.*

PROOF. Let Q be the field of fractions of R. Then:

$$0 \to R \to Q$$

is exact. So:

$$0 \to R \otimes M \to Q \otimes M$$

is exact. But $R \otimes M \cong M$ under the isomorphism $\varphi : 1 \otimes u \to u.$, where $ker\varphi = Tor(M)$. So if $u \neq 0$ is in $Tor(M)$, then $1 \otimes u \neq 0 \in R \otimes M$, but is zero in $Q \otimes M$, so $R \otimes M \to Q \otimes M$ is not injective, which is a contradiction since we said the above sequence is exact. □

LEMMA 10.149. *The converse of Lemma 10.148 is not true: if $Tor(M) = 0$, it may not be flat.*

We give a counterexample:

EXAMPLE 10.150. Let $R = F[x, y]$ and let $M = I = (x, y)$. Then M is torsion-free, but:

$$I \otimes M \to IM$$

is not an isomorphism. $x \otimes y - y \otimes x \mapsto 0$. It was one of the properties of flat modules that for any ideal in R, the above map must be an isomorphism, thus M is not flat.

Flatness is related to torsion.

LEMMA 10.151. *If R is an integral domain and Q is its field of quotients, then Q is a flat R-module.*

You can take $S^{-1}R$ for any multiplicatively closed set and this will be a flat R-module.

PROOF. The reason for this is that Q is a union of free R-modules, copies of R. It consists:

$$Q = \bigcup_{d \neq 0} d^{-1}R.$$

Let:

$$0 \to A \to B,$$

be exact. So $\varphi : A \to B$ is injective. Then $(R^*)^{-1}A \cong A \otimes Q \to_{\varphi \otimes Id} B \otimes Q \cong (R^*)^{-1}B$. So we have:

$$\varphi \otimes Id(\frac{u}{r} = \frac{\varphi(u)}{r}, u \in A, r \in R.$$

And $\frac{\varphi(u)}{r} = 0$ if and only if $a\varphi(u) = 0$ for some $a \neq 0$. Then $\varphi(au) = 0$, and since φ is injective, $au = 0$, so $\frac{u}{r} = 0$ is in $(R)^*)^{-1}A$. So $\varphi \otimes Id$ is injective. □

Refer to Remarks 10.126,10.127. For equivalent definitions of exactness. We discuss **projective and injective modules.**

Definition 10.152. Let R be commutative unital. Let M be an R-module.

Functors: $Hom_R(m, \cdot)$ and $Hom_R(\cdot, M)$.

For any R-module A, we have new modules $Hom_R(M, A)$ and $Hom_R(A, M)$.

If $\varphi : A \to B$ is a hom-sm, then we have a hom-sm $Hom(M, A) \to Hom(M, B)$. How is it defined? We have:

$$\begin{tikzcd}
A \arrow[rr, "\varphi"'] & & B \\
& M \arrow[ul, "f"] \arrow[ur, "\varphi\circ f"'] &
\end{tikzcd},$$

so $f \to \varphi \circ f$. And if we have one more module, we have:

$$\begin{tikzcd}
A \arrow[rr, "\varphi"'] & & B \arrow[r, "\psi"] & C \\
& M \arrow[ul, "f"] \arrow[ur, "\varphi\circ f"] \arrow[urr, "\psi\circ\varphi\circ f"'] & &
\end{tikzcd}.$$

So:

$$\begin{aligned}
Hom(M, A) \to Hom(M, B) \to Hom(M, C) \\
f \mapsto \varphi \circ f \mapsto \psi(\varphi \circ f) = (\psi \circ \varphi) \circ f.
\end{aligned} \tag{10.45}$$

Theorem 10.153. *If* $0 \to A \to B \to C \to 0$ *is exact, then:*

$$0 \to Hom(M, A) \overset{\tilde{\varphi}}{\to} Hom(M, B) \overset{\tilde{\psi}}{\to} Hom(M, C)$$

is exact, i.e. the functor $Hom(M, \cdot)$ *is left exact, but not exact, since exactness is not preserved on the right.*

Proof. We have:

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\varphi"] & B \arrow[r, "\psi"] & C \arrow[r] & 0 \\
& & M \arrow[ul, "f"] \arrow[u, "\varphi\circ f"] & &
\end{tikzcd}.$$

Assume that $\varphi \circ f = 0$. φ is injective by definition of exactness. And we have $\varphi(f(a)) = 0, \forall u \in M$, so $f(u) = 0, \forall u \in M$, since φ is injective, so $f = 0$. Thus we have proved that $\tilde{\varphi}$ is injective..

Now consider $f \in Hom(M, A) \mapsto \varphi \circ f \in Hom(M, B) \mapsto \psi \circ \varphi \circ f \in Hom(M, C)$. And $\psi \circ \varphi \circ f = 0$ since $\psi \circ \varphi = 0$ by exactness. So $Image(\tilde{\varphi}) \subseteq ker(\tilde{\psi})$. Now let $g \in ker(\tilde{\psi})$, that is, $\psi \circ g = 0$. Then:

$$\psi|_{g(M)} = 0.$$

So $g(M) \subseteq ker\psi$, so $g(M) \subseteq \varphi(A)$. Then we have $f : M \to A$ defined by $f(u) = \varphi^{-1}(g(u))$. So $g = \varphi \circ f = \varphi^{-1}(f)$. The inverse is well defined since φ is injective. □

We give counterexample to show that it is not exact on the right.

Example 10.154. Let $M = \mathbb{Z}_2$. Note $\mathbb{Z} \to \mathbb{Z}_2 \to 0$ is exact, we have a map $h : \mathbb{Z}_2 \to \mathbb{Z}_2$, the identity map, but there's no map g from $\mathbb{Z}_2$ to $\mathbb{Z}$ s.t. $h = \psi \circ g$, where ψ is the map from $\mathbb{Z} to \mathbb{Z}_2$.

Definition 10.155. M is **projective** if $Hom(M, \cdot)$ is exact: $\forall$ surjective $\psi : B \to C$ and $h : M \to C$ there exists $g : M \to B$ s.t. $h = \psi \circ g$:

$$\begin{tikzcd}
B \arrow[r] & C \arrow[r] & 0 \\
& M \arrow[ul, "g"] \arrow[u, "h"'] &
\end{tikzcd}.$$

So we know $Hom(M,B) \to Hom(M,C) \to 0$ is exact.

Remark 10.156. We list some properties of projective R-modules.

(1) If $M = M_1 \oplus M_2$, then M is projective if and only if M_1 and M_2 are. Proof is easy apparently.

(2) R, R^n are projective, and any free module is projective. This follows from the first property for free modules of finite rank.

Proof. Take $e_i \to c_i$. Find $b_i \in B$ s.t $\psi(b_i) = c_i$ for all i, and define $g(e_i) = b_i$. Done. □

(3) If M is a direct summand of a projective module, then it is projective. This is just a reformulation of the first property. And this is a criterion.

Theorem 10.157. *M is projective if and only if M is a direct summand of a free module: $\exists N$ s.t. $M \oplus N$ is free.*

Friday, February 2nd

Definition 10.158. Recall that M is **projective** if $\forall$ exact $B \overset{\varphi}{\to} C \to 0$ and $h : M \to C$ there exists $g : M \to B$ s.t. $h = \varphi \circ g$:

$$\begin{tikzcd}
B \arrow[r] & C \arrow[r] & 0 \\
& M \arrow[ul, "g"] \arrow[u, "h"'] &
\end{tikzcd}.$$

Definition 10.159. $Hom(M,\cdot)$ is an **exact functor:** if $0 \to A \to B \to C \to 0$ is exact, then $0 \to Hom(M,A) \to Hom(M,B) \to Hom(M,C) \to 0$ is exact. (Equivalent defn to above).

Remark 10.160. If M is projective and $B \overset{\varphi}{\to}$ is surjective then $\exists$ a section of φ : $s : M \to B$ s.t. $\varphi \circ s = Id_M$. Indeed, we have:

$$\begin{tikzcd}
B \arrow[r, "\varphi"] & M \arrow[r] & 0 \\
& M \arrow[ul, "s"] \arrow[u, "Id_M"'] &
\end{tikzcd}$$

so there exists s s.t. $\varphi \circ s = Id_M$. Recall that a section is a map from $M \to B$ s.t. it maps the image of an element from surjective hom-sm back to the same element.

Remark 10.161. If M is projective, then any short exact sequence $0 \to A \to B \to M \to 0$ splits s.t. $B \cong A \oplus M$.

In particular, since M is a quotient of a free module $F \to M \to 0$, if M is projective, then M is a direct summand of a free module, since we have a section from $M \to F$ that makes it a direct summand. Conversely, if M is a direct summand of a free module, it is projective: $F = M \oplus N$.

Definition 10.162. $0 \to A \overset{\varphi}{\to} B \overset{\psi}{\to} C \to 0$ splits "from the left" if $\exists \pi : B \to A$ s.t. $\pi \circ \varphi = Id_A$.

Proof. Let $C' = ker\pi$. We claim $\psi|_{C'}$ is isomorphic $C' \cong C$. Indeed ψ is surjective (because short exact), and if $b \in C'$ and $\psi(b) = 0$. Then $ker\psi = \varphi(A)$, by short exact, so if $b \in ker\psi$, then $b = \varphi(a)$ for some $a \in A$. Then $\pi(b) = a$ by definition of section. But if $b \in C'$, $\pi(b) = 0$, so $a = 0$, so $b = 0$. So we proved that $b \in ker\pi \Rightarrow b = 0$. So π is injective. Now we claim that $\varphi(A) + C' = B$. So since φ is a bijection, we know $\varphi(A) \cong A$.

Proof. Let $b \in B$, let $a = \pi(b)$. Then $b - \varphi(a) \in C'$, since $\pi(b - \varphi(a)) = a - a = 0$. So $b \in \varphi(A) + C'$. □

Now claim $C' \cap \varphi(A) = 0$. If $b \in C'$, then $\pi(b) = 0$, and if $b = \varphi(a)$, then $\pi(b) = \pi(\varphi(a)) = a = 0$, so $b = 0$. More work to be done here. □

We discuss injective modules. Which is related to $Hom(\cdot, M)$. Fix M. Let's consider this functor. You have module $A \Rightarrow$ module $Hom(A, M)$. If you have $A \overset{\varphi}{\to} B$, then you have $Hom(B, M) \overset{\tilde{\varphi}}{\to} Hom(A, M)$.

$$\begin{tikzcd}
A \arrow[rr, "\varphi"] \arrow[dr, "f"'] & & B \arrow[dl, "g"] \\
& M &
\end{tikzcd}$$

$f = g \circ \varphi$. We have $\tilde{\varphi} = g \circ \varphi$. This is a **contravariant functor** - it inverts arrows (morphisms). What we had before was called a **covariant** functors (”normal” ones).

Definition 10.163. **Covariant:** $A \Rightarrow F(A)$:

$$A \to B \Rightarrow F(A) \to F(B).$$

Definition 10.164. **Contravariant:** $A \Rightarrow F(A)$:

$$A \to B \Rightarrow F(B) \to F(A).$$

Note $F(B)$ is first here on the right side.

Theorem 10.165. *$Hom(\cdot, M)$ is left exact: if $0 \to A \to B \to C \to 0$ is exact, then $0 \to Hom(C, M) \to Hom(B, M) \to Hom(A, M)$ is exact.*

Proof. Left as an exercise to the reader, it is straightforward. (wtf) □

It may not be exact, tho. If $0 \to A \overset{\varphi}{\to} B$ is exact (φ is injective):

$$\begin{tikzcd}
0 \arrow[r] & A \arrow[r, "\varphi"] \arrow[d, "f"] & B \arrow[dl, "g"] \\
& M &
\end{tikzcd}$$

and we have $f : A \to M$ we need $g : B \to M$ s.t. $f = g \circ \varphi$. We give a counterexample:

Example 10.166. Consider:

$$\begin{tikzcd}
0 \arrow[r] & \mathbb{Z} \arrow[r, "\cdot 2"] \arrow[d, "Id"] & \mathbb{Z} \arrow[dl, "g"] \\
& \mathbb{Z} &
\end{tikzcd}$$

Note $2\mathbb{Z} \subseteq \mathbb{Z}$ but we have no such g. We have no map going from $2n \to n$.

Definition 10.167. M is **injective** if $\forall 0 \to A \overset{\varphi}{\to} B$ (exact) and $\forall f : A \to M$ there exists $g : B \to M$ s.t. $f = g \circ \varphi$.

Remark 10.168. *M is injective if and only if $Hom(\cdot, M)$ is an exact functor.*

Remark 10.169. (1) $M = M_1 \oplus M_2$ is injective if and only if both M_1 and M_2 are injective.
(2) R is not injective, generally speaking. ($\mathbb{Z}$ is not injective $\mathbb{Z}$-module)
(3) Q is an injective $\mathbb{Z}$-module.

Lemma 10.170. *Any module is a quotient of a free module, so, of a projective module.*

Theorem 10.171. *Any module is a submodule of an injective module.*

Monday, February 5th

Definition 10.172. A module M is **divisible** if $\forall$ nonzero divisor $a \in R$, $\forall u \in M$, there is a $v \in M$ s.t. $av = u$. That is, $M \to M$, where $v \mapsto av$ is surjective. So if R is an integral domain it is always true?

Remark 10.173. If M is injective, then M is divisible.

Remark 10.174. Let R be an integral domain, if M is divisible, and either M is torsion free or R is a PID, then M is injective.

Lemma 10.175 (**Baer's criterion**). *M is injective if $\forall$ ideal I of R, $\forall f : I \to M$ there exists $g : R \to M$ s.t $g|_I = f$. So this proves that the field of fractions is injective.*

Remark 10.176. M is projective if and only if: if M is a quotient module of some module B, $B \to M \to 0$, then we have $B \cong N \oplus M$. And in fact we have $0 \to N \to B \to M \to 0$.

Remark 10.177. Injective if and only if $0 \to M \to B$ implies $B \cong N \oplus M$. $M \subseteq B$. Then there exists $N \subseteq B$ s.t. the above is true. So M is injective if and only if if M is a submodule of B then M is a direct summand of B.

Remark 10.178. $\prod^{\infty} \mathbb{Q} \cong \bigoplus_{\alpha \in \Lambda} \mathbb{Q}$. This is only because on the left, that is a vector space. And thus it has a basis.

Lemma 10.179. *$M = \prod_{i=1}^{\infty} \mathbb{Z}$ is not free.*

Proof. Let $N = \bigoplus_{I=1}^{\infty} \mathbb{Z} \subseteq M$. Assume that M is free, let B be a basis. There exists $B' \subseteq B$ which is countable s.t. $N \subseteq N' = \mathbb{Z}B'$. For $u \in N$, let$B_u \subseteq B$ finite be s.t. $u \in RB_u$. Then:

$$B' = \cup_{u \in N} B_u.$$

which is countable. Let $\tilde{M} = M/N'$ a free module, $\cong R(B/B')$. Note B is uncountable. If K is a free $\mathbb{Z}$-module, then K is not divisible: $\forall v \in K$, $v = (0, ..., n_i, ..., n_j, 0, ...)$ v is only divisible by $\gcd(N_i, ..., n_j)$. So no element of k is divisible if it is nonzero. Recall that v is divisible if and only if $\forall k \neq 0$, there exists w s.t. $kw = v$. We claim $\tilde{M}$ has divisible elements, so we have contradiction. Take:

$$u = (\pm 1, \pm 2!, \pm 3!, \pm 4!, ...) \in M,$$

In $\tilde{M}$, $N = 0$, so take:

$$\overline{u} = (0, 0, ..., 0, k!, (k+1)!, ...) \in \tilde{M},$$

which is divisible by k for all k. We have uncountably many of such u, not all of them are in N', so there exists such u with $\overline{u} \neq 0$ in $\tilde{M}$. □

10.5 Exercises

1. *Suppose that:*

$$\begin{tikzcd}
A \arrow[r, "\psi"] \arrow[d, "\alpha"] & B \arrow[r, "\varphi"] \arrow[d, "\beta"] & C \arrow[d, "\gamma"] \\
A' \arrow[r, "\psi'"] & B' \arrow[r, "\varphi'"] & C'
\end{tikzcd}$$

is a commutative diagram of groups and that the rows are exact. Prove that:

(a) *If φ and α are surjective, and β is injective then γ is injective.*

Proof. Let $c \in ker\gamma$. Then we know there exists $b \in B$ s.t. $\varphi(b) = c$, since φ is surjective. Note that $\varphi'(\beta(b)) = \gamma(\varphi(b)) = \gamma(c) = 0$ since it is a commutative diagram. So we know $\beta(b) \in ker\varphi' = \psi'(A')$ since the bottom row is exact, so we know there exists $a' \in A'$ s.t. $\psi'(a') = \beta(b)$. And since α is surjective, we know there exists $a \in A$ s.t. $\alpha(a) = a'$. Then since $\psi'(\alpha(a)) = \beta(b)$, and the diagram is commutative, we know we must have $\beta(\psi(a)) = \psi'(\alpha(a)) = \beta(b)$. Now since β is injective, we know $b = \psi(a)$. But recall that $c = \varphi(b) = \varphi(\psi(a)) = 0$ since the top row is exact. Thus since $ker\gamma = 0 \in C$, we know that γ is injective. □

(b) *If $\psi', \alpha,$ and γ are injective, then β is injective.*

Proof. Let $\beta(b) = 0$ for some $b \in B$. Then we have $\varphi'(\beta(b)) = 0 = \gamma(\varphi(b))$ by commutativity. Since γ is injective, we know $\varphi(b) = 0$, so $b \in \psi(A)$. So there exists $a \in A$ s.t. $\psi(a) = b$. Now note that since we have commutativity we know $\beta(\psi(a)) = 0 = \psi'(\alpha(a))$. But since α and ψ' are both injective, we know $a = 0$, hence $\psi(a) = b = 0$, and β is injective. □

(c) *If φ, α and γ are surjective, then β is surjective.*

Proof. Let $b' \in B$. Then $\varphi'(b') \in C'$. So there exists $c \in C$ s.t. $\gamma(c) = \varphi'(b')$ since γ is surjective and there exists $b \in B$ s.t. $\varphi(b) = c$ since φ is surjective. So we know $\gamma(\varphi(b)) = \varphi'(\beta(b)) = \varphi'(b')$. So $\varphi'(\beta(b) - b') = 0$, so $\beta(b) - b' \in ker\varphi' = \psi'(A')$. So we know there exists $a' \in A'$ s.t. $\psi'(a') = \beta(b) - b'$. But since α is surjective and $a' \in A'$, we know there exists $a \in A$ s.t. $\psi'(\alpha(a)) = \psi'(a') = \beta(b) - b'$. So we must have that $\beta(\psi(a)) = \beta(b) - b'$ by commutativity. For $b - \psi(a)$ we then have $\beta(b - \psi(a)) = \beta(b) - \beta(b) + b' = b'$, which proves that β is surjective. □

(d) *If β is injective, α and φ are surjective, then γ is injective.*

Proof. Let $c \in C$ s.t. $\gamma(c) = 0$. Then since φ is surjective we have $b \in B$ s.t. $\varphi(b) = c$. Now take $\psi'(\beta(b)) = 0$ by commutativity since $\gamma(\varphi(b)) = 0$. Then we know $\beta(b) \in ker\varphi' = \psi'(A)$ so we have $a' \in A'$ s.t. $\psi'(a') = \beta(b)$. And since α is surjective we have $a \in A$ s.t. $\alpha(a) = a'$. So we have $\psi'(\alpha(a)) = \beta(b) = \beta(\psi(a))$ by commutativity. But since β

is injective we know $\psi(a) = b$ But then $b \in \varphi(A) = ker\varphi$ so $\varphi(b) = 0 = c$. So γ is injective. □

(e) *If β is surjective, γ and ψ' are injective, then α is surjective.*

PROOF. Let $a' \in A$. Then $\varphi'(\psi'(a)) = 0 \in C'$. Also since β is surjective we have $b \in B$ s.t. $\beta(b) = \psi'(a')$. Now $\gamma(\varphi(b)) = \varphi'(\beta(b))$ by commutativity, but $\varphi'(\beta(b)) = \varphi'(\psi'(a')) = 0$, so $\gamma(\varphi(b)) = 0$, and since γ is injective, $\varphi(b) = 0$. Thus by exactness, we have $a \in A$ s.t. $\psi(a) = b$. Now take $\psi'(\alpha(a)) = \beta(\psi(a)) = \psi'(a')$, and by injectivity of ψ', we know $\alpha(a) = a'$. So α is surjective. □

CHAPTER 11

Vector spaces

SECTION 11.1

Definitions and basic theory

Thursday, February 8th

Definition 11.1. Recall that a **linear transformation** is just an R-module homomorphism when the module is in fact a vector space.

Let R be a commutative unital ring. We know:

$$\begin{aligned} Hom_R(M_1 \oplus M_2, N) &\cong Hom_R(M_1, N) \oplus Hom_R(M_2, N) \\ Hom_R(M, N_1 \oplus N_2) &\cong Hom_R(M, N_1) \oplus Hom_R(M, N_2) \end{aligned} \tag{11.1}$$

So we have $\varphi \leftrightarrow (\varphi \circ \xi_1, \varphi \circ \xi_2)$, where $\xi : M_1 \to M_1 \oplus M_2$ and $\xi_2 : M_2 \to M_1 \oplus M_2$. Applying φ to these maps the stuff in $M_1 \oplus M_2$ to N. And we also have for the bottom one: $\varphi \leftrightarrow (\pi \circ \varphi, \pi \circ \varphi)$, where $\pi_1 : N_1 \oplus N_2 \to N_1$ and $\pi_2 : N_1 \oplus N_2 \to N_2$. In the second case, this homomorphism has coordinates, and we get them by just projecting the output of φ using π_1, π_2.

Lemma 11.2. *$Hom_R(R, R) \cong R$, proved in homework.*

Corollary 11.3. *$Hom(R^m, R^n) \cong R^{mn}$.*

$\forall M$, we have $Hom_R(R, M) \cong M$. $\varphi \mapsto \varphi(1) = u$. Then $\varphi(a) = au$ for all a. How do we construct this mapping? If we have $\varphi : R^m \to R^n$, then we have mn new homomorphisms. So let $\varphi : R^m \to R^n$. $\forall i, j$ let $\varphi_{i,j} : R \to R$ be given by $\varphi_{i,j} = \pi_i \circ \varphi \circ \xi_j \leftrightarrow a_{i,j} \in R$. What is this $a_{i,j}$? So $\varphi_{i,j}(b) = a_{i,j}b$. Any $\psi : R\ toR\ \psi \leftrightarrow \psi(1) = a$, and $\psi(b) = ab$. For a single homomorphism we have $m \times n$ numbers which define these φ:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}$$

which is called the matrix of φ. $\pi_i : R^n \to R$ and maps to $(a_1, .., a_n) \mapsto a_i$. And $\xi_j : R \to R^m$ maps $a \mapsto (0, ..., 0, a, 0, ..., 0)$, where the a is in the j-th column. The j-th column:

$$\begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} \varphi(v_j).$$

where:

$$v_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix}.$$

The i-th row $(a_{i1}, ..., a_{im})$ - the ith component of φ, the matrix of $\pi_i \circ \varphi$. We also have $\varphi + \psi \leftrightarrow A + B$ where they are the matrices of φ, ψ. And $\forall c \in R$, we have $c\varphi \leftrightarrow cA$.

Let $\varphi : R^m \to R^n$, $\psi : R^n \to R^k$. Then we have $\psi \circ phi : R^m \to R^k$. Let A be the matrix of φ and B be the matrix of ψ. Note A is $m \times n$ and B is $k \times n$. The matrix of $\psi \circ \varphi$ is called the product of B and A and is denoted by BA. Note BA is $k \times m$.

Let M be a free module.

Let M be a free module, $M \cong R^m$. Let $\{ u_1, ..., u_m \}$ be the basis in M corresponding to this isomorphism. Then $\forall u \in M$, $u = c_1 u_1 + \cdots + c_m u_m$:

$$u \leftrightarrow \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} \in R^m.$$

Let $\{ v_1, ..., v_m \}$ be another basis in M. If R is commutative, then any two bases have the same number of elements. Now:

$$u \leftrightarrow \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in R^m.$$

in this basis. So $u = b_1 v_1 + \cdots + b_m v_m$. So we do a change of basis or something like that. So we have an isomorphism from $M \to R^m$ by our first basis $\{ u_i \}$ and another by our second basis $\{ v_i \}$. Call the first one old and the second one new:

$$\begin{tikzcd}
 & R^m \arrow[dd] \\
M \arrow[ur, "\cong"] \arrow[dr, "\cong"'] & \\
 & R^m
\end{tikzcd}$$

The matrix of the isomorphism between the old and new is called the **transition matrix**.

SECTION 11.2

The matrix of a linear transformation

Friday, February 9th

So we study free modules of finite rank. We know if we have: $\varphi : R^m \to R^n \Rightarrow$ an $n \times m$ matrix:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1m} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nm} \end{pmatrix}.$$

Let $u = (c_1, ..., c_m)$, Note $\varphi(u)$ is part of a mapping:

$$1 \to u = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} \mapsto \varphi(u).$$

So the matrix of $1 \mapsto \varphi(u)$ is:

$$\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = A \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}.$$

which are the coordinates of $\varphi(u)$. We map $R \to R^m$ sending $1 \mapsto u$, and then $u \mapsto \varphi(u) \in R^n$. Remember that A is the matrix representation of the homomorphism φ.

So $Hom(R^m, R^n) \leftrightarrow Mat_{m \times n}(R) \cong R^{mn}$. The basis is given by: $\{ E_{ij} \}$ where:

$$E_{ij} = \begin{pmatrix} 0 & \cdots & 0 \\ \vdots & 1 & \vdots \\ 0 & \cdots & 0 \end{pmatrix}.$$

with a 1 as the i, j-th entry and zeroes elsewhere. So we have a basis φ_{ij} where $\varphi_{ij}(u_j) = v_i$ and $\varphi_{ij}(u_k) = 0 \ \forall k \neq j$. Where $u_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in R^m$, and $u_1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \in R_n$.

Now $M \cong R^m$, we have an "old" basis $\{ u_1, ..., u_m \}$ and a new basis $\{ v_1, ..., v_m \}$. Then we have:

$$\begin{tikzcd} & R^m \arrow[dd, "\cong"] \\ M \arrow[ur, "\cong"] \arrow[dr, "\cong"'] & \\ & R^m \end{tikzcd},$$

where the top is the ”old” and the bottom is the ”new”. This implies a transition matrix P, and we have:

$$u = c_1 u_1 + \cdots + c_m u_m = b_1 v_1 + \cdots + b_m v_m.$$

Where:

$$\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} = P \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} \Rightarrow \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = P^{-1} \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}.$$

So we have $\varphi : M \to M$ where $M \cong R^m$ and $N \cong R^n$, which gives us a matrix A of φ, corresponding to chosen bases. Change bases in M, and N, with transition matrices P and Q:

$$\begin{tikzcd}
& R^m \arrow[r, "A"] \arrow[dd, bend left, "{P,\cong}"] & R^n \arrow[d, dash, "\cong"] \arrow[dd, bend left, "{Q,\cong}"] \\
M \arrow[ur, dash, "\cong"] \arrow[dr, dash, "\cong"'] \arrow[rr, bend left, "\varphi"] & & N \arrow[d, dash, "\cong"] \\
& R^m \arrow[r, "A'"] & R^n
\end{tikzcd}.$$

In new coordinates, the matrix of φ is $QAP^{-1} = A'$.

Definition 11.4. If $\varphi : M \to M$, then after change of coordinates, with transition amtrix P, the ”new” matrix of φ is PAP^{-1}. It is called **similar matrix of** A (or **conjugate**).

Monday, February 12th

We review matrices:

$$\begin{tikzcd}
& R^n \arrow[dd] \\
V \arrow[ur, "\cong"] \arrow[dr, "\cong"'] & \\
& R^n
\end{tikzcd}$$

Recall that the vertical arrow is the map that we are representing as a matrix. We say the columns are the coordinates of elements of the old basis in the new basis. But the book’s definition has the columns as coordinates of the new basis in the old basis.

Observe:

$$\begin{tikzcd}
R^m \arrow[rrr, "A"] \arrow[ddd, "P"'] \arrow[dr, dash, "\cong"] & & & R^n \arrow[ddd, "Q"] \\
& M \arrow[r, "\varphi"] \arrow[dl, dash, "\cong"] & N \arrow[ur, dash, "\cong"] \arrow[dr, dash, "\cong"] & \\
& & & \\
R^m \arrow[rrr, "A'"] & & & R^n
\end{tikzcd}$$

where $A' = QAP^{-1} = PAP^{-1}$.

Now what about finite-dimensional vector spaces? These are free modules of finite rank over a field F.

Remark 11.5. All modules over a field are free.

What can we say about them? They are all free, so they are all projective, and injective.

Remark 11.6. All finite-dimensional vector spaces are both projective, and injective. Thus any short exact sequence splits. i.e. any subspace or quotient space is a direct summand.

Proof. Let W be a subspace of V. Find a basis B in W. Any vector space is a free module: has a basis. Then we want to construct a basis A in V, so that $B \subseteq A$. Put $U = F(A \setminus B)$. Then $V = W \oplus U$.

For finite dimensional vector spaces, $W = F\{ u_1, ..., u_k \}$. Let $B = \{ u_1, ..., u_k \}$ be a basis in W. We find $u_{k+1}, ..., u_n$ s.t. $\{ u_1, ..., u_n \}$ is a basis in V. Then $V = W \oplus U$, where $U = F\{ u_{k+1}, ..., u_n \}$. □

Remark 11.7. If $W \subseteq V$ then $\dim W \leqslant \dim V$. If $W \subset V$, then $\dim W < \dim V$.

Example 11.8. We give an example that it is not true for all modules, must be vector spaces. $2\mathbb{Z} \subset \mathbb{Z}$ with the same rank.

Remark 11.9. If $V = W \oplus U$, then $\dim V = \dim W + \dim U$.

Remark 11.10. If $\dim V = n$. If C is a linearly independent set in V, then $|C| \leqslant n$. If $|C| = n$, then C is a basis of V.

Remark 11.11. If $V = FC = Span(C)$, then $|C| \geqslant n$. If $|C| = n$, then C is a basis of V. Note here that C is not necessarily a linearly independent set in this remark.

Definition 11.12. Let V be m dimensional, and W be n dimensional. Given $\varphi : V \to W$, the **rank of a linear tranformation** $Rank\varphi = \dim \varphi(V)$.

Definition 11.13. Then **rank of matrix** A = rank of corresponding homomorphism = dimension of column space of A = subspace of F^n generated (spanned) by the columns of A.

Lemma 11.14. $Rank\varphi = \dim \varphi(V) = \dim V = \dim(ker\varphi)$.

Proof. $V = ker\varphi \oplus U$, $U \cong \varphi(V)$:

$$\begin{tikzcd} 0 \arrow[r] & ker\varphi \arrow[r] & V \arrow[r] & \varphi(V) \arrow[r] \arrow[l, bend left] & 0 \end{tikzcd}$$

□

Lemma 11.15. *The rank of the column space is equal to the rank of the row space.*

Remark 11.16. Rank is basis-invariant.

Remark 11.17. If two matrices are **similar**, then there is a linear transformation to get from one to the other.

Definition 11.18. $\varphi : V \to V$. u is an **eigenvector** of φ if $\varphi(u) = cu$ for some $c \in F$. c is called the **eigenvalue** of u, and of φ.

Remark 11.19. We discuss what it means for two modules to be ”equal” as opposed to ”isomorphic”. Consider $V = \mathbb{R}^3_{x,y,z}$. Let $W_1 = \mathbb{R}^2_{x,y}$, and let $W_2 = \mathbb{R}_x$. Then $V \cong W_1 \oplus W_2$. But they are not equal, since they live in different spaces. (isomorphic to the external direct sum), proving equality is proving ”equality” with respect to the internal direct sum object.

11.2 Exercises

1. *Let V be the collection of polynomials with coefficients in $\mathbb{Q}$ in the variable x of degree at most 5. Determine the transition matrix from the basis $1, x, x^2, ..., x^5$ (”old basis”) for V to the basis $1, 1 + x, 1 + x + x^2, ..., 1 + x + x^2 + x^3 + x^4 + x^5$ (”new”basis) for V.*

   Transition matrix (expressing the ”new” basis as linear combinations of ”old” basis:

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

2. *V is the same as above. $\varphi : V \to V$, $\varphi(p) = p'$ (differentiate). We find the matrices of φ with respect to the two bases from the above exercise.*

   Matrices of φ:

$$\begin{aligned} \varphi(1) &= 0 \\ \varphi(x) &= 1 \\ \varphi(x^2) &= 2x \\ &\vdots \end{aligned} \tag{11.2}$$

   So we have:

$$A = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

   Now for the next basis we have:

$$\begin{aligned} \varphi(1) &= 0 \\ \varphi(1 + x) &= 1 \\ \varphi(1 + x + x^2) &= 1 + 2x = -1 + 2(1 + x) \\ \varphi(1 + x + x^2 + x^3) &= 1 + 2x + 3x^2 = -1 - 1(1 + x) + 3(1 + x + x^2) \\ &\vdots \end{aligned} \tag{11.3}$$

So we have:

$$B = \begin{pmatrix} 0 & 1 & -1 & -1 & -1 & -1 \\ 0 & 0 & 2 & -1 & -1 & -1 \\ 0 & 0 & 0 & 3 & -1 & -1 \\ 0 & 0 & 0 & 0 & 4 & -1 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

8. PROOF. $\{ u_1, ..., u_n \}$ - eigenvalues of φ. Meaning that u_i are eigenvectors for all i. Then matrix of φ in this basis is:

$$A = \begin{pmatrix} c_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & c_n \end{pmatrix}.$$

□

*If the matrix A if φ is similar to a diagonal matrix, then φ has an **eigenbasis**.*

PROOF. $A = PA'P^{-1}$, A' is diagonal. Use P as a transition matrix - construct a new basis using P. Set:

$$v_i = Pu_i.$$

for all i. In this basis, the matrix of φ is A'. So $\varphi(v_i) = c_i v_i$ for all i. So we have:

$$A = \begin{bmatrix} c_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 & 0 \\ 0 & 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & 0 & 0 & \ddots & 0 \\ 0 & 0 & 0 & 0 & 0 & c_n \end{bmatrix}.$$

□

11. *Let φ be a linear transformation from the finite dimensional vector space V to itself such that $\varphi^2 = \varphi$.*
    (a) *Prove that $Image(\varphi) \cap ker\varphi = 0$.*

    PROOF. Note that $\varphi : V \to V$. Let $I = Image(\varphi)$ and let $K = ker\varphi$. Let $a \in K$. Then $\varphi(a) = 0$. Then let $a \in I$. Then there exists $b \in V$ s.t. $\varphi(b) = a$. But then note:

    $$\varphi^2(b) = \varphi(\varphi(b)) = \varphi(a) = 0 = \varphi(b) = a.$$

    So $a = 0$, hence $K \cap I = 0$. □

    (b) *Prove that $V = Image(\varphi) \oplus ker\varphi$.*

    PROOF. We prove that $V = Image\varphi + ker\varphi$. Since $Image\varphi \subseteq V$ and $ker\varphi \subseteq V$, we know that if $v \in Image\varphi$ and $w \in ker\varphi$, then $v, w \in V$, so $v + w \in V$. So $Image\varphi + ker\varphi \subseteq V$. We prove the other inclusion. Now let $a \in V$. If $a \in ker\varphi$ then we are done. So let $a \notin ker\varphi$. Then $\varphi(a) = b \neq 0 \in V$. Then we have:

$$\begin{aligned}\varphi(b-a) &= \varphi(b) - \varphi(a) = \varphi(b) - \varphi^2(a)\\ &= \varphi(b) - \varphi(\varphi(a)) = \varphi(b) - \varphi(b) = 0.\end{aligned} \tag{11.4}$$

So we know that $b - a \in ker\varphi$. So then $a - b \in ker\varphi$ since φ is a linear transformation. Now note:

$$\varphi(a) + (a-b) = b + a - b = a.$$

and since $\varphi(a) \in Image(\varphi)$ and $a - b \in ker\varphi$, we have shown $V \subseteq Image\varphi + ker\varphi$. Thus $V = Image\varphi + ker\varphi$, and since we showed they have zero intersection in the last part, we have proved $V = Image\varphi \oplus ker\varphi$. □

(c) *Prove that there is a basis of V s.t. the matrix of φ with respect to this basis is a diagonal matrix whose entries are all* 0 *or* 1.

Proof. Let $A = \{ v_1, ..., v_k \}$ be a basis for $\varphi(V)$. Then let $B = \{ v_{k+1}, ..., v_n \}$ be a basis for $ker\varphi$. We know this basis must have $n - k$ elements since $A \cup B$ must be a basis for V since we proved the direct sum in the last part. Now recall that the coefficient matrix of φ with respect to any basis C is given by (a_{ij}) where $\varphi(c_i) = \sum_j a_{ij} c_j$. So we find the matrix of φ with respect to $A \cup B$. Let $v_i \in A \cup B$. Suppose $v_i \in A$. Then $v_i = \varphi(w)$ for some $w \in V$. So we have $\varphi(v_i) = \varphi^2(w) = \varphi(w) = v_i$. So the i-th column of the i-th row must be a 1 and all other entries in that column are zero. And since $v_i \in A$, we know that $i \leqslant k$. Now let $v_i \in B$. Remember they are disjoint by part (a). Then $\varphi(v_i) = 0$, so the i-th column is all zeroes. Thus we have constructed the matrix of φ with respect to the basis $A \cup B$, and it is a diagonal matrix with only ones and zeroes along the diagonal. □

SECTION 11.3

Dual vector spaces

Friday, February 9th

Definition 11.20. If M is an R-module, then the **dual module** of M is $M^* = Hom_R(M, R) = \{ f : M \to R \}$. These elements are called ”linear forms” on M.

Sometimes this dual module is just zero.

Example 11.21. (1) $\mathbb{Z}_n^* = Hom(\mathbb{Z}_n, \mathbb{Z}) = 0$.

(2) $R^* = Hom_R(R, R) \cong R$. By $f \mapsto f(1)$.

(3) $(R^n)^* = Hom_R(R^n, R) \cong R^n$. ”the dual module of a free module of finite rank is free”. This is by $f \leftrightarrow (f(u_1), ..., f(u_n))$, where u_i are elements of the standard basis.

(4) If $M = \bigoplus_{i=1}^{\infty} R$. This is $Hom(M, R) = M^*$. Note since this is a free module, so any homomorphism is defined by its actions on the basis elements. For any choice of $f(u_i) \in R$, we have $f \in M^*$. So we can

choose any sequence of elements of R. We could do the same thing with uncountably many. So $M^* \cong \prod_{i=1}^{\infty} R = \{ (a_1, ...) : a_i \in R \}$. This is by $f \leftrightarrow (f(u_1), f(u_2), ...)$.

REMARK 11.22. If R is noncommutative and M is a left-module, then M^* is a right module. We define $f(a)(u) = f(au)$. We can check that this satisfies the structure of a right module.

$M^* \Rightarrow M^{**} = (M^*)^*$. And we have a natural homomorphism $M \to M^{**}$. An element $u \mapsto F_u$ where $F_u(f) = f(u)$. What the fuck is f. For $f \in M^*$. Note u acts on linear forms. We have a pairing: $u \in M$, $f \in M^*$, then $\langle f, u \rangle = f(u) \in R$. Elements of M^* are called **"covectors"**. And this mapping is linear with respect to u and linear with respect to f. This natural mapping is always defined, but it is not necessarily an isomorphism, since we could have that $M^* = 0$, so $M^{**} = 0$, so not injective. And we could also have that M^* and double star are much much larger than M, as in the case of infinite direct sums. Then we lose surjectivity.

We can also just write $u(f) = f(u)$.

REMARK 11.23. $M \to M^{**}$ is not necessarily an isomorphism.

LEMMA 11.24. *But if $M \cong R^n$, then $M \to M^{**}$ is a natural isomorphism.*

PROOF. This is because it maps basis vectors to basis vectors. Let $\{ u_1, ..., u_n \}$ be a basis of M.

DEFINITION 11.25. We have a **dual basis** in $M^* \cong R^n$. Note:

$$\{ f_1, ..., f_n \} : f_i(u_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases} = \delta_{ij}.$$

Note also that $R^n \to R$ matrices are $(a_1, ..., a_n)$, $f(u_i) = a_i$. Then $f_1, ..., f_n$ are the linear forms whose matrices are:

$$(1, 0, ..., 0), (0, 1, 0, ..., 0), ..., (0, ..., 0, 1).$$

In the book, the dual basis is $\{ u_1^*, ..., u_n^* \}$. Note f_1 is a mapping that maps u_1 to 1 and maps all other basis vectors to zero!! So the f_is are a basis of M^*. These are the dual basis.

I have no idea if we actually finished this proof or not. But it seems that we have moved on.

DEFINITION 11.26. Formally:

$$M^{**} = Hom(Hom(M, R), R).$$

Note if you have $Hom(R^m, R^n)$, then we have a natural homomorphism that maps i-th basis vector to j-th basis vector in the image and all other basis vectors to zero.

"Why even bother with this dual, never mind the dual of the dual?" -Ryan

"In functional analysis, it's popular. What is the dual of a measure? Something that acts on measures... There are reflexive spaces where you just return to the... $M^{**} = M$. Otherwise...(unitelligible). " - Leibman

Remark 11.27. Note that the dual basis of the dual basis is the original basis!

If $\{ f_1, ..., f_n \}$ is the dual basis of $\{ u_1, ..., u_n \}$, then images of $\{ u_1, ..., u_n \}$ in M^{**} (they are $F(u_i)$) is the dual basis of $\{ f_1, ..., f_n \}$:

$$\langle f_i, u_j \rangle = \delta_{ij}.$$

And from this, we have the conclusion of the proof from earlier. Since basis vectors go to basis vectors, we are done. We have $M \overset{F}{\to} M^{**}$ is an isomorphism. □

Now assume that we have two modules $\varphi : M \to N$ be a homomorphism, then we have the **dual homomorphism** $\varphi^* : N^* \to M^*$ defined by $\varphi^*(f) = f \circ \varphi$:

$$\begin{tikzcd} M \arrow[r, "\varphi"] \arrow[dr, "\varphi^*(f)=f\circ\varphi"'] & N \arrow[d, "f"] \\ & R \end{tikzcd}.$$

So $\star$-duality is a contravariant functor.

Tuesday, February 13th

Consider V, and $W^* \subseteq V^*$. Take a basis here:

$$\{ f_1, ..., f_k, f_{k+1}, ..., f_n \}.$$

Where up to k is a basis for W^*. So this gives us a basis $\{ u_1, ..., u_n \}$ in V, somehow...

Definition 11.28. We review the **dual of a basis**. If we have a basis $\{ u_1, ..., u_n \}$ in V, the **dual basis** in V^* is $\{ f_1, ..., f_n \}$ s.t. $\forall i$, $f_i(u_j) = \delta_{ij}$. Note any $f \in V^*$ is defined by $f(u_j)$ for $j = 1, ..., n$. Thus each f_i is uniquely defined by this definition. So matrices of $f_1, ..., f_n$ in basis $\{ u_1, ..., u_n \}$ are:

$$\begin{gathered} (1, 0, ..., 0) \\ \vdots \\ (0, ...,0, 1) \end{gathered} \tag{11.5}$$

Remark 11.29. $V^{**} \cong V$ by $u(f) = f(u)$ (this is how we are defining the action of u) and thus the dual basis of $\{ f_1, ..., f_n \}$ is $\{ u_1, ..., u_n \}$. This is because $u_j(f_i) = \delta_{ij}, \forall i, j$.

Consider $\varphi : V \to W$ a linear transformation. You have basis $\{ u_1, ..., u_m \}$ in V and $\{ v_1, ..., v_n \}$ in W. Let A be the matrix of φ in these bases. We have the dual homomorphism $\varphi^* : W^* \to V^*$ defined by $\varphi^*(g) = g \circ \varphi$:

$$\begin{tikzcd} V \arrow[r, "\varphi"] \arrow[dr, "\varphi^*(g)=g\circ\varphi"'] & W \arrow[d, "g"] \\ & F \end{tikzcd}.$$

And we have dual bases $\{ f_1, ..., f_m \}$ in V^* and $\{ g_1, ..., g_n \}$ in W^*. So what is A^*, the matrix of φ^* in these bases? Note $A = (a_{ij})$, where $a_{ij} = g_i(\varphi(u_j))$. So $g_i(u)$ is actually the i-th coordinate of u., since φ maps to W and g_i maps from W to F. Now $A^* = (b_{ji})$, then $b_{ij} = u_j(\varphi^*(g_i)) = u_j(g_i \circ \varphi) = (g_i \circ \varphi)(u_j) = a_{ij}$ (we use the definition of the action of u).

Remark 11.30. So $A^* = A^T$.

Lemma 11.31. *From this it immediately follows that* $(BA)^T = A^T B^T$.

Proof. Observe:

$$\begin{tikzcd} V \arrow[r, "A"] \arrow[rr, bend left, "BA"] & W \arrow[r, "B"] & U \end{tikzcd}.$$

$$\begin{tikzcd} V^* & W^* \arrow[l, "A^T"'] & U^* \arrow[l, "B^T"'] \arrow[ll, bend left, "(BA)^T = A^T B^T"] \end{tikzcd}$$

□

Remark 11.32. Row rank(A) = column rank(A^*) = $rank\varphi^* = rank\varphi$. So yes, row rank of A is column rank of A. But we didn't prove this last equality yet.

Remark 11.33. $*$ is a contravariant functor.

11.3 Exercises

1. *Let V be a finite dimensional vector space. Prove that the map $\varphi \mapsto \varphi^*$ in Theorem 20 from Dummit and Foote gives a ring isomorphism of End(V) with End(V^*).*

   Proof. This is an isomorphism of vector spaces, but not of rings. Note $\varphi + \psi \mapsto \varphi^* + \psi^*$ since:

$$\begin{aligned} (\varphi^* + \psi^*)(g) &= g \circ (\varphi + \psi) \\ &= g \circ \varphi + g \circ \psi \qquad (11.6) \\ &= \varphi^*(g) + \psi^*(g). \end{aligned}$$

   Isomorphism since $\varphi^* \mapsto \varphi^{**} = \varphi$ is the inverse. Why is it not an isomorphism of rings? Note $(\varphi\psi)^* = \psi^*\varphi^*$, not $\varphi^*\psi^*$. So the multiplication is not preserved.

   Note $\varphi^{**}(u) = u \circ \varphi^*$. So:

$$(u \circ \varphi^*)(g) = u(\varphi^*(g)) = u(g \circ \varphi) = g(\varphi(u)) = \varphi(u)(g).$$

   Thus $u \circ \varphi^* = \varphi(u)$. And thus $\varphi^{**}(u) = \varphi(u)$. □

2. *Let V be the collection of polynomials with coefficients in $\mathbb{Q}$ in the variable of x of degree at most 5 with $1, x, x^2, ..., x^5$ as basis. Prove that the following are elements of the dual space of V and express them as linear combinations of the dual basis:*

   (a) *$E : V \to \mathbb{Q}$ defined by $E(p(x)) = p(3)$, i.e. evaluation at $x = 3$.* Note $E \in V^*$ since it acts on polynomials, the action is linear, this is a homomorphism from V to $\mathbb{Q}$ and $V^* = Hom(V, \mathbb{Q})$. Coordinates of E is the dual basis of $\{ 1, x, x^2, ..., x^5 \}$. Dual basis of $\{ 1, x, x^2, ..., x^5 \}$ is $\{ f_0, f_1, ..., f_5 \}$ where $f_i(a_0 + a_1 x +$

$\cdots + a_5x^5) = a_1$. The coordinates of linear form in the dual basis are (to read the i-th coordinate, you apply the i-th element of the basis to this form) $u_i(E) = E(u_i)$. Recall that u_i is the i-th element in $\{ 1, x, x^2, ..., x^5 \} = \{ u_0, u_1, ..., u_5 \}$. So $E(\{ 1, x, x^2, ..., x^5 \}) = (1, 3, 3^2, ..., 3^5)$. And:

$$E = f_0 + 3f_1 + 9f_2 + \cdots + 243f_5.$$

And we can check that this is correct by applying the definition of f_i.

(b) *$\varphi : V \to \mathbb{Q}$ defined by $\varphi(p(x)) = \int_0^1 p(t)dt$. Where $\varphi \in V^*$.* Note $\varphi \leftrightarrow (1, \frac{1}{2}, \frac{1}{3}, ..., \frac{1}{6})$.

3. *Let S be any subset of V^* for some finite dimensional space V. Define $Ann(S) = \{ v \in V : f(v) = 0, \forall f \in S \}$. ($Ann(S)$ is called the annihilator of S in V.*

(a) *Prove that $Ann(S)$ is a subspace of V.*

Proof. Recall Definition 11.20. Let $v, w \in Ann(S)$. Then $f(v) = f(w) = 0$ $\forall f \in S \subseteq Hom(V, F)$, where V is a vector space over the field F. Then $f(v+w) = f(v)+f(w) = 0+0 = 0$ since f is a homomorphism. So $v + w \in Ann(S)$. Now let $r \in F$. Then $f(rv) = rf(v) = r \cdot 0 = 0$ since again f is a homomorphism. So $rv \in Ann(S)$. Thus $Ann(S)$ is a subspace by definition. □

(b) *Let W_1 and W_2 be subspaces of V^*. Prove that $Ann(W_1 + W_2) = Ann(W_1) \cap Ann(W_2)$ and $Ann(W_1 \cap W_2) = Ann(W_1) + Ann(W_2)$.*

Proof. Recall:

$$Ann(W_1 + W_2) = \{ v \in V : (f + g)(v) = 0, \forall f + g \in W_1 + W_2 \}.$$

So let $v \in Ann(W_1+W_2)$. Then with $g = 0$, we have $(f+g)(v) = f(v) = 0$, for all $f \in Ann(W_1)$. Now let $f = 0$, by same argument, $g(v) = 0$ for all $g \in W_2$, so $v \in Ann(W_1)$, so $v \in Ann(W_1) \cap Ann(W_2)$. Now let $v \in Ann(W_1) \cap Ann(W_2)$. Then $f(v) = 0$ and $g(v) = 0$ for all $f \in W_1, g \in W_2$. Then for arbitrary $f + g \in W_1 + W_2$. We have $(f + g)(v) = f(v) + g(v) = 0 + 0 = 0$. So $v \in Ann(W_1 + W_2$. So we have proved both inclusions: $Ann(W_1 + W_2) = Ann(W_1) \cap Ann(W_2)$.

Now we prove the second equality: recall:

$$Ann(W_1 \cap W_2) = \{ v \in V : f(v) = 0, \forall f \in W_1 \cap W_2 \}.$$

Let $u \in Ann(W_1)$ and $v \in Ann(W_2)$. Then for any $f \in W_1 \cap W_2$, $f(u) = 0$ and $f(v) = 0$, so $f(u + v) = f(u) + f(v) = 0 + 0 = 0$, since f is a homomorphism. So $u + v \in Ann(W_1 \cap W_2)$, so $Ann(W_1) + Ann(W_2) \subseteq Ann(W_1 \cap W_2)$.

