Math 308
4-4-1994

Solutions to Problem Set 6.

[page 295]

2. Show $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$.

Since $\sqrt{2}+\sqrt{3} \in \mathbb{Q}(\sqrt{2},\sqrt{3})$, it's obvious that $\mathbb{Q}(\sqrt{2}+\sqrt{3}) \subset \mathbb{Q}(\sqrt{2},\sqrt{3})$.
Conversely, let $a = \sqrt{2}+\sqrt{3}$. Then

$$a^2 = 5 + 2\sqrt{6}, \quad \sqrt{6} = \frac{1}{2}(a^2 - 5) \in \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Hence, $\sqrt{2}(\sqrt{2}+\sqrt{3}) = 2 + \sqrt{6} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Therefore, $\sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Since $\sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$,

$$\sqrt{3} = (\sqrt{2}+\sqrt{3}) - \sqrt{2} \in \mathbb{Q}(\sqrt{2}+\sqrt{3}).$$

Since $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2}+\sqrt{3})$, it follows that $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subset \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Hence, $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. $\square$

---

4. Find the splitting field over $x^4 + 1$ over $\mathbb{Q}$.

$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$. $x^2 + \sqrt{2}x + 1$ has roots $-\dfrac{\sqrt{2}}{2} \pm \dfrac{\sqrt{2}}{2}i$, while $x^2 - \sqrt{2}x + 1$ has roots $\dfrac{\sqrt{2}}{2} \pm \dfrac{\sqrt{2}}{2}i$. So all of the roots lie in $\mathbb{Q}(\sqrt{2}, i)$, and this is the splitting field for $x^4 + 1$ over $\mathbb{Q}$. $\square$

---

8. Let $F = \mathbb{Z}_2$ and let $f(x) = x^3 + x + 1 \in F[x]$. Suppose a is a zero of $f(x)$ in some extension of F. How many elements does $F(a)$ have? Express each member of $F(a)$ in terms of a. Write out a complete multiplication table for $F(a)$.

$x = 0$ and $x = 1$ are not roots of $x^3 + x + 1$. Hence, $x^3 + x + 1$ has no linear factors over $\mathbb{Z}_2$, so it's irreducible. It follows that $F[x]/\langle x^3 + x + 1\rangle$ has $2^3 = 8$ elements, and they have the form

$$a + bx + cx^2 + x^3 + x + 1\rangle, \qquad a, b, c \in \mathbb{Z}_2.$$

The following *Mathematica* function will compute the product of f and g in $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$:

```
mul[f_, g_] := PolynomialMod[PolynomialRemainder[f g, x^3 + x + 1, x], 2]
```

Using this function, it's easy to compute the multiplication table. In the table below, I'm writing the representative of a coset for the coset. Thus, $x + 1$ means $(x + 1) + \langle x^3 + x + 1\rangle$, and so on.

	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

$\square$

10. Let $F(a)$ be the field described in exercise 8. Show that $a+1$, a^2+1, and a^2+a+1 are all zeros of x^3+x^2+1.

I will work with $F[x]/\langle x^3+x+1\rangle$, and I'll operate with the cosets by operating with their representatives.

$$(x+1)^3+(x+1)+1 = x^3+x+1 \in \langle x^3+x+1\rangle.$$

$$(x^2+1)^3+(x^2+1)+1 = x^6+x^4+1 = (x^3+x+1)^2 \in \langle x^3+x+1\rangle.$$

$$(x^2+x+1)^3+(x^2+x+1)+1 = x^6+x^5+x^4+x^3+x^2+x+1 = (x^3+x^2+1)(x^3+x+1) \in \langle x^3+x+1\rangle.$$

It follows that the cosets represented by $x+1$, x^2+1, and x^2+x+1 are roots of x^3+x^2+1. □

---

13. Show that $\mathbb{Q}(\sqrt{2})$ is not isomorphic to $\mathbb{Q}(\sqrt{3})$.

Suppose $\phi : \mathbb{Q}(\sqrt{2}) \approx \mathbb{Q}(\sqrt{3})$ is an isomorphism.
First,

$$\phi(1) = \phi(1\cdot 1) = \phi(1)\phi(1), \quad \text{so} \quad \phi(1) = 1.$$

If n is an integer, then $\phi(n) = n\cdot\phi(1) = n$. Likewise,

$$1 = \phi(1) = \phi\left(n\cdot\frac{1}{n}\right) = n\cdot\phi\left(\frac{1}{n}\right).$$