Now we apply the result of part (c). We want to show $Ann(W_1 \cap W_2) \subseteq Ann(W_1) + Ann(W_2)$. By this result we know this is equivalent to showing:

$$Ann(Ann(W_1 \cap W_2)) = W_1 \cap W_2 \subseteq Ann(Ann(W_1) + Ann(W_2)).$$

So let B_V be a basis for V, and let B_{V^*} be a basis for V^*. Then let $\{ f_1, ..., k \}$ be a basis for W_1 and define $\{ f_l, ..., f_m \}$

as basis for W_2, without loss of generality, where $m, k \leqslant n = \dim V = \dim V^*$. Then by part (f) we know $Ann(W_1) = F(B_V \setminus \{ f_1, ..., f_k \})$ and $Ann(W_2) = F(B_V \setminus \{ f_l, ..., f_m \})$. So $Ann(W_1) + Ann(W_2) = A = F(B_V \setminus (\{ f_l, ..., f_m \} \cap \{ f_1, ..., f_k \}))$. And by part (f) again we know $Ann(A) = F(B_{V^*} \setminus (B_{V^*} \setminus F(\{ f_l, ..., f_m \} \cap \{ f_1, ..., f_k \}))) = W_1 \cap W_2$. So we have proved the other inclusion, and we are done. □

(c) *Let W_1 and W_2 be subspaces of V^*. Prove that $W_1 = W_2$ if and only if $Ann(W_1) = Ann(W_2)$.*

PROOF. Let $\{ g_1, ..., g_n \}$ be a basis of V^{**}. And we have the natural isomorphism which sends $g_i \mapsto v_i \in B_V$, the basis of V. So $V \cong V^{**}$. So V^* must have a basis $\{ f_1, ..., f_n \}$ and let $\{ f_1, ..., f_k \}$ be a basis for W_1. By part (f), we know

$$Ann(Ann(W_1)) = Ann(F \{ v_{k+1}, ..., v_n \}).$$

But again by part F and since $v_i(f_j) = f_j(v_i) = 0, \forall i \neq j$, we know $Ann(F \{ v_{k+1}, ..., v_n \}) = F \{ f_1, ..., f_k \}$. But this is exactly W_1, so $Ann(Ann(W)) = W$, and so since $Ann(W_1) = Ann(W_2)$, we know $Ann(Ann(W_1)) = Ann(Ann(W_2)) \Rightarrow W_1 = W_2$. □

(d) *Prove that the annihilator of S is the same as the annihilator of the subspace of V^* spanned by S.*

PROOF. Note $Ann(S) = \{ v \in V : f(v) = 0, \forall f \in S \}$. And note that

$$Ann(FS) = \{ v \in F : f(v) = 0, \forall f \in FS \}.$$

Now V^* is finite dimensional since we know how to generate the dual basis, and the dimension of V^* is the same as the dimension of V. So S has a finite maximal linearly independent set $B_S = \{ f_1, ..., f_k \}$. Let $v \in Ann(FS)$. Then since $1 \in F$, we know $S \subseteq FS$, so $f(v) = 0, \forall f \in S$, so $Ann(FS) \subseteq Ann(S)$.
Now let $v \in Ann(S)$. Then since $B_S \subseteq S$, we know $v \in Ann(B_S)$. Then

$$FS \subseteq FB_S = F \{ f_1, ..., f_k \} = \{ r_1 f_1 + \cdots + r_k f_k : r_i \in F, f_i \in B_S \}.$$

Then $f_i(v) = 0$ for all i since they are in B_S, and $r_i \cdot 0 = 0$, so $v \in Ann(FB_S) \subseteq Ann(FS)$ since $FS \subseteq FB_S$. Hence $Ann(S) \subseteq Ann(FS)$, and so they are equal. □

(e) *Assume V is finite dimensional with basis $v_1, ..., v_n$. Prove that if $S = \{ v_1^*, ..., v_k^* \}$ for some $k \neq n$, then $Ann(S)$ is the subspace spanned by $\{ v_{k+1}, ..., v_n \}$.*

PROOF. Note that S is some subset of the dual basis, so let's change notation to be consistent with lecture. Let $S = \{ v_1^*, ..., v_k^* \} = \{ f_1, ..., f_k \}$. Note since $k \neq n$, $\{ v_{k+1}, ..., v_n \}$ is nonempty. Let $v = r_1 v_1 + \cdots + r_n v_n \in Ann(S)$. Then $f_i(v) = 0$,

$1 \leqslant i \leqslant k$. We want to show $v \in F\{v_{k+1}, ..., v_n\}$. Suppose $v \notin F\{v_{k+1}, ..., v_n\}$, then since $v \in V$, we know there exists $i \leqslant k$ s.t. the coefficient of v_i in $r_1 v_1 + \cdots + r_n v_n$ is nonzero. But if this is true, we would have $f_i(r_1 v_1 + \cdots + r_n v_n) \neq 0$ since each of the basis vectors is linearly independent. This is a contradiction, since $f_i(v) = 0$ for all $v \in Ann(S)$. So we must have that $v \in F\{v_{k+1}, ..., v_n\}$. And hence $Ann(S) \subseteq F\{v_{k+1}, ..., v_n\}$. Now let $v \in F\{v_{k+1}, ..., v_n\}$. Then $v = r_{k+1}v_{k+1} + \cdots + r_n v_n$. Chose arbitrary $f_i \in S$. Then $i \leqslant k$, so $f(r_j v_j) = r_j f(v_j) = f_j \cdot 0 = 0$ for all $j > k$, by definition of f_i, since $i \neq j$. Thus $f_j(v) = 0$ since $j > k$ for all $v_j \in \{v_{k+1}, ..., v_n\}$. So since this holds for all $f_j \in S$, $v \in Ann(S)$, so $F\{v_{k+1}, ..., v_n\} \subseteq Ann(S)$. □

(f) *Assume V is finite dimensional. Prove that if W^* is any subspace of V^*, then* $\dim Ann(W^*) = \dim V - \dim W^*$.

Proof. We have a basis of $\{v_1, ..., v_n\}$ of V. Let $\{f_1, ..., f_n\}$ be the corresponding basis of the finite dimensional V^* (since V is finite dimensional), and without loss of generality, let $\{f_1, ..., f_k\}$ be a basis for W^*, which we know has a basis since it is a subspace. By the previous exercise, $Ann(W^*) = F\{v_{k+1}, ..., v_n\}$. So it has dimension $n-k$, and since $\dim V = n$ and $\dim W^* = k$, we are done. □

Note that parts (a),(d),(b)(i,ii,iii) are all easy.
Below is only true for finite dimensional vector spaces. Recommend: (e)⇒(f)⇒ $Ann(Ann(W)) = W$ ⇒ (c) ⇒ (b)(iv).

SECTION 11.4

Determinants

Remark 11.34. $\det AB = \det A \det B$.

Remark 11.35. $\det A = 0$ if and only if columns of A are linearly dependent.

Remark 11.36. $\det(PAP^{-1}) = \det A$.

Definition 11.37.

$$\det A = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \sum_{\sigma \in S_n} sign\sigma \prod_{i=1}^{n} a_{i,\sigma(i)}.$$

Remark 11.38. Observe:

$$\varphi : R^n \xrightarrow{\qquad\qquad} R^n$$

$$\begin{tikzcd}
\Lambda^n\varphi : \Lambda^n(R^n) \arrow[r] \arrow[d, "\cong"] & \Lambda^n(R^n) \arrow[d, "\cong"] \\
R \arrow[r, "\cdot c = \det"] & R
\end{tikzcd} \cdot$$

Remark 11.39. $\det A = \det A^T$.

Remark 11.40. $\det A$ is an alternating n-linear function of columns of A such that $\det I = 1$. This determines the determinant uniquely since $\Lambda\mathcal{T}^n(R^n) \cong R$. This space is one dimensional, so up to scaling, it is unique, and we normalize, so its completely unique. Note n-linear functions here are tensors, and for it to be alternating it must be in $\Lambda\mathcal{T}^n(R^n)$. And we have a canonical isomorphism:

$$\Lambda\mathcal{T}^n(R^n) \cong \Lambda^n(R^n).$$

11.4 Exercises

2. *Let F be a field and let $A_1, A_2, ..., A_n$ be (column) vectors in F^n. Form the matrix A whose i-th column is A_i. Prove that these vectors form a basis of F^n if and only if* $\det A \neq 0$.

   Proof. Recall Corollary 27 from Dummit and Foote, which states that if R is an integral domain, then $\det A \neq 0$ for $A \in M_n(R)$ if and only if the columns of A are R-linearly independent as elements of the free R-module of rank n.

   Now since F^n is a vector space, we know that if we have a set of n linearly independent vectors, it must be a basis. So let the column vectors A_i form a basis of F^n. Then they must be linearly independent. So by the corollary, we know $\det A \neq 0$. Now let $\det A \neq 0$. Then by the corollary, we know A_i are linearly independent over F as elements of F^n, since F is field, thus an integral domain. So then since F^n is a vector space of $\dim F^n = n$, they must form a basis, since if they didn't, we would need some other linearly independent vector to generate the missing elements of F^n, which would contradict the fact that $\dim F^n = n$. □

3. *Let R be any commutative ring with* 1*, let V be an R-module and let $x_1, ..., x_n \in V$. Assume that for some $A \in M_{n\times n}(R)$,*

$$A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = 0.$$

   Prove that $(\det A)x_i = 0$*, for all* $i \in \{ 1, 2, ..., n \}$.

   Proof. Recall Theorem 30 from Dummit and Foote, which states that if B is the transpose of the matrix of cofactors of A, then $AB = BA = (\det A)I$. So note:

$$0 = B0 = BA\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} = (\det A)I\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix} = (\det A)\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}.$$

And this is zero if and only if $(\det A)x_i = 0$ for all i. □

SECTION 11.5

Tensor algebras, symmetric and exterior algebras

Thursday, February 15th

Definition 11.41. Let M be an R-module. Let $\mathcal{T}^k(M) = M \otimes \cdots \otimes M$ where we have k copies of M. For the infinite case we have:

$$\mathcal{T}(M) = \bigoplus_{k=0}^{\infty} \mathcal{T}^k(M)$$

and this $\mathcal{T}^k(M)$ is called the **tensor algebra of** M.

We define $\mathcal{T}^0(M) = R$, and $\mathcal{T}^1 = M$. And we have:

$$(u_1 \otimes \cdots \otimes u_k) \cdot (v_1 \otimes \cdots \otimes v_l) = u_1 \otimes \cdots \otimes u_k \otimes v_1 \otimes \cdots \otimes v_l.$$

Definition 11.42. Now consider $\mathcal{S}(M) = \mathcal{T}(M)/C(M)$, where $C(M)$ is the ideal generated by tensors $u \otimes v - v \otimes u$ for $u, v \in M$. This object $\mathcal{S}(M)$ is called the **symmetric tensor algebra of** M**.** And $\mathcal{S}(M) = \oplus_{k=0}^{\infty}\mathcal{S}^k(M)$.

Note elements of the form $w \otimes u \otimes v - w \otimes v \otimes u \in C(M)$.

So we have:

Definition 11.43. **Graded ring:**

$$R = R_0 \oplus R_1 \oplus R_2 \oplus \cdots.$$

where these are submodules, not subrings. Note for $u \in R_i, v \in R_j$, then $uv \in R_{i+j}$.

Note:

$$u_1 \otimes u_2 \otimes u_3 = u_2 \otimes u_1 \otimes u_3 = u_2 \otimes u_3 \otimes u_1 = u_3 \otimes u_2 \otimes u_1 \in \mathcal{S}(M).$$

Definition 11.44. An ideal is a **graded ideal** if $I \oplus (I \cap R_k)$.

So $C(M) = \oplus(\mathcal{T}^k/C^k)$.

Remark 11.45. We don't really need any of this stuff above, and possibly some of the stuff below as well.

Definition 11.46. An **exterior algebra** is:

$$\Lambda(M) = \mathcal{T}(M)/\mathcal{A}(M),$$

where $\mathcal{A}(M)$ is the ideal in $\mathcal{T}(M)$ generated by tensors of the form $u \otimes u$ for $u \in M$. And:

$$\Lambda(M) = \bigoplus_{k=0}^{\infty} \Lambda^k(M).$$

And $\otimes$ in $\Lambda(M)$ is denoted by $\wedge$. So we have $u \wedge u = 0$ in $\Lambda(M)$ for all $u \in M$.

Now we have $\forall u, v \in M$, $u \wedge v = -v \wedge u$. And:

$$0 = (u+v) \wedge (u+v) = u \wedge v + \cdots.$$

$$u \wedge (v \wedge w) = -v \wedge u \wedge w = (v \wedge w) \wedge u.$$

And:

$$\alpha \wedge \beta = (-1)^{kl} \beta \wedge \alpha$$

if α has order k and β has order l.

If M is free of rank n, then $\forall k$ $\mathcal{T}^k(M)$ is free of rank n^k. If $\{ u_1, ..., u_n \}$ is a basis in M, then:

$$\{ u_{i_1} \otimes \cdots \otimes u_{i_k} : i_1, ..., i_k \in \{ 1, ..., n \} \}$$

is a basis in $\mathcal{T}^k(M)$.

Remark 11.47. Basis in $\mathcal{S}^k(M)$ is:

$$\{ u_{i_1} \otimes u_{i_2} \otimes \cdots \otimes u_{i_k} : i_1 \leqslant i_2 \leqslant ... \leqslant i_k \}.$$

And the rank is $\begin{pmatrix} n+k-1 \\ k-1 \end{pmatrix}$ (choose).

Remark 11.48. The basis in $\Lambda^k(M)$ is:

$$\{ u_{i_1} \wedge u_{i_2} \wedge \cdots \wedge u_{i_k} : i_1 < i_2 < ... < i_k \}.$$

Example 11.49. If $k = 3, n = 4$, then:

$$u_1 \wedge u_2 \wedge u_3, u_1 \wedge u_2 \wedge u_4, u_1 \wedge u_3 \wedge u_4, u_2 \wedge u_3 \wedge u_4$$

are the elements of $\Lambda^k(M)$. And the rank is $\binom{n}{k}$. If $k > n$ then $\Lambda^k(M) = 0$.

Example 11.50. If $k = n$, $rank = 1$ so $\Lambda^n(M) \cong R$. The only basis tensor in $\Lambda^n(M)$ is $u_1 \wedge u_2 \wedge ... \wedge u_n$. Now $\forall v_1, ..., v_n \in M$, we have:

$$v_1 \wedge v_2 \wedge \cdots \wedge v_n = cu_1 \wedge u_2 \wedge \cdots \wedge u_n, c \in R.$$

Example 11.51. Let $n = 2$, and $\{ u_1, u_2 \}$. $v_1 = au_1 + bu_2$. And $v_2 = cu_1 + du_2$. Then:

$$\begin{aligned} v_1 \wedge v_2 &= (au_1 + bu_2) \wedge (cu_1 + du_2) \\ &= acu_1 \wedge u_1 + adu_1 \wedge u_2 + bcu_2 \wedge u_1 + bdu_2 \wedge u_2 \qquad (11.7) \\ &= (ad - bc) u_1 \wedge u_2. \end{aligned}$$

Lemma 11.52. *Let M be a vector space. If* $\dim(M) = n$ *then* $v_1, ..., v_n \in M$ *are linearly independent if and only if* $v_1 \wedge ... \wedge v_n \neq 0$.

Proof. Assume M is a vector space. If $v_1, ..., v_n$ are linearly independent, they form a basis for M, so $v_1 \wedge ... \wedge v_n$ is a basis (so nonzero) element of $\Lambda^n(M)$. If they are linearly independent, they are contained in a subspace W of dimension $n-1$. So $v_1 \wedge ... \wedge v_n \in \Lambda^n(W) = 0$, since $n > \dim(W)$. □

Definition 11.53. $\mathcal{S}^k(M^*)$ - **Symmetric k-linear forms on M.**

$\Lambda^k(M^*)$ - **alternating k-linear forms on M.**

So we have $\Phi : M^k \to R$ by $(v_1, ..., v_k) \mapsto a$ such that:

$$\Phi(v_{\sigma(1)}, ..., v_{\sigma k}) = \Phi(v_1, ..., v_k) \tag{11.8}$$

for symmetric, and the following for alternating:

$$\Phi(v_{\sigma(1)}, ..., v_{\sigma k}) = sign(\sigma)\Phi(v_1, ..., v_k) \tag{11.9}$$

with $\sigma \in S_k$ a symmetric group. And we have something.

Friday, February 16th

Definition 11.54. A tensor $w \in \mathcal{T}^k(M)$ is **symmetric** if it is invariant under permutation of components:

$$\sigma(w) = w, \forall \sigma \in S_k.$$

Where S_k acts on $\mathcal{T}^k(M)$ by:

$$u_1 \otimes ... \otimes u_k \mapsto u_{\sigma(1)} \otimes ... \otimes u_{\sigma(k)}$$

for $\sigma \in S_k$.

Example 11.55. In $\mathcal{T}^2$, $u \otimes v + v \otimes u$ is symmetric.

In $\mathcal{T}^3$, $u \otimes v \otimes v + v \otimes u \otimes v + v \otimes v \otimes u$ is symmetric.

Remark 11.56. Symmetric tensors form a submodule of $\mathcal{T}^k(M)$. But not a subalgebra.

Definition 11.57. There is a natural mapping called **symmetrization:** $\forall w \in \mathcal{T}^k(M)$, let:

$$\mathrm{Sym}(w) = \frac{1}{k!} \sum_{\sigma \in S_k} \sigma(w).$$

Assume that $k!$ is a unit in R, it is the product of all its divisors.

Remark 11.58. Sym : $\mathcal{T}^k(M) \to \{ \text{Symmetric tensors in } T^k(M) \} = \mathcal{ST}^k(M)$.

Lemma 11.59. *Sym defines an isomorphism $\mathcal{S}^k(M) \to \mathcal{ST}^k(M)$. Where $\mathcal{S}^k(M) = \mathcal{T}^k(M)/\mathcal{C}^k(M)$.*

Proof. Sym is surjective since $\forall w \in \mathcal{ST}^k(M)$, we have:

$$\mathrm{Sym}(w) = w.$$

Observe:

$$\mathcal{C}^k(M) = \left\{ \sum w - 1 \otimes (u \otimes v - v \otimes u) \otimes w_2 : u, v \in M; w_1, w_2 \in \mathcal{T}(M) \right\}.$$

And $\mathrm{Sym}(\mathcal{C}^k(M)) = 0$, so $\mathcal{C}^k(M) \subseteq \ker(\mathrm{Sym})$. □

Remark 11.60. $\forall w \in \mathcal{T}^k$:

$$w - \mathrm{Sym}(w) = \frac{1}{k!} \sum_{\sigma \in S_k} (w - \sigma(w)). \tag{11.10}$$

Where $w - \sigma(w) \in \mathcal{C}^k(M)$. And if $w \in \ker(\mathrm{Sym})$, then $w = \frac{1}{k!} \sum (w - \sigma(w)) \in \mathcal{C}^k(M)$. So $\ker(\mathrm{Sym}) = \mathcal{C}^k(M)$, so $\mathcal{S}^k(M) \cong \mathcal{ST}^k(M)$.

Now why $w - \sigma(w)$? If $\sigma = \tau_1 \tau_2 \cdots \tau_r$, transpositions, then

$$w - \sigma(w) = (w - \tau_r(w)) + (\tau_r(w) - \tau_{r-1}\tau_r(w)) + \cdots + (\ - \sigma(w)).$$

Now we can do the same for alternating tensors and exterior algebra. Let $\sigma(w) = (\text{sign}\sigma)w, \forall \sigma \in S_k$.

Remark 11.61. They form a submodule of $\mathcal{T}^k(M)$.

Remark 11.62. We have a homomorphism $\text{Alt} : \mathcal{T}^k(M) \to \Lambda\mathcal{T}^k$ by

$$\text{Alt}(w) = \frac{1}{k!} \sum_{\sigma \in S_k} \text{sign}(\sigma)\sigma(w).$$

And we call this **alternation**, or **sqew-symmetrization**. It induces an isomorphism $\Lambda\mathcal{T}^k(M) \to \Lambda^k(M)$.

Observe:

$$\begin{aligned} u_1 \wedge u_2 &\leftrightarrow \frac{1}{2}\left(u_1 \otimes u_2 - u_2 \otimes u_1\right) \\ u_1 \wedge u_2 \wedge u_3 &\leftrightarrow \frac{1}{6}\Big(u_1 \otimes u_2 \otimes u_3 - u_2 \otimes u_1 \otimes u_3 - u_1 \otimes u_3 \otimes u_2 \\ &\qquad - u_3 \otimes u_2 \otimes u_2 + u_2 \otimes u_3 \otimes u_1 + u_3 \otimes u_1 \otimes u_2\Big). \end{aligned} \tag{11.11}$$

Remark 11.63. I have no idea what's going on here, where are these normalization constants coming from?

Let M be free of rank n. Then M^* is also free of rank n. So $\Lambda^n(M^*) \cong R$, so $\Lambda\mathcal{T}^n(M^*) \cong R$.

Remark 11.64. $\forall k, \Lambda\tau^k(M^*)$ is the **space of alternating k-linear mappings $M^k \to R$.** Note this space is NOT $\Lambda^k(M^*)$.

Now define $\Phi : M^k \to R$ s.t. $\forall\sigma$:

$$\Phi(u_{\sigma(1)}, ..., u_{\sigma(k)}) = \text{sign}\Phi(u_1, ..., u_k).$$

And k-linear.

Assuming that $k!$ is an unit in R:

$$\Lambda\mathcal{T}^k(M) \cong \Lambda^k(M).$$

And $\text{Alt} : \mathcal{T}^k \to \Lambda\mathcal{T}^k$.

Now let $\varphi : M \to M$ be a homomorphism. Then $\forall k$,

$$\varphi^{\otimes k} : \mathcal{T}^k(M) \to \mathcal{T}^k(M), \Lambda^k(M) \to \Lambda^k(M).$$

Remark 11.65. For $k = n$:

$$\begin{tikzcd} \Lambda^k(M) \arrow[rr] \arrow[dr, dash, "\cong"] & & \Lambda^k(M) \arrow[dl, dash, "\cong"'] \\ & R & \end{tikzcd} .$$

Where $w \mapsto cw$. Now c is a constant in R (according to Eric...)

Definition 11.66. Take a basis $\{ u_1, ..., u_n \}$ in M:

$$u_1 \wedge ... \wedge u_n \mapsto \varphi(u_1) \wedge ... \wedge \varphi(u_n) = cu_1 \wedge ... \wedge u_n.$$

Define $c = \det \varphi$.

Corollary 11.67. *The determinant doesn't depend on the choice of basis.*

Corollary 11.68. $\det(\varphi\psi) = \det \varphi \cdot \det \psi$.

Remark 11.69. The determinant is an alternating n-linear mapping of

$$(\varphi(u_1), ..., \varphi(u_n)),$$

that is, columns of the matrix of φ. So there exists only one such mapping since $\Lambda^n(M^*) \cong R$.

Note $\Phi : (|||) \to R$ s.t. $\Phi(Id) = 1 \Rightarrow \Phi = \det$.

Monday, February 19th

Let M be free, $B = \{ u_1, ..., u_n \}$ be a basis in M. Then:

$$B^{\otimes k} = \{ u_{i_1} \otimes \cdots \otimes u_{i_k} : i_1, ..., i_k \in \{ 1, ..., n \} \}$$

is a basis in $\mathcal{T}^k(M)$.

Lemma 11.70. *Basis in $\mathcal{S}^k(M)$ is:*

$$\mathcal{S}^k(B) = \{ u_{i_1} \otimes u_{i_2} \otimes \cdots \otimes u_{i_k} : i_1 \leqslant i_2 \leqslant ... \leqslant i_k \}.$$

Proof. Note that $\mathcal{S}^k(M)$ has a universal property: if $\Phi : M^k \to N$ is a k-linear symmetric mapping. Recall that symmetric means that $\Phi(u_{\sigma(1)}, ..., u_{\sigma(k)}) = \Phi(u_1, ..., u_k) \forall \sigma \in S_k$. Then there is a hom-sm $\beta : \mathcal{S}^k(M) \to N$ such that:

$$\beta(v_1 \otimes \cdots \otimes v_k) = \Phi(v_1, ..., v_k), \forall v_i \in M.$$

Now the word symmetric guarantees this homomorphism. Now we have $\alpha : \mathcal{T}^k(M) \to N$ s.t. $\alpha|_{\mathcal{C}^k(M)} = 0$. Recall that

$$\mathcal{C}^k(M) = (v_1 \otimes \cdots \otimes v_i \otimes v_{i+1} \otimes \cdots \otimes v_k - v_1 \otimes \cdots \otimes v_{i+1} \otimes v_i \otimes \cdots \otimes v_k).$$

So $\mathcal{S}^k(B)$ generates $\mathcal{S}^k(M)$. Note for $n = 2$, $k = 2$, we have $\{u_1 \otimes u_1, u_1 \otimes u_2, u_2 \otimes u_1, u_2 \otimes u_2\} = B^{\otimes 2}$, and we have:

$$\mathcal{S}^2(B) = \{ u_1 \otimes u_1, u_1 \otimes u_2, u_2 \otimes u_2 \}.$$

So now we have to prove linear independence of this set. So we want to find a 2-linear mapping which maps... something to something. First we have to choose some element which we want to use. Let $i_1 \leqslant i_2 \leqslant ... \leqslant i_k$. Define a k-linear mapping from $M^k \to R$ by sending:

$$\Phi(u_{j_1}, ..., u_{j_k}) = \begin{cases} 1 & \text{if } (j_1, ..., j_k) = \sigma(i_1, ..., i_k) \text{ for some } \sigma \in S_k \\ 0 & \text{otherwise} \end{cases}.$$

So we have basis vectors $u_{j_1} \otimes \cdots \otimes u_{j_k}$ and we want to send them to 1 only if they are some permutation of our i's. Then Φ induces a homomorphism $\beta : \mathcal{S}^k(M) \to R$ such that:

$$\beta(u_{i_1} \otimes \cdots \otimes u_{i_k}) = 1.$$

And $\beta(u_{j_1}\otimes\cdots\otimes u_{j_k}) = 0\ \forall j_1 \leqslant \ldots \leqslant j_k$ if $\neq (i_1,\ldots,i_k)$. So we only define Φ on basis vectors and expand it to the whole space by k-linearity. Now we have a hom-sm which maps our chosen vector to 1 and all other vectors to zero. This implies that $u_{i_1}\otimes\cdots\otimes u_{i_k}$ is not a linear combination of other vectors from $\mathcal{S}^k(B)$. If such a hom-sm exists it means that our chosen element is a nonzero linear combination. So what we proved is that any element from $\mathcal{S}^k(B)$ is not a linear combination of the others, so we proved this set is linearly independent and they are a basis consequently. This relies on the universal property (the induction of the hom-sm). □

So the for the homework, make Φ alternating, and add $sign\sigma$ in front of the 1 in the definition of piecewise Φ.

Lemma 11.71. *The basis in $\Lambda^k(M)$ is:*

$$\{\, u_{i_1}\wedge u_{i_2}\wedge\cdots\wedge u_{i_k} : i_1 < i_2 < \ldots < i_k \,\}.$$

Now we discuss **alternatization** of tensors. Consider

$$Alt_2 : w \mapsto \frac{1}{k!}\sum_{\sigma\in S_k} sign(\sigma)\sigma(w),$$

where $w\in\mathcal{T}^k(M)$. And we added the coefficient $\frac{1}{k!}$. But it does not appear in the book.

So we know $Alt|_{\mathcal{A}^k(M)} = 0$, so it factorizes to $\Lambda^k(M)\to\Lambda\mathcal{T}^k(M)$, which is the space of alternating tensors. And it turns out to be an isomorphism. Surjective because it sends alternating tensors into themselves, and the kernel is $\mathcal{A}^k(M)$. Recall that:

$$\mathcal{A}^k(M) = \mathcal{T}^k(M)\cap\{\text{ ideal in } \mathcal{T}(M) \text{ generated by } u\otimes u\,\}.$$

And:

$$\Lambda^k(M) = \mathcal{T}^k(M)/\mathcal{A}^k(M).$$

And $\sigma(w) = sigm(\sigma)w, \forall\sigma$. So the elements of $\Lambda\mathcal{T}^k(M)$ are just tensors with the property that if you change the order, it changes the sign. So $\mathcal{A}^k()$ is submodule of $\mathcal{T}^k(M)$ consisting of tensors having at least two equal components. So it is generated by elements of the form:

$$u_1\otimes\cdots\otimes u_{i-1}\otimes u_i\otimes u_i\otimes u_{i+2}\otimes\cdots\otimes u_k.$$

Example 11.72. For $k=2$: $u_1\wedge u_2 \mapsto \frac{1}{2}(u_1\otimes u_2 - u_2\otimes u_1)$.

So if $w\mapsto\sum sign(\sigma)\sigma(w)$, then for $k=2$, $u_1\otimes u_2 - u_2\otimes u_1 \mapsto 2(u_1\otimes u_2 - u_2\otimes u_1)$.

Remark 11.73. Still quite lost here.

We can consider this mapping without $\frac{1}{k!}$, but it will not be an isomorphism. Let's try and think of any example. For symmetric tensors, if we don't have $sign(\sigma)$ and we just take it over $\mathbb{Z}$, then the image will be $2\mathbb{Z}$. Does this make sense? But for alternating tensors? I don't know.

Definition 11.74. **Natural** means functorial. Whatever that means. So you can define it for each object, so that we have morphisms between objects and commutative diagrams and other nice stuff probably. Consider $V \cong V^*$ and $V \cong V^{**}$ but this first one is not natural. This is because we might need a different definition of the map for different specific vector space. But this second one is natural. We define it as $u \to \Phi_u$ by $\Phi_u(\varphi) = \varphi(u)$. It works for all objects in the category... I think.

Theorem 11.75. *Everything is unnatural.*

11.5 Exercises

5. *Prove that if M is a free R-module of rank n, then $\Lambda^k(M)$ is a free R-module of rank $\binom{n}{k}$ for $k = 0, 1, 2, \ldots$* Let $B = \{ u_1, \ldots, u_n \}$ be a basis in M. Equivalently, we claim:

   Lemma 11.76. *The basis in $\Lambda^k(M)$ is:*

   $$\Lambda^k(B) = \{ u_{i_1} \wedge u_{i_2} \wedge \cdots \wedge u_{i_k} : i_1 < i_2 < \ldots < i_k \}.$$

   Note this set has $\binom{n}{k}$ elements since we are choosing k from n, since $|B| = n$.

   Proof. Note that $\Lambda^k(M)$ has a universal property: If $\Phi : M^k \to N$ is a k-linear alternating mapping, then there is a hom-sm $\beta : \Lambda^k(M) \to N$ such that:

   $$\beta(v_1 \wedge \cdots \wedge v_k) = \Phi(v_1, \ldots, v_k), \forall v_i \in M.$$

   And since this basis is obtained from the natural projection of B, we know $\Lambda^k(B)$ generates $\Lambda^k(M)$.

   Let $i_1 < i_2 < \ldots < i_k$. Define a k-linear mapping from $M^k \to R$ by sending:

   $$\Phi(u_{j_1}, \ldots, u_{j_k}) = \begin{cases} sign(\sigma) & \text{if } (j_1, \ldots, j_k) = \sigma(i_1, \ldots, i_k) \text{ for some } \sigma \in S_k \\ 0 & \text{otherwise} \end{cases}$$

   So we have basis vectors $u_{j_1} \wedge \cdots \wedge u_{j_k}$ and we want to send them to $sign(\sigma)$ only if they are some permutation of our i's. Then Φ induces a homomorphism $\beta : \Lambda^k(M) \to R$ such that:

   $$\beta(v_1 \wedge \cdots \wedge v_k) = \Phi(v_1, \ldots, v_k), \forall v_i \in M.$$

   And $\beta(u_{j_1} \wedge \cdots \wedge u_{j_k}) = 0$, $\forall j_1 < \ldots < j_k$ if $\neq (i_1, \ldots, i_k)$. So we only define Φ on basis vectors and expand it to the whole space by k-linearity. Now we have a hom-sm which maps our chosen vector to $sign(\sigma)$ and all other vectors to zero. So suppose

   $$s = r_1 v_1 + \cdots + r(u_{i_1} \wedge u_{i_2} \wedge \cdots \wedge u_{i_k}) + \cdots + r_{\binom{n}{k}} v_{\binom{n}{k}} = 0.$$

   Then $\beta(s) = \beta(r(u_{i_1} \wedge u_{i_2} \wedge \cdots \wedge u_{i_k})) = 0$, since β maps all other vectors to zero. So we must have $r \neq 0$ since our basis vector is nonzero. This implies that $u_{i_1} \wedge \cdots \wedge u_{i_k}$ is not a linear combination of other vectors from $\Lambda^k(B)$. So what we proved is that any element from $\Lambda^k(B)$ is not a linear combination of the others, so we proved this set is linearly independent and thus a basis. □

12. (a) *Prove that if $f(x,y)$ is an alternating bilinear map on V (i.e. $f(x,x) = 0$ for all $x \in V$) then $f(x,y) = -f(x,y)$ for all $x, y \in V$.*

    Proof. Observe:

$$\begin{aligned} 0 &= f(x+y, x+y) = f(x+y, x) + f(x+y, y) \\ &= f(x,x) + f(y,x) + f(x,y) + f(y,y) = f(y,x) + f(x,y). \end{aligned} \tag{11.12}$$

So adding $-f(x,y)$ to both sides we have:

$$-f(x,y) = f(y,x).$$

□

(b) *Suppose that $-1 \neq 1$ in F. Prove that $f(x,y)$ is an alternating bilinear map on V (i.e. $f(x,x) = 0$ for all $x \in V$) if and only if $f(x,y) = -f(y,x)$ for all $x, y \in V$.*

Proof. The forward direction follows from part (a). For the second direction, assume $f(x,y) = -f(y,x)$. So we have $f(x,x) = -f(x,x)$. Since $-1 \neq 1$, we know $1 + 1 = r \neq 0 \in F$. So we have:

$$rf(x,x) = 0.$$

Suppose $f(x,x) \neq 0 \in W$, where W is the vector space which f maps to. Then since $r \neq 0$ we have a contradiction since $\{ f(x,x) \}$ is linearly independent. So $f(x,x) = 0$ for all $x \in V$. □

(c) *Suppose that $-1 = 1$ in F. Prove that every alternating bilinear form $f(x,y)$ on V is symmetric (i.e. $f(x,y) = f(y,x)$ for all $x, y \in V$). Prove that there is a symmetric bilinear map on V that is not alternating. [One approach: show that $\mathcal{C}^2(V) \subseteq \mathcal{A}^2(V)$ and $\mathcal{C}^2(V) \neq \mathcal{A}^2(V)$ by counting dimensions. Alternatively, construct an explicit symmetric map that is not alternating.]*

Proof. For the first part, we use part (a), so we know:

$$f(x,y) = -f(y,x) = f(y,x),$$

since $1 = -1$. For the second part, consider $f : V \to F$ given by $f(x,y) = x \cdot y$, the dot product. It is symmetric since addition in F is abelian, but it is not alternating. Note $f(x,x) = 0$ if and only if $x = 0$. □

Remark 11.77. Chapter 12 will be the primary part of the midterm, since it is practical, like linear algebra. We hope to finish it by next week. It might be only this stuff.

CHAPTER 12

Modules over principal ideal domains

SECTION 12.1

The basic theory

Tuesday, February 20th

Let V, W be finite-dimensional vector spaces over a field F. Let $\varphi : V \to W$ be a linear mapping (homomorphism). Then if we choose a basis in V, W, we get a matrix for φ. So can we choose a basis so that the matrix has an especially simple form?

We choose a basis $\{ u_1, ..., u_n \}$ in V s.t. $\{ u_1, ..., u_k \}$ is a basis in $ker\varphi$. Consider the vectors $\{ \varphi(u_{k+1}), ..., \varphi(u_n) \} \subseteq W$. They are linearly independent, and generate $\varphi(V)$. How do we know they are linearly independent? It's just because that the first k were picked to be in the kernel. We have:

$$\begin{aligned} a_{k+1}\varphi(u_{k+1}) + \cdots + a_n\varphi(u_n) &= 0 \\ \varphi(a_{k+1}u_{k+1} + \cdots + a_n u_n) &= 0 \\ a_{k+1}u_{k+1} + \cdots + a_n u_n &\in ker\varphi \\ a_{k+1}u_{k+1} + \cdots + a_n u_n &= b_1 u_1 + \cdots + b_k u_k, \end{aligned} \tag{12.1}$$

for some b_i. So $a_{k+1} = \cdots = a_n = 0$. So $\{ \varphi(u_{k+1}), ..., \varphi(u_n) \}$ is a basis in $\varphi(V)$. Call them $v_1, ..., v_{n-k}$ and add $v_{n-k+1}, ..., v_m$ to get a basis in W. In the base $\{ u_1, ..., u_n \}$,$\{ v_1, ..., v_m \}$, the matrix of φ is:

$$\left(\begin{array}{ccc|ccc} 0 & \cdots & 0 & 1 & 0 & 0 \\ \vdots & & \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & 0 & 0 & 1 \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right).$$

And if instead we choose $\{ u_{k+1}, ..., u_n, u_1, ..., u_k \}$, the matrix is:

$$\left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots & & \vdots \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right).$$

In both, we have m rows and n columns, and the nonzero square has $n - k$ columns, so that is the rank of φ.

Remark 12.1. If $\varphi : V \to W$ and $U \subseteq V$ is a subspace s.t. $\varphi(U) \subseteq L$. Choose a basis $\{ u_1, ..., u_n \}$ in V s.t. $\{ u_1, ..., u_k \}$ is a basis of U, and $\{ v_1, ..., v_m \}$ in W s.t. $\{ v_1, .., v_l \}$ is a basis in L. Then the matrix of φ has the form:

$$\left(\begin{array}{c|c} \mathrm{B} & \mathrm{C} \\ \hline 0 & \mathrm{D} \end{array}\right),$$

where $\varphi|_U : U \to L$ has matrix B. Also, φ induces a mapping $V/U \to W/L$. The matrix of this mapping is D, in bases $\{ \overline{u_{k+1}}, ..., \overline{u_n} \}$, and $\{ \overline{v_{l+1}}, ..., \overline{v_m} \}$. So B maps $U \to L$, and D maps $V/U \to W/L$. The bottom left hand corner is zero because we take a vector $\varphi(u_1)$ and write it as a column vector in W, but actually it is in L, so after a certain point, all the rest of the entries of this vector are zero.

Consider $\varphi : V \to V$. We ask the question of what is the simplest form of the matrix of φ? Or given an $n \times n$ matrix A, what is the "simplest" form of of PAP^{-1} for all invertible P?

Remark 12.2. For $\varphi : V \to W$, we consider all matrices PAQ^{-1} for invertible P, Q. And $\forall A$, there exists P, Q such that:

$$PAQ^{-1} = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots & & \vdots \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right).$$

Remark 12.3. if there is a basis $\{ u_1, ..., u_n \}$ in V s.t. $\varphi(u_i) = \lambda_i u_i$ for all i (**eigenbasis**), then in this basis, the matrix of φ is diagonal:

$$\begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}.$$

Example 12.4. For the matrix:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

there is no eigenbasis in $Mat_{2\times 2}(\mathbb{R})$.

Consider V as an $F[x]$-module, with $xu = \varphi(u)$. Then:

$$(a_n x^n + \cdots + a_1 x + a_0)u = a_n \varphi^n(u) + \cdots + a_1 \varphi(u) + a_0 u.$$

And $F[x]$ is a PID.

Chapter 12 is about fundamental theorem of finitely generated modules over PIDs.

Consider $\mathbb{Z}, F[x]$.

THEOREM 12.5. *Any finitely generated abelian group is isomorphic to a group of the form:*

$$\mathbb{Z}^k \times \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_l}.$$

DEFINITION 12.6. We introduce the rank of a module, not necessarily free. The **rank** of a module M over an ID is the maximal number of linearly independent elements in M.

LEMMA 12.7. *If $\{ u_1, ..., u_n \}$ is a maximal linearly independent set, it don't have to generate M, but $M/R\{ u_1, ..., u_n \}$ is a torsion module, because otherwise we could add one more element to this set and it would still be linearly independent.*

PROOF. Suppose $M/R\{ u_1, ..., u_n \}$ is not torsion. Then $\exists u' \in M/R\{ u_1, ..., u_n \}$ s.t. $ru' \neq 0 \in M/R\{ u_1, ..., u_n \}$ (i.e. $ru' \notin R\{ u_1, ..., u_n \}$) for all $r \in R$. But this is exactly the definition of linear independence, so then $\{ u_1, ..., u_n, u' \}$ is independent, which is a contradiction since we said $\{ u_1, ..., u_n \}$ was maximal. □

REMARK 12.8. Rank of a module is uniquely defined because we can multiply by the field of fractions. And it is equal to $\dim_F F \otimes M$. Why is it equal? Because

$$0 \to R\{ u_1, ..., u_n \} \to M \to M/R\{ u_1, ..., u_n \} \to 0,$$

where $R\{ u_1, ..., u_n \}$ is free. So F is flat, so:

$$0 \to F^n \to F \otimes M \to 0.$$

Wednesday, February 21st

DEFINITION 12.9. If R is an integral domain, M an R-module, the **rank** of M is the cardinality of a maximal linearly independent subset of M. It is uniquely defined since we can extend it to the dimension of the vector space over field of fractions of R.

REMARK 12.10. If $M = M_1 \oplus M_2$, then $\text{rank}M = \text{rank}M_1 + \text{rank}M_2$. The following is also true and a homework problem:

$$0 \to M_1 \to M \to M_2 \to 0.$$

REMARK 12.11. If N is a submodule of M, then $\text{rank}N \leqslant \text{rank}M$.

EXAMPLE 12.12. $2\mathbb{Z} \subset \mathbb{Z}$, but they both have rank 1. So you can have a proper subset with the same rank as M, but not if they are vector spaces.

THEOREM 12.13. *Let R be a PID, and M be a free R-module of rank n. Let N be a submodule of M. Then N is free, of rank $k \leqslant n$, and there is a basis $\{ u_1, ..., u_n \}$ in M and elements $a_1, ..., a_n \in R$ s.t. $\{ a_1u_1, ..., a_ku_k \}$ is a basis in N, and $a_1|a_2|\cdots|a_k$.*

Proof. By induction on n. If $n = 1$, $M \cong R$, and N is an ideal in R. Since R is a PID, we know $N = (a_1) = a_1 R$. Then $\{ 1 \}$ is a basis in M, a_1 is a basis in N.

Now let $M \cong R^n$. Let $N \neq 0$. So M has rank n. $\forall f \in M^*$, $f(N)$ is an ideal in R, so $f(N) = (a_f)$ for some $a_f \in R$. Note $f(N)$ is a linear form. Note:

$$f(x_1, ..., x_n) = c_1 x_1 + \cdots + c_n x_n.$$

For at least one f, this ideal is nonzero. So there exists f s.t. $f(N) \neq 0$, so $a_f \neq 0$ for this f. Now, R is a PID, so it's a Noetherian ring. So any collection of ideals in R has a maximal element. Choose $h \in M^*$ s.t. (a_h) is a maximal element (not maximal ideal) of the set $\{ (a_f) : f \in M^* \}$. Call it $a_1 = a_h$. So a_1 is the minimal element you can get this way. There exists $v_1 \in N$ s.t. $a_1 = h(v_1)$. So a_1 is the "minimal" element which can be obtained this way. It is maximal in the sense that it is not contained in any larger ideal. In fact this ideal is absolutely maximal, and a_1 is absolutely minimal element, but we do not need this now.

We now claim $\forall f \in M^*$, $a_1 | f(v_1)$ (in fact, $a_1 | f(v)$ $\forall v \in N$). If we apply linear forms to v_1, then a_1 divides all the results.

Proof. Put $I = \{ f(v_1) : f \in M^* \} = v_1(M^*)$, which is an ideal of R. So $I = (b)$ for some $b \in R$, since R is a PID. Now $b | a_1 = h(v_1) \in I$. Also, there is $g \in M^*$ s.t. $g(v_1) = b$. So, $b \in g(N) = (a_g)$, and since $b | a_1$, $(a_1) = (a_h) \subseteq (a_g)$. But h was chosen such that it was the maximal of all ideals of this sort, so $(a_h) = (a_g)$, so $(a_1) = (b) = I$. So $a_1 | f(v_1)$ for all f. □

In particular, if M is identified with R^n, so if some basis in M is chosen, then a_1 divides all coordinates of v_1. Remember that a **coordinate** is a linear form on $M = R^n$. It is a linear mapping from $M \to R$. So, there is $u_1 \in M$ s.t. $v_1 = a_1 u_1$. And then, $h(u_1) = 1$, since $h(v_1) = a_1$. So what do we do, we consider all forms, linear forms on all elements of N, we find vector that gives us minimal result, then we claim that it is multiple of some vector with coefficient a_1. We find a minimal element and prove that all other elements are its multiples.

Let $K = kerh$. We claim $M = Ru_1 \oplus K$, $n = Ra_1 u_1 \oplus (K \cap N)$. Note $Ra_1 = Rv_1$.

Proof. $\forall u \in M$, $u = h(u)u_1 + (u - h(u)u_1)$. Note $h(u)u_1 \in Ru_1$, and $u - h(u)u_1 \in K$, because when we apply h to this on the right, we get zero, since $h(u_1) = 1$. Also, $K \cap Ru_1 = 0$.

Also $\forall v \in N$, $v = h(v)u_1 + (v - h(v)u_1)$. Where the summand on the left is in $Ra_1 u_1$, since $a_1 | h(v)$, so $h(v)u_1 = \frac{h(v)}{a_1} v_1$. And the summand on the right is in $K \cap N$. So $K \cap Ra_1 u_1 = 0$. So this is direct sum. □

Now, fix M, use induction on rank$N$. Note $N = Rv_1 \oplus (K \cap N)$, and rank$(K \cap N) = k - 1$, so by induction, $K \cap N$ is free.

Now $M = Ru_1 + (M \cap K)$. And rank$(M \cap K) = n - 1$. And $M \cap K$ is free as a submodule of M, and this follows from above.

Now use induction on n, then $\exists$ a basis $\{ u_2, ..., u_n \}$ in $M \cap K$ such that $\{ a_2 u_2, ..., a_k u_k \}$ is a basis in $N \cap K$, $a_2 | \cdots | a_n$. Just prove $a_1 | a_2$ and we are done.

So define $f \in M^*$ by $f(\sum x_i u_i) = x_1 + x_2$. Note $u_1, \ldots, u_n$ is a basis in M. Then $f(a_1 u_1) = a_1$, where $a_1 u_1 = v_1 \in N$. So $(a_1) \subseteq f(N) = (a_f)$, so $(a_1) = f(N)$ by maximality. Also, $f(a_2 u_2) = a_2$, so $a_2 \in f(N) = (a_1)$, so $a_1 | a_2$. □

Thursday, February 22nd

We given an alternate, constructive proof of Theorem 12.13, which works for Euclidean domains.

Proof. Let R be an ED, $M = R^n$, and let N be a submodule of M. Then N is finitely generated (**bonus problem to prove this**). A module is called **Noetherian** if any submodule is finitely generated, or equivalently, if any increasing sequence of submodules stabilizes. So R^n is Noetherian if R is Noetherian. Let N be generated by $\{ v_1, \ldots, v_l \}$. Then $N = \varphi(R^l)$, where $\varphi(e_i) = v_i$. Any finitely generated module is the image, factor module, of a free module. In coordinates in R^n, the matrix of φ in the natural basis of R^n and the basis e_i is $A = (v_1 | v_2 | \ldots | v_l)$, where the v's are the columns. Now we want to find a new bases $\{ w_1, \ldots, w_l \} \in R^l$ and $\{ u_1, \ldots, u_n \} \in R^n$ s.t. the matrix of φ has simplest form. We use elementary row operations.

Definition 12.14. **Elementary operations:** if $\{ u_1, \ldots, u_n \}$ is a basis in $R^n = M$, then switching the order $u_i \leftrightarrow u_j$ corresponds to switching the i-th and j-th rows.

Example 12.15. Define:

$$A = \left(\begin{array}{c|c|c|c} a_{11} & a_{12} & \cdots & a_{1l} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nl} \end{array} \right).$$

So:

$$v = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

in $\{ u_1, \ldots, u_n \}$. Where $v = a_1 u_1 + \cdots + a_n u_n$. And the submodule is the block with 1s on the diagonal:

$$A = \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots & & \vdots \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array} \right).$$

And it is $k \times k$.

Replacing u_i by $u_i + cu_j$ corresponds to adding the j-th row multiplied by c to the i-th row.

Usually an elementary operation is multiplying a row by a constant, but we cannot do this here because not all constants are units. You can multiply rows by units, but not non-units.

Definition 12.16. Similar operations in R^l correspond to **elementary column operations**.

(1) So assume there is an element in the first columm which is not divisible by a_{11}. If a_{i1} is not divisible by a_{11}, find c s.t. $a_{i1} = ca11+r$ with $N(r) < N(a_{i1})$ (Euclidean norm). Then the first entry of $row_i - crow_1$ is r. Switch row$_1$ and row$_i$ and get a smaller $(1,1)$ entry. Applying this to the first row, and column several times, we get all a_{1k}, a_{k1} to be divisible by a_{11}. This process cannot be infinite since $N(a) \in \mathbb{N}$.

(2) Subtract multiples of row$_1$ from other rows, and the multiples of col$_1$ from other columns, and get:

$$A = \left(\begin{array}{c|ccc} b_{11} & 0 & \cdots & 0 \\ \cline{2-4} b_{21} & b_{22} & b_{23} & \cdots \\ \vdots & * & * & * \\ 0 & * & \cdots & * \end{array}\right)$$

(3) Assume there exists i, j s.t. b_{ij} not divisible by b_{11}. Add col$_j$ to col$_1$ to get b_{ij} in the first column. Go to step 1. After repeating steps 1,2,3 many times, all b_{ij} will be divisible by b_{11}.

(4) Pass to the submatrix:

$$A = \left(\begin{array}{c|cc} b_{11} & 0 & \cdots \\ \hline 0 & B' & \end{array}\right)$$

and continue.

In the end we get:

$$\left(\begin{array}{ccc|ccc} c_1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots & & \vdots \\ 0 & 0 & c_k & 0 & \cdots & 0 \\ \hline 0 & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & 0 \end{array}\right),$$

with $c_1|c_2|...|c_k$. We have a new basis $\{ u_1, ..., u_n \}$ in $M = R^n$ and $\{ c_1u_1, ..., c_ku_k \}$ is a basis in $N = \varphi(R^l)$. □

EXAMPLE 12.17. Let N be the submodule $\mathbb{Z}^3$ generated by:

$$\begin{pmatrix} 2 & 5 \\ 3 & 11 \\ 7 & 13 \end{pmatrix}.$$

So we have:

$$\begin{pmatrix} 2 & 5 \\ 3 & 11 \\ 7 & 13 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 6 \\ 2 & 5 \\ 7 & 13 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 6 \\ 0 & -7 \\ 0 & -29 \end{pmatrix} \mapsto \left(\begin{array}{c|c} 1 & 0 \\ \cline{2-2} 0 & -7 \\ 0 & -29 \end{array}\right)$$

$$\mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \\ 0 & -7 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \\ 0 & 0 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

EXAMPLE 12.18. Let $N = \mathbb{Z} \cdot \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\}$. And then:

$$A = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & -1 \\ 0 & 2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}.$$

Remark 12.19. Theorem 12.13 is not true if R is not a PID:

Example 12.20. Consider $M = R = F[x,y]$, and $N = (x,y)$. Note $\text{rank}(M) = 1$, and $M/(x)$ is a torsion module. It is not free since x, y do not have a common divisor. Note N is not free because it cannot be generated by one element. Note x, y cannot be linearly independent, since $yx - yx = 0$. Where we treat x, y as elements of N, and coefficients from R.

Example 12.21. Take $R = \mathbb{Z}$, and $M = \mathbb{Z}^n$. So M is a lattice in M in n-dimensional space. Assume we have a sublattice: we want to find a new basis such that the transformed sublattice aligns with the lattice formed by the points in $\mathbb{Z}^n$. Let u_2 be the green vector, u_1 be the blue vector. Note $N = \mathbb{Z}\{(1,1),(-1,1)\}$. Where $(1,1) = u_1$, and $(-1,1) = 2u_2 - u_1$. Note $\{u_1, u_2\}$ is a basis in M, and $\{u_1, 2u_2\}$ is a basis in N.

Thursday, February 22nd

Theorem 12.22. *If R is a PID and M is a finitely generated R-module, then M is a product of cyclic modules,*

$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m).$$

where $a_1, \dots, a_m \in R$ (non-units), and $a_1 | a_2 | \dots | a_m$, $r, a_1, \dots, a_m$ are uniquely defined, $r = rankM$, $a_1, \dots, a_m$ are called the invariant factors of M.

Proof. M is generated by n elements. Then we have:

$$0 \to N \to R^n \to M \to 0.$$

$M = R^n/N$, where N is a submodule of R^n.

Now find a basis $\{u_1, \dots, u_n\}$ in R^n s.t. $\{a_1u_1, \dots, a_ku_k\}$ is a basis on N, and $a_1 | a_2 | \dots | a_l$. Now $M = R^n/N$. So $u_1, \dots, u_k, \dots, u_n$. □

Friday, February 23rd

We do some exercises.

Lemma 12.23. *$rank(M)$ well-defined.*

Proof. Let $N = R\{x_1, \dots, x_n\}$. Then N is a maximal free submodule of M. Then we have:

$$0 \to N \to M \to M/N \to 0.$$

Where M/N is torsion. Let F be the field of fractions of R. Then F is a flat module. So:

$$0 \to N \otimes F \to M \otimes F \to (M/N) \otimes F \to 0$$

is exact. Note M/N is torsion, so then tensor product with F is zero, kills torsion. And $N \otimes F \cong F^n$ because of freedom. So we have:

$$0 \to F^n \to M \otimes F \to 0.$$

So if M has a maximal linearly independent set of cardinality n, then $M \otimes F$ is an n-dimensional F-vector space. Since "dim" is uniquely defined, n is unique. So $F^n \cong M \otimes F$ by exactness as well. □

Remark 12.24. Let M be a module over an ID. Then $\text{Tor}(M)$ is a submodule. But $M/Tor(M)$ doesn't have to be free.

Remark 12.25. If N is a max free submodule, then M/N is a torsion module, but it may be ”larger” than $\mathrm{Tor}(M)$.

Example 12.26. Let $R = F[x,y]$. Consider $M = (x,y) \subseteq F[x,y]$. It is torsion free, but not free (factorize). Also if we let $N = (x)$, then M/N is torsion module, but $Tor(M) = 0$.

Remark 12.27. If R is a principal ideal, and M is finitely generated, then:

$$M \cong R^r \oplus [R/(a_1) \oplus \cdots \oplus R/(a_m)].$$

Then:

$$M = R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m).$$

Where R^r is the free part, and the rest is the torsion part $= \mathrm{Tor}(M)$. The free part is not uniquely defined.

Remark 12.28. Let R be a principal ideal domain, and M be an R-module. Then M is free if and only if it is torsion-free.

Remark 12.29. Let R be a PID. Then $\forall a = p_1^{r_1} \cdots p_k^{r_k}$, distinct primes. Then $R/(a) \cong R/(p_1^{r_1}) \oplus \cdots \oplus R/(p_k^{r_k})$. By CRT.

Remark 12.30. if M is a finitely generated R-module, then:

$$\begin{aligned} M &\cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m) \\ &\cong R^r \oplus R/(p_1^{r_1}) \oplus \cdots \oplus R/(p_k^{r_k}), \end{aligned} \tag{12.2}$$

for some primes p_i not necessarily distinct.

Definition 12.31. These $p_1^{r_1}, ..., p_k^{r_k}$ above are called **elementary divisors** of M. (You will prove in homework that they are uniquely defined)

Definition 12.32. Note:

$$\begin{aligned} M \cong R^r &\oplus (R/(p_1^{r_1}) \oplus \cdots \oplus R/(p_1^{r_k})) \\ &\oplus (R/(p_2^{s_1}) \oplus \cdots \oplus R/(p_2^{s_l})) \\ &\oplus \cdots \oplus (), \end{aligned} \tag{12.3}$$

where p_i are distinct now. So the first row in big parentheses is the p_1-primary component. And the stuff in second set of parentheses in second row is the p_2-primary component.

Definition 12.33. **(P) - primary component of M** is:

$$\bigcup_{r=1}^{\infty} \mathrm{Ann}(p^r) = \mathrm{Ann}(p^r) : r = max\{r_1, ..., r_k\}.$$

Lemma 12.34. *The p_i-primary components are uniquely defined.*

Proof. To prove: given a finitely generated module annihilated by p^r for some r, then it is isomorphic to $R/(p^{r_1}) \oplus \cdots \oplus R/(p^{r_k})$, where $r_1, ..., r_k$ are uniquely defined. □

Monday, February 26th

THEOREM 12.35. *If M is finitely generated over a PID, then:*

$$M \cong R^r \oplus R/(p_1^{r_1}) \oplus \cdots \oplus R/(p_l^{r_l}),$$

where p_i are primes. These $p_i^{r_i}$ are uniquely defined. Two modules written this way are isomorphic if and only if all the summands are the same up to permutation.

From this you can deduce that the invariant factors of M are also uniquely defined. You have another isomorphism:

$$M \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^r.$$

$a_1, ..., a_m$ are called **invariant factors of** M and are uniquely defined up to units. Note we have invariant factors ⇒ elementary divisors. We have:

$$\begin{aligned} a_1 &= p_1^{r_{1,1}} \cdots p_{e_1}^{r_{1,l_1}} \\ a_2 &= p_1^{r_{2,1}} \cdots p_{e_1}^{r_{2,l_2}}. \\ &\vdots \end{aligned} \tag{12.4}$$

some of the exponents maybe equal to zero, but these a_i are the elementary divisors. So we are solving for the $p_i^{r_i}$'s.

And we can also go the other way around, find invariant factors from elementary divisors. We write:

$$\begin{aligned} &p_1^{r_{1,1}} \cdots p_{e_1}^{r_{1,s_1}}, \\ &p_2^{r_{2,1}} \cdots p_{e_1}^{r_{2,s_2}}, \\ &\vdots \\ &p_k^{r_{k,1}} \cdots p_{e_1}^{r_{k,s_k}} \end{aligned} \tag{12.5}$$

where $r_{1,1} \geqslant r_{1,2} \geqslant ...$, and so on for all i. Then put:

$$\begin{aligned} a_m &= p_1^{r_{1,1}} p_2^{r_{2,1}} \cdots p_k^{r_{k,1}} \\ a_m &= p_1^{r_{1,2}} p_2^{r_{2,2}} \cdots p_k^{r_{k,2}} \\ &\vdots \end{aligned} \tag{12.6}$$

Then we have $a_1 | a_2 | \cdots | a_m$.

EXAMPLE 12.36. Let our invariant factors be $2, 2 \cdot 3, 2^2 \cdot 3, 2^3 \cdot 3^2$. This gives us elementary divisors:

$$\begin{gathered} 2 \\ 2, 3 \\ 2^2, 3 \\ 2^3, 3^2. \end{gathered} \tag{12.7}$$

So just take the biggest index of each distinct prime.

Let M be a finitely generated module over a PID R. Represent M as a quotient module of R^n. Let $M \cong R^n/N$. So N is free, so has a basis. Find such a basis $\{ v_1, ..., v_k \}$ in N. And $A = (v_1 | v_2 | ... | v_k)$. Note it's an $n \times k$ matrix.

Definition 12.37. We have this matrix, it's called **the relation matrix of** M. Why is it called that? Let $\{ u_1, ..., u_n \}$ be the generating set of M used to construct the homomorphism $R^n \to M$ given by $e_i \to u_i$. The u_i are not linearly independent in general. Let:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{k1} \\ \vdots & & \vdots \\ a_{1n} & \cdots & a_{kn} \end{pmatrix}.$$

Then it must be that

$$\begin{aligned} a_{11}u_1 + \cdots + a_{1n}u_n &= 0 \\ &\vdots \\ a_{k1}u_1 + \cdots + a_{kn}u_n &= 0. \end{aligned} \tag{12.8}$$

Indeed $a_{11}e_1 + \cdots + a_{1n}e_n = v_1$, and $\varphi(v_1) = 0$. This is the definition of a relation matrix.

So we want to find a basis $\{ w_1, ..., w_n \}$ in R^n s.t. $\{ c_1w_1, ..., c_mw_m \}$ is a basis in N, with $c_1|c_2|...|c_m$. Then $M \cong R^n/N \cong R/(c_1) \oplus \cdots \oplus R/(c_m) \oplus R^{n-m}$, so $c_1, ..., c_m$ are the invariant factors of M. In Euclidean domains, we use row-column operation to reduce A to a form:

$$\left(\begin{array}{ccc} c_1 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & c_m \\ \hline 0 & \cdots & 0 \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{array}\right),$$

and "protocol" all row operations you use.

A basis in M will be $\{ \varphi(c_1w_1), ..., \varphi(c_mw_m), \varphi(w_{m+1}), ..., \varphi(w_n) \}$. Where the stuff up to index m generates the torsion part, and the stuff from $m+1$ up generates R^{n-m}. Now shouldn't the rank of A be k, since the v_i's are linearly independent? So we must have $m = k$, Professor made a mistake.

12.1 Exercises

2. *$B = \{ x_1, ..., x_n \}$ be a maximal linearly independent set in M if and only if RB is free and M/RB is torsion module.*

   Proof. (a) *$\{ x_1, ..., x_n \}$ is linearly independent if and only if*

   $$R\{ x_1, ..., x_n \}$$

   is a free module with basis $\{ x_1, ..., x_n \}$.

   Proof. Professor Leibman completed this proof in class. □

   (b) Let $\{ x_1, ..., x_n \}$ be a maximal linearly independent set. Let $y \in M$. Then $\exists a_1, ..., a_n, b$ s.t. $a_1x_1 + \cdots + a_nx_n + by = 0$ and not all of $a_1, ..., a_n, b$ are zero. If $b = 0$, then $a_1x_1 + \cdots + a_nx_n = 0$, this is impossible, since $x_1, ..., x_n$ are linearly independent. So $b \neq 0$, and $by = 0 \mod R\{ x_1, ..., x_n \}$. So

$b\overline{y} = 0 \in M/R\{ x_1, ..., x_n \}$. So $\forall \overline{y} \in M/R\{ ... \}$, $\exists b \neq 0$ s.t. $b\overline{y} = 0$.

Now we prove in the other direction. Assume that $M/R\{ x_1, ..., x_n \}$ is a torsion module. Take $\forall y \in M$. Find $b \neq 0$ s.t. $b\overline{y} = 0$, that is, $by \in R\{ x_1, ..., x_n \}$. So $by = a_1x_1 + \cdots + a_nx_n$ for some a_i, so $y, x_1, ..., x_n$ are linearly dependent, so $\{ x_1, ..., x_n \}$ is a maximal linearly independent set. We know this since we proved we could not add any other linearly independent element without making the whole set dependent. So it's maximal.

□

4. *Let R be an integral domain, let M be an R-module and let N be a submodule of M. Suppose M has rank n, N has rank r and the quotient M/N has rank s. Prove that $n = r + s$.* Use:

$$0 \to N \to M \to M/N \to 0.$$

Multiply tensor by field of fractions. Use

$$rank(M) = rank(N) + rank(M/N).$$

Proof. Let $A = \{ x_1, ..., x_s \}$, a set of elements in M whose images are a maximal independent set in M/N. And let $B = \{ x_{s+1}, ..., x_{s+r} \}$ be a maximal independent set in N. We prove A is independent in M. Suppose it weren't. Then there is $l \neq 0$ in R and $x_i \in A$ s.t. $lx_i = \sum_{j \neq i, \leqslant s} r_j x_j$. But then under the natural projection we would have a similar equality for $\overline{x_i}$ which would contradict the independence of $\overline{A}$.

We wish to show that $A \cup B$ is a maximal linearly independent set. We first show it is independent. Let $x_i \in A$. Suppose there exists a nonzero $l \in R$ s.t. $lx_i = r_{s+1}x_{s+1} + \cdots + r_{s+r}x_{s+r}$ for $r_i \in R$. Then under the natural projection $\pi : M \to M/N$, we have $\pi(lx_i) = l\pi(x_i) = 0 \in M/N$. But note $\pi(x_i)$ is in $\overline{A}$ which is an independent set in M/N so we must have $\pi(x_i) \neq 0$ and that $\nexists l \in R$ s.t. $l\pi(x_i) = 0$. This is a contradiction, so we must have that there exists no such l, so every element in A is independent of B. Now let $x_j \in B$ and suppose there exists a nonzero $l \in R$ s.t. $lx_j = r_1x_1 + \cdots + r_sx_s$. Then π maps this to $0 \in M/N$ since $lx_j \in N$, but then since $\overline{A}$ is independent in M/N, we must have $r_1 = \cdots = r_s = 0$. Then we have $lx_j = 0$ which is a contradiction since B cannot contain any torsion elements or it would not be independent. Then we have proved $A \cup B$ is independent.

Now we show $A \cup B$ is maximal. Let $y \in M$. Then since $\overline{A}$ is a maximal linearly independent set in M/N, we know there exist $c, c_1, ..., c_s$ not all zero such that:

$$c\overline{y} + c_1\overline{x_1} + \cdots + c_s\overline{x_s} = 0,$$

which implies:

$$cy + c_1x_1 + \cdots + c_sx_s = n \in N.$$

Now since B is a maximal linearly independent set in N, we know that since $n \in N$, there exists $k, c_{s+1}, ..., c_{s+r} \in R$ not all zero s.t.

$$kn = k(cy + c_1x_1 + \cdots + c_sx_s) = c_{s+1}x_{s+1} + \cdots + c_{s+r}x_{s+r}.$$

But if $k = 0$, then we must have $c_{s+1}, .., c_{s+r} = 0$ since B is independent. So we must have $k \neq 0$, thus we can write:

$$kcy = \sum_{i=1}^{s} -kc_ix_i + \sum_{i=s+1}^{s+r} c_ix_i.$$

And since we know $c, c_1, ..., c_s$ are not all zero, we have found a nonzero $kc \in R$ (since we are in an ID) s.t. kcy is a linear combination of $x_1, ..., x_{s+r}$. So we have shown that $A \cup B$ is a maximal independent set in M, since for any $y \in M$ there is kc s.t. kcy is a combination of elements in $A \cup B$.

Now we wish to show that $rank(M) = n = r + s$. So we use part (b) of Exercise 2 above. Note that R^{r+s} is a submodule of M, since $x_1, ..., x_{s+r} = A \cup B$ is a maximal linearly independent set in M, and $R(A \cup B) = R^{r+s}$, and we have closure by ring action since M is an R-module.

Lemma 12.38. *If $\{ u_1, ..., u_n \}$ is a maximal linearly independent set, it doesn't have to generate M, but $M/R\{ u_1, ..., u_n \}$ is a torsion module, because otherwise we could add one more element to this set and it would still be linearly independent.*

Proof. Suppose $M/R\{ u_1, ..., u_n \}$ is not torsion. Then

$$\exists u' \in M/R\{ u_1, ..., u_n \}$$

s.t. $ru' \neq 0 \in M/R\{ u_1, ..., u_n \}$ (i.e. $ru' \notin R\{ u_1, ..., u_n \}$) for all $r \in R$. But this is exactly the definition of linear independence, so then $\{ u_1, ..., u_n, u' \}$ is independent, which is a contradiction since we said $\{ u_1, ..., u_n \}$ was maximal. □

So by the above Lemma, we know M/R^{r+s} is torsion. Then by Exercise 2 part (b), we know $rank(M) = n = r + s$. □

5. *Consider $\mathbb{Z}[x] \sim F[x, y]$. Note $(2, x)$ is not principal.* Note M has rank 1, is torsion free, but not free. It has rank 1 because if you take one of these elements, something linearly dependent maybe, idk. Consider $M/(2)$ then x is a torsion element here since $2x = 0$. So it's a torsion module or something. And actually, it's true for any module over PID.
9. *Give an example of an integral domain R and a nonzero torsion R-module M such that $Ann(M) = 0$. Prove that if N is a finitely generated torsion R-module, then $Ann(N) \neq 0$.*

   Let $R = \mathbb{Z}$, an integral domain. Define:

   $$M = \bigoplus_{i=1}^{\infty} \mathbb{Z}/2^i\mathbb{Z}.$$

   Then $\forall a \in M$, $\exists k \in \mathbb{Z}$ such that:

   $$a = (a_1 + \mathbb{Z}/2\mathbb{Z}, ..., a_k + \mathbb{Z}/2^k\mathbb{Z}, 0, ...)$$

for some $a_1, \ldots, a_k \in \mathbb{Z}$. Thus $2^k a = 0 \in M$, so M is a torsion module. We claim that $\text{Ann}(M) = 0$. Suppose there exists a nonzero $r \in \mathbb{Z}$ s.t. $r \in Ann(M)$. Then choose $k \in \mathbb{Z}$ s.t. $r < 2^k$. Then define:

$$a = (0, \ldots, 0, 1 + \mathbb{Z}/2^k\mathbb{Z}, 0, \ldots)$$

where the nonzero entry is in the k-th position. Then since $ra = 0$, we must have $r = 0$ since r will not annihilate the nonzero entry of a since $r < 2^k$. This is a contradiction since we said $r \neq 0$. So we must have $\text{Ann}(M) = 0$.

Proof. Let R be a integral domain. Let N be finitely generated torsion R-module. Then $N \subseteq R\{x_1, \ldots, x_n\}$. And since it is torsion, there exist $\{r_1, \ldots, r_n\}$ s.t. $r_i x_i = 0$, where $r_i \neq 0\ \forall i$. Then since we have no zero divisors, $lcm(r_1, \ldots, r_n) \neq 0$, and this is in the annihilator by commutativity in R. □

11. *Let R be a PID, let a be a nonzero element of R and let $M = R/(a)$. For any prime p of R, prove that:*

$$p^{k-1}M/p^kM \cong \begin{cases} R/(p) & \text{if } k \leqslant n \\ 0 & \text{if } k > n \end{cases},$$

where n is the power of p dividing a in R.

Proof. We first treat the case where $p \nmid a$. Then since p is a prime in R, we know $\gcd(a,p) = 1$. So then we have $(p) \cap (a) = 0$. let $\pi : R \to R/(a) = M$. Then observe:

$$\pi((p)) = (p)/(a) \cong [(p) + (a)]/(a) \cong (p)/((p) \cap (a)) \cong (p)/(0) \cong (p).$$

But note that $(p) + (a) = (1) = R$, so we have shown $(p) = pM \cong R/(a) = M$, so $p^{k-1}M = p^kM = M$ for all k, and thus since $M/M \cong 0$, we have the desired result.

Now let $p \mid a$, and assume $k \leqslant n$. Then we have $a = p^n p_1^{c_1} \cdots p_l^{c_l}$, for some distinct primes p_i. Using the result of Exercise 12.1.7 and the Chinese remainder theorem, we have:

$$\begin{aligned}
\frac{p^{k-1}M}{p^kM} &= \frac{p^{k-1}R/(a)}{p^kR/(a)} \\
&\cong \frac{p^{k-1}R/(p^n)(p_1^{c_1})\cdots(p_l^{c_l})}{p^kR/(p^n)(p_1^{c_1})\cdots(p_l^{c_l})} \\
&\cong \frac{R/(p^{n-k+1})(p_1^{c_1})\cdots(p_l^{c_l})}{R/(p^{n-k})(p_1^{c_1})\cdots(p_l^{c_l})} \\
&\cong \frac{R/(p^{n-k+1}) \oplus R/(p_1^{c_1}) \oplus \cdots \oplus R/(p_l^{c_l})}{R/(p^{n-k}) \oplus R/(p_1^{c_1}) \oplus \cdots \oplus R/(p_l^{c_l})} \qquad (12.9) \\
&\cong (R/(p^{n-k+1}))/(R/(p^{n-k})) \oplus (R/(p_1^{c_1}))/(R/(p_1^{c_1})) \\
&\oplus \cdots \oplus (R/(p_l^{c_l}))/(R/(p_l^{c_l})) \\
&\cong (R/(p^{n-k+1}))/(R/(p^{n-k})) \oplus 0 \oplus \cdots \oplus 0 \\
&\cong (R/(p^{n-k+1}))/(R/(p^{n-k})) \\
&\cong R/(p).
\end{aligned}$$

Now suppose $k > n$. Then $a | p^{k-1} \Rightarrow p^{k-1}M \cong raR/(a) \cong 0$. □

12. *Let R be a PID and let p be a prime in R.*
   (a) *Let M be a finitely generated torsion R-module. Use the previous exercise to prove that $p^{k-1}M/P^kM \cong F^{n_k}$ where F is the field $R/(p)$ and n_k is the number of elementary divisors of M which are powers p^α with $\alpha \geqslant k$.*

   Proof. Recall that a module over a PID is free if and only if it is torsion free, so since M is not torsion free, it is not free, and by Theorem 6, we have:

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_l^{\alpha_l}),$$

   where the primes are not necessarily distinct, and all the α's are positive. But then by Theorem 5, since M is torsion, we know $r = 0$. So we have:

$$M \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_l^{\alpha_l}).$$

   Define $a = p_1^{\alpha_1} \cdots p_l^{\alpha_l}$. Now we apply the result of the previous exercise to each of these summands. Let s be the power of p dividing $p_i^{\alpha_i}$. We set $M' = R/(p_i^{\alpha_i})$. So we know:

$$p^{k-1}M'/P^kM' \cong \begin{cases} R/(p) & \text{if } k \leqslant s \\ 0 & \text{if } k > s \end{cases},$$

   So we have that $k \leqslant s$ for exactly n_k of the elementary divisors $p_i^{\alpha_i}$, and so each of these summands is isomorphic to F, and the rest are zero. So we have:

$$M \cong F \oplus \cdots \oplus F \cong F^{n_k}.$$

   □

   (b) *Suppose M_1 and M_2 are isomorphic finitely generated torsion R-modules. Use (a) to prove that, for every $k \geqslant 0$, M_1 and M_2 have the same number of elementary divisors p^α with $\alpha \geqslant k$. Prove that this implies M_1 and M_2 have the same set of elementary divisors.*

   Proof. Applying part (a), we have:

$$F^{n_{k_1}} \cong F^{n_{k_2}}.$$

   which tells us $n_{k_1} = n_{k_2}$ since they are isomorphic vector spaces of those dimensions. And we are done, since we iterate over the list of primes p_i in the list of elementary divisors $\{ p_i^{\alpha_i} \}$, and also iterate over k from zero to α_i for each p_i, and observe that we have exactly the same elementary divisors for M_1 and M_2 by induction. □

SECTION 12.2

The rational canonical form

Tuesday, February 27th

Remark 12.39. Let F be a field, V an n-dimensional F-vector space, and T a linear transformation $T : V \to V$. Then V gets the structure of an $F[x]$-module by $xu = T(u)$ for $u \in V$.

We state some facts about V.

Lemma 12.40. *V is a torsion module as an $F[x]$-module.*

Proof. Note that any nonzero free $F[x]$-module is isomorphic to a direct sum of copies of $F[x]$, but each copy of $F[x]$ is an infinite-dimensional vector space over F, and so if V has finite dimension over F, it must be a torsion $F[x]$ module, since its free rank must be zero. □

Lemma 12.41. *Any $F[x]$-submodule of V is a T-invariant subspace of V over F.*

Proof. Let W be such a submodule, then it is a subgroup, so $FW \subseteq W$, so $xw = T(w) \in W$. □

Remark 12.42. If $V = V_1 \oplus V_2$ as $F[x]$ modules then the summands are T-invariant.

Remark 12.43. V is cyclic if there exists $u \in V$ s.t. $F[x]u = V$.

Definition 12.44. In the above case, u is called a **cyclic vector** for V.

Remark 12.45. If u is a cyclic vector for V, then $\forall v \in V$, $v = a_k T^k(u) + \cdots + a_1 T(u) + a_0 u$ for some $a_0, \ldots, a_k \in F$.

Thus we have:

Remark 12.46. $\text{span}\left\{ u, T(u), T^2(u), \ldots \right\} = V$ for any cyclic vector u of V.

Remark 12.47. If u is a cyclic vector of V, then $V \cong F[x]/(f)$ where $(f) = Ann(u)$ as an $F[x]$ module.

Let $f(x) = x^k + \cdots + a_1 x + a_0$. Then $F[x]/(f) = \left\{ b_0 + b_1 x + \cdots + b_{k-1} x^{k-1} \mod f \right\}$, which is a k-dimensional vector space with basis $1, x, x^2, \ldots x^{k-1}$.

Now since $F[x]/(f) \cong V$, $1 \cdot u$, $xu = T(u)$, $x^2 u = T^2(u)$,...,$x^{k-1}u = T^{k-1}(u)$. We map:

$$\begin{aligned} 1 &\mapsto x \\ x &\mapsto x^2 \\ &\vdots \\ x^{k-2} &\mapsto x^{k-1} \\ x^{k-1} &\mapsto x^k = a_0 - \cdots a_{k-1} x^{k-1}. \end{aligned} \tag{12.10}$$

Definition 12.48. And we have the **companion matrix** of f where f is monic, given by:

$$A_i = \left(\begin{array}{cccc|c} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & & -a_1 \\ 0 & 1 & \ddots & & \vdots \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \vdots & & 1 & -a_{k-1} \end{array} \right).$$

Remark 12.49. Multiplication by x in $F[x]/(f)$ corresponds to the action of T on V. So in the basis $\left\{ u, T(u), ..., T^{n-1}(u) \right\}$, T has this matrix also.

Remark 12.50. Let $T : V \to V$, and $S : W \to W$, then V, W are $F[x]$-modules. What is a homomorphism $\varphi : V \to W$? φ is a homomorphism of groups under addition, and we have $\varphi(au = a\varphi(u)\ \forall a \in F$, so φ is a linear transformation $V \to W$. And additionally, $\varphi(xu) = x\varphi(u)$, where $\varphi(xu) = \varphi(T(u))$ and $x\varphi(u) = S(\varphi(u))$ typo? And the following diagram is commutative:

$$\begin{tikzcd}
V \arrow[r, "\varphi"] \arrow[d, "T"] & W \arrow[d, "S"] \\
V \arrow[r, "\varphi"] & W
\end{tikzcd}.$$

Remark 12.51. $F[x]$ is a Euclidean domain (ED).

Remark 12.52. By the fundamental theorem, V is a direct sum of cyclic submodules:

$$V = V_1 \oplus \cdots + \oplus V_m,$$

where $\forall i$, V_i is cyclic, $V_i \cong F[x]/(f_i)$. Moreover, we may choose V_i s.t. $f_1 | f_2 | ... | f_m$ (invariant factors), or so that $\forall i$, $f_i = P_i^{r_i}$, where P_i are irreducible polynomials (elementary divisors).

In each V_i, choose a "cyclic" basis $\left\{ u, Tu, ..., T^{k-1}u \right\}$ and unite these basis elements. Then in the obtained basis, the matrix of T is:

$$A = \begin{pmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \ddots & \\ 0 & & & \boxed{A_k} \end{pmatrix},$$

where $\forall i$, A_i is the companion matrix of f_i. If $f_1, ..., f_m$ are invariant factors, A is called the **rational canonical form** of the matrix of T. Both the **rational canonical form** and elementary divisors form are uniquely defined.

Remark 12.53. Any $n \times n$ matrix over F is similar to such "RCF" and "elem divisors" form matrices.

Definition 12.54. Two matrices are similar ($B = PCP^{-1}$) if and only if they have the same invariant factors or the same elementary divisors.

Remark 12.55. The invariant factors $f_1, ..., f_m$ don't depend on the field (what does this mean?)

Wednesday, February 28th

Let $\dim V = N$, $T : V \to V$. Then $\exists$ a basis in which the matrix of T is:

$$A = \begin{pmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \boxed{\ddots} & \\ 0 & & & \boxed{A_k} \end{pmatrix}$$

Thursday, March 1st

Consider $w_1, \ldots, w_n \in F[x]^n$. Where:

$$w_1 = \begin{pmatrix} x \\ 0 \\ \vdots \\ 0 \end{pmatrix} - \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, w_n = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x \end{pmatrix} - \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix}$$

Define $\tilde{N} = R\{\, w_1, \ldots, w_n \,\}$. Then $\tilde{M} = F[x]^n / \tilde{N}$ is an F-vector space of dim $\leqslant n$. In $\tilde{M}$, we have:

$$\begin{pmatrix} x \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix}, \ldots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x \end{pmatrix} = \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix}$$

And we have:

$$\begin{aligned} \begin{pmatrix} x^2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} &= x \cdot \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix} = \begin{pmatrix} a_{11}x \\ \vdots \\ a_{n1}x \end{pmatrix} = a_{11} \begin{pmatrix} x \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \cdots + a_{n1} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ x \end{pmatrix} \\ &= a_{11} \begin{pmatrix} a_{11} \\ \vdots \\ a_{n1} \end{pmatrix} + \cdots + a_{n1} \begin{pmatrix} a_{1n} \\ \vdots \\ a_{nn} \end{pmatrix} \qquad (12.11) \\ &= \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}. \end{aligned}$$

So $\forall$ element of $\tilde{M}$ can be written as $\begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} \in F$. So $\dim_F \tilde{M} \leqslant n$. So $V = F[x]^n / N$ where N has all relations, so $\tilde{N} \subseteq N$ so if $\tilde{N} \neq N$, then V is a nontrivial factor of $\tilde{M}$, so $\dim V < n$, not the case, so $N = \tilde{N}$. It's not the case since we assumed $\dim V = n$.

Observe we have $\tilde{N} \subseteq N \subseteq M$. Then we have $M/\tilde{N} = \tilde{M}$, and $V = M/N$ by definition. And $V \cong M/N \cong \big((M/\tilde{N})/(N/\tilde{N})\big) = \tilde{M}/(N/\tilde{N})$. This is by the third isomorphism theorem for modules.

Then we have $xI - A$ - relations matrix $\Rightarrow$ Smith's form. We have:

$$\left(\begin{array}{cccccc} c_1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & \ddots & 0 & \vdots & & \vdots \\ 0 & 0 & c_k & 0 & \cdots & 0 \\ 0 & \cdots & 0 & f_1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & f_k \end{array}\right),$$

where the f_i's are the invariant factors. And $f_m = m_T$ where m_T is the minimal polynomial. Now we have $\det(xI - A) = \det(Smith) = f_1 \cdots f_m$ (up to a scalar from F). Where $\det(xI - A)$ is the characteristic polynomial of T, $c_T(x)$. So $m_T | c_T$.

Corollary 12.56 (**Cayley-Hamilton theorem**). *$c_T(T) = 0$, since $m_T(T) = 0$.*

Then note $f_m | c_T$, and $f_m = m_T$ and c_T have the same irreducible factors. This is because $f_1 | f_2 | \cdots | f_m$. So $c_T | f_m^m$. If $m_T = c_T$, then $m = 1$ and we have a single rational cell in the canonical form of T.

If you know the order of the group you can write it as products of primes and write it so first divides the second... And we can do the same here for these polynomials.

We discuss the **Jordan normal form** of T. This is not universal, so its different from rational. Assume that $f_m = m_T$ splits to a product of powers of linear factors:

$$m_T(x) = (x - \lambda_1)^{r_1} \cdots (x - \lambda_k)^{r_k}.$$

This is always the case if F is "algebraically closed", for example, if $F = \mathbb{C}$. But we digress, since we assumed that f_m splits. Then also $c_T(x)$ splits, $f_1, \ldots, f_{m-1}$ split. The elementary divisors form of the matrix of T is:

$$A = \left(\begin{array}{c|ccc} A_1 & & & 0 \\ \hline & \boxed{A_2} & & \\ & & \ddots & \\ 0 & & & \boxed{A_k} \end{array}\right).$$

where $\forall i$ A_i is the companion matrix of $(x - \lambda_i)^{r_i}$ (find it the way you would for any regular companion matrix).

Remark 12.57. If two matrices have the same c_T then they have the same rational form, so they must be conjugate (if they are 2×2 matrices).

Friday, March 2nd
We do exercises from the sample exam sheet.
Monday, March 5th
We do exercises from the sample exam sheet.

12.2 Exercises

3. *Prove that 2×2 non-scalar matrices are similar if and only if they have the same characteristic polynomial.*

   Proof.

   Definition 12.58. A **scalar** matrix is a matrix of the form:

   $$\begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix} = cI.$$

   Note $\deg c_T(x) = 2$. Note we have $c_T = f_1 = m_T$ or $c_T = f_1 f_2$ s.t. $f_1 | f_2$. If we are in the second case, then $c_T = f_1 \cdot f_2$ then $f_1 = f_2 = x - c$, since we always assume that they are monic polynomials. And because at most linear. So $T = \begin{pmatrix} c & 0 \\ 0 & c \end{pmatrix}$. If $c_T = m_T$, then there exists a single rational cell whose companion matrix is c_T. So two matrices are conjugate (same thing as similar) if and only if they have same c_T, so same rational form.

   □

4. *Prove that 3 by 3 matrices are similar if and only if they have the same m_T and same c_T. Give explicit counterexample for 4 by 4.*

   PROOF. This is a case by case argument. We know the degree of c_T is 3. If $deg(m_T) = 3$ then we are done, we only have 1 invariant factor and the RCF (similarity class) is in 1-1 correspondence with invariant factors. Now suppose m_T has degree 2. Then the remaining invariant factor must have degree 1 and divide m_T, so it is just equal to c_T/m_T which is unique, so we're done. If m_T has degree 1 then all three invariant factors are equal to it and we are done. □

5. $\dim(End(F^n)) = \dim(M_{n\times n}) = n^2$. Then if we take $I, T, T^2, \ldots, T^{n^2}$ are linearly dependent in $M_{n\times n}$. So there exists $a_0, \ldots, a_n \in F$ not all zero s.t. $a_0I + a_1T + \cdots + a_{n^2}T^{n^2} = 0$, so $f(T) = 0$ for $f(x) = a_{n^2}x^{n^2} + \cdots + a_1x + a_0$. So we just took a nondegenerate transformation and made a set with identity of n^2+1 elements, used linear independence to construct a polynomial that would annihilate T, and proved that $deg(m_T) \leqslant n^2$.

10. Over $\mathbb{Q}$ take 6×6 matrices with min polynomial $m_T = (x+2)^2(x-1) = a^2b$. Find all similarity classes. Then either we have $f_1 = f_2 = m_T$, or we could have $f_1 = (x+2), f_2 = (x+2)^2, f_3 = m_T$. Or we could have $f_1 = f_2 = f_3 = (x-1)$ and $f_4 = m_T$. So the possibilities are:

$$\begin{gathered} a, a^2, a^2b \\ a, a, a, a^2b \\ b, b, b, a^2b \\ a^2b, a^2b \\ a, ab, a^2b \\ b, ab, a^2b \end{gathered} \tag{12.12}$$

   And that's it, that's the answer, no need to write anything else. But if you're asked to write the RCF then do that, and also say when Jordan exists. We write Jordan normal form for a^2b, a^2b:

$$\begin{pmatrix} -2 & 1 & & & & \\ 0 & -2 & & & & \\ & & 1 & & & \\ & & & -2 & 1 & \\ & & & 0 & -2 & \\ & & & & & 1 \end{pmatrix}.$$

18. $T^{-1} = T^2 + T$. $T^3 + T^2 - 1 = 0$, so $f = x^3 + x^2 - 1$ is irreducible over $\mathbb{Q}$. So f is the minimal polynomial and all other invariant factors divide f. So the minimal polynomial must have degree $\leqslant n^2$.

19. *$\forall A$, A, A^T are conjugate. (Number of problem not known)*

   How do we prove this, we use row operations on $xI - A$ and column operations on $xI - A^T$ and get the same Smith normal form. And the Smith normal form gives you invariant factors, and they will be the same. The result will be the same because they remain transposes of each other.

Part 4

FIELD THEORY AND GALOIS THEORY

CHAPTER 13

Field theory

SECTION 13.0

Overview of Galois theory

Wednesday, March 7th

We solve: $a_nx^n + \cdots + a_1x + a_0 = 0$, for $a_i \in \mathbb{Z}$. Then we have $a_1x + a_0 \Rightarrow x = -\frac{a_0}{a_1}$. And:

$$a_2x^2 + a_1x + a_0 = 0 \Rightarrow x = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0a_2}}{2a_2}.$$

And $x^2 - 2 = 0$, solution $x = \sqrt{2}$. Radicals: solutions of $x^n = a$, $\sqrt[n]{a}$. In 1540, Ferrari, Cardano found a cubic formula. All attempts to solve equations of degree 5 have failed. In around 1825, Abel found a example of a degree 5 equation unsolvable in radicals.

Then we have Evariste Galois, 1811-1832. We consider:

$$f(x) = x^n + \cdots + a_1x + a_0, a_i \in \mathbb{Q}.$$

We have roots $\alpha_1, ..., \alpha_n \in \mathbb{C}$. Field of f, $\mathbb{Q}(\alpha_1, ..., \alpha_n)$ is the field generated by $\alpha_1, ..., \alpha_n$. This means that we start with $\mathbb{Q}$. Then let $K_1 = \mathbb{Q}(\sqrt[3]{2})$, $K_2 = K_1(\sqrt[5]{\sqrt[3]{2} - 3})$, $K_3 = K_2(\sqrt{7})$, $K_4 = K_3(\sqrt{\sqrt{7} + \sqrt[3]{\sqrt[3]{\sqrt{\cdots}}}})$.

Definition 13.1. We construct a series of **extensions**:

$$\begin{tikzcd}
K_m \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
K_1 \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd},$$

where the K_i's are radical extensions. We need a tower of radical extensions such that $\alpha_1, ..., \alpha_n \in K_m$.

Definition 13.2. Consider the group of permutations of $\alpha_1, ..., \alpha_n$ that preserves all relations between $\alpha_1, ..., \alpha_n$. This is the group of automorphisms $\mathrm{Aut}(R/\mathbb{Q}) = \mathrm{Aut}(F)$ and is called the **Galois group** of F, $\mathrm{Gal}(F) = \mathrm{Gal}(F/\mathbb{Q})$.

Remark 13.3. Any element $\sigma \in \mathrm{Gal}(K)$ is uniquely defined by its action on $\{ \alpha_i \}$, the roots of the polynomial of which K is the splitting field.

Remark 13.4. Then for any extension F of a field K, F/K, F/K we have a group $\mathrm{Gal}(F/K)$ =$\mathrm{Aut}(F/K)$, where $\varphi : F \to F$ s.t. $\varphi|_K = Id_K$.

We have $Gal(F/E) \leqslant Gal(F/K)$. And $Gal(E/K) = Gal(F/K)/(Gal(F/E)$, where:

$$\begin{tikzcd}
F \arrow[d, dash] \\
E \arrow[d, dash] \\
K
\end{tikzcd} .$$

Galois theorem. *There exists a 1-1 correspondence between subextensions E/K of F/k and subgroups of $Gal(F/K)$. And $E \leftrightarrow Gal(F/E)$.*

Consider a tower of extensions:

$$\begin{tikzcd}
K_m \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
K_1 \arrow[d, dash] \\
\mathbb{Q} = K_0
\end{tikzcd} ,$$

then we have a series of subgroups:

$$\{ 1 \} = H_0 \leqslant H_2 \leqslant H_3 \leqslant ... \leqslant H_m.$$

Assume K_i contains all roots of 1, for a radical extension K_{i+1}/K_i, $Gal(K_{i+1}/K_i)$ is cyclic. Then H_{i+1}/H_i are cyclic, and H_m is solvable.

Remark 13.5. So if f is solvable in radicals, its field $F \subseteq K_m$, then $gal(f) = Gal(F/\mathbb{Q})$ is a quotient group of a solvable group, so it solvable (and vice versa).

Remark 13.6. So if $Gal(f)$ is not solvable, f is not solvable in radicals.

Note S_2, S_3, S_4 are solvable groups so $\forall$ polynomial of degree $\leqslant 4$ is solvable in radicals. There exists polynomials of degree 5 whose $Gal \cong S_5$ so it is not solvable in radicals.

SECTION 13.1

Basic theory of field extensions

Definition 13.7. A field is a commutative ring where all nonzero elements are invertible, so that $F^* = F \setminus \{ 0 \}$ is a group under multiplication.

Definition 13.8. The **prime subfield** of F is the subfield generated by 1.

We have $0, 1, 2 = 1 + 1, \ldots.$

Two cases:

(1) there exists minimal $n \in \mathbb{N}$ s.t. $n = 0$ in F, then F contains a copy of $\mathbb{Z}_n$. Since F has no zero divisors, n is prime, $n = p$, so $\mathbb{Z}_p \subseteq F$, for $\mathbb{Z}_p$ a prime subfield, $p = char(p)$, characteristic (finite).

(2) $\nexists n > 0$ s.t. $n = 0$ in F. Then F contains a copy of $\mathbb{Z}$. Then it contains a copy of $\mathbb{Q}$, the field of fractions of $\mathbb{Z}$. Note if you have a homomorphism:

$$\begin{tikzcd}
\mathbb{Z} \arrow[r, "\varphi"] \arrow[d] & F \\
\mathbb{Q} \arrow[ur] &
\end{tikzcd}$$

given by $\varphi(\frac{m}{n}) \mapsto \frac{\varphi(m)}{\varphi(n)}$. Then $\mathbb{Q}$ is the prime subfield, $\text{char}F = 0$.

Thursday, March 8th

Let F be a field. We defined the prime subfield in the last class. Recall that it is the subfield of F generated by 1. Then the prime subfield is either $\mathbb{Z}_p$ or $\mathbb{Q}$.

We repeat this, but recall that we always have a homomorphism, there is a unique epimorphism $\varphi : \mathbb{Z} \to F$ which sends $1 \to 1$. This is because $\mathbb{Z}$ is the universal free abelian group. We have two cases:

Case 1: $\ker \varphi \neq 0$. Then $\ker \varphi = (p)$. Then $\mathbb{Z}_p = \mathbb{Z}/(p) \subseteq F$. So $\mathbb{Z}_p$ has no zero divisors, so p is prime. We have $\mathbb{Z}_p = \mathbb{F}_p$- prime subfield of F, $\text{char}F = p$.

Case 2: $\ker \varphi = 0$. Then $\mathbb{Z} \cong \varphi(\mathbb{Z}) \subseteq F$. Then φ extends to an injective homomorphism from $\mathbb{Q} \to F$. So then F contains a copy of $\mathbb{Q}$ (prime subfield of F), and $\text{char}F = 0$.

Definition 13.9. If F is a subfield of K, then K is called an **extension** of F. Notation: K/F or:

$$\begin{tikzcd}
K \arrow[d, dash] \\
F
\end{tikzcd} .$$

Note this fraction bar notation is **not factorization!!!!** No factorization exists, since there are no nontrivial ideals.

Definition 13.10. Let K/F be an extension. Let $S \subseteq K$. The minimal subfield of K containing F and S is called the **subextension generated**

by S, denoted $F(S)$. Then:

$$F(S) = \left\{ \frac{p(s_1, \dots, s_k)}{q(s_1, \dots, s_k)} : p, q \in F[x], s_1, \dots, s_k \in S \right\}.$$

Definition 13.11. If K_1, K_2 are subfields of K, then $K_1(K_2) = K_2(K_1)$ is called the **composite of** K_1, K_2, and is denoted by K_1K_2.

Definition 13.12. Let K/F be an extension, let $\alpha \in K$. The extension $F(\alpha)/F$ is called **simple**. (An extension is simple if it is generated by a simple element, also called a primitive element.)

We have a homomorphism $\varphi : F[x] \to K$ s.t. $\varphi(p(x)) = p(\alpha)$ where $x \mapsto \alpha$.

Case 1: $\ker \varphi = 0$. Then K contains a copy of $F[x]$, so a copy of $F(x)$, the field of fractions of $F[x]$. So $F(\alpha) \cong F(x)$. Recall:

$$F(\alpha) = \left\{ \frac{p(\alpha}{q(\alpha)} : p, q \in F[x] \right\}.$$

Definition 13.13. α is said to be **transcendental** over F if and only if $p(\alpha) \neq 0$ $\forall$ nonzero $p \in F[x]$.

Example 13.14. π, e are transcendental over $\mathbb{Q}$.

Case 2: $\ker \varphi \neq 0$. Then $\ker \varphi$ is an ideal in $F[x]$, so $\ker \varphi = (f(x))$. K has no zero divisors, so (f) is a prime ideal, so f is prime = irreducible in $F[x]$. So $F[x]/(f)$ is a field. So $F(\alpha) = \varphi(F[x])$ is isomorphic to $F[x]/(f)$.

If f has degree n, then:

$$F[x]/(f) = \left\{ a_0 + a_1x + \dots + a_{n-1}x^{n-1} \mod f : a_i \in F \right\}.$$

So:

$$F(\alpha) = \left\{ a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} : a_i \in F \right\} = F[\alpha].$$

Note here that $F(\alpha) = F[\alpha]$.

And $\left\{ 1, \alpha, \dots, \alpha^{n-1} \right\}$ is a basis in $F(\alpha)$, and $[F(\alpha) : F] = n$.

13.1 Exercises

1. *$p(x) = x^3 + 9x + 6$ - irreducible in $\mathbb{Q}[x]$ by Eisenstein's. θ is a root of p. Find $(1+\theta)^{-1}$.*

   This shit is irreducible by Eisenstein. Consider

   $$\mathbb{Q}(\theta) = \left\{ a + b\theta + c\theta^2 : a, b, c \in \mathbb{Q} \right\}.$$

   Write:

$$\begin{gathered} (a + b\theta + c\theta^2)(1+\theta) = 1 \\ a + a\theta + b\theta + b\theta^2 + c\theta^2 + c\theta^3 = 1 \\ a + a\theta + b\theta + b\theta^2 + c\theta^2 - 9c\theta - 6c = 1 \\ \begin{cases} a - 6c = 1 \\ a + b - 9c = 0 \\ b + c = 0 \end{cases} . \end{gathered} \tag{13.1}$$

Note $\theta^3 = -9\theta - 6$.

Another way to do it: consider $T : \mathbb{Q}(\theta) \to \mathbb{Q}(\theta)$ where $Tu = \theta u$. The matrix of θ is:

$$\begin{pmatrix} 0 & 0 & -6 \\ 1 & 0 & -9 \\ 0 & 1 & 0 \end{pmatrix},$$

and the matrix of $(1 + \theta)$ is:

$$\begin{pmatrix} 1 & 0 & -6 \\ 1 & 1 & -9 \\ 0 & 1 & 1 \end{pmatrix} = A.$$

And we have the basis $\left\{ 1, \theta, \theta^2 \right\}$. Why is this a basis? Note $F(\alpha) \cong F[x]/(m_\alpha)$. Note $m_\alpha = x^3 + ax^2 + bx + c$. When you factorize by this ideal, you get:

$$F(\alpha) = \left\{ ax^2 + bx + c : a, b, c \in F \right\}. \tag{13.2}$$

So $F(\alpha) = \left\{ a\alpha^2 + b\alpha + c \right\}$. We just have this set of polynomials, these are equivalence classes module this polynomial. And $1, x, x^2$ is a basis in this ring. If the polynomial is irreducible, this ring is a field. If you take this ring and factorize it by this field, the cosets, equivalence classes, just correspond to poylnomials with degree < 3. Why are they independent? If you take two polynomials of this sort, their difference never belongs to the thing we are factorizing by. If m_α is reducible, it is just a ring. If it is irreducible, then the ideal is maximal, so it's a field. Now if you start with α, then you find its minimal polynomial, and we get the thing above. For each α which is algebraic, so we have an ideal generated by some polynomial, and if it is reducible we get zero divisors, but we have no zero divisors since field, so done.

And we find A^{-1}.

2. *You can look at the book to find the question.*

Proof. Use Eisenstein, it's obvious. If it's not obvious, think about it. □

3. *Show that $x^3 + x + 1$ is irreducible over $\mathbb{F}_2$ and let θ be a root. Compute the powers of θ in $\mathbb{F}_2(\theta)$.*

Proof. Suppose $p(x) = x^3 + x + 1$ were reducible over $\mathbb{F}_2$. Then since it has degree 3, we would have $(x-1) | p(x)$ or $x | p(x)$. Since we have a nonzero constant term, we know the second of these two options does not hold. Also note $p(1) = 1^3 + 1 + 1 = 1 + 1 + 1 = 1 \neq 0$, so $(x-1) \nmid p(x)$. Thus it must be irreducible over $\mathbb{F}_2$ since this field only has these two elements. □

Now consider $\mathbb{F}_2(\theta) = \left\{ a + b\theta + c\theta^2 : a, b, c \in \mathbb{F}_2 \right\}$, since θ is a root of degree 3. Note $\theta^3 = -\theta - 1$. We have:

$$\begin{aligned}
\theta^0 &= 1 \\
\theta^1 &= \theta \\
\theta^2 &= \theta^2 \\
\theta^3 &= -\theta - 1 \\
\theta^4 &= \theta^2 - \theta \\
\theta^5 &= (-\theta - 1) - \theta^2 \\
&= -\theta^2 - \theta - 1 \\
\theta^6 &= \theta + 1 - \theta^2 - \theta \\
&= 1 - \theta^2 \\
\theta^7 &= \theta - (-\theta - 1) \\
&= 1.
\end{aligned} \tag{13.3}$$

4. *Prove that $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an automorphism of $\mathbb{Q}(\sqrt{2})$.*

PROOF. Note $\sqrt{2}, -\sqrt{2}$ are conjugate, have same minimal polynomial $x^2 - 2$. We have $F(\alpha_1) \cong F(\alpha_2)$ by $\alpha_1 \leftrightarrow \alpha_2$. And we have an isomorphism $\mathbb{Q}(\sqrt{2}) \overset{\varphi}{\to} \mathbb{Q}(-\sqrt{2})$ such that $\varphi(a) = a \ \forall a \in \mathbb{Q}$, and $\varphi(\sqrt{2}) \mapsto -\sqrt{2}$.

EXAMPLE 13.15. Consider $F(x) \to F(x)$ by $x \mapsto x^2$. Note homomorphisms of fields are always injective.

□

5. *Read book for prompt.*

PROOF. Use rational root theorem $\alpha \in \mathbb{Z}$. □

SECTION 13.2

Algebraic extensions

DEFINITION 13.16. If K/F is an extension, then K is an F-vector space. $\dim_F K$ is called the **degree of K over F**, $\deg_F K = [K : F]$. It may be finite or infinite.

DEFINITION 13.17. If $\deg_F K < \infty$, then K/F is a **finite extension**.

DEFINITION 13.18. If $\deg_F K = \infty$, then K/F is an **infinite extension**.

EXAMPLE 13.19. Consider $[\mathbb{C} : \mathbb{R}] = 2$, and $[\mathbb{R} : \mathbb{Q}] = \infty$.

THEOREM 13.20. *Let K/F and E/K be finite extensions. Then E/F is an extension, and E/F is finite if and only if both $K/F, E/F$ are finite. In this case, $[E : F] = [E : K][K : F]$.*

COROLLARY 13.21. *If*

$$\begin{tikzcd}
E \arrow[d, dash] \\
K \arrow[d, dash] \\
F
\end{tikzcd}$$

is a tower of extensions, then $[E:K],[K:F] | [E:F]$.

PROOF. $\forall \gamma \in E$, $\gamma = \delta_1\beta_{j_1} + \cdots + \delta_k\beta_{j_k}$ for some $j_1, ..., j_k \in J$ and $\delta_1, ..., \delta_k \in K$. $\forall l <$ $\delta_l = a_{l,1}\alpha_{i_1} + \cdots + a_{l,t}\alpha_{i_t}$ for some $i_1, ..., i_t \in J$, $a_{l,1}, ..., a_{l,t} \in F$. So $\gamma = \sum_{i,j} c_{i,j}\alpha_i\beta_j$, $c_{i,j} \in F$. So $\{ \alpha_i\beta_j \}$ spans E over F. If $\sum c_{ij}\alpha_i\beta_j = 0$, then $\sum_j \left(\sum_i c_{ij}\alpha_i\right)\beta_j = 0$, where the thing in the parentheses is in K. So $\forall j$, $\sum_i c_{ij}\alpha_i = 0 <$ so $\forall i$, $c_{ij} = 0$. □

DEFINITION 13.22. f is the **minimal polynomial of** α, notation $m_{\alpha,F}$.

REMARK 13.23. $g(\alpha) = 0$ if and only if $f|g$.

EXAMPLE 13.24. (1) $F = \mathbb{R}$, $\alpha = i$. Them $m_{\alpha,\mathbb{R}} = x^2 + 1$. So $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$.

(2) $F = \mathbb{Q}, \alpha = \sqrt{2}$, Then $m_{\alpha,\mathbb{Q}} = x^2 - 2$. And $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/(x^2-2)$.

Friday, March 9th

We reiterate some of the stuff done yesterday.

We have an extension K/F where $\alpha \in K$, and we consider the simple extension $F(\alpha)/K$.

Case 1: $\nexists f \in F[x]$ s.t. $f(\alpha) = 0$. Then α is called **transcendental** over F. Then we have $F(\alpha) \cong F(x)$ - field of rational functions. We have $f(x) \leftrightarrow f(\alpha)$. So different rational functions have different values at α. And $[F(\alpha) : F] = \infty$. But actually, there is the theory of transcendental extensions, but it is beyond the scope of this class.

Case 2: $\exists f \in F[x]$ s.t. $f(\alpha) = 0$. Then we have $\varphi : F[x] \to K$ given by $g(x) \mapsto g(\alpha)$ which has nonzero kernel. Then $ker\varphi = (m_{\alpha,F})$, where $m_{\alpha,F}$ is an irreducible polynomial called the **minimal polynomial** of α. And $f(\alpha) = 0$ if and only if $m_{\alpha,F}|f$.

Now:

$$F(\alpha) = F[\alpha] = \left\{ a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in F \right\}.$$

And $n = deg(m_{\alpha,F})$. Now $\left\{ 1, \alpha, ..., \alpha^{n-1} \right\}$ is a basis of $F(\alpha)$, and $[F(\alpha) : F] = n = deg(m_{\alpha,F})$, is called **the degree of** α over F, also denoted $\deg_F\alpha$.

EXAMPLE 13.25. Let $\alpha = \sqrt{2+\sqrt{2}}, F = \mathbb{Q}$. Then we have $\alpha^2 = 2 + \sqrt{2}$, $\alpha^2 - 2 = \sqrt{2}$, and $(\alpha^2-2)^2 - 2 = 0$.

So $f(\alpha) = 0$ for $f(x) = x^4 - 4x^2 + 2$. This is irreducible by **Eisenstein's criterion.** So it's the minimal polynomial of α.

Or, if we know $\deg f = 4 \overset{?}{=} [\mathbb{Q}(\alpha) : \mathbb{Q}]$?

Example 13.26. Consider $\alpha = s\sqrt{2} + \sqrt{3}$. Then we have:

$$\begin{aligned} \alpha^2 &= 5 + 2\sqrt{6} \\ (\alpha^2 - 5)^2 &= 24 \\ \alpha^4 - 10\alpha^2 + 1 &= 0 \\ f(x) &= x^4 - 10x + 1. \end{aligned} \tag{13.4}$$

Note this polynomial does not have any roots because any root must divide the last coefficient. So it has no rational roots, and thus it's irreducible over $\mathbb{Q}$. If it has a root over $\mathbb{Q}$, then it must be integer root by Gauss lemma, and thus it must divide the last coefficient, but none of the factors of -1 are roots.

Okay, so why is this the minimal polynomial? If we know that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, then f is the minimal polynomial $m_{\alpha,\mathbb{Q}}$. Is this degree easy to compute? No, because... We consider multiplication by α as a linear transformation of some vector space. But we will not do this just yet, so don't worry about it.

Remark 13.27. We have a homomorphism $\varphi : F[x] \to K$ given by $f(x) \mapsto f(\alpha)$. We assume it is not injective. And then we have $ker\varphi = (m)$. Then we have $F[x]/(m) \subseteq K$. But this ring is a principal ideal domain, any prime ideal is a maximal ideal, so $F[x]/(m)$ is a field, and it's just the field generated by α, and the elements are just polynomials in α as seen above.

Example 13.28. Take $\alpha = \sqrt{2}, F = \mathbb{Q}$. Then we have $\left\{ a = b\sqrt{2} : a, b \in \mathbb{Q} \right\}$. Note this ring is a field since we can divide elements. Note:

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}. \tag{13.5}$$

Remark 13.29. It's too early for this, but consider the following:

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2}, \sqrt{3}) \arrow[dl, dash, "2"] \arrow[dr, dash, "2"] & \\
Q(\sqrt{2}) \arrow[dr, dash, "2"] & & \mathbb{Q}(\sqrt{3}) . \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}$$

The labels are the degrees.

Remark 13.30. If K/F is finite, then, since $F(\alpha)/F$ is a subextension of K/F, we have $\deg_F \alpha = [F(\alpha) : F] | [K : F]$.

Example 13.31. If $[K : F] = 6$, $\alpha \in K$, then $\deg_F \alpha = 1, 2, 3$, or 6. And it is 1 only in the case when $\alpha \in F$, $m_\alpha = x - a$, where $a = \alpha$ (according to Eric).

Lemma 13.32. *Let $K/E/F$, where $\alpha \in K$ is algebraic over F. Then α is algebraic over E. And we have $f(\alpha) = 0$ for $f \in F[x] \subseteq E[x]$. Recall that algebraic means "not transcendental", i.e. it satisfies some polynomial, maybe. Now we have $m_{\alpha,F} \overset{?}{\leftrightarrow} m_{\alpha,E}$. Since $m_{\alpha,F}(\alpha) = 0$ (over E, though, it may be reducible), and $m_{\alpha,F} \in E[x]$, we have $m_{\alpha,E} | m_{\alpha,F}$, and $\deg_E \alpha \leqslant \deg_F \alpha$.*

Example 13.33. Let $\alpha = \sqrt[6]{2}, F = \mathbb{Q}, E = \mathbb{Q}(\sqrt{2})$. Note:

$$\begin{aligned} m_{\alpha,F} &= x^6 - 2 \\ m_{\alpha,E} &= x^3 - \sqrt{2}. \end{aligned} \tag{13.6}$$

Remark 13.34. Take any finite extension. We have $F(\alpha)/F$ and let K/F be finite. Take $\alpha \in K$. If $F(\alpha_1) \neq K$, take $\alpha_2 \in K \setminus F(\alpha_1)$. If $F(\alpha_1, \alpha_2) \neq K$, take $\alpha_3 \in K/F(\alpha_1, \alpha_2)$, and repeat. We get a tower of simple extensions:

$$\begin{tikzcd}
F(\alpha_1, ..., \alpha_n) = K \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
F(\alpha_1, \alpha_2, \alpha_3) = F(\alpha_1, \alpha_2)(\alpha_3) \arrow[d, dash] \\
F(\alpha_1, \alpha_2) = F(\alpha_1)(\alpha_2) \arrow[d, dash] \\
F(\alpha_1) \arrow[d, dash] \\
F
\end{tikzcd}.$$

Then we have:

$$\begin{aligned} &= [F(\alpha_1) : F] \cdot [F(\alpha_1, \alpha_2) : F(\alpha_1)] \cdots [F(\alpha_1, ..., \alpha_n) : F(\alpha_1, ..., \alpha_{n-1})] \\ &\leqslant \deg_F \alpha_1 \cdot \deg_F \alpha_2 \cdots \deg_F \alpha_n. \end{aligned} \tag{13.7}$$

K/F-extension, K_1, K_2 are subfields of K containing F, or: $K_1/F, K_2/F$ are subextensions of K/F. Composite: K_1K_2/F. Is this finite? Who knows... In fact when we deal with algebraic extensions, something is not needed because rational functions are not equal to polynomials. What this something is, I don't know, I missed it.

Definition 13.35. Note K_1K_2 is the smallest field containing both. We take all linear combinations of both products and quotients.

Proposition 13.36. *If $K_1/F, K_2/F$ are finite extensions, then K_1K_2/F is also finite, and $[K_1K_2 : F] \leqslant [K_1 : F] \cdot [K_2 : F]$. We have:*

$$\begin{tikzcd}
 & K_1K_2 & \\
K_1 \arrow[ur, dash, "\leqslant m"] & & K_2 \arrow[ul, dash, "\leqslant n"'] \\
 & F \arrow[ul, dash, "n"] \arrow[ur, dash, "m"'] &
\end{tikzcd}.$$

And note $n, m | [K_1K_2 : F] \leqslant nm$.

Proof. Let $\{ \alpha_1, ..., \alpha_n \}$ be a basis of K_1 over F, and $\{ \beta_1, ..., \beta_m \}$ be a basis of K_2 over F. Then $K_1K_2 = F(\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m) = F[\alpha_1, ..., \alpha_n, \beta_1, ..., \beta_m]$, since these elements are algebraic. Note this notation does not denote span, it denotes the field generated by these elements. We have:

$$\begin{aligned} F(\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_m) &= F(\alpha_1)(\alpha_2)\cdots(\alpha_n)\beta_1)\cdots(\beta_m) \\ &= F[\alpha_1][\alpha_2]\cdots[\beta_m]. \end{aligned} \tag{13.8}$$

Note they are algebraic because they belong to finite extensions, if you have a transcendental element, it must generate an infinite extension.

Now any product of α_i's is their linear combination, and the same for β_j's. So if you take a polynomial in both sets, it is just a linear combination. Formally, any element $\gamma \in K_1K_2$ is just a linear combination of $\alpha_i\beta_j$ where $i = 1, \dots, n, j = 1, \dots, m$. Thus $[K_1K_2 : F] \leqslant nm$.

Why is it less equal: Trivial example is $K_1 = K_2$. It's degree is not n^2, it's just n.

So why is it not $n + m$. It is because elements in this space are *products* of linear combinations, not sums. □

Corollary 13.37. *If $(n, m) = 1$, then $[K_1K_2 : F] = nm$, where $n = [K_1 : F], m = [K_2 : F]$.*

Example 13.38. It may be that $K_1 \cap K_2 \neq \varnothing$. We have:

$$\begin{tikzcd}
 & K_1K_2 \arrow[dl, dash, "n_2"'] \arrow[dr, dash, "m_2"] & \\
K_1 \arrow[dr, dash, "n_1"] \arrow[ddr, dash, "n"'] & & K_2 \arrow[dl, dash, "m_1"'] \arrow[ddl, dash, "m"] \\
 & K_1 \cap K_2 \arrow[d, dash, "d"] & \\
 & F &
\end{tikzcd}.$$

Now let $d = [K_1 \cap K_2 : F]$. Then we have $n_1 = n/d, m_1 = m/d$, and we have $n_2 \leqslant m_1$, and $m_2 \leqslant n_1$. Then we have $K_1K_2 = n_2n \leqslant m_1n = \frac{mn}{d}$. If they have nontrival intersection, then the degree of this extension will be strictly less than mn.

Monday, March 19th

Remark 13.39. So what is the difference between $F(\alpha)$ and $F[\alpha]$? Note:

$$\begin{gathered} F(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)} : p, q \in F[x] \right\}. \\ F[\alpha] = \{ p(\alpha) : p \in F[x] \} \cong F[x]/(m_{\alpha,F}). \end{gathered} \tag{13.9}$$

If α is algebraic over F, then $F(\alpha) \cong F[\alpha]$.

If E/K, K/F are finite, then E/F is finite, and we have $[E : F] = [E : K][K : F]$. Recall $[K : F] = \dim_F K$. We have:

$$\begin{tikzcd}
E \arrow[d, dash, "m"] \arrow[dd, dash, bend right=60, "mn"'] \\
K \arrow[d, dash, "n"] \\
F
\end{tikzcd}.$$

Note if $F \subseteq K_1, K_2 \subseteq K$, $K_1/F, K_2/F$ are finite, then the composite K_1K_2/F is finite. Observe:

$$\begin{tikzcd}
& K_1K_2 & \\
K_1 \arrow[ur, dash, "\leqslant m"] & & K_2 \arrow[ul, dash, "\leqslant n"'] . \\
& F \arrow[ul, dash, "n"] \arrow[ur, dash, "m"'] &
\end{tikzcd}$$

Remark 13.40. We have $K_1K_2 = K_1(K_2) = K_1[K_2]$ where this last equality holds if they are finite.

Example 13.41. (1) Observe:

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt{2}, \sqrt{3}) & \\
Q(\sqrt{2}) \arrow[ur, dash, "2"] & & \mathbb{Q}(\sqrt{3}) \arrow[ul, dash, "2"'] . \\
& \mathbb{Q} \arrow[ul, dash, "2"] \arrow[ur, dash, "2"'] &
\end{tikzcd}$$

Note $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = Q(\sqrt{2}, \sqrt{3})$. And $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$, and $\sqrt{3}$ is a root of $x^2 - 3$. And $x^2 - 3 = m_{\sqrt{3}, \mathbb{Q}(\sqrt{2}}$.

Note $\mathbb{Q}(\sqrt{2}) = \left\{ a + b\sqrt{2} : a, b \in \mathbb{Q} \right\}$.

(2) Consider $\mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2})$.

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt[4]{2}, \sqrt[6]{2}) \arrow[dr, "2"] & \\
\mathbb{Q}(\sqrt[4]{2}) \arrow[ur, dash, "3"] & & \mathbb{Q}(\sqrt[6]{2}) \\
& \mathbb{Q}(\sqrt{2}) \arrow[ul, dash, "2"] \arrow[ur, dash, "3"'] \arrow[d, dash, "2"] & . \\
& \mathbb{Q} &
\end{tikzcd}$$

Note $x^6 - 2 = m_{\sqrt[6]{2}, \mathbb{Q}}$. The minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}(\sqrt{2})$ is $m_{\sqrt[4]{2}, \mathbb{Q}(\sqrt{2})} = x^2 - \sqrt{2}$. Now we have:

$$m_{\sqrt[6]{2}, \mathbb{Q}(\sqrt[4]{2})}(x) = x^3 - (\sqrt[4]{2})^2 = x^3 - \sqrt{2}.$$

Note:

$$\frac{2^{\frac{1}{4}}}{2^{\frac{1}{6}}} = 2^{\frac{1}{4} - \frac{1}{6}} = 2^{\frac{1}{12}}.$$

Remark 13.42. If the degree of the element is the same as the degree of the extension then the element generates the extension.

Remark 13.43. Note $\mathbb{Q}(\sqrt[6]{2}) = \mathbb{Q}(\sqrt[6]{2}, \sqrt{2})$.

So we have $x^6 - 2 = (x^3 - \sqrt{2})(x^3 + \sqrt{2})$. And:

$$x^3 - \sqrt{2} = m_{\sqrt[6]{2},\mathbb{Q}(\sqrt{2})} = m_{\sqrt[6]{2},\mathbb{Q}(\sqrt[4]{2})}.$$

The difference between this example and the last one is that they have a common subfield or something.

(3) Consider $\omega = e^{2\pi i/3} = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$. So we have $\omega^3 = 1$, a primitive 3rd root of unity.

We have $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3})$. And we have $\sqrt{-3} = \sqrt{3}i$ and:

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt[3]{2},\omega) \arrow[dl, dash, "2"'] \arrow[dr, "2"] & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[dr, dash, "3"'] & & \mathbb{Q}(\omega\sqrt[3]{2}) . \\
& \mathbb{Q} \arrow[ur, dash, "3"'] &
\end{tikzcd}$$

And so the min. polynomial is $x^3 - 2$. Now their intersection is trivial, and they have no subextension...? When we adjoin one of these elements, the minimal polynomial of the other extension simplifies? When in the original field $\mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2})$ when we adjoin $\sqrt[3]{2}$ then the minimal polynomial of $\omega\sqrt[3]{2}$ is no longer $x^3 - 2$. Note it is $x^3 - 2$ over $\mathbb{Q}$. But over $\mathbb{Q}(\sqrt[3]{2})$, we know:

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2} + \sqrt[3]{4}).$$

And this factor on the right is the min polynomial of $\omega\sqrt[3]{2}$ over $\mathbb{Q}(\sqrt[3]{2})$. Note the total degree in this case is 6, but it is not true that the degree of this divides mn, not true in general. Do we have some systematic method to determine the minimal polynomial? How do we know we can split as in the above example? There is a systematic way, there is an algorithm, it is a linear algebra problem. But it's too computational or something. Why do we use radicals? We use them because we have nice notation for them, we can write $\sqrt[3]{2}$ is the root of $x^3 - 2$. There is nothing special about these polynomials. They are just used for convenience.

(4) We give an example of a tower which is not a composite. Consider:

$$\begin{tikzcd}
\mathbb{Q}(\sqrt[5]{\sqrt{2} + \sqrt[3]{3}}) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) . \arrow[d, dash] \\
\mathbb{Q}
\end{tikzcd}$$

Why is the middle element algebraic? This is because $\mathbb{Q}(\sqrt{2} + \sqrt[3]{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, and we have:

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & & \mathbb{Q}(\sqrt[3]{3}) \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd} .$$

We have $x^5 - (\sqrt{2} + \sqrt[3]{3})$.

Definition 13.44. An extension K/F is **algebraic** if $\forall \alpha \in K$, α is algebraic over F.

Remark 13.45. If K/F is finite, then it is algebraic (since $\forall \alpha \in K$, $F(\alpha)/F$ is finite.

Remark 13.46. The converse is not true, we may have algebraic but not finite field extensions.

Lemma 13.47. *If K/F is algebraic and finitely generated, then it is finite.*

Proof. Let $K = F(\alpha_1, ..., \alpha_n)$ where each α_i is algebraic over F. Then K is a tower of finite extensions:

$$K = F(\alpha_1, ..., \alpha_n)/F(\alpha_1, ..., \alpha_{n-1})/.../F(\alpha_1)/F.$$

So it is finite.

Proposition 13.48. *A tower, or a composite, of algebraic extensions is algebraic.*

Proof. We know that this is true for finite extensions (why?) but algebraic are not the same as finite. But almost the same. Let $E/K, K/F$ be algebraic. Let $\alpha \in E$. We want to show that is algebraic over F as well. Then $f(\alpha) = 0$ for some $f \in K[x]$. Then α satisfies some polynomial over K. Let $L = F(\beta_1, ..., \beta_n)$ where β_i are the coefficients of f. Note f is nonzero. Then L/F is finite, α is algebraic over L, $L(\alpha)/F$ is finite, so $L(\alpha)/F$ is finite, so α is algebraic over F. Note $L \subseteq K$. So E is algebraic over F. □

Let $K_1/F, K_2/F$ be algebraic. Want to prove K_1K_2/F is algebraic. Let $\alpha \in K_1K_2$. Then:

$$\alpha = \frac{f(\beta_1, ..., \beta_n, \gamma_1, ..., \gamma_m)}{g(\beta_1, .., \beta_n, \gamma_1, ..., \gamma_m)}, f, g \in F[x_1, ..., x_{n+m}], \beta_i \in K_1, \gamma_i \in K_2.$$

Thus $\alpha \in F(\beta_1, ..., \beta_n, \gamma_1, ..., \gamma_m)$ - finite extension of F. so α is algebraic over F, so K_1K_2 is algebraic over F. □

Tuesday, March 20th

We review the big proof we did in class yesterday. We proved that if $E/K, K/F$ are algebraic, then E/F is algebraic. And we also proved that if $K_1, K_2 \subseteq K$, and $K_1/F, K_2/F$ are algebraic, then K_1K_2/F is algebraic.

Remark 13.49. If $\alpha, \beta \in K$ are algebraic over F, then $\alpha + \beta, \alpha\beta, \alpha/\beta$ are also algebraic over F. $(\alpha + \beta, \alpha\beta, \alpha/\beta \in F(\alpha, \beta) = F(\alpha)F(\beta))$

Remark 13.50. Let K/F be an extension. Let:

$$E = \{ \alpha \in K : \alpha \text{ is algebraic over } F \}.$$

Then E is a field, E/F is algebraic (the maximal algebraic subextension of K/F), and $|forall \alpha \in K \setminus E$, α is transcendental over E. Note that it is transcendental over F by definition. Every element that is not in E is transcendental over E since if α is transcendental over E, then $E(\alpha)/E/F$ is a tower of algebraic extensions, so α is algebraic over F, so $\alpha \in E$. Note of course every element of F is of course algebraic over F, since we can write $x - \alpha$. Elements of F are exactly algebraic elements of degree 1 since we can use a linear polynomial.

Note we cannot factorize fields. But we can say that K/E is transcendental in the sense that all elements are transcendental. It has no algebraic torsions.

So, $\sqrt{2} + \sqrt[3]{3}$, $\sqrt[5]{\sqrt{2} + \sqrt[3]{3}} + 2\sqrt[4]{5}$ is algebraic over $\mathbb{Q}$ since anything we can construct with algebraic elements is algebraic.

Note if α is a root of $x^3 + \beta x^2 + \gamma x + 2$, where β is a root of $x^5 - 3x^2 + 1$, and γ is a root of $x^2 + x + 1$, then α is algebraic over $\mathbb{Q}$. If you use algebraic elements of the field as coefficients of your polynomial, then the roots of the polynomial are also algebraic.

Remark 13.51. Algebraic elements generate extensions of finite degree.

How to find the minimal polynomial? First we need some finite extension where this element lives, say $\sqrt{2} + \sqrt[3]{3} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{3})$, which is a 6-dimensional vector space over $\mathbb{Q}$, with basis $\{ 1, \sqrt{2}, \sqrt[3]{3}, \sqrt{2}\sqrt[3]{3}, \sqrt[3]{9}, \sqrt{2}\sqrt[3]{9} \}$. We have:

$$\begin{tikzcd}
 & \mathbb{Q}(\sqrt{2}, \sqrt[3]{3}) \arrow[dl, dash, "3"'] \arrow[dr, dash, "2"] & \\
Q(\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt[3]{3}) \arrow[dl, dash, "3"] \\
 & \mathbb{Q} &
\end{tikzcd}.$$

Let α be algebraic, $\alpha \in K$, K/F finite. Then α acts on K by multiplication, $\beta \mapsto \alpha\beta$, and this is a linear transformation of K as an F-vector space.

The whole space is a direct sum of minimal α-invariant cyclic subspaces.

So note $F(\alpha)$ is α-invariant. And $\forall \beta \in K$, $\beta F(\alpha)$ is α-invariant. If $\{ 1, \beta_1, ..., \beta_k \}$ is a basis of K over $F(\alpha)$, then:

$$K = F(\alpha) \oplus \beta_1 F(\alpha) \oplus ... \oplus \beta_k F(\alpha).$$

This is the decomposition of K into α-invariant subspaces. And each of these subspaces is cyclic. Note the basis of K/F is $\{ 1, \alpha, ..., \alpha^{n-1}, \beta_1, \beta_1\alpha, ..., \beta_1\alpha^{n-1}, ... \}$.

Definition 13.52. And $F(\alpha)$ is α-cyclic: the basis in $F(\alpha)$ is $1, \alpha, ..., \alpha^{n-1}$ where $N = \deg_F \alpha$.

Definition 13.53. Recall that a vector space V is T-cyclic if $\exists u \in V$ s.t. $\{ u, Tu, ..., T^{n-1}u \}$ is a basis in V.

Also, $\beta_i F(\alpha)$ is α-cyclic for any i. And so this is the decomposition of K into cyclic, α-invariant subspaces. If we consider α as a linear transformation, then the minimal polynomial is simply the minimal polynomial of α.

LEMMA 13.54. *The minimal polynomial is the minimal polynomial of the linear transformation $T(\beta) = \alpha\beta$.*

PROOF. Note $m_{\alpha,F}$ is the minimal polynomial of α over F. Then $m_{\alpha,F}(\alpha)\beta = 0 \ \forall\beta$, so T satisfies $m_{\alpha,F}(T) = 0$. And $\forall f \in F[x]$ with degree $< n$, we know $f(T) \neq 0$, since $f(\alpha) \neq 0$. So $f(\alpha) = f(T)1 \neq 0$. So $m_{\alpha,F}$ is the minimal polynomial of T.

Simpler proof:

$$\begin{aligned} f(T)\cdot 1 &= f(\alpha) \\ f(T)\beta &= f(\alpha)\beta, \forall\beta \\ \Rightarrow f(T) = 0 &\Leftrightarrow f(\alpha) = 0. \end{aligned} \tag{13.10}$$

□

REMARK 13.55. The rational canonical form of T is:

$$A = \begin{pmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \ddots & \\ 0 & & & \boxed{A_k} \end{pmatrix},$$

where all blocks are identical, they are equal to the companion matrix of $m_{\alpha,F}$.

REMARK 13.56. The characteristic polynomial of T is $m_{\alpha,F}^{k+1}$ where $k+1 = [K : F(\alpha)]$, so $K = F(\alpha)$ if and only if the characteristic polynomial is equal to the minimal polynomial.

EXAMPLE 13.57. $\alpha = \sqrt{2} + \sqrt{3}$. We have $\alpha^2 = 5 + 2\sqrt{6}$ and $(\alpha^2 - 5)^2 = 24$. Then we have $\alpha^4 - 10\alpha^2 + 1 = 0$. So is $x^4 - 10x^2 + 1$ the min poly?

Consider $V = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a $\mathbb{Q}$-vector space. Basis is $\{\, 1\sqrt{2}, \sqrt{3}, \sqrt{6}\,\}$. Define $T(\beta) = \alpha\beta$, $T : V \to V$. We have:

$$\begin{tikzcd} & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\ Q(\sqrt{2}) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\sqrt{3}) \arrow[dl, dash, "2"] . \\ & \mathbb{Q} & \end{tikzcd}$$

The basis of $\mathbb{Q}(\sqrt{2})$ is $\{\, 1, \sqrt{2}\,\}$ and basis of $\mathbb{Q}(\sqrt{3})$ is $\{\, 1, \sqrt{3}\,\}$. Note all elements of $\mathbb{Q}(\sqrt{2})$ are of the form $a + b\sqrt{2} \overset{?}{=} \sqrt{3}$. But then we would have $(a + b\sqrt{2})^2 = 3$ but this has no rational solution. Note the product of the basis elements are always a spanning set. And now we map:

$$\begin{aligned} 1 &\mapsto \sqrt{2} + \sqrt{3} \\ \sqrt{2} &\mapsto 2 + \sqrt{6} \\ \sqrt{3} &\mapsto \sqrt{6} + 3 \\ \sqrt{6} &\mapsto 2\sqrt{3} + 3\sqrt{2}. \end{aligned} \tag{13.11}$$

Thus the matrix of T is:

$$\begin{pmatrix} 0 & 2 & 3 & 0 \\ 1 & 0 & 0 & 3 \\ 1 & 0 & 0 & 2 \\ 0 & 1 & 1 & 0 \end{pmatrix}.$$

We're doing something, I don't know what it is. We have $1, \alpha, \alpha^2, \alpha^3$. We have:

$$\begin{aligned} \alpha &= \sqrt{2} + \sqrt{3} \\ \alpha^2 &= 5 + 2\sqrt{6} \\ \alpha^3 &= 5\sqrt{2} + 5\sqrt{3} + 6\sqrt{2} + 4\sqrt{3} \\ &= 11\sqrt{2} + 9\sqrt{3}. \end{aligned} \tag{13.12}$$

So we have:

$$\begin{pmatrix} 1 & 0 & 5 & 0 \\ 0 & 1 & 0 & 11 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 2 & 0 \end{pmatrix}.$$

And the rows are linearly independent. So V is α-cyclic, so $\deg_{\mathbb{Q}} \alpha = 4$.

Recall we had this direct summand form and we proved that minimal polynomial equivalence using that.

Pronunciation guide: `vee-ECK-tor`.

Consider $\beta = \sqrt{6}$ and then $\mathbb{Q}(\beta) \neq V$ because something is 2-dimensional, dunno why or what. The matrix has two blocks or something. The RCF is:

$$\left(\begin{array}{cc|cc} 0 & 6 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 \end{array}\right).$$

Definition 13.58. conjugate!elements Let K/F be an algebraic extension, and let $\alpha_1, \alpha_2 \in K$, and let $m_{\alpha_1,F} = m_{\alpha_2,F}$. α_1, α_2 are called **conjugate**.

Remark 13.59. Then $F(\alpha_1) \cong F[x]/(f) \cong F(\alpha_2)$.

Example 13.60.
(1) $i, -i$ are conjugate over $\mathbb{R}$ (and $\mathbb{Q}$). Minimal polynomial is $x^2 + 1$. $\pm\sqrt{a}$ are conjugate.
(2) $\sqrt[3]{3}$, $\sqrt[3]{3}\omega$, $\sqrt[3]{3}\omega^2$ are conjugate over $\mathbb{Q}$ where $\omega = e^{2\pi i/3}$.

Wednesday, March 21st

Methods of finding $m_{\alpha,F}$ We discuss several methods to find the minimal polynomial. We have at least five. Let $\alpha = \sqrt{2} + \sqrt{3}$.

(1) Find f such that $f(\alpha) = 0$ and prove that f is irreducible.
(2) Find f s.t. $f(\alpha) = 0$ and prove that $\deg f = \deg_F \alpha$. How do we find this? Either guess, or use $\deg_F \alpha = \dim \mathit{span}\left\{ 1, \alpha, \alpha^2, \dots \right\}$.
(3) Find the matrix of $Tu = \alpha u$ in some basis, find the Smith form, and find the minimal polynomial of T.
(4) Find the matrix of T, find the characteristic polynomial c_T, and there is a good chance that this is the minimal polynomial, and if not, we proved yesterday that it is a power of the minimal polynomial. Represent $c_T = f^*$ where f is irreducible, then $f = m_{\alpha,F}$. If c_T is irreducible, then it is also m_T.
(5) This is the easiest way: find powers of α in some basis, and find the minimal linear relations between them.

Example 13.61. We apply method 5 to α. $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and basis is $\left\{ 1, \sqrt{2}, \sqrt{3}, \sqrt{6} \right\}$. We have:

$$1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \alpha = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \end{pmatrix}, \alpha^2 = \begin{pmatrix} 5 \\ 0 \\ 0 \\ 2 \end{pmatrix}, \alpha^3 = \begin{pmatrix} 0 \\ 11 \\ 9 \\ 0 \end{pmatrix}, \alpha^4 = \begin{pmatrix} 49 \\ 0 \\ 0 \\ 20 \end{pmatrix}. \tag{13.13}$$

We have:

$$\alpha^2 = (\sqrt{2} + \sqrt{3})(\sqrt{2} + \sqrt{3}) = 5 = 2\sqrt{6}.$$

Solve the equation $\alpha^4 = x_1 + x_2\alpha + x_3\alpha^2 + x_4\alpha^3$. We have:

$$\begin{cases} x_1 + 5x_3 = 49 \\ x_2 + 11x_4 = 0 \\ x_2 + 9x_4 = 0 \\ 2x_3 = 20 \end{cases}.$$

So we have $x_2 = x_4 = 0$, $x_3 = 10, x_1 = -1$. Then we have $m_{\alpha,F} = x^4 - 10x^2 - 1$.

Remark 13.62. Something something look at this:

$$K = F(\alpha) \oplus F(\alpha)\beta_1 \oplus \cdots \oplus F(\alpha)\beta_k.$$

And all the companion matrices are identical.

Example 13.63. let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$, and let $\beta = \sqrt{6}$. Matrix of β is:

$$\begin{pmatrix} 0 & 0 & 0 & 6 \\ 0 & 0 & 3 & 0 \\ 0 & 2 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}.$$

We have:

$$\begin{aligned} 1 &\mapsto \sqrt{6} \\ \sqrt{2} &\mapsto 2\sqrt{3} \\ \sqrt{3} &\mapsto 3\sqrt{2} \\ \sqrt{6} &\mapsto 6. \end{aligned} \tag{13.14}$$

The characteristic polynomial is $(x^2-6)^2$. And $m_{\beta,\mathbb{Q}} = x^2-6$. Smith form is:

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & x^2-6 & \\ & & & x^2-6 \end{pmatrix}.$$

Now we continue with theory.

Definition 13.64. $\alpha_1, \alpha_2 \in K$ are **conjugate** over $F \subseteq K$ if $m_{\alpha_1,F} = m_{\alpha_2,F}$. In this case, $F(\alpha_1) \cong F(\alpha_2)$ under the isomorphism φ s.t. $\varphi|_F = Id_F$, $\varphi(\alpha_1) = \varphi(\alpha_2)$. Note:

$$\begin{aligned} F(\alpha_1) \cong F[x]/(f) \cong F(\alpha_2) \\ \alpha_1 \leftrightarrow x \mod f \leftrightarrow \alpha_2. \end{aligned} \tag{13.15}$$

Remark 13.65. Any α has at most $\deg_f \alpha = \deg m_{\alpha,F}$ conjugates, counting itself.

Remark 13.66. Let $f \in F[x]$ be irreducible. If K/F is an extension, $\alpha \in K$, $f(\alpha) = 0$, then $f = m_{\alpha,F}$, since it is irreducible, and $m_{\alpha,F}|f$.

If $K_1/F, K_2/F$, $\alpha_1 \in K_1, \alpha_2 \in K_2$, and $f(\alpha_1) = f(\alpha_2) = 0$, then still $F(\alpha_1) \cong F(\alpha_2)$ under isomorphism that is identical on F and that maps $\alpha_1 \to \alpha_2$ for the same reason as above. We have:

$$\begin{tikzcd} \alpha_1 \arrow[rr, leftrightarrow] & & \alpha_2 \\ F(\alpha_1) \arrow[rr, "\cong"] & & F(\alpha_2) \; . \\ & F \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Definition 13.67. If $f \in F[x]$ is irreducible, α is a root of f in some extension K of F, then $F(\alpha)$ is **obtained by adjoining a root of f.**

Remark 13.68. Such an extension always exists, it is $K = F[x]/(f)$. (Then $K = F(\alpha)$.

If we start with an abstract field, how do we know there exists a larger field which contains a root of an irreducible polynomial?

In K, $f(\overline{x}) = \overline{f(x)} = 0$ where $\overline{x} = x \mod f$.

Example 13.69.

(1) $F = \mathbb{R}, f = x^2+1$. Define $K = \mathbb{R}[x]/(x^2+1)$. Put $\alpha = \overline{x} \in K$. Then:

$$\alpha^2 + 1 = \overline{x}^2 + 1 = \overline{x^2+1} = 0.$$

Then $K = F(\alpha)$.

(2) $F = \mathbb{Q}$, $f = x^3-2$, put $K = \mathbb{R}[x]/(x^3-2)$. Then $\alpha = \overline{x} \in K$.

If f is reducible, decompose it into irreducible components: $f = f_1 \cdots f_k$. Then adjoin a root α of f_1, then $f(\alpha) = 0$. But now the result depends on our choice of irreducible. They will be different fields.

Remark 13.70. So the operation of "adjoining a root of f" is not a well-defined operation.

Lemma 13.71. *Let $\varphi : F_1 \to F_2$ be an isomorphism, let $f_1 \in F_1[x]$, $f_2 \in F_2[x]$ be such that $\varphi(f_1) = f_2$. φ applies to coefficients of f_1 and transforms into f_2. Also assume that they are irreducible. Let α_1 be a root of f_1 and α_2 be a root of f_2, in some larger fields, not in this field, since they are irreducibe $\Rightarrow$ they don't have roots in this field. Then φ extends to an isomorphism $F_1(\alpha_1) \overset{\cong}{\to} F_2(\alpha_2)$ such that $\varphi(\alpha_1) = \alpha_2$. And:*

$$\begin{tikzcd}
F_1(\alpha_1) \arrow[r, "\varphi"] & F_2(\alpha_2) \\
F_1 \arrow[r, "\varphi"] \arrow[u, leftrightarrow] & F_2 \arrow[u, leftrightarrow]
\end{tikzcd}$$

is commutative.

Proof. Note $F_1[x] \overset{\varphi}{\to} F_2[x]$ is given by $\varphi((f_1)) = (f_2)$. So:

$$F_1(\alpha_1) \cong F_1[x]/(f_1) \overset{\cong}{\to} F_2[x]/(f_2) \cong F_2(\alpha_2),$$

and this is given by $\alpha_1 \leftrightarrow \overline{x} \leftrightarrow \alpha_2$. □

13.2 Exercises

3. *Find the minimal polynomial of $\alpha = 1 + i$ over $\mathbb{Q}$.*

Note $\alpha^2 = 1 - 1 + 2i = 2i$. And $\alpha^4 = -4$, so $\alpha^4 + 4 = 0$. So $m_\alpha = x^4 + 4$? I don't think so, because α belongs to $\mathbb{Q}(i)$, which has degree 2, so α has degree at most 2. So that is not the minimal polynomial, it must be reducible. Try again. Write $(\alpha - 1)^2 = i^2 = -1$, so $\alpha^2 - 2\alpha + 1 = -1$, so $\alpha^2 - 2\alpha + 2 = 0$. So $m_\alpha = x^2 - 2x + 2$. We can see it's irreducible since it has no roots in $\mathbb{Q}$.

Desmond: $\mathbb{Q}$ is in general, kind of a comfortable field. If we're in a less familiar field, is there a systematic way to find the minimal polynomial?

Leibman: There are algorithms, you must be able to make computations. There are some algorithms, I am not sure.

4. *Find $\deg_{\mathbb{Q}} \alpha$ for $\alpha_1 = 2 + \sqrt{3}$ and $\alpha_2 = 1 + \sqrt[3]{2} + \sqrt[3]{4}$.*

Note $\alpha_1 \in \mathbb{Q}(\sqrt{3})$ - deg 2, so $\deg_{\mathbb{Q}} \alpha_1 = 2$. Again the degree of the root must divide the degree of the extension. $\alpha_2 \in \mathbb{Q}(\sqrt[3]{2})$ - degree 3, so $\deg_{\mathbb{Q}} \alpha_2 = 3$.

Remark 13.72. The degree of the root divides the degree of the extension.

5. *$F = \mathbb{Q}(i)$. Prove that $x^3 - 2$ is irreducible over F.*

Proof. Find the roots and see that none of them are in F. It is easy. There is a simpler argument based on the degree. The root of the polynomial must be of degree 3, but the extension has degree 2, so the element cannot belong to $F = \mathbb{Q}(i)$. □

6. *Prove that $F(\alpha_1, ..., \alpha_n) = F(\alpha_1)...F(\alpha_n)$.*

Proof. This should be easy, and obvious, if a field contains blank and all blank then it must contain blank′. □

8. *Let F be a field of characteristic $\neq 2$. Let D_1 and D_2 be elements of F, neither of which is a square in F. Prove that $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 4 over F if $D_1 D_2$ is not a square in F and is of degree 2 over F otherwise. When $F(\sqrt{D_1}, \sqrt{D_2})$ is of degree 4 over F, the field is called a* ***biquadratic extension of*** *F.*

Proof. Assume $D_1 D_2$ is not a square. Suppose $\sqrt{D_1}, \sqrt{D_2}$ are linearly dependent. Then we have $\sqrt{D_1} = \alpha\sqrt{D_2} + \beta$ for some $\alpha, \beta \in F$. Suppose for contradiction that $\beta = 0$. Then we have:

$$\begin{aligned} \sqrt{D_1} &= \alpha\sqrt{D_2} \\ D_1 &= \alpha^2 D_2 \\ D_1 D_2 &= \alpha^2 D_2^2. \end{aligned} \tag{13.16}$$

But we said $D_1 D_2$ is not a square, so we have a contradiction, so we must have that $\beta \neq 0$. And $\alpha \neq 0$ since otherwise $\sqrt{D_1} \in F \Rightarrow D_1$ is a square in F.

Then:

$$D_1 = (\alpha\sqrt{D_2} + \beta)^2 = \alpha^2 D_2 + 2\alpha\beta\sqrt{D_2} + \beta^2,$$

and since we are over a field of characteristic $\neq 2$, we know that $2 \neq 0 \Rightarrow 2\alpha\beta \neq 0$, so we must have that $\sqrt{D_2} \in F$ which means that D_2 is a square in F, contradiction, so $\sqrt{D_1}, \sqrt{D_2}$ must be linearly independent over F. Thus $m_{\sqrt{D_1}, F(\sqrt{D_2}} = x^2 - D_1$, and so the degree of $F(\sqrt{D_1}, \sqrt{D_2})$ over $F(\sqrt{D_2})$ is 2. Since D_2 is not a square in F, we know $m_{\sqrt{D_2}, F} = x^2 - D_2$, which as degree 2, so $F(\sqrt{D_2})$ has degree 2 over F, and note these are both finite extensions. Recall that if E/K, K/F are finite, then E/F is finite, and we have $[E : F] = [E : K][K : F]$. So $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 4$.

If $D_1 D_2$ is a square, we would have $\sqrt{D_1}\sqrt{D_2} = a$ for some integer a. Thus $\sqrt{D_1} = \frac{a}{\sqrt{D_2}}$, and so $F(\sqrt{D_1}, \sqrt{D_2}) = F(\sqrt{D_2})$. Then we showed $F(\sqrt{D_2})$ has degree 2 over F, so $[F(\sqrt{D_1}, \sqrt{D_2}) : F] = 2$. □

9. *Let F be a field of characteristic $\neq 2$. Let a, b be elements of the field F with b not a square in F. Prove that a necessary and sufficient condition for $\sqrt{a + \sqrt{b}} = \sqrt{m} + \sqrt{n}$ for some m and n in F is that $a^2 - b$ is a square in F. Use this to determine when the field $\mathbb{Q}(\sqrt{a + \sqrt{b}})(a, b \in \mathbb{Q})$ is biquadratic over $\mathbb{Q}$.*

Proof. Let $a^2 - b$ be a square in F. Then:

$$\left(\sqrt{a + \sqrt{b}}\right)^2 \left(\sqrt{a - \sqrt{b}}\right)^2 = (a + \sqrt{b})(a - \sqrt{b}) = a^2 - b = c^2, \tag{13.17}$$

for some $c \in F$. Then we have $\sqrt{a^2 - b} \in F$. Define $m = \frac{a + \sqrt{a^2 - b}}{2}$ and $n = \frac{a - \sqrt{a^2 - b}}{2}$, which are well defined since we said the characteristic of our field is not 2. Then we have:

$$\begin{aligned} m &= \frac{2a + 2\sqrt{a^2 - b}}{4} \\ &= \frac{(a + \sqrt{b}) + 2\sqrt{a^2 - b} + (a - \sqrt{b})}{4} \\ &= \left(\frac{\sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}}}{2} \right)^2 \\ \Rightarrow \sqrt{m} &= \frac{\sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}}}{2}. \end{aligned} \tag{13.18}$$

Similarly, we have:

$$\sqrt{n} = \frac{\sqrt{a + \sqrt{b}} - \sqrt{a - \sqrt{b}}}{2} \tag{13.19}$$

Thus:

$$\sqrt{m} + \sqrt{n} = \frac{\sqrt{a + \sqrt{b}} + \sqrt{a - \sqrt{b}}}{2} + \frac{\sqrt{a + \sqrt{b}} - \sqrt{a - \sqrt{b}}}{2} = \sqrt{a + \sqrt{b}}. \tag{13.20}$$

So we have shown the claim holds in the first direction.

Assume we have the following:

$$\begin{aligned} \sqrt{a + \sqrt{b}} &= \sqrt{m} + \sqrt{n} \\ a + \sqrt{b} &= m + n + 2\sqrt{mn}. \end{aligned} \tag{13.21}$$

Now we claim we must have $a = m + n$ and $b = 4mn$. Suppose $\sqrt{b} = c + 2\sqrt{mn}$ for some $c \in F$. Then $b = c^2 + 4c\sqrt{mn} + 4mn$. Since $\text{char}F \neq 2$, and $b \in F$, we know we must have either $\sqrt{mn} \in F$, or $c = 0$. If $\sqrt{mn} \in F$, then $\sqrt{b} \in F$, which means b is a square, contradiction. So we must have $c = 0$, thus the claim holds. Then we have:

$$\begin{aligned} a^2 - b &= (a + \sqrt{b})(a - \sqrt{b}) \\ &= (m + n + 2\sqrt{mn})(m + n - 2\sqrt{mn}) \\ &= m^2 + mn - 2m\sqrt{mn} + mn + n^2 - 2n\sqrt{mn} + 2m\sqrt{mn} + 2n\sqrt{mn} - 4mn \\ &= m^2 + n^2 - 2mn \\ &= (m - n)^2. \end{aligned} \tag{13.22}$$

Thus if $a^2 - b$ is a square, then we have:

$$\mathbb{Q}(\sqrt{a + \sqrt{b}}) = \mathbb{Q}(\sqrt{m} + \sqrt{n}) = \mathbb{Q}(\sqrt{m}, \sqrt{n}). \tag{13.23}$$

Clearly the degree is either 2 or 4, but if it is 2, then we would have $m = n$ which would give us b is a square, contradiction, so the degree is 4. So $\mathbb{Q}(\sqrt{a + \sqrt{b}})$ is biquadratic. □

10. *Find the degree of the extension.* $K = \mathbb{Q}(\sqrt{3 + 2\sqrt{2}})$. *What is* $[K : \mathbb{Q}]$*?*

    We have:

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{3+2\sqrt{2}}) \arrow[d, dash, "2"] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"] \\
\mathbb{Q}
\end{tikzcd}\quad .$$

Note it is tempting to say that the degree is 4, but this is false since $\alpha = (1+\sqrt{2})^2 = 3+2\sqrt{2}$. So $\sqrt{\alpha} = 1+\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. So when we adjoin the root of α we do nothing, it is already in $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\sqrt{3+2\sqrt{2}})$.

12. *K/F, $[K : F] = p$ - prime. Then there exist no proper nontrivial subextensions: $K/E/F \Rightarrow E = K$ or $E = F$.*

 Proof. $[E : F] | [K : F]$, so $= 1$ or p. □

13. *Suppose $F = \mathbb{Q}(\alpha_1, \alpha_2, ..., \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for $i = 1, 2, ..., n$. Prove that $\sqrt[3]{2} \notin F$.*

 Proof. Since these roots are all quadratic, we know that the degree of $\mathbb{Q}(\alpha_i)$ over $\mathbb{Q}(\alpha_1, ..., \alpha_{i-1})$ is at most 2, and if α_i is generated by $\alpha_1, ..., \alpha_{i-1}$ then the degree is 1. Thus these are all finite extensions, and then by induction, we know that $F/\mathbb{Q}$ has finite degree, and it's degree is the product of all the extensions $\mathbb{Q}(\alpha_i)/\mathbb{Q}(\alpha_1, ..., \alpha_{i-1})$. Since these are all 1 or 2, we know $[F : \mathbb{Q}] = 2^k$ for some integer positive integer k (positive since the first extension has degree 2 over $\mathbb{Q}$). But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, and if $\sqrt[3]{2} \in F$, then we would have $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] | 2^k$, which is not the case. Thus $\sqrt[3]{2} \notin F$. □

14. *Prove that $[F(\alpha) : F]$ is odd $\Rightarrow F(\alpha) = F(\alpha^2)$.*

 Proof. We have:

$$\begin{tikzcd}
F(\alpha) \arrow[d, dash, "1 \text{ or } 2"] \arrow[dd, dash, bend right, "odd"'] \\
F(\alpha^2) \arrow[d, dash] \\
F
\end{tikzcd}\quad .$$

In the middle thing, α is a root of $x^2 = \alpha^2$. $2 \nmid [F(\alpha) : F]$, so $[F(\alpha) : F(\alpha^2)] = 1$. □

16. *Let K/F be an algebraic extension and let R be a ring contained in K and containing F. Show that R is a subfield of K containing F.*

 Proof. Since K/F is algebraic, we know that $\forall \alpha \in K$, α is algebraic over F. So α is the root of some polynomial $p(x) \in F[x]$. So let $r \in R$, nonzero, we wish to construct an inverse r^{-1} for r.

Then we have:

$$\begin{aligned} p(r) &= a_n r^n + \cdots + a_1 r + a_0 = 0 \\ a_0 &= -a_n r^n - \cdots - a_2 r^2 - a_1 r \\ 1 &= -\frac{a_n}{a_0} r^n - \cdots - \frac{a_2}{a_0} r^2 - \frac{a_1}{a_0} r \\ \frac{1}{r} &= -\frac{a_n}{a_0} r^{n-1} - \cdots - \frac{a_2}{a_0} r - \frac{a_1}{a_0}. \end{aligned} \tag{13.24}$$

This is well defined since r is nonzero. Thus we have found r^{-1}, and it is an element of r since $a_i \in F \subseteq R$, and since we have additive and multiplicative closure in R. Thus we have inverses in R and it is a field. □

20. *Show that if the matrix of the linear transformation "multiplication by α" considered in the previous exercise is A then α is a root of the characteristic polynomial of A. This gives an effective procedure for determining an equation of degree n satisfied by an element α in an extension of F of degree n. Use this procedure to obtain the monic polynomial of degree 3 satisfied by $\sqrt[3]{2}$ and by $1 + \sqrt[3]{2} + \sqrt[3]{4}$.*

Proof. Let $c_A = a_n x^n + \cdots + a_1 x + a_0$ be the characteristic polynomial of the matrix A of multiplication by α. Then we know:

$$c_A(A) = a_n A^n + \cdots + a_1 A + a_0 = 0, \tag{13.25}$$

where 0 represents the 0 matrix. Then replacing A with α, we have:

$$c_A(\alpha) = a_n \alpha^n + \cdots + a_1 \alpha + a_0 = 0, \tag{13.26}$$

which makes sense since α must be an eigenvalue of A since $Ar = \alpha r$. So it must be a root by definition. □

Now we find a monic polynomial of degree 3 satisfied by $\sqrt[3]{2}$. We have a basis $\left\{ 1, \sqrt[3]{2}, \sqrt[3]{4} \right\}$. We set $k = \begin{pmatrix} a \\ b \\ c \end{pmatrix}$. We solve for A knowing:

$$\begin{aligned} A \begin{pmatrix} a \\ b \\ c \end{pmatrix} &= \sqrt[3]{2} \begin{pmatrix} a \\ b \\ c \end{pmatrix} \\ &= (\sqrt[3]{2} a + \sqrt[3]{4} b + 2c) \\ \Rightarrow A &= \begin{pmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}. \end{aligned} \tag{13.27}$$

And the characteristic polynomial of A is $x^3 - 2$.

Using the exact same basis, we find that for $\alpha = 1 + \sqrt[3]{2} + \sqrt[3]{4}$,

$$A = \begin{pmatrix} 1 & 2 & 2 \\ 1 & 1 & 2 \\ 1 & 1 & 1 \end{pmatrix} \tag{13.28}$$

Thus the characteristic polynomial is given by $x^3 - 3^2 - 3x - 1$.

SECTION 13.3

Classical straightedge and compass constructions

This section is constructions with a ruler and compass; we will skip it until after we hit Galois theory.

Thursday, April 12th

And we're back. Note this is a straightedge, not a ruler, since we can't measure arbitrary distances with a straightedge. Given a set $S \subseteq \mathbb{R}^2$. We are allowed to:

(1) $\forall s_1, s_2 \in S$, we can connect the line through s_1, s_2.

(2) $\forall s_1, s_2, s_3 \in S$, we can construct a circle centered at s_1 of radius $\text{dist}(s_2, s_3)$. We can find the intersection of any two lines, or a line and a circle, or two circles to produce more points.

Let's try to translate this problem to the analytic level. We introduce coordinates in the plane. If the plane is $\mathbb{R}^2$, then we already have coordinates. Then each point is given by its coordinate. Let F be the field generated by the coordinates of "given" points. What new numbers can we get? We can add numbers, multiply them, subtract them, and divide them, using the legal operations. How do we add two elements of F?

Also, for $x \in F$, $x > 0$, we can construct $\sqrt{x}$. Finally, we can construct all elements of the quadratic closure of F, the minimal field containing and F and closed under $\sqrt{\cdot}$.

Definition 13.73. ELements of this field are called **constructible** (from S) numbers.

Claim. *Only constructible numbers can be constructed using our operations.*

Proof. Setting $y = ax + b$, $a, b \in F$, $y = cx + d$, $c, d \in F$, new point satisfies $ax + b = cx + d$, so $x \in F$. For points on a circle or intersection points of two circles, these solutions are of quadratic equations, so they are contained in a quadratic extensions of F. □

Remark 13.74. A number is constructible (from F) if it is contained in a finite tower of quadratic extensions of F.

Definition 13.75. Call such extensions: $K = K_n / K_{n-1} / \ldots / K_0 = F$ with $[K_{i+1} : K_i] = 2 \ \forall i$ **polyquadratic.**

In particular, if α is constructible, $\deg_F \alpha = 2^k$ for some k.

Example 13.76. (1) Bisection of an angle: is possible.

(2) But a trisection is not possible, generally speaking. Our F is $\mathbb{Q}(\cos\theta, \sin\theta)$, we want $\alpha = \cos(\theta/3)$.

$$\cos\theta = 4\cos^3(\theta/3) - 3\cos(\theta/3) = 4\alpha^3 - 3\alpha. \tag{13.29}$$

So α is a root of $4x^3 - 3x - \cos\theta = f$. If F is irreducible, $\deg_F \alpha = 3$, and α is not constructible. For instance, for $\theta - \pi/3$, $\cos\theta = \frac{1}{2}$, so $f = 4x^3 - 3x - \frac{1}{2}$, so $F = \mathbb{Q}(\sqrt{3})$. So $2f = 8x^3 - 6x - 1$. $y = 2x$, so we have $y^3 - 3y - 1$ is irreducible over $\mathbb{Q}$, over $\mathbb{Q}(\sqrt{3})$? f has no roots in $\mathbb{Q}(\sqrt{3})$ either, so is irreducible over $\mathbb{Q}(\sqrt{3})$.

(3) "Doubling a cube". Construct $\alpha \in \mathbb{R}$ such that $\alpha^3 = 2$. Impossible! α has degree 3 over $\mathbb{Q}$.

(4) "Squaring a circle": construct α such that $\alpha^2 = \pi$. Not solvable over $\mathbb{Q}$, $\sqrt{\pi}$ is not constructible over $\mathbb{Q}$.

Remark 13.77. Any subextension of a polyquadratic extension is polyquadratic, and any composite of such extensions is also polyquadratic.

Proof. If you have:

$$\begin{tikzcd}
K_n = K \supseteq L & & L \\
K_{n-1} \arrow[u, dash] & & L \cap K_{n-1} \arrow[u, dash] \\
\vdots \arrow[u, dash] & \Rightarrow & L \cap K_{n-2} \arrow[u, dash] , \\
K_1 \arrow[u, dash] & & \vdots \arrow[u, dash] \\
F \arrow[u, dash] & & F \arrow[u, dash]
\end{tikzcd}$$

each of the extensions in the right tower is either quadratic or trivial. (No idea why). □

Theorem 13.78. *Given a field $F \subseteq \mathbb{R}$, $\alpha \in R$, is constructible from F if and only if α is contained in a real polyquadratic extension of F (a tower of quadratic extensions).*

$$\begin{tikzcd}
K_n \\
\vdots \arrow[u, dash, "2"'] \\
K_1 \arrow[u, dash, "2"'] \\
F \arrow[u, dash, "2"']
\end{tikzcd} .$$

Remark 13.79. The composite of two polyquadratic extensions is polyquadratic.

Proof.
$$\begin{tikzcd}
K_n & & & L_m \\
\vdots \arrow[u, dash, "2"'] & & \iddots \arrow[ur, dash, "2"] & \\
K_1 \arrow[u, dash, "2"'] & L_1 \arrow[ur, dash, "2"] & & \\
F \arrow[u, dash, "2"'] \arrow[ur, dash, "2"] & & &
\end{tikzcd} .$$

And we get:

$$\begin{tikzcd}
K_nL_m \arrow[d, dash, "\leqslant 2"] & \\
\vdots \arrow[d, dash, "\leqslant 2"] & \\
K_nL_1 \arrow[d, "\leqslant 2"] & \\
K_n \arrow[d, dash, "2"] & . \\
\vdots \arrow[d, dash, "2"] & \\
K_1 \arrow[d, dash, "2"] & \\
F &
\end{tikzcd}$$

So $\forall i$, $[K_nL_{i+1} : K_nL_i] \leqslant [L_{i+1} : L_i] = 2$. So, K_nL_{i+1}/K_nL_i is either trivial or quadratic. □

We are in characteristic 0. So the Galois closure of a polyquadratic extension is polyquadratic.

Remark 13.80. The Galois group of a Galois polyquadratic extensions is a 2-group, since it has order 2^n for some n.

Remark 13.81. Conversely, if K/F is Galois and $\text{Gal}(K/F)$ is a 2-group, then $\text{Gal}(G/F)$ has a normal series.

$$1 = H_0 \lhd H_1 \lhd \cdots H_n = \text{Gal}(K/F), \tag{13.30}$$

with $|H_{i+1} : H_i| = 2$ for all i. So K is a tower of polyquadratic extensions.

Corollary 13.82. *Any subextension of a polyquadratic extension is polyquadratic.*

Proof. We may assume that K is Galois. Let $G = \text{Gal}(K/F)$. Let $L \subseteq K$, let $H = \text{Gal}(K/L)$. Then by Sylow's theorem, there is a sequence:

$$H \lhd H_1 \lhd H_2 \lhd \ldots \lhd G, \tag{13.31}$$

with $H_{i+1} : H| = 2$. So, there exists a tower of subfields $L/K_{n-1}/\ldots/F$ such that $[K_i : K_{i-1}] = 2, \forall i$. □

Definition 13.83. $z = x + iy \in \mathbb{C}$ is **constructible** if x, y are constructible.

Claim. *$z = x + iy \in \mathbb{C}$ is constructible over $F \subseteq \mathbb{R}$ if and only if z is an element of a polyquadratic extension.*

Proof. If z is constructible, then x, y are constructible, so $x \in K_1, y \in K_2$, where K_1, K_2 are polyquadratic extensions of F, so $z \in K_1 K_2(i)$, which is also polyquadratic.

If $z \in K$ polyquadratic, then $\overline{z} \in \overline{K}$. Then $x = \frac{z+\overline{z}}{2}, y = \frac{z-\overline{z}}{2} \in K\overline{K}(i) \cap \mathbb{R}$, which is a real polyquadratic extension of F. So x, y are constructible, so z is constructible. □

Theorem 13.84. *$\alpha \in \mathbb{C}$ is constructible from $F \subseteq \mathbb{R}$ if and only if $\mathrm{Gal}(m_{\alpha,F})$ is a 2-group.*

Example 13.85. Constructions of regular n-gons. $F = \mathbb{Q}$. Equivalently, for which n is $\omega = e^{2\pi i/n}$ constructible? Minimal polynomial is $\Phi_i, \mathrm{Gal}(\Phi_n/\mathbb{Q}) = \mathbb{Z}_n^* hasorder\varphi(n)$.

Remark 13.86. ω is contructible if and only if $\varphi(n) = 2^k$ for some k.

If $N = 2^r p_1^{s_1} \cdots p_l^{s_l}$, then $\varphi(n) = 2^{r-1} p_1^{s_1-1}(p_1 - 1) \cdots p_l^{s_l-1}(p_l - 1)$, so it must be that $s_1 = \cdots = s_l = 1$, and $\forall i$, $p_i - 1$ is a power of 2.

Definition 13.87. **Fermat's primes:** $3, 5, 17, 257, ...$ (they are of the form $2^{2^r} + 1$).

So $3, 6, 12, 10, 20, 30$-gons are constructible, and $7, 9, 22$-gons are not. So we need $n = 2^r p_1 \cdots p_l$, for distinct Fermat primes.

SECTION 13.4
Splitting fields and algebraic closures

Definition 13.88. Let $f \in F[x]$. An extension K/F is a **splitting field of** f if in K, f splits "completely": $f = f_1 \cdots f_k$, where f_i are linear, so $f = c(x - \alpha_1) \cdots (x - \alpha_k)$, and K is the minimal field with this property.

Remark 13.89. For any subfield $E \subsetneq K$, f doesn't split in K. Equivalently, $K = F(\alpha_1, ..., \alpha_k)$.

Theorem 13.90. *$\forall f \in F[x]$, the splitting field of f exists, and is unique up to isomorphism.*

Proof. You take f, if it doesn't split completely, it has nonlinear irreducible component, adjoin roots, you will get a splitting field. Okay, now for the formal proof. Let $f = g_1 \cdots g_m$ where g_i are irreducible. If one of g_i is not linear, adjoin a root α of g_i, then in $F(\alpha)$, $g_i(x) = h_i(x)(x - \alpha)$, $\deg h_i = \deg g_i - 1$, and continue... until all irreducible polynomials are linear. There is more to this proof, it follows from preceeding lemma. □

Note $[F(\alpha) : F] = \deg_F(\alpha) = \deg g_i$.

Behold, a tower:

$$\begin{tikzcd}
F(\alpha_1,...,\alpha_n) \arrow[d, dash] \\
\vdots \arrow[d, dash] \\
F(\alpha_1,\alpha_2) \quad \cdot \arrow[d, dash] \\
F(\alpha_1) \arrow[d, dash] \\
F
\end{tikzcd}$$

Proposition 13.91. *Let $K = F(\alpha_1,...,\alpha_n)$, the splitting field of F,α_i the roots of f, then $[K : F] \leqslant n!$. Note* $\deg f = n$.

Proof. $[F(\alpha_1) : F] \leqslant n$. Over $F(\alpha_1)$, $f = (x-\alpha_1)\tilde{f}$, $\deg \tilde{f} = n-1$, K is the splitting field of $\tilde{f}$ over $F(\alpha_1)$. We have:

$$[K : F] = \deg_F \alpha_1 \cdot \deg_{F(\alpha_1)} \alpha_2 \cdots \deg_{F(\alpha_1,\ldots,\alpha_{n-1})} \alpha_n.$$

We know $\deg_F \alpha_1 \leqslant n$, and $\deg_{F(\alpha_1)} \alpha_2 \leqslant n-1$, and so on. By induction, $[K : F(\alpha_1)] \leqslant (n-1)!$, so $[K : F] \leqslant n!$. □

Example 13.92. $\deg f = 2$, $f = (x-\alpha_1)(x-\alpha_2)$. Then $F(\alpha_1)$ is the splitting field.

Thursday, March 22nd

Let $f \in F[x] \Rightarrow$ splitting field K of f. This is the minimal field where f splits ocmpletely, $f(x) = c(x-\alpha_1)\cdots(x-\alpha_n)$. We have $K = F(\alpha_1,...,\alpha_n)$, and $[K : F] \leqslant n!$.

Get the rest from Paul for this day.

Example 13.93. We give some examples:

Friday, March 23rd

We do exercises from several sections.

Monday, March 26th

Definition 13.94. K/F is said to be **normal** if:

(1) it is algebraic and $\forall \alpha \in K$, $m_{\alpha,F}$ splits completely over K.
(2) Or: if an irreducible polynomial over F has a root in K, then it splits over K.
(3) Or: $\forall \alpha \in K$, **all conjugates of α are in** K. This is to say, if you take an element $\alpha \in K$, all its conjugates in any *larger* field are in K.

Why are they equivalent definitions?

Proof. m_α splits completely over K. $m_\alpha(x) = (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n), \alpha_i \in K$. That is, all conjugates of α are in K. □

We always assume $K \subseteq \overline{F}$ - algebraic closure of F. K is normal if for any element in K, all conjugates of α in $\overline{F}$ are in K.

Definition 13.95. The **normal closure** of an extension K/F is the minimal extension which contains all conjugates of all elements of K/F.

Definition 13.96. A **conjugate** is a root of the same minimal polynomial: $\sqrt{2} \mapsto -\sqrt{2}$; $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$.

What does it mean to split completely in K? I don't know. Paul doesn't either.

Example 13.97. Any extension of degree 2 is normal. $\forall \alpha \in K \setminus F$, $m_{alpha,F}(x) = x^2 + ax + b$, and over K, $m_{\alpha,F}(x) = (x-\alpha)(x-\beta)$.

Remark 13.98. In the book, this notion of normal extensions is not introduced, but it's very standard.

Theorem 13.99. *A finite extension K/F is normal if and only if K is a splitting field of some $f \in F[x]$.*

K is a splitting field means it is normal for just one polynomial. K is a splitting field of f if $\forall$ root α of f, all conjugates of α are in K. That is, "K is normal for generators of K over F."

Example 13.100. $\mathbb{Q}(\sqrt[3]{2}/\mathbb{Q})$ - not normal.

Proof. ($\Rightarrow$) Let $K = F(\alpha_1, ..., \alpha_n)$, let$f = m_{\alpha_1,F} \cdots m_{\alpha_n,F}$. Then f splits over K, since all irreducible components of f split, and K is generated by the roots of f. So, K is a splitting field of f.

($\Leftarrow$) Let K be a splitting field of $f \in F[x]$, where f is arbitrary. And let $\alpha \in K$. Let β be a conjugate of α in some larger field, say the algebraic closure of F. We have to show that $\beta \in K$. Consider the diagram:

$$\begin{tikzcd}
K \arrow[d, dash] & & K' \arrow[d, dash] \\
F(\alpha) \arrow[rr, dash, "\overset{\varphi}{\cong}"] & & F(\beta) \\
& F \arrow[ul, dash] \arrow[ur, dash] &
\end{tikzcd}.$$

We also have:

$$\begin{tikzcd}
& K' & \\
K \arrow[ur, dash, "\subseteq"] & & F(\beta) \arrow[ul, dash, "f"'] \\
& F \arrow[ul, dash, "f"] \arrow[ur, dash] &
\end{tikzcd}.$$

Let K' be the splitting field of f over $F(\beta)$. K is a splitting field of f over $F(\alpha)$ as well. Note $\varphi(\alpha) = \beta$. So φ extends to an isomorphism $K \xrightarrow{\cong} K'$. But actually, $K \subseteq K$, since K' is the splitting field of f over a larger field: if E/F,

$f \in F[x]$, K is the splitting field of f over F, then the splitting field $\tilde{K}$ of f over E contains K: $K = F(\alpha_1, ..., \alpha_n)$, $\tilde{K} = E(\alpha_1, ..., \alpha_n)$.

So $K \subseteq K'$. But $\dim_F K' = \dim_F K$, so $K' = K$, and so $\beta \in K' = K$. □

Properties:

(1) If $K/E/F$ are extensions and K/F is normal, then K/E is normal.
(2) If $K_1/F, K_2/F$ are normal, then $(K_1 \cap K_2)/F$ is normal. (trivial) Note $K_1, K_2 \subseteq K$.
(3) If $K_1, K_2 \subseteq K$, $K_1/F, K_2/F$ are normal and finite (finiteness not needed), then $(K_1K_2)/F$ is normal.

Proof. K_1 is a splitting field of f_1, since finite, K_2 is a splitting field of f_2, so K_1K_2 is a splitting field of f_1f_2 (using previous result about splitting fields). So K_1 is generated by some roots of some polynomial, and all other roots of this polynomial are here. So all conjugates of generators are here. □

Separable extensions

$\alpha \in K$, $\deg_F \alpha = n$. Number of conjugates of α? $\leqslant n$. Every polynomial has exactly n roots counting multiplicities. It is n if and only if $m_{\alpha,F}$ has no multiple roots. If f is irreducible, may f have multiple roots?

Definition 13.101. An extension K/F is **separable** if and only if:

(1) the minimal polynomial over F of every element is separable.
(2) every element of K is the root of a separable polynomial over F.

Remark 13.102. Note f has a multiple root if and only if it is a common root with it's derivative f', i.e. if and only if $f(\alpha) = f'(\alpha) = 0$.

Tuesday, March 27th

Definition 13.103. A polynomial f is **separable** if it has no multiple roots (in any extension of F). This is so if and only if $f'(\alpha) \neq 0$ $\forall$ root α of f.

Definition 13.104. An algebraic over F element α is **separable** if $m_{\alpha,F}$ is a separable polynomial. In this case, α has exactly n conjugates, counting α itself, where $n = \deg_F \alpha$.

Definition 13.105. A field is called **perfect** if any irreducible $f \in F[x]$ is separable.

Remark 13.106. Let $f \in F[x]$ be irreducible. Then f is not separable if f and f' have a common root α. But f is the minimal polynomial of α, so this is only possible if $f' = 0$.

Corollary 13.107. *So any field of characteristic 0 is perfect.*

Proof. When the characteristic is zero, then $\deg f' = \deg f - 1 \neq 0$ (unless f = constant), so f is separable. □

Remark 13.108. In char p: for $f = x^p - a$, $f' = px^{p-1} = 0$, since $p = 0$ in a characteristic p field.

Let:

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

Then:

$$f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \cdots + 2a_2 x + a_1.$$

So $f'(x) = 0$ if and only if $k a_k = 0$ for all k, so either $a_k = 0$ or $k = 0$, that is $a_k = 0$, or $p|k$. Setting $n = mp$, $f'(x) = 0$ if and only if:

$$f(x) = a_{mp} x^{mp} + a_{(m-1)p} x^{(m-1)p} + \cdots + a_p x^p + a_0,$$

that is $f(x) = g(x^p)$ for some $g \in F[x]$ $(g(x) = a_{mp} x^m + a_{(m-1)p} x^{(m-1)} + \cdots + a_p x + a_0)$. So if $\mathrm{char} f = p$, and f is irreducible and nonseparable, then $f(x) = g(x^p)$.

Definition 13.109. The mapping $\varphi : F \to F$, $\varphi(a) = a^p$, is called the **Frobenius endomorphism** of F. It is a homomorphism: $\forall a, b, (ab)^p = a^p b^p$. And:

$$\begin{aligned}(a = b)^p &= a^p + p a^{p-1} b + \binom{p}{2} a^{p-2} b^2 + \cdots + p a b^{p-1} + b^p \\ &= a^p + b^p,\end{aligned} \tag{13.32}$$

since all the middle terms go to zero.

Definition 13.110. If it is surjective, it is called the **Frobenius automorphism** of F.

So Frobenius endomorphism is an automorphism if and only if $\forall a \in F$, $\exists \sqrt[p]{a} \in F$, that is b s.t. $b^p = a$. This $\sqrt[p]{a}$ is unique, since $\ker\varphi = 0$.

Proposition 13.111. *F is perfect if and only if its Frobenius is surjective.*

Proof. Assume that Frobenius is surjective. Let $f(x) = g(x^p) = a_n x^{np} + \cdots + a_1 x^p + a_0$. $\forall k$, let $b_k = \sqrt[b]{a_k}$, so that $f(x) = b_n^p x^{np} + \cdots + b_1^p x^p + b_0^p$. Then we know

$$f(x) = (b_n x^n + \cdots + b_1 x + b_0)^p,$$

by the Frobenius homomorphism, and it is reducible. So there are no irreducible polynomials of this form $g(x^p)$, so F is perfect.

Now if Frobenius is not surjective: if there exists a s.t. $\alpha = \sqrt[p]{a} \notin F$, then $f = x^p - a$ is irreducible, but $f' = 0$, and f has multiple root: $f(x) = (x - \alpha)^p$. α is not in F, and the minimal polynomial of α divides $f(x)$, and is the form $(x - \alpha)^k$ for some $k > 1$ and it has multiple roots, so F is not perfect. So α is a multiple root of its minimal polynomial, so its derivative is zero, so we must have that it is equal to f. So $m_{\alpha,F} = (x - \alpha)^k$, $k \geqslant 2$ (actually $k = p$) so α is inseparable, and F is not perfect. □

Example 13.112. Examples of perfect and non-perfect things.

(1) Any finite field is perfect.

Proof. Frobenius $\varphi : F \to F$ is injective, so it is surjective, since we are mapping to and from a finite space. □

(2) The field $\mathbb{F}_p(t)$ (rational functions over $\mathbb{F}_p$) is not perfect: $\sqrt[p]{t} \notin \mathbb{F}_p(t)$, $t \in \mathbb{F}_p(t)$. $x^p - t$ is irreducible but inseparable.

REMARK 13.113. Galois theory deals only with separable extensions. The non-separable results are not impressive.

13.4 Exercises

1. *Find splitting field of $x^4 - 2$.*

   We have four roots in the plane. $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. We just adjoin them and this will be the splitting field. It is $\mathbb{Q}(\sqrt[4]{2}, i)$. It is of degree 8. We know this since $\sqrt[4]{2}$ gives you 4 and adding i gives you 2 more, multiply to 8.
2. *Find the splitting field and its degree over $\mathbb{Q}$ for $x^4 + 2$.*

   We have four roots in the plane. Observe:

$$\begin{aligned} x^4 &= -2 \\ x^2 &= \pm i\sqrt{2} \\ x &= \pm\sqrt{i\sqrt{2}}, \pm i\sqrt{i\sqrt{2}} \\ &= \pm\sqrt{i}\sqrt[4]{2}, \pm i\sqrt{i}\sqrt[4]{2}. \end{aligned} \tag{13.33}$$

   We adjoin them and this will be the splitting field. It is $\mathbb{Q}(\sqrt{i}\sqrt[4]{2}, i)$. The first root $\sqrt{i}\sqrt[4]{2}$ is of degree 4 since $x^4 + 2$ has degree 4 and it is a root of this irreducible polynomial. And i has degree 2 and is linearly independent, so we know the splitting field has degree 8 over $\mathbb{Q}$.
3. *Find splitting field of $x^4 + x^2 + 1$ over $\mathbb{Q}$.*

$$x^4 + x^2 + 1 = \frac{x^6 - 1}{x^2 - 1}.$$

   There is no general rule, you should just know this. The roots are $\pm\frac{1}{2}\pm\frac{\sqrt{-3}}{2}$. Note $\sqrt{-3} = i\sqrt{3}$. These are roots of unity of degree 6. We suspect it is $\mathbb{Q}(\sqrt{-3})$. So then these roots would be $\alpha, \alpha^2, \alpha^4, \alpha^5$. but note we have:

$$\frac{x^6 - 1}{x^2 - 1} = \frac{(x^3 - 1)(x^3 + 1)}{(x - 1)(x + 1)} = (x^2 + x + 1)(x^2 - x + 1).$$

SECTION 13.5

13.5 Exercises

5. *For any prime p and any nonzero $a \in \mathbb{F}_p$, prove that $x^p - x + a$ is irreducible and separable over $\mathbb{F}_p$. [For the irreducibility: One approach – prove first that if α is a root then $\alpha + 1$ is also a root. Another approach – suppose it's reducible and compute derivatives.]*

PROOF. Suppose α is a root. Then we have $\alpha^p - \alpha + a = 0$. Behold:

$$\begin{aligned}(\alpha+1)^p - (\alpha+1) + a &= \left(\sum_{k=0}^{p} \binom{p}{k}\alpha^k\right) - \alpha - 1 + a \\ &= \left(\sum_{k=1}^{p-1} \binom{p}{k}\alpha^k\right) + \alpha^p - \alpha + a \\ &= \sum_{k=1}^{p-1} \binom{p}{k}\alpha^k \\ &= \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!}\alpha^k.\end{aligned} \tag{13.34}$$

We claim that $\frac{p!}{k!(p-k)!}$ is divisible by p for all integer values of k in the range $[1, p-1]$. Note for these values of k that $p \nmid (k!(p-k)!)$ but that $p|p!$, and the binomial coefficient is an integer, so we must have that $p|\left(\frac{p!}{k!(p-k)!}\right)$. Thus:

$$\sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!}\alpha^k \mod p \equiv 0.$$

And since we are over $\mathbb{F}_p$, we know that $\alpha + 1$ must then be a root. Now note that by induction, we have that if any $\alpha \in \mathbb{F}_p$ is a root, then all elements of $\mathbb{F}_p$ are roots, hence 0 is a root. So we have:

$$0^p - 0 + a = 0 \Rightarrow a = 0,$$

which is a contradiction, since we said $a \neq 0$. So we must have that $\nexists \alpha \in \mathbb{F}_p$ such that α is a root of the given polynomial. So let α be a root, then $\alpha \notin \mathbb{F}_p$. Then consider the extension $\mathbb{F}_p(\alpha)$. It must contain $\alpha + k$, for all $k \in \mathbb{F}_p$. Then $f(x)$ must be the product of all minimal polynomials. Also since $\mathbb{F}_p(\alpha) \cong \mathbb{F}_p(\alpha + k)$ we know that they all have the same degree, say m. Then $p = km$, which tells us $k = 1$ since p prime. Then we must have that the minimal polynomial is f and it is irreducible. Now we show that it is separable. Simply recall from Proposition 37 in the book that every irreducible polynomial over a finite field is separable. □

SECTION 13.6

Cyclotomic polynomials and extensions

DEFINITION 13.114. $\forall$ field F, roots of $x^n = 1$ are called the **roots of unity**.

In any extension of F, roots of unity form a group under multiplication, of order $\leqslant n$. (If $\alpha^n = 1, \beta^n = 1$, then $(\alpha\beta)^n = 1$)

It can have order $< n$ when you are in a finite field and you have the case of multiple roots.

DEFINITION 13.115. The splitting field of $x^n - 1$ is called the n-th **cyclotomic extension of** F.

Definition 13.116. Generators of this group are called **primitive roots of unity**.

Remark 13.117. Over $\mathbb{Q}$: roots of unity of degree n are $1, \omega, ..., \omega^{n-1}$, where $\omega = e^{2\pi i/n}$. Think of them on a circle. Primitive roots of unity are ω^k with $(k,n) = 1$. If $(k,n) = d > 1$, then $(\omega^k)^{n/d} = 1$, so ω^k is a root of unity degree n/d.

Thursday, March 29th

Definition 13.118. The **n-th cyclotomic field** is the splitting field of $x^n - 1 \in \mathbb{Q}[x]$.

Let it be K, $K = \mathbb{Q}(\omega)$, $\omega = e^{2\pi i/n}$. All roots of $x^n - 1$ are $1, \omega, ..., \omega^{n-1}$. If $(k,n) \neq 1<$ then the root ω^k is not primitive, and satisfies $x^m - 1$ for $m = \frac{n}{(n,k)}$.

So what is $[K : \mathbb{Q}] =$? It is equal to $\deg_{\mathbb{Q}} \omega = \deg_{\mathbb{Q}} \alpha$ for any primitive root α (since $K = \mathbb{Q}(\alpha)$).

Definition 13.119.

$$\Phi_n(x) = \prod_{\alpha} (x - \alpha) = \prod_{(k,n)=1} (x - \omega^k), \tag{13.35}$$

where α is a primitive n-th root of unity.

Lemma 13.120. *$x^n - 1 = \prod_{d|n} \Phi_d(x)$.*

Proof. Each root of 1 of degree n is a primitive root α of 1 of degree d for some $d|n$. This $d = |alpha|$ in $\left\{ 1, \omega, ..., \omega^{n-1} \right\}$ minimal d s.t. $\alpha^d = 1$. So then

$$x^n - 1 = \prod_{\alpha^n = 1} (x - \alpha) = \prod_{d|n} \prod_{\alpha \text{ primitive dth root}} (x - \alpha) = \prod_{d|n} \Phi_d(x).$$

□

Proposition 13.121. *$\forall n$, $\Phi_n \in \mathbb{Z}[x]$, $\deg \Phi_n = \varphi(n)$, the totient function.*

Proof. By induction. We have:

$$\Phi_n(x) = \frac{(x^n - 1)}{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}.$$

And we have by induction that this is a monic polynomial from $\mathbb{Z}[x]$. So $\Phi_n \in \mathbb{Q}[x]$. And then by Gauss's Lemma, $\Phi_n \in \mathbb{Z}[x]$. Recall that Gauss's Lemma states that if $f|g$ over $\mathbb{Q}$ and the content of f $c(f)$ is 1, then $f|g$ over $\mathbb{Z}$. □

EXAMPLE 13.122.

$$\begin{aligned}
&\Phi_1(x) = x - 1\\
&\Phi_2(x) = x + 1 = \frac{x^2 - 1}{x - 1}\\
&\Phi_3(x) = \frac{x^3 - 1}{x - 1} = x^2 + x + 1\\
&\Phi_4(x) = \frac{x^4 - 1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4 - 1}{(x - 1)(x + 1)} = x^2 + 1\\
&\Phi_5(x) = \frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1\\
&\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 = \prod_{k-1}^{p-1}(x - \omega^k), \omega = e^{2\pi i/p}, \forall p \in \mathbb{P}\\
&\Phi_6(x) = \frac{x^6 - 1}{\Phi_1\Phi_2\Phi_3} \overset{?}{=} \Phi_3(-x) = x^2 - x + 1.
\end{aligned} \tag{13.36}$$

Note the coefficients are **NOT** always ±1!

THEOREM 13.123. *$\forall n$, Φ_n is irreducible over $\mathbb{Q}$. So $[\mathbb{Q}(\omega) : \mathbb{Q}] = \varphi(n)$. All primitive roots of unity of degree n are conjugate.*

PROOF. Assume that Φ_n is reducible, f is its irreducible factor, $\Phi_n(x) = f(x)g(x)$. All roots of Φ_n are distinct, so it's separable. Let α be a root of f, α is a primitive root of 1 of degree n.

We claim that $\forall p \in \mathbb{P}$ s.t. $p \nmid n$, α^p is also a root of f. If so, then all primitive roots of unity of degree n are roots of f, so $f = \Phi_n$. (any such root is $\omega^{p_1 p_2 \cdots p_k}$, $p_i \nmid n$)

PROOF. α^p is also a primitive root, so is a root of Φ_n. Assume it is a root of g, so $g(\alpha^p) = 0$, so α is a root of $g(x^p)$ so $f | g(x^p)$. . And now pass to the field $\mathbb{F}_p$ by $\mathbb{Z} \mapsto \mathbb{Z}/(p)$. Over $\mathbb{F}_p <$ $g(x^p) = g(x)^p$. (In $\mathbb{F}_p$, $a^p = a$ $\forall p$, so $(x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0)^p = x^{pn} + a_{n-1}(x^p)^{n-1} + \cdots + a_0)$ So $f | g^p$ over $\mathbb{F}_p$. So Φ_n is not separable over $\mathbb{F}_p$. If so, $x^n - 1$ is not separable over $\mathbb{F}_p$. But $(x^n - 1)' = nx^{n-1}$ has no common roots with $x^n - 1$. □

Then $f = \Phi_n$ which is a contradiction since we assumed Φ_n is reducible, so it must be irreducible. □

13.6 EXERCISES

6. *Prove that for n odd, $n > 1$, $\Phi_{2n}(x) = \Phi_n(-x)$.*

   PROOF. Let n be odd, and let $\varphi(x)$ be Euler's totient function. Then $\varphi(n) = \varphi(2n)$ since the only factor of $2n$ which is not already a factor of n is 2, and $2 \nmid n$ since n is odd. So then $\Phi_{2n}(x)$ has the same degree as $\Phi_n(-x)$. So they both have the same number of roots. But note we know that if ω is an n-th root of unity, then we know that $-\omega$ is also an n-th root of unity and also a $2n$-th root of unity. Then the roots of $\Phi_n(-x)$ are also roots of $\Phi_{2n}(x)$, and since we already proved that they have the same number of roots, we know they are the same polynomial. (Note I got the idea for this proof from Jack Peltier) □

CHAPTER 14

Galois theory

SECTION 14.1

Basic definitions

Friday, March 30th

Let E/F be an extension, K/F be a finite subextension ($F \subseteq K \subseteq E$).

Definition 14.1. **Embeddings** of K to E over F: homomorphisms $\varphi : K \to E$ such that $\varphi|_F = \mathrm{Id}_F$. It may be that $\varphi(K) = K$, but φ is non-trivial: $\varphi \neq \mathrm{Id}_K$.

Definition 14.2. If φ is such an embedding of K, then $\varphi(K)$ is called a **conjugate** of K.

Lemma 14.3. *If $\alpha \in K$, φ is an embedding, then $\varphi(\alpha)$ is conjugate of α.*

Proof. If $f = m_{\alpha,F}$, then $\varphi(f) = f \in F[x]$, where $\varphi(f)$ is φ applied to the coefficients of f. So φ maps roots of f to roots of f. We have:

$$f(\alpha) = 0 \Rightarrow \varphi(f(\alpha)) = 0. \tag{14.1}$$

And $f(\varphi(\alpha)) = \varphi(f(\alpha))$. So $\varphi(K)$ consists of conjugates $\varphi(\alpha)$ of elements α of K. So, if K/F is normal, then $\varphi(K) = K$, $\forall \varphi$. (K/F is normal means that $\forall \alpha \in K$, all conjugates of α are in K) □

If K/F is simple, $K = F(\alpha)$. Under any embedding φ, $\varphi(\alpha)$ is a conjugate of α, and $\varphi(\alpha)$ defines φ. So the number of embeddings of K over F is just the number of conjugates of α over F in E. So, the number of embeddings is always $\leqslant \deg_F \alpha$ and is equal to $\deg_F \alpha$ if and only if α is separable and $m_{\alpha,F}$ splits in E.

Example 14.4. (1) Embeddings of $\mathbb{Q}(i)$ over $\mathbb{Q}$ into $\mathbb{C}$. We may have $i \mapsto i$ or $i \mapsto -i$. The embeddings are:

$$\begin{cases} z \mapsto z \\ z \mapsto \overline{z} \end{cases}. \tag{14.2}$$

We define $\overline{z}$ to be the complex conjugate. Note both images are $\mathbb{Q}(i)$.

(2) Embeddings of $\mathbb{C}$ into $\mathbb{C}$ over $\mathbb{R}$. We have the same:

$$\begin{cases} z \mapsto z \\ z \mapsto \overline{z} \end{cases} . \tag{14.3}$$

(3) Embeddings of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ into $\mathbb{C}$. We have three:

$$\begin{tikzcd} & \sqrt[3]{2} \\ \sqrt[3]{2} \arrow[ur, mapsto] \arrow[r, mapsto] \arrow[dr, mapsto] & \omega\sqrt[3]{2} . \\ & \omega^2\sqrt[3]{2} \end{tikzcd}$$

And $\omega = e^{2\pi i/3}$. Note $\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\omega\sqrt[3]{2}), \mathbb{Q}(\omega^2\sqrt[3]{2})$ are conjugates of $\mathbb{Q}(\sqrt[3]{2})$ in $\mathbb{C}$.

(4) We give an example of a time when the number of embeddings is less than the degree of α. Consider $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[8]{3})$, and $E = \mathbb{Q}(\sqrt[8]{3}, i)$. Then we have $\alpha\omega^k$, $\omega = \frac{1+i}{\sqrt{2}}$. In E, α only has 4 conjugates, so there exist only 4 embeddings.

Let φ be an embedding of K_1 with $K_2 = \varphi(K_1)$. Consider $K_1(\alpha)$, $\alpha \in E$. We have:

$$\begin{tikzcd} K_1(\alpha) \arrow[r, "\psi"] \arrow[d, dash] & L \arrow[d, dash] \\ K_1 \arrow[r, "\varphi"] \arrow[dr, dash] & K_2 . \arrow[d, dash] \\ & F \end{tikzcd}$$

What are embeddings of $K_1(\alpha)$ extending φ: $\psi : K_1(\alpha) \to E$ such that $\psi|_{K_1} = \varphi$. Any such ψ is uniquely defined by $\psi(\alpha)$. Let $f = m_{\alpha,K_1}$. Then $\psi(\alpha)$ must be a root of $\varphi(f)$. Indeed, $f(\alpha) = 0$, so $\psi(f(\alpha)) = 0$. But $\psi(f(\alpha)) = \psi(f)(\psi(\alpha)) = \varphi(f)(\psi(\alpha))$.

We have $\varphi(f) \in K_2[x]$ and is irreducible, so $\varphi(f)$ is the minimal polynomial of $\psi(\alpha)$.

Conversely, if $\beta \in E$ is a root of $\varphi(f)$, then we can extend up to $K_1(\alpha)$ by defining $\psi(\alpha) = \beta$, since $K_2(\beta) \cong K_1(\alpha)$. So, we have $\leqslant n$ embeddings ψ extending φ, where $n = \deg \varphi(\alpha) = \deg f = \deg_{K_1} \alpha$. And: we have exactly n extensions if and only $\varphi(f)$ is separable and splits in E.

Let $g = m_{\alpha,F}$. Then both $f|g$, so $\varphi(f)|g$. So if g is separable and splits and E, we have exactly n extensions of φ.

Now let $K = F(\alpha_1, ..., \alpha_k)$. Then we have a tower of extensions:

$$\begin{tikzcd}
K = F(\alpha_1)\cdots(\alpha_k) \arrow[r] & K_2 \\
\vdots \arrow[u, dash] & \vdots \arrow[u, dash] \\
F(\alpha_1)(\alpha_2) \arrow[r] \arrow[u, dash] & F(\beta_1,\beta_2) \arrow[u, dash] \ . \\
F(\alpha_1) \arrow[r, "\cong"] \arrow[u, dash] & F(\beta_1) \arrow[u, dash] \\
F \arrow[u, dash] \arrow[ur, dash] &
\end{tikzcd}$$

$\forall i$ we have m_i choices how to extend the embedding of $F(\alpha_1,...,\alpha_{i-1})$, where $m_i \leqslant n_i = \deg_{F(\alpha_1,...,\alpha_{i-1})} \alpha_i$. Totally, we have $\leqslant n_1 n_2 \cdots n_k = [K : F]$ embeddings. If E/F is normal and separable, then we have exactly $[K : F]$ embeddings of K over F into E.

THEOREM 14.5. *Let $E/K/F$. Then there are $\leqslant [K : F]$ embeddings of K over F to E. If E/F is normal and separable, then there are exactly $[K : F]$ embeddings.*

If $\exists \alpha \in K$ s.t. α has $< \deg_F \alpha$ conjugates in E (that is, α is not separable, or $m_{\alpha,F}$ doesn't split in E) then we have $< n$ embeddings of K.

This is true because $K = F(\alpha, \alpha_1, ..., \alpha_k)$ and for this α we find less than the correct number of conjugates, so when we adjoin the rest, we cannot get all the ones needed.

COROLLARY 14.6. *If K is a splitting field of a separable polynomial, then K is normal and separable.*

Thursday, April 5th

DEFINITION 14.7. Let K/F be finite, $[K : F] = n$. K/F is **Galois** if:

(1) it is normal and separable.
(2) $|\mathrm{Aut}(K/F)| = n$.
(3) $K = F(\alpha_1, ..., \alpha_k)$ s.t. α_i are separable and all their conjugates are in K.
(4) K is a splitting field of a separable polynomial.

So we have 4 equivalent definitions.

DEFINITION 14.8. If L/F is finite and separable, let $L = F(\alpha_1, ...\alpha_k)$. Adjoin all conjugates of α_i, they are still separable. Then we get an extension K, generated by separable elements whose conjugates are in K, so K is Galois (the minimal Galois extension of F containing K). K/F is called the **Galois closure** of L/F. (It is the normal closure of L/F).

DEFINITION 14.9. Recall that an element α is **separable** if and only if it is a root of a separable polynomial.

THEOREM 14.10. *(1) If $K = F(\alpha_1, ..., \alpha_k)$ s.t. all conjugates of α_i are in K, then K/F is normal.*
(2) If $K = F(\alpha_1, ..., \alpha_k)$ where α_i are separable, then K/F is separable.

Proof. (1) Any embedding of K over F into a larger field is an automorphism of K. This implies that K/F is normal. (If α in K has conjugate $\beta \notin K$, consider $\varphi : F(\alpha) \overset{\cong}{\to} F(\beta), \alpha \mapsto \beta$, and extend it to $K \to E$. We proved that if we have an isomorphism of fields and K is a splitting field of some polynomial, then take the splitting field of the image of this polynomial, and we'll have an isomorphism. Observe:

$$\begin{tikzcd}
K \arrow[r, "\overset{\cong}{\varphi}"] \arrow[d, dash] & K' \arrow[d, dash] \\
F(\alpha) \arrow[r, "\cong"] & F(\beta)
\end{tikzcd}.$$

Where K' is the splitting field of some polynomial. □

Proof. (2) Adjoin all conjugates of α_i. Then we get an extension of K generated by "normal", separable elements. So this extension is Galois, so it is separable, so K/F is separable. □

Definition 14.11. Let $f \in F[x]$. The **Galois group of f (over F)**, $\mathrm{Gal}(F/F)$ or just $\mathrm{Gal}(f)$, is $\mathrm{Gal}(K/F)$, where K is a splitting field of f.

Example 14.12. $\mathrm{Gal}(x^3 - 2/\mathbb{Q}) \cong S_3$.
$\mathrm{Gal}((x^3 - 2)(x^3 - 3)/\mathbb{Q}) \cong V_4$.

Definition 14.13. Galois extension K/F is **abelian** if $\mathrm{Gal}(K/F)$ is abelian. K/F is <insert nice property here> if $\mathrm{Gal}(K/F)$ is <insert nice property here>. (cyclic, nilpotent, solvable,...)

Example 14.14. $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ is abelian, $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})/\mathbb{Q}$ is not. $\mathbb{F}_{p^n}/\mathbb{F}_p$ is cyclic ($\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle\varphi\rangle \cong \mathbb{Z}_n$), where φ is Frobenius.

Example 14.15. $G = \mathrm{Gal}(x^n - 1/\mathbb{Q})$ $=\mathrm{Gal}(K/\mathbb{Q})$, $k = \mathbb{Q}(\omega)$, $\omega = e^{2\pi i/n}$. $|G| = [K : \mathbb{Q}] = \varphi(n)$. Conjugates of ω are ω^k, $(k, n) = 1$, where ω^k are roots of Φ_n. $\forall \varphi \in G$ is defined by $\varphi(\omega)$ which is one of ω^k, $(k, n) = 1$. So $G = \{ \varphi_k : (k, n) = 1 \}$, $\varphi_k(\omega) = \omega^k$. $\forall k, l$, $\varphi_k\varphi_l(\omega) = \varphi_k(\omega^l) = \omega^{kl}$. So $\varphi_k\varphi_l = \varphi_{kl}$. So $G \cong \mathbb{Z}_n^*$. $\forall n$. then n-th cyclotomic polynomial extension is abelian.

Let K/F be Galois, $\mathrm{Gal}(K, F) = G$. Let L/F be a subextension, $F \subseteq K \subseteq K$. We have:

$$\begin{tikzcd}
K \arrow[dd, dash, bend right, "G"'] \arrow[d, dash, bend left] \\
L \\
F
\end{tikzcd}.$$

Then K/F is Galois. Let $H = \mathrm{Gal}(K/L)$. We have:

$$\begin{aligned} H &= \{ \varphi : K \to K : \varphi \text{ fixes } K : \varphi(\alpha) = \alpha, \forall \alpha \in L \} \\ &\leqslant G = \{ \varphi : K \to K : \varphi \text{ fixes } F : \varphi(\alpha) = \alpha \forall \alpha \in F \}. \end{aligned} \tag{14.4}$$

Note $H \leqslant G$. We also have:

$$|H| = [K : L] = \frac{[K : F]}{[L : F]} = \frac{|G|}{[L : F]}. \tag{14.5}$$

So $[L : F] = |G : H|$.

And $L \Rightarrow H = \mathrm{Gal}(K/L) \leqslant G$.

Let $H \leqslant G$.

Definition 14.16. $\mathrm{Fix}(H) = \{\, \alpha \in K : \varphi(\alpha) = \alpha, \forall \varphi \in H \,\}$. $\mathrm{Fix}(H)$ is a subfield of K and contains F. So $H \Rightarrow L = \mathrm{Fix}(H) \subseteq K$.

Theorem 14.17 (**Fundamental Galois theorem (short version)**). *These two operations:*

$$K \mapsto H = \mathrm{Gal}(K/L)H \mapsto K = \mathrm{Fix}(H) \tag{14.6}$$

are inverses of each other. So, subextensions L/F of K/F are in bijection with subgroups $H \leqslant G$. Note $L \subseteq K$ and $H \subseteq G$.

Proof. Just the idea of the proof. Consider:

$$L \mapsto H = \mathrm{Gal}(K/L) \mapsto \mathrm{Fix}(H) \overset{?}{=} L. \tag{14.7}$$

Note $L \subseteq \mathrm{Fix}(H)$. And $[K : L] = n \Rightarrow |H| = n$. So it is enough to show that $[K : \mathrm{Fix}(H)] = n$. We must also sow that

$$H \mapsto L = \mathrm{Fix}(H) \mapsto \mathrm{Gal}(K/L) \overset{?}{=} H. \tag{14.8}$$

We know $H \subseteq \mathrm{Gal}(K/L)$. We know $|H| = n$. $[L : K] \Rightarrow |\mathrm{Gal}(K/L)| = [K : L]$. If we prove that $[K : L] = n$, we are done, where $L = \mathrm{Fix}(H), n = |H|$. □

Proposition 14.18. *Let K be a field, let $G \leqslant \mathrm{Aut}(K)$, finite, let $F = \mathrm{Fix}(G)$, then $[K : F] = |G|$.*

Friday, March 6th

Theorem 14.19 (**Galois theorem - full version**). *Let K/F be a Galois extension, let $g = \mathrm{Gal}(K/F)$. Then*

1. *The correspondence: subextension $L/F \leftrightarrow$ subgroup $H \leqslant G$ defined by $H = \mathrm{Gal}(K/L)$, $L = \mathrm{Fix}(H)$ is injective with $|H| = [K : L], |G : H| = [L : F]$. We postpone the proof until Monday. The idea is to prove that if we define subextension this way, then the degree of K/L will be exactly the order of H, and this is the key point of the proof.*
2. *If $L_1 \leftrightarrow H_1, L_2 \leftrightarrow H_2$, then $L_1 \subseteq L_2$ if and only if $H_1 \geqslant H_2$ and $[L_2 : L_1] = |H_1 : H_2|$. So there exists only finitely many subextensions of K/F, and the diagram of subextensions is the same as the diagram of subgroups of G drawn* ***upside down****:*

$$\begin{tikzcd}
 & 1 \arrow[dl, dash, "n_1"'] \arrow[d, dash, "n_2"] \arrow[dr, dash, "n_4"] & & & & K \arrow[dl, dash, "n_1"'] \arrow[d, dash, "n_2"] \arrow[dr, dash, "n_4"] & \\
H_1 \arrow[dr, dash, "m"'] & H_2 \arrow[d, dash] & H_4 \arrow[ddl, dash] & \leftrightarrow & L_2 \arrow[dr, dash, "m"'] & L_2 \arrow[d, dash] & L_4 \arrow[ddl, dash] . \\
 & H_3 \arrow[d, dash] & & & & L_3 \arrow[d, dash] & \\
 & G & & & & F &
\end{tikzcd}$$

(3) If $L_1 \leftrightarrow H_1, L_2 \leftrightarrow H_2$, then $L_1 \cap L_2 \leftrightarrow \langle H_1, H_2\rangle$ and $L_1L_2 \leftrightarrow H_1 \cap H_2$. And the following diagram is the proof:

$$\begin{tikzcd}
 & L_1L_2 \arrow[rrrr, leftrightarrow] \arrow[dl, dash] \arrow[dr, dash] & & & & H_1 \cap H_2 \arrow[dl, dash] \arrow[dr, dash] & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] & & H_1 \arrow[dr, dash] & & H_2 . \arrow[dl, dash] \\
 & L_1 \cap L_2 & & & & \langle H_1, H_2\rangle &
\end{tikzcd}$$

Since $L_1 \cap L_2$ is the max subfield contained in L_1 and L_2, it corresponds to the minimum subgroup countaining H_1 and H_2, which is $\langle H_1, H_2\rangle$. And...

(4) If $L \leftrightarrow H$, then any embedding $L \leftrightarrow L$ is given by some $\varphi \in G$. $\varphi_1, \varphi_2 \in G$ define the same embedding $\varphi|_L = \varphi_2|_L$ if and only if $\varphi_1 = \varphi_2 \mod H$. So embeddings $\leftrightarrow$ cosets G/H.

(5) Any conjugate of L (result of an embedding) is of the form $\varphi(L)$, $\varphi \in G$. The subgroup, corresponding to $\varphi(L)$ is $\varphi H \varphi^{-1}$. So conjugate subextensions $\leftrightarrow$ conjugate subgroups:

$$\varphi(L) \leftrightarrow \varphi H \varphi^{-1}.$$

(6) If $L \leftrightarrow H$, then L is normal if and only if $H \trianglelefteq G$. In this case, L/F is Galois, and $\mathrm{Gal}(L/F) = G/H$. If L is normal, then the extension from F to L is normal.

Proof. (2) If $L_1 \subseteq L_2$, then $H_1 = \mathrm{Gal}(K/L_1) = \{\,\varphi \text{ fixes } L_1\,\}$. And $H_2 = \mathrm{Gal}(K/L_2) = \{\,\varphi \text{ fixes } L_2\,\}$. Then we have:

$$|H_1 : H_2| = \frac{|H_1|}{|H_2|} = \frac{[K : L_1]}{[K : L_2]} = [L_2 : L_1]. \tag{14.9}$$

□

Proof. (4) If you have some $\varphi : L \to K$, then observe:

$$\begin{tikzcd}
K \arrow[r, "\overset{\cong}{\varphi\in G}"] \arrow[d, dash] & K \arrow[d, dash] \\
L \arrow[r, "\overset{\cong}{\varphi}"] & L' .
\end{tikzcd}$$

And the number of embeddings $L \to K$ given by elements of G is $|G : H|$. But the number of embeddings from $L \to K$ is just the degree of L which is $[L : F] = |G : H|$. □

Proof. (5) $\forall \alpha \in L$, $\forall \psi \in H$:

$$\varphi\psi\varphi^{-1}(\varphi(\alpha)) = \varphi(\psi(\alpha)) = \varphi(\alpha). \tag{14.10}$$

So , $\varphi H \varphi^{-1}$ fixes $\varphi(L)$. □

Proof. (6) L is normal if and only if $\varphi(L) = L$ $\forall \varphi \in G$ if and only if $\varphi H \varphi^{-1} = H$ $\forall \varphi \in G$ if and only if $H \trianglelefteq G$. Let's use the first isomorphism theorem. Let $D = \mathrm{Gal}(L/F)$. $\forall \varphi \in G$, $\varphi(L) = L$, so $\varphi|_L \subseteq D$, so we have a homomorphism $G \to D$ given by $\varphi \mapsto \varphi|_L$. It is surjective since $\forall$ element if D extends to some $\varphi \in G$. Its kernel is $H = \mathrm{Gal}(K/F)$. So $D \cong G/H$. □

Example 14.20. (1) $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $\mathrm{Gal}(K/\mathbb{Q}) \cong V_4 = \{ 1, \varphi_1, \varphi_2, \varphi_3 \}$. $1 = Id_K$.

$$\varphi_1 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \varphi_2 : \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \quad \varphi_3 = \varphi_1\varphi_2 : \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases} \tag{14.11}$$

We have:

$$\begin{tikzcd}
 & 1 \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & & & & K \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
\langle\varphi_1\rangle \arrow[dr, dash, "2"'] & \langle\varphi_2\rangle \arrow[d, dash, "2"] & \langle\varphi_3\rangle \arrow[dl, dash, "2"] & & L_1 \arrow[dr, dash, "2"'] & L_2 \arrow[d, dash, "2"] & L_3 \arrow[dl, dash, "2"] \; . \\
 & G & & & & \mathbb{Q} &
\end{tikzcd}$$

$L_1 = \mathrm{Fix}(\langle\varphi_1\rangle) = \mathrm{Fix}(\varphi_1) = \mathbb{Q}(\sqrt{3})$. And $L_2 = \mathrm{Fix}(\varphi_2) = \mathbb{Q}(\sqrt{2})$. And $L_3 = \mathrm{Fix}(\varphi_3) = \mathbb{Q}(\sqrt{6})$.

(2) $K = \mathbb{Q}(\sqrt[3]{2}, \omega)$, $\omega = e^{2\pi i/3}$. $\mathrm{Gal}(K/\mathbb{Q}) \cong S_3$.

Remark 14.21. Roots of coprime elements are rationally independent over $\mathbb{Q}$.

Monday, April 9th

Remark 14.22. K/F is Galois if and only if K is a splitting field of a separable polynomial $f \in F[x]$.

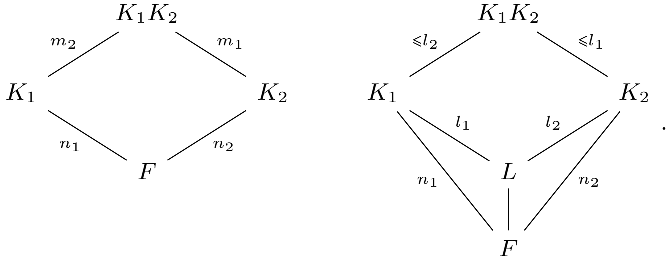
Proof. Just the idea. So $K = F(\alpha_1, ..., \alpha_k)$ such that α_i are separable and K contains all of their conjugates. So K/F is Galois if all elements are separable and all their conjugates are in K. We claim that it is sufficient to just show this on the generators. This is a nontrivial fact. This is a sort of counting. We prove that if we have $K = (\alpha_1, .., \alpha_k)$, then $|\mathrm{Aut}(K/F)| = [K : F]$, and from this it follows that all elements of K are "good" (separable and all conjugates are in K), and K/F is thus Galois. So if there is a bad element, then we can construct a tower which doesn't have enough automorphisms. □

Tuesday, April 10th

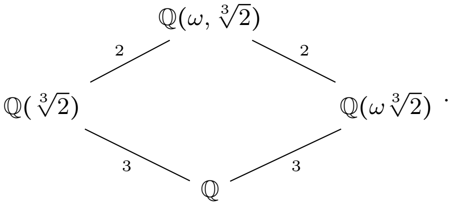
We have $Tu_i = \lambda_i u_i$.

$$\begin{aligned} \lambda_1(a_1u_1 + \cdots + a_nu_n = 0 \\ T : a_1\lambda_1u_1 + \cdots a_n\lambda_nu_n = 0. \end{aligned} \tag{14.12}$$

Composite of K_1, K_2. Let K/F be Galois, let $K_1/F, K_2/F$ be subextensions. We have:



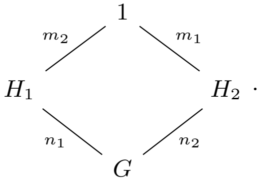
Where $m_2 \leqslant n_2, m_1 \leqslant n_1$. Why can it be that $m_1 < n_1, m_2 < n_2$? One reason: $K_1 \cap K_2 \neq F$. Then $m_2 \leqslant l_2 < n_2$, and $m_1 \leqslant l_1 < n_1$. Example:


$\mathbb{Q}(\omega, \sqrt[3]{2})$
2
2
$\mathbb{Q}(\sqrt[3]{2})$
$\mathbb{Q}(\omega\sqrt[3]{2})$.
3
3
$\mathbb{Q}$

Neither of these extensions are normal. But what if $K_1 \cap K_2 = F$?

Note $G = \langle H_1, H_2\rangle \geqslant H_1H_2$. And $H_1 \cap H_2 = 1$. We have $|H_1| = m_2, |H_2| = m_2$. If $G > H_1, H_2$, which is not a group, then $n_1 > m_1, n_2 > m_2$. But if $H_1 \trianglelefteq G$, then $G = \langle H_1, H_2\rangle = H_1H_2$, $|G| = m_1m_2$.

We have for the Galois group:



Theorem 14.23. *IF $K_1/F, K_2/F$ are subextensions of a Galois extension $K_1 \cap K_2 = F$, and K_1/F is normal, then $[K_1K_2 : F] = [K_1 : F][K_2 : F]$. $(m_1 = n_1, m_2 = n_2)$.*

Monday, April 16th

Proof that $\sqrt{3} \notin \mathbb{Q}(\sqrt[8]{2})$?

Proposition 14.24. *Let $a > 0$, and let $x^n - a$ be irreducible. Let $K = \mathbb{Q}(\sqrt[n]{a})$. Then the only subfields of K are of the form $\mathbb{Q}(\sqrt[d]{a}), d|n$.*

Proof. Let $L \subseteq K$, $[L : \mathbb{Q}] = d$ (to prove $L = \mathbb{Q}(\sqrt[d]{a})$). Let f be the minimal polynomial of $\sqrt[n]{a}$ over L. Then $\deg f = \frac{n}{d}$, and:

$$f \mid (x^n - a) = \prod_{k=0}^{n-1}(x - \omega^k \sqrt[n]{a}), \tag{14.13}$$

where $\omega = e^{2\pi i/n}$. So:

$$f(x) = \prod_{i=1}^{n/d} (x - \omega^{k_i} \sqrt[n]{a}), \tag{14.14}$$

for some k_i. So we have:

$$f(x) = x^{n/d} + \cdots \pm \omega^k \sqrt[d]{a} \in L[x], kk_1 + \cdots + k_{n/d}, \tag{14.15}$$

so, $\omega^k \sqrt[d]{a} \in L \subseteq \mathbb{R}$, so $\omega^k \in \mathbb{R}$, so $\omega^k = \pm 1$. So $\pm \sqrt[d]{a} \in L$, so $\mathbb{Q}(\sqrt[d]{a}) \subseteq L$. $x^d - a$ is irreducible over $\mathbb{Q}$: if $x^d - a = g(x)h(x)$, then ${}^n - a = g(x^{n/d})h(x^{n/d})$ - impossible. So, $[\mathbb{Q}(\sqrt[d]{a}) : \mathbb{Q}] = d = [L : \mathbb{Q}]$, so $L = \mathbb{Q}(\sqrt[d]{a})$. □

If so ,then the only subfield of $\mathbb{Q}(\sqrt[8]{2})$ of degree 2 is $\mathbb{Q}(\sqrt{2})$, but $\mathbb{Q}(\sqrt{3}) \neq \mathbb{Q}(\sqrt{2})$, so $\sqrt{3} \notin \mathbb{Q}(\sqrt[8]{2})$.

14.1 Exercises

6. We have:

$$\operatorname{Aut}(F(t)) = \left\{ t \mapsto \frac{at+b}{ct+d} : a, b, c, d \in F, ad - bc \neq 0 \right\}. \tag{14.16}$$

Here we have $f(t) \mapsto f\left(\frac{at+b}{ct+d}\right)$.

7. $\operatorname{Aut}(\mathbb{R}) = ?$

This is the trivial group. Why? Any automorphism must preserve positive numbers, since they are characterized by the square root. This property is preserved by any automorphism (having a root). $a = b^2 \Rightarrow \varphi(a) = \varphi(b)^2 <$ so $a > 0$ if and only if $\varphi(a) > 0$. So $\forall \varphi$ preserves the order: $a > b$ if and only if $a - b > 0$ if and only if $\varphi(a - b) > 0$ if and only if $\varphi(a) > \varphi(b)$. And it fixes $\mathbb{Q}$ since each rational goes to itself. $\forall a \in \mathbb{R}$ is defined by $\{ r \in \mathbb{Q} : r < a \} = A_a$, which is preserved by φ, so $\varphi(a) = a$. If we have two different real numbers a, b, then they have two different sets of rational numbers which are less than them. Within any two real numbers, there is a rational number (density of rationals in $\mathbb{R}$). So $\varphi(A_a) = A_{\varphi(a)}$, so $\varphi(a) = a$ since φ preserves order.

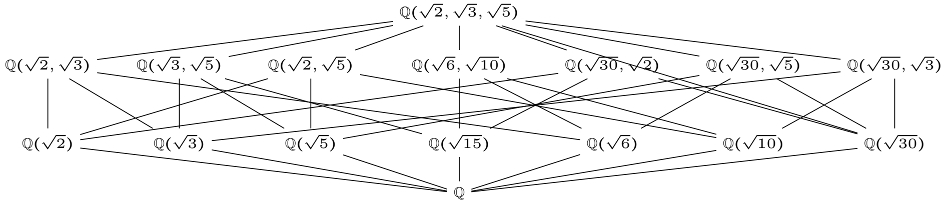
Consider $\operatorname{Aut}(\mathbb{C}) = \operatorname{Aut}(\mathbb{C}/\mathbb{Q})$ =huge... Why?

$$\begin{tikzcd}
\mathbb{Q}(i) \arrow[rr, "i \mapsto -i"] \arrow[dr, dash] & & \mathbb{Q}(i) \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

14.2 Exercises

3. *Determine the Galois group of* $(x^2 - 2)(x^2 - 3)x^2 - 5)$. *Determine all the subfields of the splitting field of this polynomial.*

We draw the subfield lattice of $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})/\mathbb{Q}$. Note that every nonidentity element is of order 2, and the whole group is of order 8, so the Galois group is isomorphic to $\mathbb{Z}_2^3$.


$\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$
$\mathbb{Q}(\sqrt{2},\sqrt{3})$
$\mathbb{Q}(\sqrt{3},\sqrt{5})$
$\mathbb{Q}(\sqrt{2},\sqrt{5})$
$\mathbb{Q}(\sqrt{6},\sqrt{10})$
$\mathbb{Q}(\sqrt{30},\sqrt{2})$
$\mathbb{Q}(\sqrt{30},\sqrt{5})$
$\mathbb{Q}(\sqrt{30},\sqrt{3})$
$\mathbb{Q}(\sqrt{2})$
$\mathbb{Q}(\sqrt{3})$
$\mathbb{Q}(\sqrt{5})$
$\mathbb{Q}(\sqrt{15})$
$\mathbb{Q}(\sqrt{6})$
$\mathbb{Q}(\sqrt{10})$
$\mathbb{Q}(\sqrt{30})$
$\mathbb{Q}$

.

4. *p is prime, find* $\mathrm{Gal}(x^p-2)$ *over* $\mathbb{Q}$.

REMARK 14.25. The Galois group of a polynomial is the Galois group of its splitting field.

So we first construct its splitting field. We have $K = \mathbb{Q}(\alpha,\omega)$, $\alpha = \sqrt[p]{2}, \omega = e^{2\pi i/p}$. K is the splitting field of $x^p - 2$. And $K = \mathbb{Q}(\alpha)\mathbb{Q}(\omega)$.

$$\begin{tikzcd}
 & L \arrow[dl, dash, "p-1"'] \arrow[dr, dash, "p"] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "p"] & & \mathbb{Q}(\omega) \arrow[dl, dash, "\varphi(p)=p-1"] \\
 & \mathbb{Q} &
\end{tikzcd}\;.$$

So $[K:\mathbb{Q}] = p(p-1) = |G|$. $\varphi \in G$ is defined by $\varphi(\alpha), \varphi(\omega)$. Observe:

$$\begin{aligned}\varphi(\alpha) &= \alpha\omega^k && \text{for some } k = 0,\dots,p-1\\ \varphi(\omega) &= \omega^l && \text{for some } l = 1,\dots,p-1.\end{aligned} \tag{14.17}$$

Let $\varphi_{k,l}$ be such φ. They say determine the elements of the Galois group. The elements are determined, but we do not have group yet, we need the multiplication table. So we construct it:

$$\begin{aligned}\varphi_{k_1,l_1}\varphi_{k_2,l_2}(\alpha) &= \varphi_{k_1,l_1}(\alpha\omega^{k_2} = \alpha\omega^{k_1}\omega^{l_1k_2} = \alpha\omega^{k_1+l_1k_2}\\ \varphi_{k_1,l_1}\varphi_{k_2,l_2}(\omega) &= \varphi_{k_1,l_1}(\omega^{l_2}) = \omega^{l_1l_2}.\end{aligned} \tag{14.18}$$

So $\varphi_{k_1,l_1}\varphi_{k_2,l_2} = \varphi_{k_1+l_1k_2 \mod p, l_1l_2 \mod p}$. Recall:

$$\mathrm{Hol}(\mathbb{Z}_p) \cong \mathbb{Z}_p \rtimes \mathbb{Z}_p^*. \tag{14.19}$$

Observe:

$$(k_1,l_1)(k_2,l_2) = (k_1 + l_1k_2, l_1l_2). \tag{14.20}$$

Similarly for holomorphs:

$$(a_1,\psi_1)(a_2,\psi_2) = (a_1 + \psi_1(a_2), \psi_1,\psi_2). \tag{14.21}$$

$H \rtimes \mathrm{Aut}(H)$. It's important that p is prime, since we need $p, \varphi(p)$ to be relatively prime.

7. $x^8 - 2$ *over* $\mathbb{Q}$. *Find all subfields of the splitting field* K *of* $x^8 - 2$ *which are Galois (sufficient to find normal in this case, since they are already separable) over* $\mathbb{Q}$.

Let $\alpha = \sqrt[8]{2}, \omega = e^{2\pi i/8}$. Then $K = \mathbb{Q}(\alpha, \omega) = \mathbb{Q}(\alpha)\mathbb{Q}(\omega)$ (is this last equality always true?)

$$\begin{tikzcd}
& K \arrow[dl, dash, "2"'] \arrow[dr, dash, "4"] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "4"'] & & \mathbb{Q}(\omega) \arrow[dl, dash, "2"] \\
& \mathbb{Q}(\sqrt{2}) \arrow[d, dash, "2"'] & \\
& \mathbb{Q} &
\end{tikzcd}.$$

Note $\omega = \frac{1+i}{\sqrt{2}}, \omega^2 = i$. So $\sqrt{2} \in \mathbb{Q}(\omega)$. Note $\sqrt{2} = \frac{1+i}{\omega} = \frac{1+\omega^2}{\omega}$. And $\sqrt{2} = \alpha^4$. We know the top left degree is 2, since the extension of K of over the two side fields must be nontrivial, and the degrees must be $\geqslant$ the degrees diagonally across from them on the diagram. Thus the other is 4. So $[K : \mathbb{Q}] = 16 = |G|$. Note $\mathbb{Q}(\alpha)/\mathbb{Q}$ - not normal. $\mathbb{Q}(\omega)/\mathbb{Q}$ - normal. Not normal since $\alpha\omega \notin \mathbb{Q}(\alpha)$. $\mathbb{Q}(i)/\mathbb{Q}$ is normal, $i = \omega^2$.

We have:

$$\begin{aligned} \alpha &\mapsto \alpha\omega^k, k = 0, ..., 7 \\ \omega &\mapsto \omega^l, l = 1, 3, 5, 7 \end{aligned} \tag{14.22}$$

So let's try again. Try:

$$\begin{tikzcd}
& K = \mathbb{Q}(\alpha, i) \arrow[dl, "2"'] \arrow[dr, dash, "8"] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "8"'] & & \mathbb{Q}(i) \arrow[dl, dash, "2"] \\
& \mathbb{Q} &
\end{tikzcd}.$$

We have:

$$\begin{aligned} \alpha &\mapsto \alpha\omega^k \\ i &\mapsto \pm i \\ \varphi : \alpha &\mapsto \alpha\omega \\ i &\mapsto i \\ \psi : \alpha &\mapsto \alpha \\ i &\mapsto -i. \end{aligned} \tag{14.23}$$

And $\sqrt{2} = \alpha^4$. $\varphi(\sqrt{2}) = (\alpha\omega)^4 = -\sqrt{2}$. $\varphi(i) = i$, so $\varphi(\omega) = -\frac{1+i}{\sqrt{2}} = -\omega$. Observe:

$$\alpha, \alpha\omega, \alpha\omega^2, \alpha\omega^3, \alpha\omega^4 = -\alpha, -\alpha\omega, -\alpha\omega^2, -\alpha\omega^3. \tag{14.24}$$

$$\varphi : \alpha \mapsto \alpha\omega \mapsto -\alpha\omega^2 \mapsto -\alpha\omega^3 \mapsto -\alpha\omega(-\omega^3) = -2 \mapsto -\alpha\omega \mapsto \alpha\omega^2 \mapsto \alpha\omega^3 \mapsto \alpha. \tag{14.25}$$

So $|\varphi| = 8, |\psi| = 2$.

$$\begin{aligned} \psi\varphi\psi^{-1} : \alpha \overset{\varphi}{\mapsto} \alpha\omega \overset{\psi}{\mapsto} \alpha\omega^3 \\ i \mapsto i \end{aligned} \tag{14.26}$$

$G = \langle r, s | r^8 = s^2 = 1, srs^{-1} = r^3 \rangle$.
Not D_{16}.

8. *K/F is Galois, $[K : F] = p^n$, p a prime. Prove that $\forall k < n$, K has a subfield L such that $[L : F] = p^k$.*

   Proof. Recall Sylow's theorem. $\forall k$, G has a subgroup of order p^k. So $|G : H| = p^{n-k}$, and the corresponding subfield L satisfies $[L : F] = p^{n-k}$. If $[K : F] = n$, $p^k | n$, then $\exists L$ s.t. $[K : L] - p^k$, so $[L : F] = n/p^k$. □

10. *Determine the Galois group of the splitting field over $\mathbb{Q}$ of $x^8 - 3$.*

    Let $\alpha = \sqrt[8]{3}$ and $\omega = e^{2\pi i/8}$. Note:

$$\omega^2 = e^{2\pi i/4} = e^{\pi i/2} = \sqrt{e^{\pi i}} = \sqrt{-1} = i.$$

And $\omega = \sqrt{e^{2\pi i/4}} = \sqrt{i} = \frac{1+i}{\sqrt{2}}$. Note $\sqrt{2} = \frac{1+i}{\omega} = \frac{1+\omega^2}{\omega}$. So $\sqrt{2} \in \mathbb{Q}(\omega)$. Now the roots of $f(x) = x^8 - 3$ are $\alpha\omega^k$ where $k = 0, \dots, 7$, and thus the splitting field is $\mathbb{Q}(\alpha, \omega)$. We write out our options for constructing the automorphisms in the Galois group. We have 8 options to map α to and 4 options to map ω to (since $\varphi(8) = 4$):

$$\begin{aligned} &\alpha \mapsto \alpha\omega^k, k = 0, \dots, 7 \\ &\omega \mapsto \omega, \omega^3, \omega^5, \omega^7. \end{aligned} \tag{14.27}$$

Since none of these combinations give us equivalent maps, we have exactly $8 \cdot 4 = 32$ automorphisms in our group, thus $|\text{Gal}(f(x))| = |G| = 32$. So let $\varphi_{k_1,l_1}, \varphi_{k_2,l_2} \in G$, where $\varphi_{k,l} : \alpha \mapsto \alpha\omega^k, \varphi_{k,l} : \omega \mapsto \omega^l$. Then we have:

$$\begin{aligned} &\varphi_{k_2,l_2} \circ \varphi_{k_1,l_1}(\alpha) = \varphi_{k_2,l_2}(\alpha\omega^{k_1}) = \alpha\omega^{k_2}\omega^{k_1 l_2} = \alpha\omega^{k_2 + k_1 l_2} \\ &\varphi_{k_2,l_2} \circ \varphi_{k_1,l_1}(\omega) = \varphi_{k_2,l_2}(\omega^{l_1}) = \omega^{l_1 l_2}. \end{aligned} \tag{14.28}$$

Thus $\varphi_{k_2,l_2} \circ \varphi_{k_1,l_1} = \varphi_{k_2 + k_1 l_2 \mod 8, l_1 l_2 \mod 8}$, and this multiplication rule completely defines the Galois group. Furthermore, from this we see $G \cong \mathbb{Z}_8 \rtimes V_4$, the nontrival semidirect product of $\mathbb{Z}_8$ and the Klein 4-group.

12. $G = \text{Gal}(x^4 - 14x^2 + 9)$.

    Call it $f(x)$. The roots of f are $\alpha = \sqrt{7 + 2\sqrt{10}}, -\alpha$, $\beta = \sqrt{7 - 2\sqrt{10}}, -\beta$. $K = \mathbb{Q}(\alpha, \beta)$. Observe:

$$\begin{tikzcd}
& K \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash, "4"'] & & \mathbb{Q}(\beta) \ . \arrow[dl, dash, "4"] \\
& \mathbb{Q} &
\end{tikzcd}$$

But $\alpha\beta = 3$, since $\alpha^2\beta^2 = 49 - 40 = 9$. So $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$. So $[K : \mathbb{Q}] = 4$. So $G \cong \mathbb{Z}_4$ or V_4.

$$\begin{aligned}
\varphi : \alpha &\mapsto -\alpha \\
-\alpha &\mapsto \alpha \\
\beta = 3/\alpha &\mapsto -\beta \\
-\beta &\mapsto \beta \\
\varphi : \alpha &\mapsto \beta \\
-\alpha &\mapsto -\beta \\
\beta = 3/\alpha &\mapsto 3/\beta = \alpha \\
-\beta &\mapsto -\alpha.
\end{aligned} \tag{14.29}$$

Since $\varphi^2 = 1$. So it's V_4.

13. *Prove that if the Galois group of the splitting field of a cubic over $\mathbb{Q}$ is the cyclic group of order 3, then all the roots of the cubic are real.*

    Proof. Suppose the Galois group of the splitting field of a cubic $f(x)$ is $\mathbb{Z}_3$. Note since this is a group of the form $\mathbb{Z}_p$ for p prime, we know that it has non nontrivial proper subgroups. Suppose we had an non-real root. Then we know that if $K/\mathbb{Q}$ is the splitting field of f, then $i \in K \Rightarrow \mathbb{Q}(i)/\mathbb{Q}$ is a subextension of K. But note that $\mathbb{Q}(i)/\mathbb{Q}$ has degree 2, and the Galois theorem gives us a bijection between nontrivial subgroups of the Galois group and nontrivial subextensions, hence $[K : \mathbb{Q}] = 3$. If $\mathbb{Q}(i)$ were a subextension of K, we would have $2|3$, a contradiction, so all roots must be real. □

14. *Show that $K = \mathbb{Q}(\sqrt{2+\sqrt{2}})$ is a cyclic quartic field, i.e., is a Galois extension of degree 4 with a cyclic Galois group.*

    Proof. Recall that an extension is Galois if and only if it is the splitting field of a separable polynomial. Note that $\alpha = \sqrt{2+\sqrt{2}}$ is a root of $f(x) = (x^2-2)^2-2 = x^4-4x^2+2$. We show that this is the minimal polynomial of α by showing it is irreducible. Note that $2 \nmid 1$, the leading coefficient, and $2|-4, 2$, and $2^2 \nmid 2$, so it is irreducible by Eisenstein's criterion. So $\deg \alpha = 4 \Rightarrow [K : \mathbb{Q}] = 4$. Note the roots of f are $\pm\sqrt{2 \pm \sqrt{2}}$, and so it has no multiple roots $\Rightarrow$ it is separable. So we need only prove that K is the splitting field of f. Clearly we have $x - \alpha$ and $x + \alpha$ for the roots of the form $\pm\sqrt{2+\sqrt{2}}$. So we need only show $\sqrt{2-\sqrt{2}} \in K$. Note since $\alpha^2 = 2 + \sqrt{2}$, we know $\sqrt{2} \in K$. But $\frac{\sqrt{2}}{\sqrt{2+\sqrt{2}}}\frac{\sqrt{2-\sqrt{2}}}{\sqrt{2-\sqrt{2}}} = \frac{\sqrt{2}\sqrt{2-\sqrt{2}}}{\sqrt{4-2}} = \sqrt{2-\sqrt{2}} = \beta$, thus $\pm\beta \in K$, and hence K is the splitting field of f, so K is Galois. Now note since all 3 conjugates of α also have degree 4, we know that all automorphsims of K are given by $\alpha \mapsto \alpha, -\alpha, \beta, -\beta$. Denote these by $1, \varphi_1 ..., \varphi_3$, respectively. Then we know:

$$\beta = \frac{\alpha^2 - 2}{\alpha}. \tag{14.30}$$

So:

$$\varphi_2(\beta) = \varphi_2\left(\frac{\alpha^2 - 2}{\alpha}\right) = \frac{\beta^2 - 2}{\beta} = -\frac{\sqrt{2}}{\beta} = -\alpha. \tag{14.31}$$

Thus the order of φ_2 is > 2 which means it must be 4 since our group has order 4, so we know that our group must be isomorphic to $\mathbb{Z}_4$. □

15. *(Biquadratic Extensions) Let F be a field of characteristic $\neq 2$.*
    (a) *if $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2, D_1D_2 is a square in F, prove that K/F is a Galois extension with* $\mathrm{Gal}(K/F)$ *isomorphic to the Klein 4-group.*

    Proof. Since D_1, D_2 are not squares, we know $F(\sqrt{D_1})/F$ and $F(\sqrt{D_2})/F$ are both extensions of degree 2. And since D_1D_2 is not a square, we know that $F(\sqrt{D_2})/F(\sqrt{D_1})$ is a nontrivial extension (has degree 2). Thus we know that K/F has degree 4. We wish to first show it is Galois. Let $\alpha = \sqrt{D_1}, \beta = \sqrt{D_2}$. Then $m_{\alpha,F} = x^2 - D_1, m_{\beta,F} = x^2 - D_2$. And since the roots of these are $\pm\alpha, \pm\beta$, we know they are both separable, so α, β are separable, so K/F is separable. Also, K is normal since the only conjugates of α, β are $-\alpha, -\beta$, so K/F is normal and separable, thus it is Galois. We enumerate the automorphisms of K in the Galois group G. We have choices of mappings:

    $$\begin{aligned} &\alpha \mapsto \alpha, -\alpha \\ &\beta \mapsto \beta, -\beta. \end{aligned} \tag{14.32}$$

    So we have:

    $$\begin{aligned} 1 : \alpha &\mapsto \alpha, & \beta &\mapsto \beta \\ \varphi_1 : \alpha &\mapsto -\alpha, & \beta &\mapsto \beta \\ \varphi_2 : \alpha &\mapsto \alpha, & \beta &\mapsto -\beta \\ \varphi_3 : \alpha &\mapsto -\alpha, & \beta &\mapsto -\beta. \end{aligned} \tag{14.33}$$

    Clearly, each has order 2, so it is V_4. □

    (b) *Conversely, suppose K/F is a Galois extension with* $\mathrm{Gal}(K/F)$ *isomorphic to V_4. Prove that $K = F(\sqrt{D_1}, \sqrt{D_2})$ where $D_1, D_2 \in F$ have the property that none of D_1, D_2, D_1D_2 is a square in F.*

    Proof. Suppose K/F is Galois with $G = \mathrm{Gal}(K/F)$ isomorphic to V_4. By the Galois theorem, we know that the subgroup lattice of G is in (flipped) bijection with the subextension lattice of K/F. So since we know the lattice of V_4, we know the structure of the subextensions of K:

$$\begin{tikzcd}
 & 1 \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & & & & K/F \arrow[dl, dash, "2"'] \arrow[d, dash, "2"] \arrow[dr, dash, "2"] & \\
A \cong \mathbb{Z}_2 \arrow[dr, dash, "2"'] & B \cong \mathbb{Z}_2 \arrow[d, dash, "2"] & C \cong \mathbb{Z}_2 \arrow[dl, dash, "2"] & & L_1 \arrow[dr, dash, "2"'] & L_2 \arrow[d, dash, "2"] & L_3 \arrow[dl, dash, "2"] \\
 & V_4 & & & & F &
\end{tikzcd}.$$

Since they are of degree 2, all of L_1, L_2, L_3 must be of the form $F(\sqrt{D_i})$ for some D_i not a square in F. Furthermore D_iD_j cannot be a square in F, otherwise L_i, L_j are the same extension, which is a contradiction. □

16. *Find the Galois group of $x^4 - 2x^2 - 2$.*

Roots: $\alpha_1 = \sqrt{1+\sqrt{3}}, -\alpha_1, \alpha_2 = \sqrt{1-\sqrt{-3}}, -\alpha_2$. We have the splitting field:

$$\begin{tikzcd}
 & K = \mathbb{Q}(\alpha_1, \alpha_2) \arrow[dl, dash, "2"'] \arrow[dr, dash, "2"] & \\
\mathbb{Q}(\alpha_1) \arrow[dr, dash, "2"'] & & \mathbb{Q}(\alpha_2) \arrow[dl, dash, "2"] \\
 & \mathbb{Q}(\sqrt{3}) \arrow[d, dash, "2"] & \\
 & \mathbb{Q} &
\end{tikzcd}.$$

So $[K : \mathbb{Q}] = 8$. Note α_1 is of degree 4 since it is root of polynomial of degree 4 which is irreducible by Eisenstein's criterion. For this reason $x^n - 2$ are all irreducible. $G = \mathrm{Gal}(K/\mathbb{Q}) = ?$. Note $\alpha_1\alpha_2 = \sqrt{-2} = \beta$, because $\alpha_1^2\alpha_2^2 = -2$. Then we have:

$$\begin{tikzcd}
 & K = \mathbb{Q}(\alpha_1, \beta) \arrow[dl, dash, "2"'] \arrow[dr, dash, "4"] & \\
\mathbb{Q}(\alpha_1) \arrow[dr, dash, "4"'] & & \mathbb{Q}(\beta) \arrow[dl, dash, "2"] \\
 & \mathbb{Q} &
\end{tikzcd}.$$

Then we have:

$$\begin{aligned} \alpha_1 &\mapsto \pm\alpha_1, \pm\alpha_2 \\ \beta &\mapsto \pm\beta. \end{aligned} \tag{14.34}$$

We want an automorphism of order 4.
Try this one:

$$\begin{aligned} \varphi : \alpha_1 &\mapsto \alpha_2 \\ \beta &\mapsto -\beta. \end{aligned} \tag{14.35}$$

Then:

$$\begin{gathered} \alpha_2 = \frac{\beta}{\alpha_1} \mapsto -\frac{\beta}{\alpha_2} = -\alpha_1 \\ \alpha_1 \mapsto \alpha_2 \mapsto -\alpha_1 \mapsto -\alpha_2 \mapsto \alpha_1. \end{gathered} \tag{14.36}$$

So $|\varphi| = 4$.

Define:

$$\psi : \alpha_1 \mapsto \alpha_1 \\ \beta \mapsto -\beta. \tag{14.37}$$

Then $|\psi| = 2$. So we have:

$$\psi\varphi\psi^{-1} : \alpha_1 \mapsto -\alpha_2 \\ \beta \mapsto -\beta, \tag{14.38}$$

so $\psi\varphi\psi^{-1} = \varphi^{-1}$. And:

$$\psi : \alpha_2 = \frac{\beta}{\alpha_1} \mapsto -\frac{-\beta}{\alpha_1} = -\alpha_2. \tag{14.39}$$

So:

$$G = \langle \varphi, \psi | \varphi^4 = \psi^2 = 1, \psi\varphi\psi^{-1} = \varphi^{-1} \rangle \cong D_8. \tag{14.40}$$

SECTION 14.3

Finite fields

Let F be a finite field of char p. Then F is finite-dimensional $\mathbb{F}_p$ vector space ($\mathbb{F}_p = \mathbb{Z}_p$). If $[F : \mathbb{F}_p] = n$, then F is n-dimensional $\mathbb{F}_p$-vector space. So $|F| = p^n$.

Consider the group $F^* = F \setminus \{ 0 \}$ under multiplication. $|F^*| = p^n - 1$. And F^* is cyclic $\cong \mathbb{Z}_{p^n-1}$. So $\forall \alpha \neq 0$ in F, we have $\alpha^{p^n-1} = 1$. So $\alpha^{p^n} = \alpha$, $\forall \alpha \in F$. So, all p^n elements of F are roots of the polynomial $x^{p^n} - x$. So F is a splitting field of $x^{p^n} - x$.

Let p be a prime, let $n \in \mathbb{N}$. Consider $f = x^{p^n} - x \in \mathbb{F}_p[x]$. Let K be the splitting field of F. Let $F = \left\{ \alpha \in K : \alpha^{p^n} = \alpha \right\}$. Then F is a subfield of K.

Theorem 14.26. *For any prime p, for any $n \in \mathbb{N}$, there exists a unique field of order p^n, which is the splitting field $x^{p^n} - x$.*

Wednesday, March 28th

Theorem 14.27. *Let p be prime. $\forall n \in \mathbb{N}$, there exists a unique (up to isomorphism) field having p^n elements, notation $\mathbb{F}_p$. ($\mathbb{F}_p = \mathbb{Z}_p$, but $\mathbb{F}_{p^n} \neq \mathbb{Z}_{p^n}$ for $n \geqslant 2$) And this field is the splitting field of $x^{p^n} - x$, and consists of the roots of this polynomial.*

Remark 14.28. $\mathbb{F}_p^n \cong \mathbb{F}_p \oplus \cdots \oplus \mathbb{F}_p$ as an $\mathbb{F}_p$-module.

Now $\mathbb{Z}_{p^n}$ is a ring, but of course it's not a field, there is not relation between it and $\mathbb{F}_{p^n}$.

Remark 14.29. $\mathbb{F}_{p^n}^*$ is a cyclic group, $\exists \alpha \in \mathbb{F}_{p^n}$ such that:

$$\left\{ 1, \alpha, \alpha^2, \ldots, \alpha^{p^n-1} \right\} = \mathbb{F}_{p^n} \setminus \{ 0 \}.$$

So $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$, so $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a simple extension of degree n. And $\deg_{\mathbb{F}_p} \alpha = n$, α is a root of an irreducible polynomial of degree n from $\mathbb{F}_p$. This is because it has degree n and is algebraic. We get this because the extension has degree n. So $\forall n$, such a polynomial exists, and $\mathbb{F}_{p^n}$ is the splitting field of this polynomial. So $\mathbb{F}_p \cong \mathbb{F}_p[x]/(f)$. It is not a unique polynomial, but the resulting fields will be isomorphic.

Example 14.30. For $p = 2$, $n = 3$, the irreducible polynomials of degree 3 are:

$$x^3 + x + 1, x^3 + x^2 + 1 \tag{14.41}$$

When you factorize by these polynomials, you get the same field:

$$\mathbb{F}_8 \cong \mathbb{F}_2[x]/(x^3 + x + 1) \cong \mathbb{F}_2[x]/(x^3 + x^2 + 1).$$

So what are the relations between these fields? We have $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$. For what m do we have $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$? Note $[\mathbb{F}_{p^m} : \mathbb{F}_p] = m$, and it must divide $n = [\mathbb{F}_{p^n} : \mathbb{F}_p]$ so this is a necessary condition, and in fact it is a sufficient condition as well.

Proposition 14.31. *$\forall m|n$, there exists a unique subfield of $\mathbb{F}_{p^n}$ isomorphic to $\mathbb{F}_{p^m}$.*

Lemma 14.32. *If $m|n$, then $x^{m-1}|x^{n-1}$.*

Proof. Indeed, if $\frac{n}{m} = d$, then:

$$\frac{x^{n-1}}{x^{m-1}} = 1 + x^d + \cdots + x^{m-1}d.$$

□

Now we apply this Lemma twice. So, if $m|n$, then $p^m - 1|p^n - 1$, so $x^{p^m-1} - 1|x^{p^n-1} - 1$. And we could continue like this. So, $x^{p^m} - x|x^{p^n} - x$. Now $\mathbb{F}_{p^n}$ contains all the roots of $x^{p^n} - x$ and so all roots of $x^{p^m} - x$ which form $\mathbb{F}_{p^m}$.

Example 14.33. Observe:

$$\begin{tikzcd}
 & & \mathbb{F}_{p^{12}} \arrow[dl, dash] \arrow[dr, dash] & \\
 & \mathbb{F}_{p^6} \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{F}_{p^4} \arrow[dl, dash] \\
\mathbb{F}_{p^3} \arrow[dr, dash] & & \mathbb{F}_{p^2} \arrow[dl, dash] & \\
 & \mathbb{F}_p & &
\end{tikzcd}.$$

And this is exactly the same as the subgroup lattice for $\mathbb{Z}_{12}$.

Remark 14.34. Every element $\beta \in \mathbb{F}_{p^n}$ is a root of an irreducible over $\mathbb{F}_p$ polynomial of degree $m|n$. And any such polynomial splits in $\mathbb{F}_{p^n}$ (since the splitting field of this polynomial is $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$). So $x^{p^n} - x$ is the product of all monic irreducible over $\mathbb{F}_p$ polynomials of degree m with $m|n$.

Note β is a root of it's minimal polynomial, which is an irreducible of degree dividing n. If it's not containing in the union of these subfields seen in the lattice, then it is a generating element and the polynomial has degree n.

Every irreducible monic polynomial of degree $m|n$ is a factor of $x^{p^n} - x$.

Remark 14.35. $(x^{p^n} - x)' = -1$, so this polynomial has no multiple roots, so all irreducible components have exponent 1 in $x^{p^n} - x$. Note it's -1 since $p^n = 0$ in our field.

Example 14.36. $p = 2$, $n = 2$, for $m = 1$, these are $x, x+1$, for $m = 2$, these are just x^2+x+1, so it must be that $x^4 - x = x^4 + x = x(x+1)(x^2+x+1)$, since we are over $\mathbb{F}_2$.

Definition 14.37. Let $\forall n$, $\psi(n)$ be the number of monic irreducible over $\mathbb{F}_p$ polynomials of degree n. Then:

$$\deg(x^{p^n} - x) = p^n = \sum_{m|n} m \cdot \psi(m).$$

So:

$$\psi(n) = \frac{1}{n}\left[p^n - \sum_{\substack{m|n \\ m<n}} m \cdot \psi(m)\right].$$

Example 14.38. For $n = 1$: $\psi(1) = p$ $(x - a : a \in \mathbb{F}_p)$.

$n = 2$, $\psi(2) = (p^2 - p)/2$. And $p = 2 \Rightarrow \psi(2) = 1$, and $p = 3 \Rightarrow \psi(2) = 3$. And for this case, they are:

$$\begin{cases} x^2 + 1 \\ x^2 - x - 1 \\ x^2 + x - 1 \end{cases}. \tag{14.42}$$

Remark 14.39. Algebraic closure of $\mathbb{F}_p$. It's enough to adjoin all roots of all irreducible monic polynomials. But they don't form a sequence, if you want to get a sequence, you get the algebraic closure of $\mathbb{F}_p$ is:

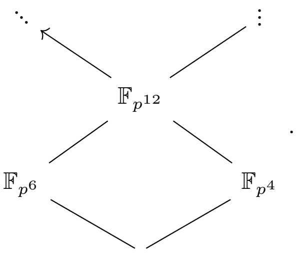
$$\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}. \tag{14.43}$$

And we have:

$$\mathbb{F}_p \subseteq \mathbb{F}_{p^2} \subseteq \mathbb{F}_{p^{3!}} \subseteq \mathbb{F}_{p^{4!}} \subseteq \ldots \tag{14.44}$$

Each element of this field is an element of one of these in this subset sequence. It wasn't even necessary for them to form a sequence to make this definition, but it's easier to see this way.

Paul: Why is it factorial? **Leibman:** We want it to form a sequence, if we don't use factorial, they form a **net**, not a sequence. We'd get something like this:



The homework will depend on what we get through tomorrow.

14.3 Exercises

4. *Construct a finite field of 16 elements and find a generator for the multiplicative group. How many generators are there?*

We simply need to construct an irreducible polynomial of degree 4 over $\mathbb{F}_2$. Consider $f(x) = x^4 + x^3 + x^2 + x + 1$. Clearly $1, 0$ are not roots. So we need to check if it is divisible by any irreducible quadratics. So it would have to b $(x^2 + x + 1)^2$, as this is the only such quadratic. We have:

$$\begin{aligned}(x^2 + x + 1)^2 &= x^4 + x^3 + x^2 + x^3 + x^2 + x + x^2 + x + 1 \\ &= x^4 + x^2 + 1.\end{aligned} \tag{14.45}$$

So f is irreducible. Thus $\mathbb{F}_2[x]/(f) \cong \mathbb{F}_{2^4}$, a finite field of 16 elements. Note that the multiplicative group of this field is isomorphic to $\mathbb{Z}_{15}$ since we have 15 nonzero elements. Since we want to know how many generators we have, recall that the generators of $\mathbb{Z}_{15}$ are exactly those whose equivalence classes are coprime with the order. So we have $\varphi(15) = 8$ generators.

$$\begin{aligned}(x+1)^2 &= x^2 + 1 \\ (x+1)(x^2+1) &= x^3 + x + x^2 + 1 \\ (x+1)(x^3+x^2+x+1) &= x^4 + x^3 + x^2 + x + x^3 + x^2 + x + 1 \\ &= x^4 + 1 \\ (x+1)^5 &= (x+1)(x^4+1) = x^5 + x + x^4 + 1.\end{aligned} \tag{14.46}$$

And since $\mathbb{Z}_5$ is the largest subgroup in the lattice of $\mathbb{Z}_15$, we know that the elements with largest order not equal to 15 have order 5, and this element has order > 5 since $(x+1)^5 \neq 1$. So it must have order 15. Thus $x + 1$ is a generator.

8. *Determine the splitting field of the polynomial $f(x) = x^p - x - a$ over $\mathbb{F}_p$ where $a \neq 0, a \in \mathbb{F}_p$. Show explicitly that the Galois group is cyclic. [Show $\alpha \mapsto \alpha + 1$ is an automorphism.]*

Proof. Suppose α is a root. Then we have $\alpha^p - \alpha + a = 0$. Behold:

$$\begin{aligned}(\alpha+1)^p - (\alpha+1) - a &= \left(\sum_{k=0}^{p} \binom{p}{k} \alpha^k\right) - \alpha - 1 - a \\ &= \left(\sum_{k=1}^{p-1} \binom{p}{k} \alpha^k\right) + \alpha^p - \alpha - a \\ &= \sum_{k=1}^{p-1} \binom{p}{k} \alpha^k \\ &= \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} \alpha^k.\end{aligned} \tag{14.47}$$

We claim that $\frac{p!}{k!(p-k)!}$ is divisible by p for all integer values of k in the range $[1, p-1]$. Note for these values of k that $p \nmid (k!(p-k)!)$ but that $p|p!$, and the binomial coefficient is an integer, so we must have that $p|\left(\frac{p!}{k!(p-k)!}\right)$. Thus:

$$\sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!}\alpha^k \mod p \equiv 0.$$

And since we are over $\mathbb{F}_p$, we know that $\alpha+1$ must then be a root. The roots of f are $\alpha+k$ for $k = 0, ..., p-1$, hence f is separable, and so $\mathbb{F}_p(\alpha)$ is the splitting field of a separable polynomial, and thus is Galois. And we have an automorphism $\varphi : \alpha \mapsto \alpha + 1$ because an inverse is given by $\alpha \mapsto \alpha - 1 = \alpha + p - 1$, these are both field homomorphisms, and they map $\mathbb{F}_p(\alpha) \to \mathbb{F}_p(\alpha)$, so then G must be cyclic since any other automorphism maps $\alpha \mapsto \alpha + k$ which is φ^k. □

SECTION 14.4

Composite extensions and simple extensions

Wednesday, April 11th

Consider $\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_k}$, where $\pi \in \mathbb{N}$, primes.

Claim. *If $n_1, ..., n_l \in \mathbb{N}$ are square-free and distinct, then $\sqrt{n_1}, ..., \sqrt{n_l}$ are $\mathbb{Q}$-linearly independent.*

Proof. Let $p_1, ..., p_k$ be all prime divisors of $n_1, ..., n_l$:

$$n_1, ..., n_l \in \left\{ \prod p_{i_1} \cdots p_{i_j} \right\}, \tag{14.48}$$

where $\prod_{i \in S} p_i = p_S, S \subseteq \{ 1, ..., K \}$. So $p_{\{1,3,4\}} = p_1 p_3 p_4$.

$\Leftarrow$

Claim. *If $p_1, ..., p_k$ are distinct primes, then $\left\{ \sqrt{p_S} : S \subseteq \{ 1, ..., k \} \right\}$ are $\mathbb{Q}$-linearly independent.*

$\Uparrow$

Claim.

$$[\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_k}) : \mathbb{Q}] = 2^k. \tag{14.49}$$

This claim gives us $\text{Gal}(\mathbb{Q}()/\mathbb{Q}) \cong \mathbb{Z}_2^k$.

Proof. Induction on k. Assume true for $p_1, ..., p_k$. Let p_{k+1} be another prime. Assume that $\sqrt{p_{k+1}} \in \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_k})$. So $\sqrt{p_{k+1}} = \sum_{S \subseteq \{1,...,k\}} a_s \sqrt{p_S}, a_S \in \mathbb{Q}$. If $a_S \neq 0$ for only one S, then $p_{k+1} = a_S^2 p_S$-impossible. Note $p_\varnothing = 1$. If $a_S \neq 0$ for at least two S, $a_{S_1}, a_{S_2} \neq 0$, then $\exists i, S_1, S_2$ such that $i \in S_1, i \notin S_2, a_{S_1}, a_{S_2} \neq 0$. Let $\varphi \in \text{Gal}(\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_k})/\mathbb{Q}) = \mathbb{Z}_2^k$ be defined by:

$$\varphi : \begin{cases} \sqrt{p_i} \mapsto -\sqrt{p_i} \\ \sqrt{p_j} \mapsto \sqrt{p_j}, \forall j \neq i \end{cases}. \tag{14.50}$$

Then:

$$\begin{aligned}\varphi(\sqrt{p_{S_1}}) &= -\sqrt{p_{S_1}}\\ \varphi(\sqrt{p_{S_2}}) &= \sqrt{p_{S_2}}\\ \varphi(\sqrt{p_{k+1}} &= \pm\sqrt{p_{k+1}}.\end{aligned} \tag{14.51}$$

So $\varphi(k) : \pm\sqrt{p_{k+1}} = \sum_S a_S(\pm\sqrt{p_S})$, where we have + for $\sqrt{p_{S_2}}$ and − for $\sqrt{p_{S_2}}$. Subtract or add $(*)$ and $\varphi(*)$ to kill $\sqrt{p_{k+1}}$ then we will have a nontrivial linear combination of $\sqrt{p_S}$ which is = 0, contradiction. □

□

Note $\sqrt{7} = a_0 + a_1\sqrt{3} + a_2\sqrt{15}$.

Observe:

$$\begin{tikzcd}
& K = K_1K_2 \arrow[dl, dash, "n_2"'] \arrow[dr, dash, "n_1"] & & & & 1 \arrow[dl, dash, "n_2"'] \arrow[dr, dash, "n_1"] & \\
K_1 \arrow[dr, dash, "n_1"'] & & K_2 \arrow[dl, dash, "n_2"] & \leftrightarrow & H_1 \arrow[dr, dash, "n_1"'] & & H_2\ . \arrow[dl, dash, "n_2"] \\
& F = K_1 \cap K_2 & & & & G &
\end{tikzcd}$$

We have $H_1 \cap H_2 = 1$, $\langle H_1, H_2\rangle = G$. If $H_1 \trianglelefteq G$, then $G = H_1H_2$.

REMARK 14.40. If $H_1, H_2 \trianglelefteq G$, then $G = H_1 \times H_2$.

So if $K_1/F, K_2/F$ are both normal, then:

$$\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K/K_1) \times \mathrm{Gal}(K/K_2). \tag{14.52}$$

Also, $G/H_1 \cong H_2, G/H_2 \cong H_1$. So:

$$\begin{aligned}\mathrm{Gal}(K_1/F) &\cong \mathrm{Gal}(K/K_2)\\ \mathrm{Gal}(K_2/F) &\cong \mathrm{Gal}(K/K_1).\end{aligned} \tag{14.53}$$

So $\mathrm{Gal}(K/F) \cong \mathrm{Gal}(K_1/F) \times \mathrm{Gal}(K_2/F)$.

Observe:

$$\begin{tikzcd}
& \mathbb{Q}\left(\sqrt{p_1}, ..., \sqrt{p_k}\right) = K \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt{p_1}) \arrow[dr, dash, "2"'] & \cdots \arrow[d, dash] & \mathbb{Q}(\sqrt{p_k})\ . \arrow[dl, dash] \\
& \mathbb{Q} &
\end{tikzcd}$$

Since $[K : \mathbb{Q}] = 2^k$, $\mathbb{Q}(\sqrt{p_i}) \cap \mathbb{Q}(\sqrt{p_1}, ..\cancel{\sqrt{p_i}}.., \sqrt{p_k}) = \mathbb{Q}$. S:

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_k})/\mathbb{Q}) \cong \prod_{i=1}^{k} \mathrm{Gal}(\mathbb{Q}(\sqrt{p_i})/\mathbb{Q}) \cong \mathbb{Z}_2^k. \tag{14.54}$$

Consider:

$$\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_k}) \overset{\supseteq}{=} \mathbb{Q}(\sqrt{p_1} + \cdots + \sqrt{p_k} = \alpha). \tag{14.55}$$

Then α has 2^k conjugates: $\pm\sqrt{p_1}, ..., \pm\sqrt{p_k}$ - all distinct. So $\deg_{\mathbb{Q}} \alpha = 2^k$, so $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_k})$.

THEOREM 14.41. *If K/F is finite and separable, then it has only finitely many subextensions.*

Proof. If it is Galois, then subextensions correspond to subgroups, and finitely many subgroups gives us finitely many subextensions. But we do not assume this. Let E/F be the Galois closure (= normal closure) of K/F. Then E/F has only finitely many subextensions (since $\mathrm{Gal}(E/F)$ has only finitely many subgroups), so K/F has finitely many subextensions. □

If this is not separable, it is not true, it may be that there are infinitely many subgroups.

Theorem 14.42 (**On the primitive element**). *If K/F is finite and separable, then there is $\alpha \in K$ such that $K = \mathbb{F}(\alpha)$. (α is called "primitive" for K.)*

Proof. **Case 1:** F is finite.

Then K is also finite, $K = \mathbb{F}_{p^r}$ for some p, r, and then $K = \mathbb{F}_p(\alpha)$, where α is a generator of K^*. For finite fields we know they are simple over $\mathbb{F}_p$.

Case 2: F is infinite.

Then K, as an F-vector space, is not a union of finitely many proper subspaces. So there is no α which does not belong to any subextension, so $K = F(\alpha)$. (**not sure if this statement is correct, please help**) □

Thursday, April 12th

There was a question about nonexistence of a primitive element in a non-separable extension.

Example 14.43. Let $K = \mathbb{F}_p(x, y)$, $F = \mathbb{F}_p(x^p, y^p)$. K/F is non-separable, and $[K : F] = p^2$. Note x satisfies $t^p - x^p$. y satisfies $t^p - y^p$. So total degree is p^2. The property is that $\forall \alpha \in K \smallsetminus F$, $[F(\alpha) : F] = p$. So α is not primitive. There are infinitely many subfields. What is α?

$$\begin{aligned} \alpha &= \frac{f(x,y)}{g(x,y)}, f, g \in \mathbb{F}_p(x,y) \\ \alpha^p &= \frac{f(x^p,y^p)}{g(x^p,y^p)} \in F. \end{aligned} \tag{14.56}$$

When Professor Leibman proved the theorem of the primitive element, we used the following Lemma:

Lemma 14.44. *Let F be an infinite field, V is an F-vector space, and $V_1, \ldots, V_k$ be proper subspaces. Then $V \neq \bigcup_{i=1}^k V_i$.*

Proof. Assume $V_1 \notin \bigcup_{i=2}^k V_i$. If it belongs to the union then we can nix it from the list. Take $u \in V_1 \smallsetminus \bigcup_{i=1}^k V_i$, $v \notin V_1$. Let $L = \{ u + av : a \in F \}$, the straight line through these two points. Then $L \cap V_1 = \{ u \}$. And $\forall i = 2, \ldots, k$, $|L \cap V_I| \leqslant 1$, since if $u + a_1 v, u + a_2 v \in V_i$, then $L \subseteq V_i$ (it is a straight line), but $u \in V_i$. So:

$$\left| L \cap \left(\bigcup_{i=1}^k V_i \right) \right| \leqslant k, \tag{14.57}$$

but L is infinite, so $L \notin \bigcup_{i=1}^k V_i$. □

From this it follows that if an extension has only finitely many subextensions, then it has a primitive element. And from Galois theory, it follows that if you have a Galois extension, it has only finitely many subextensions, since the Galois group has only finitely many subgroups.

We discuss the fundamental theorem of algebra: that $\mathbb{C}$ is algebraically closed. Equivalently: $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$. Any polynomial $f \in \mathbb{R}[x]$ splits in $\mathbb{C}$.

(1) If $\deg f$ is odd, then f has a root in $\mathbb{R}$, so is reducible unless $\deg f = 1$.
(2) Any quadratic extension of $\mathbb{R}$ is isomorphic to $\mathbb{C}$.
(3) $\mathbb{C}$ has no nontrivial quadratic extensions.

$x^2 + ax + b$ means roots are $\frac{-a\pm\sqrt{a^2-4b}}{2} = \frac{-a\pm ci}{2} \in \mathbb{C}$. If $a^2 - 4b \geqslant 0$ then roots are in $\mathbb{R}$.

Proof. Let $f \in \mathbb{R}[x]$, let K be it's splittinf field. Let $G = \mathrm{Gal}(f) = \mathrm{Gal}(K/\mathbb{R})$. Let H be the Sylow 2-subgroup of G, so that $|G : H|$ is odd. Recall this is a maximal subgroup whose order is a power of 2. And $|G| = 2^k p_1^{r_1} \cdots p_l^{r_l}$. $|H| = 2^k$. Let $L = \mathrm{Fix}(H)$. Then $[L : \mathbb{R}] = |G : H|$ is odd. But this is impossible since take any element $\alpha \in L \smallsetminus \mathbb{R}$. Then $\deg m_{\alpha,\mathbb{R}}$ is odd. It divides the degree of L. So it is reducible, impossible unless $\alpha \in \mathbb{R}$ (linear polynomials are irreducible). So $G = H$, and is a 2-group, $|G| = 2^k$. Any 2-group has a normal series of subgroups, $1 = N_0 < N_1 < \ldots < N_k = G$ such that $\forall i$, $N_{i+1}/N_i \cong \mathbb{Z}_2$. So K has a tower of subextensions:

$$\begin{tikzcd}
1 \arrow[d, dash] & & K \arrow[d, dash] \\
N_1 \arrow[d, dash] & & K_1 \arrow[d, dash] \\
\vdots \arrow[d, dash] & & \vdots \arrow[d, dash] \\
G = N_k & & K_k = \mathbb{R}
\end{tikzcd},$$

such that $\forall i$, $[K_i : K_{i+1}] = 2$. But then $K_{k-1} \cong \mathbb{C}$, so K_{k-2}/K_{k-1} cannot exist, and then tower is just $\mathbb{C}/\mathbb{R}$.

□

14.4 Exercises

1. *Find the Galois closure of* $\mathbb{Q}(\sqrt{1+\sqrt{2}})$ *over* $\mathbb{Q}$.
We have:

$$\begin{tikzcd}
\mathbb{Q}(\sqrt{1+\sqrt{2}}) \arrow[d, dash] & \mathbb{Q}(\sqrt{1-\sqrt{2}}) \arrow[d, dash] \\
\mathbb{Q}(\sqrt{2}) \arrow[d, dash] & \mathbb{Q}(-\sqrt{2}) \arrow[dl, dash] \\
\mathbb{Q} &
\end{tikzcd}.$$

We need to find the conjugates of the generator. So the answer is:

$$K = \mathbb{Q}(\sqrt{1+\sqrt{2}}, \sqrt{1-\sqrt{2}}). \tag{14.58}$$

Note the conjugates of $\sqrt{1+\sqrt{D}}$ are $\pm\sqrt{1\pm\sqrt{2}}$. Note $\alpha = \sqrt{1+\sqrt{2}}$. This satisfies $x^2-(1+\sqrt{2}) = m_{\alpha,\mathbb{Q}(\sqrt{2})}$. Also $x^2-(1-\sqrt{2})$. To make sure the top extension is nontrivial, we need to check that there is no element in $\mathbb{Q}(\sqrt{2})$ such that $(a+b\sqrt{2})^2 \overset{?}{=} 1+\sqrt{2}$.

5. *p-extensions. (p is prime).* These are polycyclic extensions where each extension has degree p. Equivalently, Galois closure has degree p^k, and Galois group is a p-group. Picture is the same as that for constructible numbers, except instead of 2, we have p. The theory is parallel to the theory of p-groups. Note p-extension of p-extension is p-extension.

SECTION 14.5

Cyclotomic extensions and abelian extensions over $\mathbb{Q}$

Definition 14.45. A Galois extension K/F is **abelian** if $\mathrm{Gal}(K/F)$ is abelian.

Definition 14.46. If G is abelian, $G \cong \mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_k}$, so if K/F is abelian, then K is a **direct composite**, $K = K_1K_2\cdots K_k$ of cyclic subextensions.

We have:

$$\begin{tikzcd}
 & & K \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
K_1 \arrow[drr, dash, "n_1"'] & K_2 \arrow[dr, dash, "n_2"] & K_3 \arrow[d, dash, "n_3"] & \cdots \arrow[dl, dash] & K_k \arrow[dll, dash, "n_k"] \\
 & & F & &
\end{tikzcd},$$

such that $\forall i, K_i \cap \prod_{j\neq i} K_j = F$. Then $K_1 = \mathrm{Fix}(\mathbb{Z}_{n_2}\times\cdots\times\mathbb{Z}_{n_k})$. Let's say that K is a **direct composite** of K_1 and K_2 if:

$$[K:F] = [K_1:F][K_2:F].$$

Remark 14.47. IF K/F is abelian, then $\forall$ subextension L/F is normal. In particular, $\forall\alpha\in K$. $F(\alpha)/F$ is normal (all conjugates of α are in $F(\alpha)$).

Example 14.48. Cyclotomic extension $\mathbb{Q}(\omega)/\mathbb{Q}$, $\omega = e^{2\pi i/n}$. Conjugates of ω are ω^k, $(k,n)=1$.

We discuss cyclotomic extensions. Note:

$$\mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q}) \cong \mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{r_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{r_k}}^*, \tag{14.59}$$

where $n = p_1^{r_1} \cdots p_k^{r_k}$.

SECTION 14.6

Galois groups of polynomials

Monday, April 16th

Definition 14.49. A polynomial $f(x_1, \ldots, x_n)$ is **symmetric** if

$$f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$$

$\forall \sigma \in S_n$.

Example 14.50. $x_1x_2^2 + x_2x_1^2 + x - 1x_3^2 + x_3x_1^2 + x_2x_3^2 + x_3x_2^2 \in F[x_1, x_2, x_3]$. In $F[x_1, x_2]$, $x_1^3 + x_2^3 + 2x_1x_2 - 3x_1^2x_2 - 3x_1x_2^2$.

Remark 14.51. Elementary symmetric polynomials:

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + x_2x_3 + \cdots + x_{n-1}x_n \\ s_3 &= \sum_{i<j<k} x_ix_jx_k, \\ &\vdots \\ s_n &= x_1x_2\cdots x_n. \end{aligned} \tag{14.60}$$

Tuesday, April 17th

$x_1, \ldots, x_n$ are variables.

Definition 14.52. **Elementary symmetric polynomials**:

$$\begin{aligned} s_1 &= x_1 + x_2 + \cdots + x_n \\ s_2 &= x_1x_2 + x_1x_3 + x_2x_3 + \cdots + x_{n-1}x_n \\ s_3 &= \sum_{i<j<k} x_ix_jx_k, \\ &\vdots \\ s_n &= x_1x_2\cdots x_n. \end{aligned} \tag{14.61}$$

Remark 14.53. If:

$$\begin{aligned} f(x) &= x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \\ &= (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n) \\ &= x^n - (\alpha_1 + \cdots + \alpha_n)x^{n-1} + (\alpha_1\alpha_2 + \cdots + \alpha_{n-1}\alpha_n)x^{n-2} - \cdots \pm \alpha_1\alpha_2\cdots\alpha_n. \end{aligned} \tag{14.62}$$

So:

$$\begin{aligned} a_{n-1} &= -s_1(\alpha_1, \ldots, \alpha_n) \\ a_{n-2} &= s_2(\alpha_1, \ldots, \alpha_n) \\ a_{n-k} &= (-1)^k s_k(\alpha_1, \ldots, \alpha_n). \end{aligned} \tag{14.63}$$

So the coefficients of a polynomial are ± elementary symmetric polynomials of its roots.

Theorem 14.54. *Any symmetric polynomial is a polynomial in elementary symmetric polynomials:*

$$f(x_1,...,x_n) = g(s_1(x_1,...,x_n),...,s_n(x_1,...,x_n)), \tag{14.64}$$

for some g.

Corollary 14.55. *Any symmetric expression (polynomial) of the roots of a polynomial $f = x_n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ is a polynomial expression in $a_{n-1},...,a_0$.*

Example 14.56. For $f = x^2 + bx + c$, with roots α_1, α_2, we have:

$$(\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (-b)^2 - 4c = b^2 - 4c. \tag{14.65}$$

Consider the field $K = F(x_1,...,x_n)$ - field of rational functions in x_i. Take:

$$f = (x - x_1)\cdots(x - x_n) = x^n - s_1x^{n-1} + s_2x^{n-2} + \cdots \pm s_n, \tag{14.66}$$

$f \in L[x]$, where $l = F(s_1,...,s_n)$, $s_i = s_i(x_1,...,x_n)$. Then K is the splitting field of f over L. So, $[K : F] \leqslant N!$. The group S_n acts on K by permuting $x_1,...,x_n$, and $L \subseteq \mathrm{Fix}(S_n)$, which is the field of symmetric rational functions. We proved that $[K : \mathrm{Fix}(S_n)] = |S_n| = n!$. So $L = \mathrm{Fix}(S_n)$, so any symmetric rational function is in L. So we get that any symmetric rational function in $x_1,...,x_n$ is a rational function in $s_1,...,s_n$.

Corollary 14.57.

$$\mathrm{Gal}(K/L) = S_n. \tag{14.67}$$

Corollary 14.58. *For any finite group G, there exists a Galois extension K/E with* $\mathrm{Gal}(K/E) \cong G$.

Proof. Let K/L be as above. For n such that $G \leqslant S_n$, let $E = \mathrm{Fix}(G)$. Then $\mathrm{Gal}(K/E) = G$. □

Solvability of polynomials in radicals.

Are we allowed to use $\sqrt[n]{1}$? We will start with allowing this, but each root of unity can be expressed as classical radicals. But let's start by assuming that all roots of unity are obtainable. We want to solve polynomials in radicals, find the roots as expressions in radicals. We will allow using roots of unity first. We are in an abstract environment, not $\mathbb{C}$. We start by assuming that F contains roots of unity. Let n be given, and let F be a field of characteristic not dividing n. What are roots of unity in F? Roots of unity of degree n in F are roots of the polynomial $x^n - 1$. If the characteristic doesn't divide n, then the polynomial is separable. Assume that they are all in F, so we have n roots of unity. They form a group under multiplication, which is cyclic. This follows from the following fact:

Lemma 14.59. *Any finite subgroup of F^* is cyclic.*

Remark 14.60. The group of roots of unity in $\mathbb{C}$ is not cyclic nor finite, but the group of roots on unity of degree n is both.

So there is a primitive root of unity, ω, such that all roots are $1, \omega, \omega^2, ..., \omega^{n-1}$. Let $a \in F$, and consider the field $K = F(\sqrt[n]{a})$ - a **simple radical extension**.

THEOREM 14.61. *K/F is Galois for the just-defined K, and* $\mathrm{Gal}(K/F)$ *is cyclic.*

PROOF. Let $\alpha = \sqrt[n]{a}$ - root of $x^n - a$. All other roots of $x^n - a$ are

$$\alpha, \alpha\omega, \alpha\omega^2, ..., \alpha\omega^{n-1}.$$

So the polynomial splits in K, so K/F is Galois. □

We have automorphisms $\varphi_m : K \to K$, $\alpha \mapsto \alpha\omega^m$ for some m, and any $\varphi \in \mathrm{Gal}(K/F)$ is of this sort. Also note:

$$\varphi_m \varphi_l = \varphi_{m+l} : \alpha \mapsto \alpha\omega^{m+l}. \tag{14.68}$$

So we have a homomorphism $\mathrm{Gal}(K/F) \to \mathbb{Z}_n$ defined by $\varphi_m \mapsto m$, which is injective since φ_m is uniquely defined by m. So, $\mathrm{Gal}(K/F) \cong$ a subgroup of $\mathbb{Z}_n$, so is cyclic. This is under the assumption that $\omega \in F$. If not, we note that $\mathrm{Gal}(x^3 - 2/\mathbb{Q}) \cong S_3$ - since $\omega = e^{2\pi i/3} \notin \mathbb{Q}$. And $\mathrm{Gal}(x^3 - 2/\mathbb{Q}(\omega)) \cong \mathbb{Z}_3$.

It turns out that the converse is true: any cyclic extension is radical.

THEOREM 14.62. *(Assuming $\omega \in F$.) Let K/F be cyclic (K/F is Galois, and* $\mathrm{Gal}(K/F)$ *is cyclic). And also, we always assume that the characteristic of the* $\mathrm{char}F \nmid n$*. Then K/F is simple radical: $K = F(\alpha)$ such that $\alpha^n \in F$.*

PROOF. For $\alpha \in K$, the **Lagrange resolvent** of α is:

$$(\alpha, \omega) = \alpha + \omega\varphi(\alpha) + \omega^2\varphi^2(\alpha) + \cdots + \omega^{n-1}\varphi^{n-1}(\alpha). \tag{14.69}$$

Let φ be such that $\mathrm{Gal}(K/F)$ is generated by φ. So $\mathrm{Gal}(K/F) = \{1, \varphi, ..., \varphi^{n-1}\}$.

Let $\gamma = (\alpha, \omega)$. ($\gamma \neq 0$?) Then:

$$\begin{aligned}\varphi(\gamma) &= \varphi(\alpha) + \omega\varphi^2(\alpha) + \cdots + \omega^{n-1}\varphi^n(\alpha) \\ &= \omega^{-1}\gamma.\end{aligned} \tag{14.70}$$

Note $\varphi^n(\alpha) = \alpha$. So we have $\varphi(\gamma^n) = \omega^{-n}\gamma^n = \gamma^n$. So γ^n is fixed by φ, so by $\mathrm{Gal}(K/F)$, so $\gamma^n \in F$.

γ has n distinct conjugates $\gamma, \omega^{-1}\gamma, \omega^{-2}\gamma, ..., \omega^{-(n-1)}\gamma$, so $\deg_F \gamma = n$, so $K = F(\gamma)$ with $\gamma^n \in F$. □

Thursday, April 19th

THEOREM 14.63. *$f \in F[x]$ is solvable in radicals if and only if* $\mathrm{Gal}(f/F)$ *is solvable.*

PROOF. (⇒) Assume that all roots of f are contained in polyradical extensions. If f is irreducible, it's enough if just one root is contained in a polyradical extension. Take the Galois closure of the composite of all these extensions, it will be a polyradical Galois extension (because the composite of polyradical extensions is polyradical). So, let K/F be a Galois polyradical extension containing the splitting field of f. Let $N \leqslant [K : F]$, let ω be a primitive root of unity of degree n. Let $F' = F(\omega)$, $K' = KF' = K(\omega)$. So we have the diagram:

$$\begin{tikzcd}
 & K' \arrow[dl, dash] \arrow[d, dash] \\
K \arrow[d, dash, "polyradical"'] & F' \arrow[dl, dash] , \\
F &
\end{tikzcd}$$

so K'/F' is also polyradical, since if $K_{i+1} = K_i(\sqrt[n]{a_i})$, then $F'K_{i+1} = F'K_i(\sqrt[n]{a_i})$. And K'/F' is Galois, $\omega \in F'$, so K'/F' is Galois polyquadratic extension, so $\mathrm{Gal}(K'/F')$ is polycyclic = solvable. $\mathrm{Gal}(K'/F') \trianglelefteq \mathrm{Gal}(K'/F)$ since F'/F is Galois. And $\mathrm{Gal}(K'/F)/\mathrm{Gal}(K'/F') = \mathrm{Gal}(F'/F)$ - abelian (cyclotomic extension). So,

$$1 \to \mathrm{Gal}(K'/F') \to \mathrm{Gal}(K'/F) \to \mathrm{Gal}(F'/F) \to 1 \tag{14.71}$$

where the groups on the left and right are solvable, so the middle must be solvable. Note $\mathrm{Gal}(f/F)$ is a factor group of $\mathrm{Gal}(K'/F)$, so is also solvable.

($\Leftarrow$) Assume $\mathrm{Gal}(f/F)$ is solvable. Let K be the splitting field of f, let $N = [K : F]$, let ω be a primitive root of unity of degree N. Let $F' = F(\omega)$, $K' = K(\omega) = KF'$. We have

$$\begin{tikzcd}
 & K' \arrow[dl, dash] \arrow[d, dash] \\
K \arrow[d, dash] & F' \arrow[dl, dash] . \\
F &
\end{tikzcd}$$

And K'/F' is Galois. Now K/F is polycyclic.

Claim. *K'/F' is also polycyclic.*

Lemma 14.64. *If K_2/K_1 is cyclic, then $\forall F'$, K_2F'/K_1F' is cyclic.*

Lemma 14.65. *If G is finite, G is solvable if and only if it is polycyclic.*

□

Proof. Why? Because if G is solvable,

$$1 = H_0 \triangleleft H_1 \triangleleft H_2 \triangleleft \ldots \triangleleft H_m = G \tag{14.72}$$

$$H_{i+1}/H_i \text{ - abelian } \forall i \tag{14.73}$$

and these are products of cyclic groups and have series with cyclic factors. So we have:

$$N_1 \triangleleft N_2 \triangleleft \ldots = H_{i+1}/H_i, \tag{14.74}$$

with N_{j+1}/N_j cyclic for all j. Then:

$$H_i \triangleleft H_iN_1 \triangleleft H_iN_2 \triangleleft \ldots \triangleleft H_{i+1} \triangleleft \ldots \tag{14.75}$$

□

Definition 14.66. A **polyradical** extension is an extension of the form:

$$\begin{tikzcd}
K_n \arrow[d, dash] \arrow[ddd, dash, bend left=50, "polyradical\ ."] \\
\vdots \arrow[d, dash] \\
K_1 \arrow[d, dash] \\
F
\end{tikzcd}$$

And the short lines are the simple radical extensions.

Remark 14.67. If $\mathrm{Gal}(f/F) \cong S_n$ with $n \geqslant 5$, then f is not solvable in radicals.

Consider polynomials of the form $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$, where a_i are symbols. Consider $f(x) \in \mathbb{Q}(a_0, a_1, .., a_{n-1})[x]$. Then we have:

$$\mathrm{Gal}(f/\mathbb{Q}(a_0, ..., a_{n-1})) \cong S_n, \tag{14.76}$$

so for $n \geqslant 5$, the "general" polynomial is not solvable.

Consider $A_n \lhd S_n$, we have $|S_n : A_n| = 2$. So, if $\mathrm{Gal}(f/F) \cong S_n$, then K/F must contain a subextension of degree 2 (where K is the splitting field of f). $E = F(d)$, $d^2 \in F$. $\forall$ even $\sigma \in S_n$, $\sigma(d) = d$. $\forall$ odd $\sigma \in S_n$, $\sigma(d) = -d$. So we have $d = \prod_{i<j}(\alpha_j - \alpha_i)$. Now d^2 is a symmetric polynomial in α_i, so d^2 is a polynomial in coefficients of f, so $d^2 \in F$.

Definition 14.68. $D = d^2 = \prod_{i<j}(\alpha_j - \alpha_i)^2$ is called the **discriminant** of a polynomial f, whose foots are $\alpha_1, ..., \alpha_n$.

Example 14.69. $n = 2$. $f(x) = x^2 + bx + c$. $d = (\alpha_2 - \alpha_1)$. Then

$$D = (\alpha_2 - \alpha_1)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (-b^2) - 4c = b^2 - 4c. \tag{14.77}$$

Friday, April 20th

Let $f \in F[x]$, $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = (x - \alpha_1)\cdots(x - \alpha_n)$. The discriminant of f is $\prod_{i<j}(\alpha_i - \alpha_j)^2$, and is a polynomial in a_i.

For $n = 2$, $f = x^2 + b + c$, $D = b^2 - 4c$.

For $n = 3$, $f = x^3 + px + q$, $D = -4p^3 - 27q^2$.

If $f = x^3 + ax^2 + bx + c$, then replacing $x + \frac{a}{3}$ by x, we get the above).

For $n = 4$, $f = x^4 + px^2 + qx + r$, $D = 16p^4r - 4p^3q^2 - \cdots$.

Theorem 14.70. *$\mathrm{Gal}(f/F) \leqslant A_n$ if and only if $\sqrt{D} \in F$. ($D = d^2$ for some $d \in F$).*

Proof. Let $d = \prod_{i<j}(\alpha_i - \alpha_j)$, $d = \sqrt{D}$. Any permutation of the roots of f:

$$\sigma(d) = \begin{cases} d & \text{if } \sigma \text{ is even,} \\ -d & \text{if } \sigma \text{ is odd.} \end{cases} \tag{14.78}$$

$\mathrm{Gal}(f) \leqslant A_n$ if and only if d is fixed by $G = \mathrm{Gal}(f)$, if and only if $d \in F$. □

Cubic: $f(x) = x^3 + px + q$ - irreducible. Let $G = \mathrm{Gal}(f) \leqslant S_3$. Any root can be sent to any other root. Or we can say that the order of the group is the degree of the splitting field. We want to show that G contains a 3-cycle for sure. G is transitive on the roots, or $3||G|$, so $G \geqslant A_3 \cong \mathbb{Z}_3$. So either $G \cong S_3$, or $G \cong A_3 \cong \mathbb{Z}_3$.

Definition 14.71. For groups, a group action being **transitive** means any element can be sent to any other element.

Note $A_3 = \langle (1,2,3) \rangle$. So $G \cong S_3$ if and only if $\sqrt{D} \notin F$, $G \cong \mathbb{Z}_3$ if and only if $\sqrt{D} \in F$.

If $F \subseteq \mathbb{R}$, if f has 1 real and 2 non-real roots, then $\mathrm{Gal}(f) \cong S_3$, because $\mathbb{Z} \mapsto \overline{z}$ acts as a transposition of 2 roots of f.

Example 14.72. (1) $x^3 + x + 1$. $D < 0$, $\mathrm{Gal}(f/\mathbb{Q}) \cong S_3$.

(2) $x^3 - 3x + 1$. $D = 81$, $\sqrt{D} \in \mathbb{Q}$, so $\mathrm{Gal}(f/\mathbb{Q}) \cong \mathbb{Z}_3$. If you adjoin one root, you already get all the roots, since they are expressible in the first root.

Note $\mapsto -i$ is an automorphism of all of $\mathbb{C}$, so it's definitely an automorphism of other stuff...?

Theorem 14.73 (**Casus irreducibilis**). *If f is irreducible, has all 3 roots real, then you cannot express these roots as only real radicals, you need to use complex numbers. You need $\omega = \frac{-1+\sqrt{-3}}{2}$.*

Jake: Can you give us an example of this fact?
Leibman: This is a negative fact, there are no examples.

Definition 14.74. **Cardano formulas:**

$$\begin{aligned} A &= \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3}D}, \\ B &= \sqrt[3]{-\frac{27}{2} - \frac{3}{2}\sqrt{-3}D}, \\ AB &= -3p. \\ \alpha_1 &= \frac{A+B}{2}, \\ \alpha_2 &= \frac{\omega^2 A + \omega B}{3}, \\ \alpha_3 &= \frac{\omega A + \omega^2 B}{3}. \end{aligned} \tag{14.79}$$

Quartics: $x^4 + px^2 + qx + r$ - irreducible.
S_4 is solvable:

$$\begin{tikzcd}
1 \arrow[dd, no head, "4"'] \arrow[dr, no head] & & & K \arrow[dd, no head, "4"'] \\
& \mathbb{Z}_2 \arrow[dl, no head] & & \\
V_4 \arrow[d, no head, "3"] & & \rightarrow & L \arrow[d, no head, "3"'] & . \\
A_4 \arrow[d, no head, "2"'] & & & F(\sqrt{D}) \arrow[d, no head, "2"'] \\
S_4 & & & F
\end{tikzcd}$$

If $\sqrt{D} \in F$, then $G \leqslant A_4$. Note L/F is the splitting field of some polynomial whose roots are:

$$\begin{aligned}
\Theta_1 &= (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) \\
\Theta_2 &= (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4) \qquad (14.80) \\
\Theta_3 &= (\alpha_1 + \alpha_4)(\alpha_2 + \alpha + 3).
\end{aligned}$$

This polynomial is: $h(x) = x^3 + 2px^2 + (p^2 - 4r)x + q^2$ is the resolvent cubic of f. A nice fact is that $D(h) = D(f)$.

Let $G = \mathrm{Gal}(f)$. If h is irreducible, then if $\sqrt{D} \notin F$, then $G \nleqslant A_4$, $6 \mid |G|$, so $G \cong S_4$. If $\sqrt{D} \in F$, then $G \leqslant A_4$, $3||G|$, so $G = A_4$.

If h is reducible, then: if $\Theta_1, \Theta_2, \Theta_3 \in F$, then $G \cong V_4$. If only $\Theta_1 \in F$, then $G \cong D_8$, or $\mathbb{Z}_4$.

Take $K = F(x_1, ..., x_n)$, G acts on these variables, $\mathrm{Fix}(F) = L$, $\mathrm{Gal}(K/L) \cong G$, then take α-primitive of K/L, $f = m_{\alpha,L}$. I don't know what this means.

CHAPTER A

Category theory

We discuss objects, morphisms.

$A \to B$.

We call this pair of an object and a morphism a **category**. An object A is **repelling** if for any other object B, there is a single morphism from A to this object.

And **attracting** if there exists a single morphism from $B \to A$.

Another terminology: **initial** and **terminal** objects.

If such an object exists in a category, it is unique.

Lemma A.1. *Any such (repelling or attracting) object is unique up to isomorphism.*

Proof. If there are two such universal objects, then there is a single unique morphism $\varphi_1 : A_1 \to A_2$. And a single unique morphism $\varphi_2 : A_2 \to A_1$ and their composition is a single morphism $\varphi_1\varphi_2 : A_2 \to A_2$, which must be the identity on A_2, and $\varphi_2\varphi_1$ is the identity on A_1. □

Consider the category of groups with n marked elements, where a morphism between $(G, a_1, ..., a_n)$ and $(H, b_1, ..., b_n)$ is a hom-sm $\varphi : G \to H$ s.t. $\varphi(a_i) = b_i$ for all elements.

Then $F_n = \langle a_1, ..., a_n \rangle$, the free group with n generators, is a universal repelling object in this category.

Given $\forall H$, $b_1, ..., b_n \in H$, we have a unique hom-sm $\varphi : F_n \to H$ s.t. $\varphi(a_i) = b_i \ \forall i$.

So the category is a set of all pairs of objects an morphisms which satisfies the properties of the definition of the category. So the category above is the type of group (groups with n marked elements) and the type of morphism.

We define a new category, where R is a unital ring:

- objects = R-modules with n marked elements $(a_1, ..., a_n)$.
- morphisms = R-hom-sms s.t. $\varphi(a_i) = b_i \ \forall i$.

Then the universal repelling object is:

$$(R^n, e_1, ..., e_n),$$

where $e_1 = (1, 0, ..., 0)$, $e_2 = (0, 1, 0, ..., 0)$ and so on.

Given $(M, u_1, ..., u_n)$, define $\varphi : R^n \to M$ by $(a_1, ..., a_n) \to a_1u_1 + \cdots + a_nu_n$. And note that $\varphi(e_i) = i_i$.

Definition A.2. The direct product of R-modules M_1, M_2 is:

$$M_1 \times M_2 = \{(u_1, u_2) : u_i \in M_i\},$$

with:

$$(u_1, u_2) + (v_1, v_2) = (u_1 + v_1, u_2 + v_2),$$
$$a(u_1, u_2) = (au_1, au_2),$$

where $a \in R$. It is also called the **direct sum**, and denoted by $M_1 \oplus M_2$.

Now we define the category.

Category. Objects are modules M with hom-sms $\varphi_1 : M_1 \to M$, $\varphi_2 : M_2 \to M$.

Morphisms: hom-sms $\varphi_1 : M \to N$ identical on M_1, M_2:

$$\begin{tikzcd}
 & M_1 & \\
M \arrow[ur, "\varphi_1"] \arrow[rr, "\varphi"] & & N \cdot \arrow[ul, "\psi_1"'] \\
 & M_2 \arrow[ul, "\varphi_2"] \arrow[ur, "\psi_2"'] &
\end{tikzcd}$$

Friday, January 12th

We give an example of a category where the morphisms are not well-defined mappings.

Define: Objects = groups.

Morphisms = classes of conjugate hom-sms.

Definition A.3. Reacll that $\varphi \equiv \psi$ (these two hom-sms are **conjugate**) if $\psi(g) = a\varphi(g)a^{-1}$ for some $a \in H$, where $\varphi, \psi : G \to H$.

We give an other example of a category:

Objects = topological spaces.

Morphisms = classes of homotopic continuous mappings. Note that these morphisms are not mappings because images of points are not uniquely defined.

CHAPTER B

SAMPLE PROBLEMS TO MIDTERM I

1. *Prove that if R is an integral domain, then $Tor(M)$ is a submodule of M (called the torsion submodule of M).*

   PROOF. We know $\text{Tor}(M)$ is a subset of M by its definition. We first prove it is an additive subgroup. Let $m \in \text{Tor}(M)$. Then $\exists r \in R$, $r \neq 0$ s.t. $rm = 0$. Then consider $-m \in M$. From exercise 1 we know $-m = (-1)m$, so we have:

   $$r(-m) = r(-1)m = (-1)rm = (-1)0 = 0,$$

   since R is commutative. So we have that $-m \in \text{Tor}(M)$ as well, hence we have additive inverses. We check that it has additive closure. Let $m, n \in \text{Tor}(M)$. Then we have $r, s \in R$, neither being zero, s.t. $rm = 0, sn = 0$. Now consider $m + n$. We have:

   $$rs(m+n) = rsm + rsn = srm + rsn = s0 + r0 = 0.$$

   Since we have no zero divisors, since R is an integral domain, we know $rs \neq 0$, so $m + n \in \text{Tor}(M)$, we have additive closure, and $\text{Tor}(M)$ is a subgroup of M. Now we need only check that it is closed under the left action of R. So let $r \in R$ and $m \in \text{Tor}(M)$. Then consider rm. We assume $r \neq 0$, since otherwise $rm = 0$ which is in our subgroup. And we know $\exists s \in R$, $s \neq 0$ s.t. $sm = 0$. Now we have $srm = rsm = r0 = 0$, so rm is in $\text{Tor}(M)$. So it's a submodule. □

   PROOF. An easier proof. Using the submodule criterion, we just need an $s \in R$ s.t. $s(x + ry) = 0$ by definition of $Tor(M)$ since we want to show an arbitrary $x + ry \in Tor(M)$. But taking s to be the product of the two annihilators of x, y we have that s and it is nonzero since integral domain. Done. □

2. *If R is a PID and M an R-module, and a_1, a_2 relatively prime, prove $Ann(a_1a_2) = Ann(a_1) \oplus Ann(a_2)$.*

   PROOF. Let $I = (a_1), J = (a_2)$. Then since we are in a PID, we know $Ann(a_1) = Ann(I)$ and the same for J. Then note that I, J are comaximal since a_1, a_2 are relatively prime, and we are in a PID, thus $I + J = (1) = R$. Also note that $Ann(a_1a_2) = Ann(I \cap J)$ since $(a_1a_2) = (a_1) \cap (a_2)$. Let $m \in Ann(I + J) = Ann((1)) = Ann(R)$ since I, J are comaximal, and R is commutative and unital. So $rm = 0$ for all $r \in R$. So then $m \in Ann(I)$, and since $0 \in Ann(J)$, we may write $m = m + 0$, so $m \in Ann(I) + Ann(J)$. And thus $Ann(I + J) \subseteq Ann(I) + Ann(J)$. The other inclusion is trivial. So we have that $Ann(a_1a_2) = Ann(a_1) + Ann(a_2)$. By Theorem 10.67, we have have that their intersection is trivial since if $m \neq 0$ and $a_1m = 0$ and $a_2m = 0$. Since a_1, a_2 are coprime we have $r, s \in R$ s.t. $ra_1 + sa_2 = 1$. So we also have $ra_1m = 0$ and $sa_2m = 0$. So then we have:

$$(ra_1 + sa_2)m = 1m = m = 0.$$

So $Ann(a_1) \cap Ann(a_2) = 0$. So by Theorem 10.67 we know $Ann(a_1a_2) = Ann(a_1) \oplus Ann(a_2)$. □

3. *Let M be a module S be a subset of R, and I be the ideal generated by S. Prove that $Ann(S) = Ann(I)$ in M.*

   Proof. Let $m \in Ann(S)$. Then $sm = 0$ $\forall s \in S$. Note $I = RS$. Let $i \in I$. Then $i = rs'$ for some $s' \in S$. Then we have:

   $$im = rs'm = r \cdot 0 = 0,$$

   since m annihilates s'. Now let $m \in Ann(I)$. Then $im = 0$ $\forall i \in I$. Note $S \subseteq I$ since we just take $r = 1$ in the expression rs which is the form taken by every element in I. So $m \in Ann(S)$. □

4. (a) *Give an example of a submodule that is not a direct summand: $L \subseteq M$, but $M = L \oplus N$ for no submodule N of M.*

   Let $M = \mathbb{Z}^2$. Note that two linearly independent vectors $(a, b), (c, d)$ span a direct summand if and only if the determinant of:

   $$\begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

   is ±1. Let $L = (2, 3)$, the subgroup generated by $(2, 3)$ and let $K = (2, 5)$. Then we have:

   $$\det \begin{pmatrix} 2 & 2 \\ 3 & 5 \end{pmatrix} = 4 \neq \pm 1,$$

   so the subgroup $L + K$ is not a direct summand. It is easy to see that it is in fact a submodule.

   BETTER EXAMPLE Consider $2\mathbb{Z}$. This is easily seen to be a submodule of $\mathbb{Z}$ over itself. But $2\mathbb{Z}$ is not a direct summand, since any other nontrivial submodule K has $K \cap 2\mathbb{Z} = 0$, since you can just multiply by 2 since $2 \in \mathbb{Z} = R$.

   (b) *Give an example of a torsion free module which is not a free module.*

   Consider $\mathbb{Q}$ over $\mathbb{Z}$. It is not a free module since any two nonzero rationals are linearly dependent, we can find integers such that a linear combination of them is zero. And thus if it was free, it would be free of rank 1. But $Q \ncong \mathbb{Z}$. And it is torsion free since the product of any two nonzero rationals is nonzero.

5. *Establish the universal property of the direct sum: for any module homomorphisms $\varphi : M \to K$ and $\psi : N \to K$ there exists a unique homomorphism $\eta : M \oplus N \to K$ s.t. $\eta|_M = \varphi$ and $\eta|_N = \psi$.*

   Proof. Let $\varphi : M \to K$ and let $\psi : N \to K$ be hom-sms. Let $\eta(m,n) = \varphi(m) + \psi(n)$. Suppose there were another map ν which also has this property. Call it γ. Then we must have $\gamma(u,v) = \gamma(u,0) + \gamma(0,v) = \varphi(u) + \psi(v) = \eta(u,v)$. So its unique. □

6. *Prove that for any three modules M, N and K we have:*

   $$Hom(M \otimes N, K) \cong Hom(M,K) \oplus Hom(N,K).$$

   Proof. Let $H = \mathrm{Hom}_R(A \times B, M)$, $H_A = \mathrm{Hom}_R(A,M)$, and $H_B = \mathrm{Hom}_R(B,M)$. Let $\Phi : H_A \times H_B \to H$ be given by $\Phi((\varphi,\psi)) = \varphi + \psi$, where $\varphi \in H_A, \psi \in H_B$. We prove this is an isomorphism of R-modules.

   Homomorphism: Observe:

$$\begin{aligned}\Phi((\varphi_1,\psi_1) + (\varphi_2,\psi_2)) &= \Phi((\varphi_1 + \varphi_2, \psi_1 + \psi_2)) = \varphi_1 + \psi_1 + \varphi_2 + \psi_2 \\ &= \Phi((\varphi_1,\psi_1)) + \Phi((\varphi_2,\psi_2)).\end{aligned} \tag{B.1}$$

   In the above expression, the first equality comes from the definition of addition in $H_A \times H_B$. The second and third equalities comes from the definition of Φ. And we also know:

$$\Phi(r(\varphi,\psi)) = \Phi((r\varphi, r\psi)) = r\varphi + r\psi = r(\varphi + \psi) = r\Phi((\varphi,\psi)),$$

   hence Φ preserves mult. by R, by the definition of scalar multiplication on the R-module $H_A \times H_B$, and the definition of Φ.

   Surjectivity: Let $\varphi \in H$. Then $\varphi : A \times B \to M$. So let $\varphi \in H_A$ be given by $\varphi(a) = \varphi(a,0)$, and let $\psi \in H_B$ be given by $\varphi(b) = \varphi(0,b)$. Then we have: $\Phi((\varphi,\psi)) = \varphi$. Then Φ is surjective.

   Injectivity: Let $\Phi((\varphi_1,\psi_1)) = \varphi_1+\psi_1 = \varphi_2+\psi_2 = \Phi((\varphi_2,\psi_2)) \in H_A \times H_B$. Then note that

   $$(\varphi_1 + \psi_1)(a,0) = \varphi_1(a) = \varphi_2(a) = (\varphi_2 + \psi_2)(a,0),$$

   and the same holds when we let $a = 0$, and use an arbitrary b value, so we get that $\psi_1 = \psi_2$ as well. Hence Φ is injective. And thus it is an isomorphism. □

7. *If M is an R-module, prove that $Hom_R(R^n, M) \cong M^n$ as R-modules.*

   Proof. Now $\mathrm{Hom}(R^n, M) \cong M^n$, since we map $\varphi \mapsto (\varphi(e_1), ..., \varphi(e_n))$. **THIS IS THE WAY TO DO IT, THE CHECKS ARE EASY, JUST REMEMBER BASIS BASIS BASIS.** Or we can use the exercise from the last homework:

   $$Hom(A \oplus B, M) \cong Hom(A,M) \oplus Hom(B,M),$$

   since:

$$Hom(R^n, M) \cong Hom(R,M)^n \cong Hom(R,M) \oplus \cdots \oplus Hom(R,M) \cong M^n,$$

by induction using the above statement, and considering R as an R-module over itself. □

8. *Assume that a module has a finite basis: a linearly independent set $B = \{ u_1, ..., u_n \}$ that generates M, $M = RB$. Prove that M is free, $M \cong R^n$.*

   PROOF. Let $\varphi : R^n \to M$ be given by $(e_1, ..., e_n) \mapsto (u_1, ..., u_n)$. Sapienti sat. □

9. *Let M be a module and let B be a maximal linearly independent subset of M (exists by Zorn's lemma).*

   (a) *Prove that the module RB is free.*

   PROOF. Note B doesn't have to generate M. So what can we say about the submodule generated by B. The submodule RB has as basis (B), a linearly independent system which generates this module. **So, it's free.** Since we can use the map defined in Exercise 8. to show that $RB \cong R^n$ where n is the cardinality of B or $RB \cong \prod_{\alpha \in \Lambda} R_\alpha$ if B is infinite. □

   PROOF. Leibman's proof. Any $u \in RB$ can be written:

$$u = \sum_{\alpha \in \Lambda} a_\alpha v_\alpha,$$

   $a_\alpha \in R, v_\alpha \in B$, $a_\alpha = 0$ for all but finitely many $\alpha \in \Lambda$. It is unique since B is linearly independent. Since if you have two representations, subtract one from the other, you have a linear combination, it will contradict some stuff. Isomorphism $RB \leftrightarrow \bigoplus_{\alpha \in \Lambda} R$ where $u \leftrightarrow (a_\alpha)_{\alpha \in \Lambda}$. □

   (b) *Prove that M/RB is a torsion module.*

   PROOF. We assume R is unital, since otherwise, B may not be in RB. Or we could define RB as $RB \cup B$. Indeed, suppose for contradiction that $\exists u \in M$ s.t. $\overline{u} \equiv u \mod RB$ is not a torsion element, this means that $au \notin RB$ $\forall a \neq 0 \in R$. This is because "0" in the quotient module is the kernel, RB so au cannot be in RB. Then we just set these to zero, allowing the coefficients to be arbitrary, we are just trying to show that they are linearly independent:

$$au + c_1 v_1 + \cdots + c_k v_k = 0,$$

   with $v_i \in B, c_i \in R, a \in R$, then $a = 0$, since if a was nonzero, then:

$$au = -c_1 v_1 - \cdots - c_k v_k \in RB.$$

   so:

$$c_1 v_1 + \cdots c_k v_k = 0,$$

   so $c_i = 0$ for all i, so $\{u\} \cup B$ is linearly independent, contradiction, since B was the largest linearly independent set in M. So we have a contradiction.
   So for any u, there exists a nonzero a s.t. $a\overline{u} \in RB$, so $au + c_1 v_1 + \cdots c_k v_k = 0$ for some $c_i \in R, v_i \in B$. Hence $a\overline{u} = 0 \in M/RB$, and thus M/RB is a torsion module. □

PROOF. Leibman's proof. M/RB is torsion module. If $v \in M$ is such that $av \neq 0 \mod RB$ $\forall a \neq 0$, then $B \cup \{ v \}$ is linearly independent. Why? If $av + \sum a_\alpha v_\alpha = 0$ for some $a_\alpha, v_\alpha \in B$, then $a = 0$, so... Done. If R has zero divisors then no element is linearly dependent, so you cannot find them, since we can divide 0. So must have R is an integral domain. □

10. *Prove that $\mathbb{Z}_n \otimes \mathbb{Z}_m \cong \mathbb{Z}_d$ as groups, where $d = \gcd(n, m)$.*

PROOF. Define $\varphi : \mathbb{Z}_n \otimes \mathbb{Z}_m \to \mathbb{Z}_d$ by $\varphi(\bar{k} \otimes \bar{l}) = kl \mod d$. If you add a multiple of n to k, the result will be the same because $d|n$, and same for m ($(\bar{k}, \bar{l}) \mapsto kl \mod d$ is bilinear). Why is it a homomorphism? This is easy to check so we omit it, just check that the additive subgroup is preserved and the action of $\mathbb{Z}$ is preserved. Let's check that it is surjective. Note that $1\otimes 1 \mapsto 1$, and 1 generates $\mathbb{Z}_d$. So done: $\varphi(1 \otimes a) = a \mod d$, so φ is surjective. Or maybe better to just define an inverse, since injectivity looks hard to prove. So let $\varphi(l \otimes k) = lk \equiv 0 \mod d$. Then $lk = jd$ for some integer j. And note that we have:

$$l \otimes k = lk(1 \otimes 1) = jd(1 \otimes 1).$$

And since d is the gcd, we can write $d = xn + ym$ for some integers x, y. So we have:

$$\begin{aligned} l \otimes k &= jd(1 \otimes 1) = j(xn + ym)(1 \otimes 1) \\ &= j(xn(1 \otimes 1) + ym(1 \otimes 1)) \\ &= j(x(n \otimes 1) + y(1 \otimes m)) \\ &= j(0 \otimes 0 + 0 \otimes 0) = 0. \end{aligned} \tag{B.2}$$

So $ker\varphi = 0$ and it is injective, and hence an isomorphism. □

11. *Let $G = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}^2$.*
    (a) *Find the dimension of the $\mathbb{Z}_2$ vector space $\mathbb{Z}_2 \otimes_{\mathbb{Z}} G$.*
    $\mathbb{Z}_2 \otimes G \cong (\mathbb{Z}_2 \otimes \mathbb{Z}_2) \oplus (\mathbb{Z}_2 \otimes \mathbb{Z}_3) \oplus (\mathbb{Z}_2 \otimes \mathbb{Z}_4) \oplus (\mathbb{Z}_2 \otimes \mathbb{Z})^2$ by the next exercise 12.
    So its $\cong \mathbb{Z}_2 \oplus 0 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2^2$. So its $\cong \mathbb{Z}_2^4$.
    (b) When you multiply by $\mathbb{Q}$, it will kill all torsions, so we only have $\mathbb{Z}^2$ left. And so we have $G \otimes \mathbb{Q} \cong \mathbb{Q}^2$.
12. *Prove that for any three modules M, N, K:*

$$(M \oplus N) \otimes K \cong (M \otimes K) \oplus (N \otimes K).$$

PROOF. Map $((m, n), k) \mapsto ((m \otimes k), (n \otimes k))$. This map is clearly seen to be bilinear, and so it induces a module hom-sm:

$$\varphi : (M \oplus N) \otimes K \to (M \otimes K) \oplus (N \otimes K)$$

given by $\sum_i (m_i, n_i)\otimes k_i \to (\sum_i m_i \otimes k_i, \sum_i n_i \otimes k_i)$. Now consider the mappings $(m, k) \to (m, 0) \otimes k$ and $(n \otimes k) \to (0, n) \otimes k$, which map from $M \times K$ and $N \times K$ respectively to $(M \oplus N) \otimes K$. These are also easily seen to be bilinear, and they induce module homomorphisms

φ_1,φ_2 defined as expected. So define $\psi : (M \otimes K) \oplus (N \otimes K) \to (M \oplus N) \otimes K$ for which:

$$(m \otimes k_1, n \otimes k_2) \mapsto \varphi_1(m \otimes k_1) + \varphi_2(n \otimes k_2) = (m, 0) \otimes k_1 + (0, n) \otimes k_2 \tag{B.3}$$

Now note that

$$\begin{aligned} \varphi(\psi(m \otimes k_1, n \otimes k_2) &= \varphi((m,0) \otimes k_1 + (0,n) \otimes k_2) \\ &= (m \otimes k_1 + 0 \otimes k_2, 0 \otimes k_1 + n \otimes k_2) \\ &= (m \otimes k_1 + 0, 0 + n \otimes k_2) \\ &= (m \otimes k_1, n \otimes k_2). \end{aligned} \tag{B.4}$$

And so $\varphi = \psi^{-1}$. And so ψ is invertible and thus is a module isomorphism. □

13. *Let V be an n-dimensional vector space with basis $\{ u_1, ..., u_n \}$. Explain why $\mathbb{C} \otimes_{\mathbb{R}} V$ has structure of a $\mathbb{C}$-vector space.*

    Consider $V \cong \mathbb{R}^n$, basis $\{ u_1, ..., u_n \}$. We have $\mathbb{C}$-basis in $\mathbb{C} \otimes_{\mathbb{R}} V$ which is $\{ 1 \otimes u_1, ..., 1 \otimes u_n \}$. And over $\mathbb{R}$ we have $\mathbb{C} \otimes_{\mathbb{R}} V$:

$$\{ 1 \otimes u_1, ..., 1 \otimes u_n, i \otimes u_1, ..., i \otimes u_n \} .$$

    Note $\mathbb{R}^2 \otimes V \cong V^2 = V \oplus V$. This is because $R^2 = R \oplus R$. And then we have $(\mathbb{R} \oplus \mathbb{R}) \otimes V = (\mathbb{R} \otimes V) \oplus (\mathbb{R} \otimes V)$. And since we are taking the tensor over $\mathbb{R}$ already $(\mathbb{R} \otimes V) \cong V$.

    Note that $V \cong R^n$ so $\mathbb{C} \otimes V \cong (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{R})^n \cong C^n$. So rewriting:

$$\mathbb{C} \otimes (\oplus \mathbb{R} u_i) \cong \oplus(\mathbb{C} \otimes \mathbb{R} u_i) \cong \oplus \mathbb{C} u_i .$$

14. $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}$.

    PROOF. Define an isomorphism by $\frac{m}{n} \otimes \frac{k}{l} \mapsto \frac{nk}{ml}$. Just check. But let's use our advanced knowledge instead:

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0,$$

    and multiply this by $\mathbb{Q}$:

$$0 \to \mathbb{Z} \otimes \mathbb{Q} \to \mathbb{Q} \otimes \mathbb{Q} \to (\mathbb{Q}/\mathbb{Z}) \otimes \mathbb{Q} \to 0.$$

    We have exactness on left since $\mathbb{Q}$ is flat. If R integral domain field of fractions is flat refer to Lemma 10.151. So $0 \to \mathbb{Z} \otimes \mathbb{Q} \to \mathbb{Q} \otimes \mathbb{Q} \to 0$ is exact. And $\mathbb{Q}/\mathbb{Z} = 0$. So we have $\mathbb{Q} \cong \mathbb{Z} \otimes \mathbb{Q} \cong \mathbb{Q} \otimes \mathbb{Q}$. □

16. *Prove that $R[x] \otimes R[x] \cong R[x, y]$ as R-algebras.*

    PROOF. Take $x^n \otimes y^m \mapsto x^n y^m$. □

19. PROOF. $M = \bigoplus M_\alpha$.

$$0 \to A \to_\varphi B.$$

$$0 \to A \otimes M \to_{\varphi \otimes Id} B \otimes M \cong \bigoplus_{\alpha \in \Lambda} (A \otimes M_\alpha) \to \bigoplus_{\alpha \in \Lambda} (B \otimes M_\alpha).$$

    On the left we have $a \otimes u \mapsto \varphi(a) \otimes u$, and on the right we have $(a \otimes u_\alpha)_{\alpha \in \Lambda} \mapsto (\varphi(a \otimes u_\alpha)_{\alpha \in \Lambda}$. Because the map commutes with the direct sum, its injective if and only if each component is. So then we have:

$$\bigoplus N_\alpha \xrightarrow{\psi} \bigoplus K_\alpha,$$

where $(v_\alpha) \mapsto (\psi_\alpha(v_\alpha))$. ψ is injective if and only if ψ_α are all injective. For all α $\psi_\alpha = \psi|_{N_\alpha}$. So if ψ is injective, ψ_α is injective. If ψ_α are all injective:

$$\psi((v_\alpha)_{\alpha\in\Lambda}) = (\psi_\alpha(v_\alpha))_{\alpha\in\Lambda} = 0.$$

if and lonly if $\psi_\alpha(v_\alpha) = 0$ for all α if and only if $v_\alpha = 0$ for all α. So ψ is injective. □

21. *Give an example of a non-flat torsion-free module.*

Consider $M = I = (x, y) \subseteq R = F[x, y]$. Then we have:

$$0 \to I \to R.$$

And

$$M \otimes I \to R \otimes I \cong I$$

is not injective, since $x \otimes y - y \otimes x \mapsto 0$. **ASK LEIBMAN**

22. *Every projective module is flat.*

Proof. First show it must be a direct summand of a free module, and this it is flat. □

CHAPTER C

Common exam mistakes

On 4(a). Define $(R/I)\otimes M \to M$ by $\overline{a}\otimes u \to au$. Take b s.t. $\overline{b}=\overline{a}$. Then we have $\overline{b}\otimes u \to bu$ but $bu \neq au$.

On 3, constructing $\varphi : S\otimes R[x] \to S[x]$. To prove injectivity, you can't just check simple tensors!!!!! You need to construct an inverse homomorphism. You define $sx^n \mapsto s\otimes x^n$, since $S[x]$ is a free module over S.

Recall:

Definition C.1. A is an S-algebra if and only if it is an S-module and a ring s.t. $(s\alpha)\beta = \alpha(s\beta) = s(\alpha\beta)$ for $s\in S, \alpha, \beta \in A$. So $S[x]$ in the above is an S-algebra if S is commutative.

CHAPTER D

SAMPLE PROBLEMS TO MIDTERM II

Friday, March 2nd, 2018

1. *Let M, N be R-modules. Define a homomorphism $\Phi : M^* \otimes N \to Hom(M, N)$ by $\Phi(f \otimes v)(u) = f(u)v$.*

   (a) *Prove that Φ is well-defined.*

   PROOF. We use the universal property. If we have a bilinear map γ such that:

$$\begin{tikzcd}
 & M^* \times N \arrow[dl, "\beta"'] \arrow[dr, "\gamma"] & \\
M^* \otimes N \arrow[rr, "\Phi"] & & \mathrm{Hom}(M, N)
\end{tikzcd}$$

   is commutative, then we have induced homomorphism Φ which is well-defined. So let $\gamma : M^* \times N \to Hom(M, N)$ be given by $(f \times v)(u) \mapsto f(u)v$. We check that it is bilinear:

$$\begin{aligned}
(f + g)(u)v &\mapsto (f + g)(u)v = f(u)v + g(u)v \\
af(u) \times v &\mapsto af(u)v = a(f(u)v) \\
f(u) \times av &\mapsto f(u)av = af(u)v \\
f \times (v + w) &\mapsto f(u)(v + w) = f(u)v + f(u)w.
\end{aligned} \tag{D.1}$$

   And so we see that it is bilinear by the definition of a module and since R is commutative. Hence the induced map Φ is well-defined. □

   (b) *If M and N are free modules of finite rank, $\{ u_1, ..., u_m \}$ is a basis in M, $\{ f_1, ..., f_m \}$ is the dual basis in M^*, and $\{ v_1, ..., v_n \}$ is a basis in N, prove that*

$$\{ \Phi(f_i \otimes v_j) : i = 1, ..., m, j = 1, ..., n \}$$

   is a basis in $Hom(M, N)$. Deduce that Φ is an isomorphism.

   PROOF. Let $f_i \in M^*$ and $v_j \in N$ s.t. $\Phi(f_i \otimes v_j)(u) = 0 \in Hom(M, N)$. We wish to prove that Φ is injective, so we will show $f_i \otimes v_j = 0$. Note we have $\Phi(f_i \otimes v_j)(u) = f_i(u)v_j = 0$

by the definition of Φ. So note since N is free, it is torsion-free, and thus we know that $f_i(u)v_j = 0$ means $f_i(u) = 0\ \forall u$, or $v_j = 0 \in N$. But in either of these cases, we then know $f_i \otimes v_j = 0 \in M^* \otimes N$. So we have shown Φ is injective. Now note we know that $M^* \cong R^m$, and $N \cong R^n$. So $M^* \otimes N \cong R^{mn}$ by Remark 10.97, and since M is free of rank m, we know $Hom(M,N) \cong Hom(R^m, R^n) \cong R^{mn}$ by Corollary 11.3. Thus we know $M^* \otimes N \cong Hom(M,N)$. And since we have an injective map between these two, it must be an isomorphism. □

2. *Let M, N, K be free modules of finite rank over a commutative unital ring R, and let $\varphi : M \to N$ and $\psi : N \to K$ be homomorphisms considered as tensors from $N \otimes M^*$ and $K \otimes N^*$ respectively. Show that the composition $\psi \circ \varphi : M \to K$ corresponds to the contraction of the $N^* \otimes N$-part of the tensor $\psi \otimes \varphi \in K \otimes N^* \otimes N \otimes M^*$. (Hint: Either check this for simple tensors and use linearity, or use the coordinate presentation of tensors.)*

Proof. Recall that the contraction homomorphism is $f \otimes v \mapsto f(v) \in R$. We take simple tensors $k \otimes g \in K \otimes N^*$ and $n \otimes f \in N \otimes M^*$. Then we have:

$$\begin{aligned}\psi \otimes \varphi &= (k \otimes g) \otimes (n \otimes f) \mapsto k \otimes g(n) \otimes f \\ &= k \otimes g(n) f \in K \otimes M^* \cong M^* \otimes K \cong Hom(M,K)\end{aligned} \tag{D.2}$$

by the previous exercise. Define $\psi = g(u)k \in Hom(N,K)$ and $\varphi = f(u)n \in Hom(M,N)$. Then $(\psi \circ \varphi)(u) = \psi(\varphi(u)) = g(f(u)n)k = f(u)g(n)k$. So we define $\Phi : K \otimes M^* \to Hom(M,K)$ by $\Phi(k \otimes g(n)f)(u) = f(u)g(n)k$. And since these are all free modules, hence torsion free, we know if $\Phi(k \otimes g(n)f)(u) = 0$, then one of $f(u), g(n), k$ must be identically zero, which means $k \otimes g(n)f = 0$. So it's injective and this an isomorphism since we already showed that $K \otimes M^* \cong M^* \otimes K \cong Hom(M,K)$. Hence for any such ψ, φ, extending from simple tensors by linearity, we know they are in 1-1 correspondence with the simple tensors $k \otimes g$ and $n \otimes f$, and since we know the contraction maps $\psi \otimes \varphi \mapsto k \otimes g(n)f$, and the isomorphism Φ maps $k \otimes g(n)f \mapsto f(u)g(n)k = (\psi \circ \varphi)(u)$, we are done. □

3. *Let M be a free module of rank 2 over a commutative unital ring R, let $\{ u_1, u_2 \}$ be a basis of M, let $\{ u_1^*, u_2^* \}$ be the dual basis of M^*, and let $f \in M^*$ have coordinates $(4,5)$ in this basis. What are the coordinates of f in the basis dual to $\{ 2u_1, 3u_2 \}$?*

We define $\{ g_1, g_2 \}$ to be our new dual of $\{ 2u_1, 3u_2 \}$. Define $g_1 = \frac{1}{2}u_1^*$ and $g_2 = \frac{1}{3}u_2^*$. Then $g_1(2u_1) = \frac{1}{2}u_1^*(2u_1) = \frac{1}{2}2 = 1$ and so on, it works for the new basis. So $f = (4u_1^*, 5u_2^*) = 8g_1 + 15g_2$.

4. *Let M be a free module of finite rank over a commutative unital ring R; then bilinear forms on M are represented by tensors from $M^* \otimes M^*$. Prove that a bilinear form β on M is symmetric (that is*

$\beta(u,v) = \beta(v,u)$ for all $u, v \in M$) if and only if the corresponding tensor is symmetric.

Note that bilinear forms can be represented as $n \times n$ matrices, and they are symmetric if and only if the corresponding matrix is symmetric. Recall that this means that $A = A^T$. But the entries of the matrix are just the coordinates of the corresponding tensor written in the natural basis.

Leibman's tip: Map $f_1 \otimes f_2 \mapsto \beta(u_1, u_2) = f_1(u_1)f_2(u_2)$.

5. *Let M be a module over a commutative unital ring R and let w be a symmetric covariant n-tensor (that is, a symmetric tensor from $\mathcal{T}^n(M)$). Prove that w defines a homomorphism $\mathcal{S}^n(M) \to R$ (that is, an element of $(\mathcal{S}^n(M)^*)$.*

Let $w \in \mathcal{T}^n(M^*)$, w is symmetric, and $\sigma(w) = w$ for all $\sigma \in S_n$. Then $S^n(M)$ which is called the **symmetric tensor product**, is equal to $\mathcal{T}^n(M)/\mathcal{C}^n$, where $\mathcal{C}^n(M)$ is generated by the relation $u \otimes v - v \otimes u$, it is the submodule generated by $\alpha - \sigma(\alpha)$, for $\alpha \in \mathcal{T}^n(M)$, for $\sigma \in S_n$. These two definitions of $\mathcal{C}^n(M)$ are equivalent, you can use whichever you like. We claim that if we have a symmetric, covariant tensor, it acts on $\mathcal{T}^n(M)$:

$$(f_1 \otimes \cdots \otimes f_n)(u_1 \otimes \cdots \otimes u_n) = f_1(u_1) \cdots f_n(u_n) \in R.$$

Where the first part of the product is in $\mathcal{T}^n(M^*)$ and the second half of the product is in $\mathcal{T}^n(M)$. So the tensor product of f's is our w and the tensor product of u's is our α. Covariant tensors act on contravariant tensors. The question is whether or not w acts on the factor module. So we want to know if we have $w : \mathcal{T}^n(M)/\mathcal{C}^n(M) \to R$. It is true when $w(\mathcal{C}^n(M)) = 0$. Note we already had $w : \mathcal{T}^n(M) \to R$ by our action. Now w check that w maps $\mathcal{C}^n(M)$ to zero. So take:

$$w(\alpha - \sigma(\alpha) = w(\alpha) - w(\sigma(\alpha)) = w(\alpha) - (\sigma^1(w))(alpha) = 0.$$

But we assumed $\sigma(w) = w$, so we must have $\sigma^{-1}(w) = w$.

Example D.1. Let $\sigma = (123)$.

$$\begin{aligned}(f_1 \otimes f_2 \otimes f_3)(\sigma(u_1 \otimes u_2 \otimes u_3)) &= (f_1 \otimes f_2 \otimes f_3)(u_2 \otimes u_3 \otimes u_1)\\ &= f_1(u_2)f_2(u_3)f_3(u_1)\\ &= \sigma^{-1}(f_1 \otimes f_2 \otimes f_3)(u_1 \otimes u_2 \otimes u_3) \qquad (D.3)\\ &= (f_3 \otimes f_1 \otimes f_2)(u_1 \otimes u_2 \otimes u_3)\\ &= f_3(u_1)f_1(u_2)f_2(u_3).\end{aligned}$$

Note we applied σ to the indices, not to the locations.

Proof. Let N be a module, $K \subseteq N$. Let $f \in N^*$, $f : N \to R$. Is f defined on N/R? In other words, does f induce a homomorphism $N/K \to R$? So do we have $f \in (N/K)^*$? This is so if $f(K) = 0$ (then $\forall u \in N$, $f(u+k) = f(u)$) The problem was to show that if you have a symmetric tensor w, that it maps elements of $\mathcal{C}^n(M) \to 0$.

He would be happy with the row $w(\alpha - \sigma(\alpha)) = \cdots = 0$. But you need to know that definition of $\mathcal{C}^n(M)$. □

6. *Let* $\{ u_1, u_2, u_3 \}$ *be a basis in a vector space* V.

The main idea of this problem is to know the definition of $V \wedge V = \Lambda^k(V)$. Note here our $V = M$ and $\dim V = n = 3$.

REMARK D.2. The basis in $\Lambda^k(M)$ is:

$$\{ u_{i_1} \wedge u_{i_2} \wedge \cdots \wedge u_{i_k} : i_1 < i_2 < \ldots < i_k \}.$$

(a) *Find a basis in the space* $V \wedge V$ *(don't justify!)*
So this part is just asking us to write exactly the above set. Note $V \wedge V = \Lambda^2(V)$.
Our basis is: $\{ u_1 \wedge u_2, u_2 \wedge u_3, u_1 \wedge u_3 \}$. There are always $\binom{n}{k}$ basis wedges, where $n = \dim V$ and k is the power of Λ.

(b) *Find the coordinates of the tensor* $x_1u_1 + x_2u_2 + x_3u_3 \wedge y_1u_1 + y_2u_2 + y_3u_3$ *in this basis.*
Observe:

$$\begin{aligned}(x_1u_1 \wedge y_1u_1 + y_2u_2 + y_3u_3) + (x_2u_2 \wedge y_1u_1 + y_2u_2 + y_3u_3) + (x_3u_3 \wedge y_1u_1 + y_2u_2 + y_3u_3)\\ = x_1u_1 \wedge y_2u_2 + x_1u_1 \wedge y_3u_3 + x_2u_2 \wedge y_1u_1\\ +x_2u_2 \wedge y_3u_3 + x_3u_3 \wedge y_1u_1 + x_3u_3 \wedge y_2u_2\\ = (x_1y_2 - x_2y_1)(u_1 \wedge u_2) + (x_2y_3 - y_2x_3)(u_2 \wedge u_3) + (x_1y_3 - x_3y_1)(u_1 \wedge u_3).\end{aligned} \tag{D.4}$$

7.

The main idea of this problem is to know how the $\wedge$ operator works, namely that a vector wedge itself is 0 and that you get a negative when you try to commute.

PROOF. So we have two bases and for each v_i we can write $v_1 = a_{11}u_1 + \cdots + a_{1n}u_n$ and so on for all v_i's. Then we wedge them all together and write:

$$v_1 \wedge \ldots \wedge v_n = a_{11}u_1 + \cdots + a_{1n}u_n \wedge \ldots \wedge a_{n1}u_1 + \cdots + a_{nn}u_n,$$

and recall that $u_i \wedge u_i = 0$ and $u \wedge v = -v \wedge u$. So all the terms with repeated u_i's will die, and we get $c(u_1 \wedge \ldots \wedge u_n)$ for some ring element c. And we can do the same for the u_i's writing them as linear combinations of the v's and wedgeing all these combinations together, getting $u_1 \wedge \ldots \wedge u_n = b(u_1 \wedge \ldots \wedge u_n)$ and so we must have $b = c^{-1}$ and so it's a unit. □

8. (a) Consider $\mathbb{Z} \to \mathbb{Z}$ given by multiplication by two.
(b) Let $\varphi : M \to N \to 0$, both modules free, same rank, surjective since exact on right. We are over an integral domain. Assume not injective, so $K = ker\varphi \neq 0$ And:

$$0 \to K \to M \to N \to 0$$

where $\varphi : M \to N$ and so K nonzero implies the image of the embedding from $k \to M$ is nonzero, so then $K \neq 0$, so $rank(K) \geqslant 1$. But we know ranks are additive. $rank(M) = rank(K) + rank(N) > rank(N)$, contradiction.

REMARK D.3. $rank(M) = 0$ if and only if it is a torsion module.

9.

REMARK D.4. if you have $\varphi : M \to N$ a monomorphism, then since its injective the image of an independent set is independent, so if we take a maximal set $\{ u_1, ..., u_n \} \to \{ \varphi(u_1), ..., \varphi(u_n) \}$ in M, its image is linearly independent in N. Since $n = rank(N)$, $\{ \varphi(u_1), ..., \varphi(u_n) \}$ is a maximal linearly independent subset, which is equivalent to saying that the quotient is a torsion module.

10. *Let $M_1 \cong \mathbb{Z}^4/N_1$ and $M_2 \cong \mathbb{Z}^4/N_2$, where N_1 is a submodule of $\mathbb{Z}^4$ generated, in some basis $\{ u_1, ..., u_4 \}$ of $\mathbb{Z}^4$, by $\{ u_1, 2u_2, 6u_3 \}$, and N_2 is a subgroup of $\mathbb{Z}^4$ generated, in some basis $\{ v_1, ..., v_4 \}$ of $\mathbb{Z}^4$, by $\{ v_1, 3v_2, 6v_3 \}$.*
    (a) *Are N_1, N_2 isomorphic?* Note that N_1, N_2 are submodules of $\mathbb{Z}^4$ which is free, so they must be free because **we have a theorem that says over a PID, submodules of free modules are free**, and so since they are generated by 3-element sets they are both free of rank 3 and so they are isomorphic.
    (b) *What are the ranks of the modules M_1, M_2?* They are both rank 1. We know this because we can write:

$$\begin{aligned} M_1 &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z} \\ M_2 &\cong \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z} \end{aligned} \tag{D.5}$$

    which is only true when we are over a PID by the fundamental theorem.
    (c) *Are M_1 and M_2 isomorphic?*
    NO! We have:

$$\begin{aligned} M_1 &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z} \\ M_2 &\cong \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z} \end{aligned} \tag{D.6}$$

    Two modules are isomorphic if and only if they have the same rank and the same invariant factors, so these are not isomorphic, since they have different invariant factors, recall the invariant factors are the $a_1, ..., a_k$ that generate the ideals that we mod by.

11. *Let N be the sublattice of $\mathbb{Z}^3$ generated by (insert vectors here), and let $M = \mathbb{Z}^3/N$.*
    (a) *Find the invariant factors of M.*
    Step 1: Write the matrix of the generators. It is:

$$\begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & -1 \\ 1 & 1 & 3 \end{pmatrix}.$$

    Step 2: Use elementary row operations to write the matrix in the form:

$$\begin{pmatrix} a_1 & & \\ & a_2 & \\ & & a_3 \end{pmatrix} = \begin{pmatrix} 1 & & \\ & 2 & \\ & & -2 \end{pmatrix}$$

    Then the invariant factors are exactly the diagonal elements $1, 2, -2$. Recall that when we're working over $F[x]$, invariant factors are polynomials, but since we are over $\mathbb{Z}$ here, invariant factors are just elements of the ring $\mathbb{Z}$ (the a_i's from the Fundamental theorem).

(Leibman's solution) We have:

$$\begin{pmatrix} 1 & -1 & 1 \\ 1 & -1 & -1 \\ 1 & 1 & 3 \end{pmatrix} \mapsto \begin{pmatrix} a_1 & & \\ & a_2 & \\ & & a_3 \end{pmatrix}.$$

And we need $a_1|a_2|a_3$. So then there is a basis $\{ u_1, u_2, u_3 \}$ such that $\{ a_1u_1, a_2u_2, a_3u_3 \}$ is a basis in N. And we have a_1, a_2, a_3 invariant factors. And $M \cong \mathbb{Z}_{a_1} \oplus \mathbb{Z}_{a_2} \oplus \mathbb{Z}_{a_3}$. Then $|M| = a_1a_2a_3$.

(b) *Find the cardinality of M.*

Over $\mathbb{Z}$, the cardinality of M is $|M| = a_1a_2a_3$, the absolute value of product of invariant factors. But we can check this by writing:

$$M \cong \mathbb{Z}/(1) \oplus \mathbb{Z}/(2) \oplus \mathbb{Z}/(-2) \cong 0 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \cong V_4.$$

12. *Let G be an additively written abelian group defined by its generators u_1, u_2, u_3 and relations $2u_1+4u_2+10u_3 = 0$ and $4u_1 = 2u_2$. Represent G as a product of cyclic groups.*

Just do the same thing we did above. We have a group $G \cong \mathbb{Z}^3/N$ where N is the relations module and:

$$N = \mathbb{Z}\left\{ \begin{pmatrix} 2 \\ 4 \\ 10 \end{pmatrix}, \begin{pmatrix} 4 \\ -2 \\ 0 \end{pmatrix} \right\}.$$

Now we map:

$$\begin{pmatrix} 2 & 4 \\ 4 & -2 \\ 10 & 0 \end{pmatrix} \mapsto \begin{pmatrix} a & 0 \\ 0 & b \\ 0 & 0 \end{pmatrix}.$$

And we have $a = 2$ somehow and $\mathbb{Z}_a \times \mathbb{Z}_b$.

We write:

$$\begin{cases} a_{11}u_1 + a_{21}u_2 + a_{31}u_3 = 0 \\ a_{12}u_1 + a_{22}u_2 + a_{32}u_3 = 0 \end{cases}$$

Then $e_i \mapsto u_i$ then $a_{11}e_1 + a_{21}e_2 + a_{31}e_3, a_{12}e_1 + a_{22}e_2 + a_{32}e_3$ span the kernel of the homomorphism $\mathbb{Z}^3 \to M$. Then the relations matrix is:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \\ a_{31} & a_{32} \end{pmatrix}.$$

Then we have:

$$\begin{pmatrix} b_1 & 0 \\ 0 & b_2 \\ 0 & 0 \end{pmatrix} \Rightarrow \begin{cases} b_1v_1 = 0 \\ b_2v_2 = 0 \end{cases}$$

Where these things on the right are the "new" relations. And they imply $\mathbb{Z}_{b_1} \times \mathbb{Z}_{b_2} \times \mathbb{Z}$.

13. *Prove that over a PID, a finitely generated module is projective if and only if it is free.*

PROOF. Note that over a PID, we know that any finitely generated module is torsion-free if and only if it is free.

We show that a free module is projective. Note that M is projective if and only if M is a direct summand of a free module, i.e. if there exists an R-module N s.t. $M \oplus N$ is free.

But M is already free, so $M \oplus 0$ is free and so M is projective.

Now we prove a projective module is torsion-free. Now note the ring R itself is always flat, and $M_1 \oplus M_2$ is flat if and only if M_1, M_2 are both flat, so $M \cong R^n$ is flat since all the copies of R are flat.

Now recall that a property of flat modules is that if $Tor(M) \neq 0$, then M is not flat, so if M is flat, we must have $Tor(M) = 0$, so M must be torsion free. And thus by the theorem stated at the beginning since it is finitely-generated, we know it is free. So M is free if and only if it is projective. □

14. *The Smith normal form of a matrix A is:*

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & x+2 & 0 \\ 0 & 0 & 0 & (x+2)(x^2+3) \end{pmatrix}.$$

Find the rational canonical form of A and the characteristic polynomial of A.

Recall that the characteristic polynomial of A, $c_A = \prod f_i$ where f_i are the invariant factors. And in the Smith normal form, the f_i's along the diagonal which are not constants are the invariant factors. So $f_1 = x + 2$ and $f_2 = (x+2)(x^2+3)$. So $c_A = f_1 \cdot f_2 = (x+2)(x+2)(x^2+3)$. So the elementary divisors are the factors of the invariant factors with powers, so the elementary divisors are: $(x+2), (x+2), (x^2+3)$. The companion matrix of an invariant factor is a $k \times k$ matrix where k is the highest degree of the polynomial. Recall:

DEFINITION D.5. And we have the **companion matrix** of $f = x^k + a_{k-1}x^{k-1} + \cdots + a_1 x + a_0$ where f is monic, given by:

$$A_i = \left(\begin{array}{cccc|c} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & & & -a_1 \\ 0 & 1 & \ddots & & \vdots \\ 0 & 0 & \ddots & & \vdots \\ \vdots & \vdots & & 1 & -a_{k-1} \end{array}\right).$$

So for $f_1 = x+2$ we have: $A_1 = (2)$ and for $f_2 = (x+2)(x^2+3) = x^3 + 2x^2 + 3x + 6$, we have:

$$A_2 = \begin{pmatrix} 0 & 0 & -6 \\ 1 & 0 & -3 \\ 0 & 1 & -2 \end{pmatrix}.$$

Then our rational canonical form is in general given by:

$$A = \begin{pmatrix} \boxed{A_1} & & & 0 \\ & \boxed{A_2} & & \\ & & \ddots & \\ 0 & & & \boxed{A_k} \end{pmatrix},$$

Hence:

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -6 \\ 0 & 1 & 0 & -3 \\ 0 & 0 & 1 & -2 \end{pmatrix}.$$

15. *Determine all similarity classes of matrices over $\mathbb{Q}$ with characteristic polynomial $x^4 - 4x + 3 = (x^2 + 2x + 3)(x - 1)^2$.*

Recall that the **characteristic polynomial is just the product of all the invariant factors**. So we find all possible lists of invariant factors, keeping in mind that we must have $f_1|f_2|...|f_m$. First let $IF = \left\{ x^4 - 4x + 3 \right\}$. Then our matrix in RCF is just the single companion matrix:

$$A_1 = \left(\begin{array}{ccc|c} 0 & 0 & 0 & -3 \\ 1 & 0 & 0 & 4 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array} \right).$$

And recall that **similar matrices have the same invariant factors**. Now let $IF = \left\{ (x^2 + 2x + 3)(x - 1), (x - 1) \right\}$. Clearly this is the only other list which will satisfy the definition of invariant factors (to check this just take all combinations of factors of the characteristic polynomial and check if list divides sequentially). And in this case we write the invariant factors from smallest to largest $f_1 = x - 1$ and $f_2 = x^3 + x^2 + x - 3$ and find their companion matrices:

$$\begin{gathered} A_1 = (1) \\ A_2 = \begin{pmatrix} 0 & 0 & 3 \\ 1 & 0 & -1 \\ 0 & 1 & -1 \end{pmatrix}. \end{gathered} \tag{D.7}$$

Then the matrix written in rational canonical form is:

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 1 & 0 & -1 \\ 0 & 0 & 1 & -1 \end{pmatrix}.$$

And these are the two similarity classes.

16. *Assume that a linear tranformation T of a 5-dimensional space satisfies $T^3 = 1$. What can be the rational canonical forms of T?*

My solution. Note that $f(x) = x^3 - 1$ is a polynomial s.t. $f(T) = 0$. But note for any such polynomial we must have that $m_T | f$, by definition of the minimal polynomial. So we know $m_T | x^3 - 1$. Since we factor $x^3 - 1 = (x-1)(x^2+x+1)$, we know:

$$m_T \in \left\{ x^3 - 1, x - 1, x^2 + x + 1 \right\}.$$

But also note that $m_T = f_m$, the largest invariant factor, and we must have that $f_1 | f_2 | ... | f_m$ and that $f_1 \cdots f_m = c_T$, the characteristic polynomial of T, which has degree the same as the dimension of our space, which is given as 5.

Case 1: Let $m_T = x^2 + x + 1$. Then since this does not factor over $\mathbb{Q}$, we know that $f_1 = \cdots = f_m = x^2 + x + 1$. Then we know $c_T = (x^2 + x + 1)^n$ for some integer n, which is impossible because that will always have even degree, and c_T must have degree 5. So this is impossible.

Case 2: let $m_T = x - 1$. Then $T - I = 0$ which means $T = I$. And we know **RCF of the identity matrix I is exactly I.**

Case 3: Let $m_T = x^3 - 1$. Then we have two possible subcases for the lists of invariant factors. We note here that we can have two invariant factors which are the same. **Subcase A:** $f_3 = x^3 - 1, f_2 = x - 1, f_3 = x - 1$. Then we have $A_1 = A_2 = (1)$ companion matrices. And we have:

$$A_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Hence the RCF is:

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Subcase B: $f_2 = x^3 - 1, f_1 = x^2 + x + 1$. Then we have:

$$A_1 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

And the RCF matrix is just the 5 by 5 matrix with A_1 as the top block and the companion matrix A_3 from the previous subcase as the next block.

Leibman's solution: $T : V \to V$. T satisfies $x^3 - 1 = (x-1)(x^2 + x + 1)$. But what field this is over matters since we don't know if this right part factors, so we assume it's over $\mathbb{Q}$. Over $\mathbb{C}$ it splits completely, and if one of the factors is the minimal polynomial, then it's just a scalar matrix. So we assume V is a $\mathbb{Q}$-vector space. If $m_T(x) = x - 1$, then we have $T = I$. If $m_T(x) = x^2 + x + 1$, then we have $f_1 = f_2 = f_3 = x^2 + x + 1$, so $\deg(\prod f_i)$ is even, and $\neq 5$. Last case is $m_T(x) = x^3 - 1$, then either $f_1 = f_2 = x - 1$, $f_3 = x^3 - 1$, or $f_1 = x^2 + x + 1$, $f_3 = x^3 = 1$. We have:

$$A = \left(\begin{array}{c|c|ccc} 1 & 0 & & & 0 \\ \hline 0 & 1 & & & \\ \hline & & 0 & 0 & 1 \\ & & 1 & 0 & 0 \\ 0 & & 0 & 1 & 1 \end{array}\right).$$

Or:

$$A = \left(\begin{array}{c|c|ccc} 0 & -1 & & & 0 \\ \hline 1 & -1 & & & \\ \hline & & 0 & 0 & 1 \\ & & 1 & 0 & 0 \\ 0 & & 0 & 1 & 1 \end{array}\right).$$

And elementary divisors $x^2 + x + 1$, $x^2 + x + 1, x - 1$.

17. *The characteristic polynomial of an $\mathbb{R}$-matrix A is $c_A = (x-2)(x^2 + 3)$.*

   (a) *Find the minimal polynomial of A.*
   Note we must have that the largest invariant factor $f_m = m_A$, the minimal polynomial, and that the invariant factors multiply to c_A. So $m_A | c_A$. So in **Case 1**, we have that $m_A = x - 2$, then all other invariant factors must also be $x - 2$, but c_A is not a power of $x - 2$, so this is impossible. So then in **Case 2** we have $m_A = (x^2 + 3)$, and we have a similar problem, so we are left with **Case 3** in which $m_A = c_A = (x - 2)(x^2 + 3) = x^3 + 3x - 2x^2 - 6$. Thus we only have a single invariant factor.

   (b) *Find the rational canonical form of A.*
   Recall that the RCF of A is the matrix with each of the companion matrices of the invariant factors as its diagonal blocks. But we only have the one invariant factor, so:

$$A_1 = \begin{pmatrix} 0 & 0 & 6 \\ 1 & 0 & -3 \\ 0 & 1 & 2 \end{pmatrix}.$$

   (c) *Find a matrix of the form* $\begin{pmatrix} * & 0 & 0 \\ 0 & * & * \\ 0 & * & * \end{pmatrix}$ *which is similar to A.*
   We just find the companion matrices of the factors of the characteristic polynomial c_A up to powers. So the companion matrix of $x - 2$ is just (2) and the companion matrix of $x^2 + 3$

is $\begin{pmatrix} 0 & -3 \\ 1 & 0 \end{pmatrix}$. So we have:

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 0 & -3 \\ 0 & 1 & 0 \end{pmatrix}.$$

Which is similar to A. Recall that **two matrices are similar if and only if they have the same characteristic polynomial and the same characteristic polynomial and** $n \leqslant 3$. Note this does not work for $n > 3$.

(d) *If A has Jordan canonical form, find it.*

Remark D.6. Jordan canonical form = canonical Jordan form = Jordan normal form.

Recall that we have Jordan form if and only if we can write the **minimal polynomial** as a product of powers of linear factors (splits). But this is not true since we are not over an algebraically closed field, and $x^2 + 3$ does not split.

18. *Find the Jordan canonical form of the matrix whose rational canonical form is* $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & -3 \\ 0 & 1 & 3 \end{pmatrix}$*.*

Since we clearly only have one block by inspection, our minimal polynomial is the only invariant factor, and it's also c_A. So this invariant factor must have degree 3 since our single companion matrix is 3 by 3, and it is monic and the remaining coefficients are $-3, 3, -1$ so it is $m_T = x^3 - 3x^2 + 3x - 1$. Now we want to factor this. Try $x = 0$, it's not a root, so try $x = 1$. It is a factor, so it's divisible by $x - 1$. And we get $(x-1)(x^2-2x+1) = (x-1)^3$. So we have a single elementary divisor. And its Jordan block is the whole Jordan canonical form. Recall that the Jordan form of a divisor $(x - \lambda)^k$ is a $k \times k$ matrix with λ's on the diagonal, and 1's above the diagonal. So our Jordan form is:

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

19. **Possible exam problem: Prove rank**$\varphi^* = rank\varphi$**.**

CHAPTER E

Tensors outside of algebra

Wednesday, February 14th ♡

Let M be an R-module. Consider $M \otimes M^* \to R$ which is naturally induced by $(u, f) \mapsto f(u)$, which is bilinear.

Definition E.1. The above homomorphism is called **contraction of tensors**.

Let M is a free module of finite rank (for example, a finite dimensional vector space). Usually we define contraction restricted to vector spaces. We choose a basis $\{ u_1, ..., u_n \}$ in M a dual basis $\{ f_1, ..., f_n \}$ in M^*. Then what is contraction in coordinates? First what elements of $M \otimes M^*$? Then:

$$\{ u_i \otimes f_j : i, j = 1, .., n \}$$

form a basis in $M \otimes M^*$. $\forall w \in M \otimes M^*$:

$$w = \sum_{i,j=1}^{n} a_{ij} u_i \otimes f_j .$$

How do we know this is a basis in $M \otimes M^*$? Recall:

$$(M_1 \oplus M_2) \otimes N \cong (M_1 \otimes N) \oplus (M_2 \otimes N).$$

Then let $M \oplus Ru_i, N = \oplus Rv_j$, then what is the tensor product of these? Obvious. Done.

Going back to the task at hand, we define a_{ij} as the **coordinates of** w.

Definition E.2. The **contraction** of w is:

$$\sum a_{ij} f_j(u_i) = \sum a_{ij} \delta_{ij} = \sum_{i=1}^{n} a_{ij} = trace \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}.$$

So ”trace” is a function of a tensor, not its matrix.

Let M, N be R-modules. Consider $N \otimes M^*$. We have a homomorphism $N \otimes M^* \to Hom(M, N)$ given by $v \otimes f \mapsto \varphi \in Hom(M, N)$, where $\varphi(u) = f(u)v$. In fact this is a composition of contraction. We take $v \otimes f \otimes u$ and contract it to get $f(u)v$. So in fact we take $N \otimes M^* \otimes M$ and contract it. Note the above map is bilinear. In general it doesn't have to be an isomorphism. If N, M are free modules of finite rank, then we claim that it is an isomorphism.

LEMMA E.3. *If N, M are free modules of finite rank, then $N \otimes M^* \to Hom(M, N)$ given by $v \otimes f \mapsto \varphi \in Hom(M, N)$, where $\varphi(u) = f(u)v$ is an isomorphism.*

PROOF. let M, N be free of ranks m, n and let $\{ u_1, ..., u_n \}$ and $\{ v_1, ..., v_m \}$ be their bases. Let $\{ f_1, ..., f_n \}$ be the dual basis in M^*. Then $\{ v_j \otimes f_i \}$ is the basis in $N \otimes M^*$ as proven above. So let's check what homomorphism corresponds to this tensor. For any i, j:

$$v_j \otimes f_i \mapsto \varphi_{ij}, \varphi_{ij}(u_k) = f_i(u_k)v_j = \delta_{ik}v_j = \begin{cases} v_j & i = k \\ 0 & i \neq k \end{cases}.$$

where the matrix of φ_{ij} is a matrix with n rows and m columns with zeroes everywhere except the i-th column of the j-th row, where there is a 1. So $\{ \varphi_{ij} \}$ is a basis in $Hom(M, N)$. So, $N \otimes M^* \to Hom(M, N)$ is an isomorphism. □

So homomorphisms $M \to N$ are tensors from $N \otimes M^*$.

So we have $Hom(M, M) \cong M \otimes M^*$.

"Trace" is defined on $M \otimes M^*$. So in $Hom(M, M)$, and doesn't depend on the choice of basis. So "trace of a hom-sm" is well-defined.

What is trace??

REMARK E.4. You have a mapping $M \otimes M^* \to R$ defined by $u \otimes f \mapsto f(u)$. And note that this is independent of basis:

$$\begin{tikzcd}
& M \otimes M^* \arrow[r] \arrow[ddl, leftrightarrow] & R \\
& u \otimes f \arrow[r, mapsto] \arrow[ddl, leftrightarrow] & f(u) \\
Hom(M, M) & & . \\
\varphi(v) = f(v)u & &
\end{tikzcd}$$

Composition of homomorphisms: $M \to N \to K$ - they are given by tensors from $N \otimes M^*$ and $K \otimes N^*$.

DEFINITION E.5. **Composition** is contraction of a tensor from $K \otimes N^* \otimes N \otimes M^*$ with respect to N.

If we have $M \overset{\varphi}{\to} N \overset{\psi}{\to} K$. Apply $\psi \circ \varphi(u)$, take $\psi \in K \otimes N^*$, and $\varphi \in N \otimes M^*$, and $u \in M$ so we have:

$$\psi \otimes (\varphi \otimes u).$$

Contract $M^* \otimes M$ and then $N^* \otimes N$, so the composition $\psi \circ \varphi$ is the result of contraction of $N^* \otimes N$.

In coordinates:

$$\begin{aligned} \varphi &\leftrightarrow (a_{ij}) \\ \psi &\leftrightarrow (b_{kl}) \\ \psi \otimes \varphi &\leftrightarrow (b_{kl} a_{ij}) \\ \psi \circ \varphi &\leftrightarrow \left(\sum_{i=1}^{n} b_{ki} a_{ij} \right) = (c_{kj}). \end{aligned} \tag{E.1}$$

Definition E.6. A **bilinear form** is a mapping $\beta : M \times M \to R$ s.t. everything is preserved.

Remark E.7. Bilinear forms ↔ tensors from $M^* \otimes M^*$ given by $f \otimes g \mapsto \beta$, and $\beta(u,v) = f(u)g(v)$. The trace is not defined here. **Seriously wtf is the trace?**.

Definition E.8. $M \otimes M \otimes \cdots \otimes M \otimes M^* \otimes \cdots \otimes M^*$ where we have k copies of M and l copies of M^* are called (k,l)-tensors, or tensors of (k,l)-type. And $\dim = n^{k+l}$, where $n = \dim M$. Then it is k-times contravariant and l times covariant tensors. Bilinear forms are $(0,2)$-tensors.

Remark E.9. Each tensor from this space is represented by a $k+l$-dimensional matrix. $n \times n \times \cdots \times n$, $k+l$ times. There is a tradition to write coordinates:

$$a^{i_1,\dots,i_k}_{j_1,\dots,j_l}.$$

where contravariant on top, and covariant on bottom.

Consider $\nabla f = df$ - $(0,1)$-tensor, covector. Christofel symbols $\Gamma^i_{j,l}$. Curvature tensor: $R^i_{j,k,l}$.

CHAPTER F

Sample problems to midterm III

1. *If K/F is a finite extension, prove that it is algebraic.*

   Proof. Let F be a field and K an extension with $[K : F] = n < \infty$. Let $\alpha \in K$. Then the dimension of K over F is n. So we know that $\{ 1, \alpha, ..., \alpha^n \}$ are linearly dependent. So there exists a_i not all zero such that $a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$. Then we know $f(x) = a_0 + a_1x + \cdots + a_nx^n$ is a nonzero polynomial in $F[x]$ for which α is a root, so α is algebraic. So K/F is algebraic since this holds for all α. □

2. *Find the minimal polynomial over $\mathbb{Q}$ of $\sqrt{2} + 2\sqrt{5}$.*

   Let's just try taking powers. Observe:

$$\begin{aligned}(\sqrt{2} + 2\sqrt{5})^2 &= 2 + 4\sqrt{10} + 20 \\ &= 22 + 4\sqrt{10}.\end{aligned} \tag{F.1}$$

   So take $x^2 - 22$ and we get $4\sqrt{10}$. So square this and we get:

$$16 \cdot 10 = 160.$$

   So if we take $f(x) = (x^2 - 22)^2 - 160$, we get zero when we plug in $\sqrt{2} + 2\sqrt{5}$. So we know $m_{\alpha,\mathbb{Q}}|f(x)$. We know $[Q(\sqrt{2}) : \mathbb{Q}] = 2$, and $[\mathbb{Q}(2\sqrt{5}) : Q(\sqrt{2})] = 2$, since these two elements are linearly independent over $\mathbb{Q}$. So the degree of $\mathbb{Q}(\sqrt{2}, 2\sqrt{5})$ over $\mathbb{Q}$ is 4. It can easily be shown that $\mathbb{Q}(\sqrt{2}, 2\sqrt{5}) = \mathbb{Q}(\sqrt{2} + 2\sqrt{5})$. And since our polynomial has degree 4, it must be minimal.

3. *Find the degree and minimal polynomial over $\mathbb{Q}$ of a root α of the polynomial $x^2 + \beta x + 2$, where β is a root of $x^2 + x + 1$.*

   Observe:

$$\begin{aligned}\beta &= \frac{-1 \pm \sqrt{-3}}{2} \\ \beta\overline{\beta} &= \frac{-1 + \sqrt{-3}}{2} \cdot \frac{-1 - \sqrt{-3}}{2} \\ &= \frac{1 + 3}{4} = 1.\end{aligned} \tag{F.2}$$

Then we take:

$$(x^2 + \beta x + 2)(x^2 + \overline{\beta} x + 2) = x^4 - x^3 + 5x^2 - 2x + 4. \tag{F.3}$$

By the rational root theorem, all rational roots of this polynomial are of the form $\pm a/\pm 1$ where $a|4$. And none of these work.

4. *Find the degree of the extension* $\mathbb{Q}(\alpha)/\mathbb{Q}$ *where* $\alpha = \sqrt{1 + \sqrt[3]{2}}$.

We find the minimal polynomial. Note:

$$\begin{aligned} \alpha^2 &= 1 + \sqrt[3]{2} \\ (\alpha^2 - 1)^3 &= 2 \\ (\alpha^2 - 1)^3 - 2 &= 0 \end{aligned} \tag{F.4}$$

So we know $f(\alpha) = 0$ for:

$$\begin{aligned} f(x) &= (x^2 - 1)^3 - 2 \\ &= (x^4 - 2x^2 + 1)(x^2 - 1) - 2 \\ &= x^6 - x^4 - 2x^4 + 2x^2 + x^2 - 1 - 2 \\ &= x^6 - 3x^4 + 3x^2 - 3. \end{aligned} \tag{F.5}$$

By the rational root theorem, all the rational roots are of the form $\frac{\pm p}{\pm q}$ where $p|(-3)$ and $q|1$, training coefficient, leading coefficient. So then our possible roots are $-3, 3, -1, 1$.

Since all terms have even degree, we have:

$$\begin{aligned} f(3) = f(-3) &= 729 - 3(81) + 27 - 3 = 510 \\ f(1) = f(-1) &= 1 - 3 + 3 - 3 = -2. \end{aligned} \tag{F.6}$$

Now by Eisenstein's, it's irreducible since 3 divides all but leading coefficient, doesn't divide leading coefficient, and 9 doesn't divide last.

5. *Prove that any extension of prime degree p has no nontrivial proper subextensions.*

Proof. Let $E/K/F$ be a tower of extensions. Then let $[E : F] = p$, prime. Then since it's finite, we know $[E : F] = [E : K][K : F]$. So $[K : F]$ is either 1 or p. Either way it's done. □

6. *If* K/F *and* L/F *are subextensions of an extension* E/F *with* $[K : F] = n$ *and* $[L : F] = m$ *being relatively prime, prove that* $[KL : F] = nm$.

Proof. We have:

$$\begin{tikzcd}
& K_1K_2 & \\
K_1 \arrow[ur, dash, "\leqslant m"] & & K_2 \arrow[ul, dash, "\leqslant n"'] . \\
& F \arrow[ul, dash, "n"] \arrow[ur, dash, "m"'] &
\end{tikzcd}$$

Now note that $n|[KL : F]$ and $m|[KL : F]$. But since $(n, m) = 1$, we must have nm. □

7. *Find a basis of the field $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ as a vector space over $\mathbb{Q}$.*

   It is $\{1, \sqrt[3]{2}, \sqrt[3]{4}, \sqrt{3}, \sqrt[3]{2}\sqrt{3}, \sqrt[3]{4}, \sqrt{3}\}$, since these two generators are linearly independent.

8. *Find a basis of the field $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3})$ as a vector space over $\mathbb{Q}$.*

   Multiply them together, you should get 9.

13. *Let $\overline{F}$ be an algebraic closure of a field F. Prove that for every finite extension K/F there is a copy of it in $\overline{F}/F$. (That is, there is a monomorphism $\varphi : K \to \overline{F}$ such that $\varphi|_F = Id_F$.*

   Proof. Let $K = F(\alpha_1, ..., \alpha_n)$. $\exists \varphi : F(\alpha_1) \leftrightarrow \overline{F}$ by $\alpha_1 \mapsto \beta_1$ - root of $m_{\alpha_1,F}$ in $\overline{F}$. There exists extension of $\varphi : F(\alpha_1, \alpha_2) \to \overline{F}$, by $\alpha_2 \mapsto \beta_2$- root of $m_{\alpha_2,F(\alpha_1)}$ in $\overline{F}$. □

14. *Moreover, (using Zorn's Lemma) prove that for every algebraic extension K/F there is a copy of it in $\overline{F}/F$.*

   Proof. Consider the set S of embeddings $\varphi : L \to \overline{F}$ where F maps to both of these as well, where $K/L/F$. Define $\varphi_1 \leqslant \varphi_2$ if $L_1 \subseteq L_2$, and $\varphi_2|_{L_1} = \varphi_1$.

   By Zorn, $\exists$ max element in S. $\varphi : L \to \overline{F}$. If $L \neq K$, $\alpha \in K \setminus L$. then φ can be extended to $L(\alpha)$. □

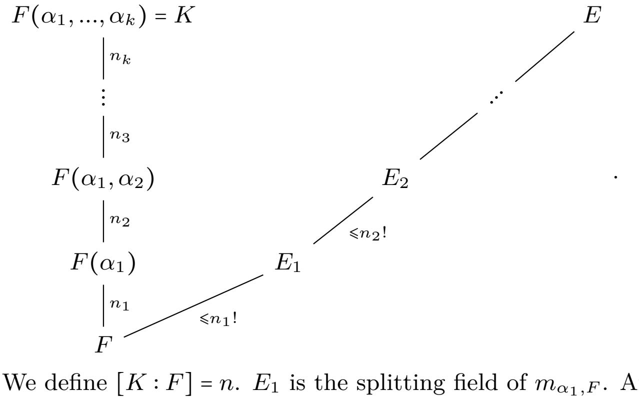
16. **Statement is wrong, ask Ryan.**

17. $K = F(\alpha_1, ..., \alpha_k)$.

   Adjoin all conjugates of $\alpha_1, ...\alpha_k$. Let $f = m_{\alpha_1,F} \cdots m_{\alpha_k,F}$. Let E be the splitting field of F. These are all equal.

18. We need to use induction for this one.

   We have:



   We define $[K : F] = n$. E_1 is the splitting field of $m_{\alpha_1,F}$. And we have $[E_1 : F] \leqslant n_1!$. We have E_2 - the splitting field of $m_{\alpha_2,F}$ such that $[E_2 : F] \leqslant n_1! n_2!$.

   We know that $n = n_1 \cdots n_k$. We have $n_1! \cdots n_k! \leqslant n!$.

20. *$K_1/F, K_2/F$ normal. Prove that K_1K_2/F are normal.*

   Recall the theorem that says **normal extension is exactly the splitting field.** Define an element is **normal** if all its conjugates are in the same field. Take generators of K_1, K_2, take their minimal polynomials, multiply them all, and this will be the splitting field of that polynomial.

22. (a) *Prove that the polynomial $x^n - x$ is separable over every field.*

Proof. $f' = nx^{n-1} - 1$. If the characteristic is $n-1$, then $f'|f$. Then $n = 1$. Then we have an issue. **So this problem statement is incorrect.** □

24. *Give an example of a non-separable field extension.*

Consider $x^p - t = f$. We have $f' = 0$. So f is inseparable. We claim f is irreducible.

Proof. Let $\alpha = \sqrt[p]{t}$. Then $f = (x-\alpha)^p$ in $F(\alpha)$. If $f = gh$, then $g = (x-\alpha)^k$, where $h = (x-\alpha)^{p-k}$. We have $g, h \in F[x]$, with g irreducible. Then $\deg \alpha = \deg g = k$. Then α is separable. But this is a contradiction. But g is separable, so cannot have multiple roots. Inseparable polynomials only contain powers of p as exponents. g is separable since it is not of the form:

$$a_n x^{np} + a_{n-1} x^{(n-1)p} + \cdots.$$

Recall that we are trying to prove that f is irreducible. We need an inseparable, irreducible polynomial. □

26. *Prove that for any prime p and any $n \in \mathbb{N}$, there exists an irreducible polynomial $f \in \mathbb{F}_p[x]$ of degree n.*

Proof. We proved that $\forall p, \forall n, \exists F$ s.t. $[F : \mathbb{F}_p] = n$ (F is the splitting field of $x^{p^n} - x$)

Then $f^* = \langle \alpha \rangle$, so $F = \mathbb{F}_p(\alpha)$. So $\deg_{\mathbb{F}_p} \alpha = n$, so $f = m_{\alpha, \mathbb{F}_p}$ is irreducible of deg n. □

CHAPTER G

Sample problems to final

Monday, April 23rd

1. *Using the theorem on the primitive element, prove easily that if K/F is a separable extension of degree n and E is a field containing K, then there are at most n distinct embeddings of K into E, and if E is normal, then there are exactly n such embeddings.*

   PROOF. Recall the theorem on the primitive element states:

   > If K/F is finite and separable, then there is $\alpha \in K$ such that $K = F(\alpha)$. (α is called "primitive" for K.)

   Note we already have that K/F is finite and separable. So we know there exists $\alpha \in K$ such $K = F(\alpha)$. Note that any embedding φ of K into E must be such that $\varphi|_F = \mathrm{Id}_F$. So we are mapping $\varphi : F(\alpha) \to E$. Now φ is uniquely defined by its action on α, and it must send α to a conjugate of α. Since our extension is of degree n, we know there are at most n conjugates of α in K. Thus we know there are at most n embeddings of K into E.

   Now if E is normal, we know all conjugates of α are in E, so we have all n, so there are exactly n embeddings. □

2. *Explain why the Galois group of a separable polynomial of degree n is isomorphic to a subgroup of S_n.*

   PROOF. Let f be a separable polynomial of degree n. Recall that the Galois group of f is the Galois group of its splitting field. Also recall that if K is the splitting field of a separable polynomial, then K is normal and separable. Thus K is Galois by definition. Now $\forall \varphi \in \mathrm{Gal}(K)$, we know that φ is uniquely defined by its action on α_i, the roots of f, and since it is an automorphism, we know that φ maps α_i to some other root of f. Since f is separable, we know it has no multiple roots, and thus each automorphism is simply a permutation of the indices of the roots, and since there are n roots. Since $\mathrm{Gal}(K/F)$ is a group, we can injectively map to S_n, and the image under this map will be a subgroup of S_n isomorphic to $\mathrm{Gal}(K)$. □

3. *K/F separable, $[K:F]=n$. Prove that E-Galois closure $\Rightarrow [E:F]\leqslant n!$.*

   Proof. Let $K=F(\alpha_1,\dots,\alpha_k)$. Since K is finite and separable, we may apply the primitive element theorem, so $K=F(\alpha)$ for some $\alpha\in K$, so let $f=m_{\alpha,F}$. Now since K is separable, by definition, we know that f is separable. We claim that E is the splitting field of f. So we must check, does f split in E? It does because ALL roots of f are in E since we get all conjugates of α since it is Galous (normal) closure. And since E is minimal such closure, we know that it is a splitting field. Since $\deg f=n$, we know $[E:F]\leqslant n!$ by a result from group theory. (**ask leibman**) □

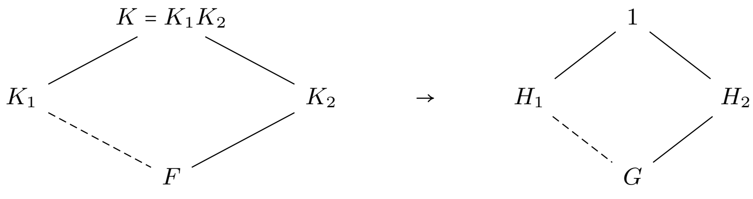
   Proof. **Leibman's proof:** The Galois closure is the splitting field of something. Why? Write $K=F(\alpha_1,\dots,\alpha_k)$. Take $f=m_{\alpha_1}\cdots m_{\alpha_k}$. Then E is a splitting field of f. Find α such that $K=F(\alpha)$. Let $f=m_{\alpha,F}$, then E is a splitting field of f. $H\leqslant G$ such that $|G:H|\leqslant n$, then $\exists N\leqslant H$ such that $N\trianglelefteq G$, and $|G:N|\leqslant n!$. This result is from group theory. Note $H\leftrightarrow K$, $N\leftrightarrow E$, then E/F is normal, $K\subseteq E$, and $[E:F]\leqslant n!$. E is Galois closure since it is normal.

   And $K=\bigcap_{a\in G}aHa^{-1}$. We have $\mathrm{Gal}\to S_n$ by $\varphi\mapsto$ action on the conjugates of α. So $|G|\leqslant n!$, so $[E:F]\leqslant n!$. □

4. *Let K/F be a Galois extension with $[K:F]=n$, if p is a prime such that $p^r|n$, prove that there is a subextension L/F of K/F with $[L:F]=n/p^r$.*

   Proof. □

6. Note K/F is Galois.



Note the dotted line represents normal inclusion. So $H_1\trianglelefteq G$. And we have:

$$\begin{aligned} K=K_1K_2 &\iff H_1\cap H_2=1\\ K_1\cap K_2=F &\iff \langle H_1,H_2\rangle=G\\ K_1/F\text{is normal} &\iff H_1\trianglelefteq G. \end{aligned}\tag{G.1}$$

So we know $\langle H_1,H_2\rangle=H_1H_2$, and $G=H_1\rtimes H_2$. And thus $G/H_1\cong H_2$. So $G\cong H_1\rtimes(G/H_1)$. So we have $H_1=\mathrm{Gal}(K/K_1)$ and $H_2=\mathrm{Gal}(K/K_2)$.

Remark G.1. $\mathbb{Q}(\sqrt[n]{a})/\mathbb{Q}$ not normal for $n \geqslant 3$, (if $x^n - a$ is irreducible). Conjugates of $\sqrt[n]{a}$ are $\omega^k \sqrt[n]{a}$, $k = 0, \ldots, n-1$, and $\omega \notin \mathbb{R}$, so $\omega \sqrt[n]{a} \notin \mathbb{Q}(\sqrt[n]{a})$. So the Galois closure of $\mathbb{Q}(\sqrt[n]{a})$ is not abelian.

We discuss the Galois group of $x^n - a$, where $a \in \mathbb{Q}$, $a > 0$. let $\alpha = \sqrt[n]{a}$. The splitting field is $\mathbb{Q}(\alpha, \omega)$. And $\omega = e^{2\pi i/n}$. Observe:

$$\begin{tikzcd}
& K \arrow[dl, dash] \arrow[dr, dash, "\mathbb{Z}_n"] & \\
\mathbb{Q}(\alpha) \arrow[dr, dash] & & \mathbb{Q}(\omega) \cdot \arrow[dl, dashed, dash, "z_n^*"] \\
& \mathbb{Q} &
\end{tikzcd}$$

Note K is a radical extension, it is obtained from $\mathbb{Q}(\omega)$ by adjoining α. And note $\mathbb{Q}(\omega)$ contains a primitive root of unity of degree n. We prove that the stuff on the edge from $\mathbb{Q}(\omega)$ to K ($\mathrm{Gal}(K/\mathbb{Q}(\omega))$) is cyclic. Note we have $\varphi_k : \alpha \to \omega^k \alpha$. So $G = \{ \varphi_k \text{ for some } k \}$. So we have a homomorphism $G \to \mathbb{Z}_n$, given by $k \to \varphi_k$. It is injective since the φ are uniquely defined. Since target space is finite, it's an isomorphism. We know that the top right bar is cyclic. $\mathbb{Q} = \mathbb{Q}(\alpha) \cap \mathbb{Q}(\omega)$? If so, $\mathrm{Gal} \cong \mathbb{Z}_n \rtimes \mathbb{Z}_n^*$. The claim is that if n is odd, $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\omega) = \mathbb{Q}$. Let's postpone this, Leibman does not know. If we assume n is prime, then $\mathbb{Q}(\alpha)$ has no subextensions, so it's trivial.

CHAPTER H

Module theory definitions and results

CHAPTER I

Field theory definitions and results

Definition I.1. ∀ field F, roots of $x^n = 1$ are called the **roots of unity**.

Definition I.2. The splitting field of $x^n - 1$ is called the n-th **cyclotomic extension of** F.

Definition I.3. Generators of this group are called **primitive roots of unity**.

Definition I.4. The **n-th cyclotomic field** is the splitting field of $x^n - 1 \in \mathbb{Q}[x]$.

Definition I.5. Galois extension K/F is **abelian** if $\mathrm{Gal}(K/F)$ is abelian. K/F is <insert nice property here> if $\mathrm{Gal}(K/F)$ is <insert nice property here>. (cyclic, nilpotent, solvable,...)

Definition I.6. An extension K/F is **algebraic** if $\forall \alpha \in K$, α is algebraic over F.

Remark I.7. If K/F is finite, then it is algebraic (since $\forall \alpha \in K$, $F(\alpha)/F$ is finite.

Definition I.8. The **normal closure** of an extension K/F is the minimal extension which contains all conjugates of all elements of K/F.

Definition I.9. A **conjugate** is a root of the same minimal polynomial: $\sqrt{2} \mapsto -\sqrt{2}$; $\sqrt[3]{2} \mapsto \omega \sqrt[3]{2}, \omega^2 \sqrt[3]{2}$.

Definition I.10. If G is abelian, $G \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$, so if K/F is abelian, then K is a **direct composite**, $K = K_1 K_2 \cdots K_k$ of cyclic subextensions.

We have:

$$\begin{tikzcd}
 & & K \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
K_1 \arrow[drr, dash, "n_1"'] & K_2 \arrow[dr, dash, "n_2"] & K_3 \arrow[d, dash, "n_3"] & \cdots \arrow[dl, dash] & K_k \arrow[dll, dash, "n_k"] \\
 & & F & &
\end{tikzcd},$$

such that $\forall i, K_i \cap \prod_{j \neq i} K_j = F$. Then $K_1 = \mathrm{Fix}(\mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k})$. Let's say that K is a **direct composite** of K_1 and K_2 if:

$$[K : F] = [K_1 : F][K_2 : F].$$

Definition I.11. A **polyradical** extension is an extension of the form:

$$\begin{tikzcd}
K_n \arrow[d, dash] \arrow[ddd, dash, bend left, "polyradical"] \\
\vdots \arrow[d, dash] \\
K_1 \arrow[d, dash] \\
F
\end{tikzcd}.$$

And the short lines are the simple radical extensions.

Definition I.12. $D = d^2 = \prod_{i<j}(\alpha_j - \alpha_i)^2$ is called the **discriminant** of a polynomial f, whose foots are $\alpha_1, ..., \alpha_n$.

Definition I.13. **Elementary symmetric polynomials**:

$$\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= x_1x_2 + x_1x_3 + x_2x_3 + \cdots + x_{n-1}x_n \\
s_3 &= \sum_{i<j<k} x_i x_j x_k, \\
&\vdots \\
s_n &= x_1 x_2 \cdots x_n.
\end{aligned} \tag{I.1}$$

Let E/F be an extension, K/F be a finite subextension ($F \subseteq K \subseteq E$).

Definition I.14. **Embeddings** of K to E over F: homomorphisms $\varphi : K \to E$ such that $\varphi|_F = \mathrm{Id}_F$. It may be that $\varphi(K) = K$, but φ is non-trivial: $\varphi \neq \mathrm{Id}_K$.

Definition I.15. If φ is such an embedding of K, then $\varphi(K)$ is called a **conjugate** of K.

Definition I.16. If K/F is an extension, then K is an F-vector space. $\dim_F K$ is called the **degree of** K **over** F, $\deg_F K = [K : F]$. It may be finite or infinite.

Definition I.17. If $\deg_F K < \infty$, then K/F is a **finite extension**.

Definition I.18. If $\deg_F K = \infty$, then K/F is an **infinite extension**.

Definition I.19. The mapping $\varphi : F \to F$, $\varphi(a) = a^p$, is called the **Frobenius endomorphism** of F. It is a homomorphism: $\forall a, b, (ab)^p = a^p b^p$. And:

$$\begin{aligned}
(a = b)^p &= a^p + pa^{p-1}b + \binom{p}{2} a^{p-2}b^2 + \cdots + pab^{p-1} + b^p \\
&= a^p + b^p,
\end{aligned} \tag{I.2}$$

since all the middle terms go to zero.

Definition I.20. If it is surjective, it is called the **Frobenius automorphism** of F.

Definition I.21. Let K/F be finite, $[K:F]=n$. K/F is **Galois** if:

(1) it is normal and separable.
(2) $|\mathrm{Aut}(K/F)|=n$.
(3) $K=F(\alpha_1,...,\alpha_k)$ s.t. α_i are separable and all their conjugates are in K.
(4) K is a splitting field of a separable polynomial.

So we have 4 equivalent definitions.

Definition I.22. If L/F is finite and separable, let $L=F(\alpha_1,...\alpha_k)$. Adjoin all conjugates of α_i, they are still separable. Then we get an extension K, generated by separable elements whose conjugates are in K, so K is Galois (the minimal Galois extension of F containing K). K/F is called the **Galois closure** of L/F. (It is the normal closure of L/F).

Remark I.23. If $K=F(\alpha)$, then the Galois closure of K is the splitting field of $m_{\alpha,F}$.

Proof. Note that K itself is not necessarily the splitting field of f because the conjugates of α may not be in K. It is the normality of the Galois closure E (the fact that E contains all conjugates of α) which gives us that f must decompose into linear factors. Otherwise we could have some roots of F but not all (think imaginary). □

Definition I.24. Recall that an element α is **separable** if and only if it is a root of a separable polynomial.

Definition I.25. Let $f\in F[x]$. An extension K/F is a **splitting field of** f if in K, f splits "completely": $f=f_1\cdots f_k$, where f_i are linear, so $f=c(x-\alpha_1)\cdots(x-\alpha_k)$, and K is the minimal field with this property.

Definition I.26. Consider the group of permutations of $\alpha_1,...,\alpha_n$ that preserves all relations between $\alpha_1,...,\alpha_n$. This is the group of automorphisms $\mathrm{Aut}(R/\mathbb{Q})=\mathrm{Aut}(F)$ and is called the **Galois group** of F, $\mathrm{Gal}(F)=\mathrm{Gal}(F/\mathbb{Q})$.

Remark I.27. Any element $\sigma\in\mathrm{Gal}(K)$ is uniquely defined by its action on $\{\alpha_i\}$, the roots of the polynomial of which K is the splitting field.

Definition I.28. K/F is said to be **normal** if:

(1) it is algebraic and $\forall\alpha\in K$, $m_{\alpha,F}$ splits completely over K.
(2) Or: if an irreducible polynomial over F has a root in K, then it splits over K.
(3) Or: $\forall\alpha\in K$, **all conjugates of** α **are in** K. This is to say, if you take an element $\alpha\in K$, all its conjugates in any *larger* field are in K.

Theorem I.29 (**On the primitive element**). *If K/F is finite and separable, then there is $\alpha\in K$ such that $K=\mathbb{F}(\alpha)$. (α is called "primitive" for K.)*

Definition I.30. An extension K/F is **separable** if and only if:

(1) the minimal polynomial over F of every element is separable.
(2) every element of K is the root of a separable polynomial over F.

Theorem I.31 (**Galois theorem - full version**). *Let K/F be a Galois extension, let $g = \mathrm{Gal}(K/F)$. Then*

(1) The correspondence: subextension $L/F \leftrightarrow$ subgroup $H \leqslant G$ defined by $H = \mathrm{Gal}(K/L)$, $L = \mathrm{Fix}(H)$ is injective with $|H| = [K : L], |G : H| = [L : F]$. We postpone the proof until Monday. The idea is to prove that if we define subextension this way, then the degree of K/L will be exactly the order of H, and this is the key point of the proof.

(2) If $L_1 \leftrightarrow H_1, L_2 \leftrightarrow H_2$, then $L_1 \subseteq L_2$ if and only if $H_1 \geqslant H_2$ and $[L_2 : L_1] = |H_1 : H_2|$. So there exists only finitely many subextensions of K/F, and the diagram of subextensions is the same as the diagram of subgroups of G drawn ***upside down****:*

$$\begin{tikzcd}
 & 1 \arrow[dl, dash, "n_1"'] \arrow[d, dash, "n_2"] \arrow[dr, dash, "n_4"] & & & & K \arrow[dl, dash, "n_1"'] \arrow[d, dash, "n_2"] \arrow[dr, dash, "n_4"] & & \\
H_1 \arrow[dr, dash, "m"'] & H_2 \arrow[d, dash] & H_4 \arrow[ddl, dash] & \leftrightarrow & L_2 \arrow[dr, dash, "m"'] & L_2 \arrow[d, dash] & L_4 \arrow[ddl, dash] & . \\
 & H_3 \arrow[d, dash] & & & & L_3 \arrow[d, dash] & & \\
 & G & & & & F & &
\end{tikzcd}$$

(3) If $L_1 \leftrightarrow H_1, L_2 \leftrightarrow H_2$, then $L_1 \cap L_2 \leftrightarrow \langle H_1, H_2\rangle$ and $L_1L_2 \leftrightarrow H_1 \cap H_2$. And the following diagram is the proof:

$$\begin{tikzcd}
 & L_1L_2 \arrow[dl, dash] \arrow[dr, dash] \arrow[rrr, leftrightarrow] & & & H_1 \cap H_2 \arrow[dl, dash] \arrow[dr, dash] & & \\
L_1 \arrow[dr, dash] & & L_2 \arrow[dl, dash] & H_1 \arrow[dr, dash] & & H_2 \arrow[dl, dash] & . \\
 & L_1 \cap L_2 & & & \langle H_1, H_2\rangle & &
\end{tikzcd}$$

Since $L_1 \cap L_2$ is the max subfield contained in L_1 and L_2, it corresponds to the minimum subgroup countaining H_1 and H_2, which is $\langle H_1, H_2\rangle$. And...

(4) If $L \leftrightarrow H$, then any embedding $L \leftrightarrow L$ is given by some $\varphi \in G$. $\varphi_1, \varphi_2 \in G$ define the same embedding $\varphi|_L = \varphi_2|_L$ if and only if $\varphi_1 = \varphi_2 \mod H$. So embeddings $\leftrightarrow$ cosets G/H.

(5) Any conjugate of L (result of an embedding) is of the form $\varphi(L)$, $\varphi \in G$. The subgroup, corresponding to $\varphi(L)$ is $\varphi H \varphi^{-1}$. So conjugate subextensions $\leftrightarrow$ conjugate subgroups:

$$\varphi(L) \leftrightarrow \varphi H \varphi^{-1}.$$

(6) If $L \leftrightarrow H$, then L is normal if and only if $H \trianglelefteq G$. In this case, L/F is Galois, and $\mathrm{Gal}(L/F) = G/H$. If L is normal, then the extension from F to L is normal.

Index