Therefore, $\phi\left(\dfrac{1}{n}\right) = \dfrac{1}{n}$. So if m and n are integers and $n \ne 0$, then

$$\phi\left(\frac{m}{n}\right) = m\cdot\phi\left(\frac{1}{n}\right) = \frac{m}{n}.$$

Summary: ϕ takes each rational number to itself.
Now suppose $\phi(\sqrt{2}) = a + b\sqrt{3}$, where $a, b \in \mathbb{Q}$. Then

$$2 = \phi(2) = \phi(\sqrt{2})^2 = (a+b\sqrt{3})^2 = a^2+3b^2+2ab\sqrt{3}.$$

If $b = 0$, this says $a^2 = 2$, a contradiction since a is rational. If $a = 0$, this says $3b^2 = 2$, a contradiction since b is rational. If a and b are nonzero, then $\sqrt{3} = \dfrac{2-a^2-3b^2}{2ab}$. This is a contradiction, because the fraction on the right is rational, but $\sqrt{3}$ is not.
Therefore, there is no such map ϕ, and $\mathbb{Q}(\sqrt{2})$ is not isomorphic to $\mathbb{Q}(\sqrt{3})$. □

[Problems from homework sheet]

1. If V is a vector space over a field F and W is a subspace of V, the **quotient vector space** V/W is the abelian group V/W with scalar multiplication given by

$$a\cdot(v+W) = av+W, \qquad a \in F, v \in V.$$

a. Show that V/W is a vector space over F.

V/W is an additive abelian group. I only need to show that the scalar multiplication satisfies the appropriate axioms. Let $a, b \in F$, $u, v \in V$.

$$(a+b)(v+W) = (a+b)v+W = (av+bv)+W = (av+W)+(bv+W) = a(v+W)+b(v+W).$$

$$a\left[(u+W)+(v+W)\right]=a\left[(u+v)+W\right]=a(u+v)+W=(au+av)+W=$$
$$(au+W)+(av+W)=a(u+W)+a(v+W).$$
$$1(v+W)=v+W.$$
$$a\left[b(v+W)\right]=a(bv+W)=a(bv)+W=(ab)v+W=(ab)(v+W).$$

Therefore, V/W is a vector space over F. □

Let $\{w_a\}_{a\in A}$ be a basis for W. Enlarge it to a basis for V; that is, find vectors $\{v_b\}_{b\in B}$ such that $\{w_a\}_{a\in A}\cup\{v_b\}_{b\in B}$ is a basis for V. (This is possible because every linearly independent subset of a vector space may be enlarged to a basis.) In this situation, it's possible to show that $\{v_b+W\}_{b\in B}$ is a basis for V/W.

b. Let $V=\mathbb{R}^3$, considered as an $\mathbb{R}$-vector space in the usual way. Let $W=\langle 1,1,1\rangle$. Find a basis for V/W.

Take $\langle 1,1,1\rangle$ and enlarge it to a basis for $V=\mathbb{R}^3$:

$$\left\{\begin{bmatrix}1\\1\\1\end{bmatrix},\begin{bmatrix}1\\0\\0\end{bmatrix},\begin{bmatrix}0\\1\\0\end{bmatrix}\right\}.$$

By the remarks above,

$$\left\{\begin{bmatrix}1\\0\\0\end{bmatrix}+W,\begin{bmatrix}0\\1\\0\end{bmatrix}+W\right\}$$

is a basis for V/W.

---

c. Let $\langle x^3\rangle$ be the principal ideal in $\mathbb{R}[x]$ generated by x^3. $\langle x^3\rangle$ is a subspace of $\mathbb{R}[x]$, if $\mathbb{R}[x]$ is regarded as a vector space over $\mathbb{R}$. In this way, the quotient ring $\dfrac{\mathbb{R}[x]}{\langle x^3\rangle}$ is also an $\mathbb{R}$-vector space. Find an $\mathbb{R}$-basis for the quotient vector space $\dfrac{\mathbb{R}[x]}{\langle x^3\rangle}$.

By the Division Algorithm, if $f\in\mathbb{R}[x]$, then

$$f(x)=x^3\cdot q(x)+r(x),\quad \text{where}\quad \deg r<\deg x^3=3.$$

Hence, $f(x)+\langle x^3\rangle=r(x)+\langle x^3\rangle$. Note that $r(x)$ can be written in the form $a+bx+cx^2$, so $f(x)+\langle x^3\rangle$ is an $\mathbb{R}$-linear combination of the cosets in $\{1+\langle x^3\rangle, x+\langle x^3\rangle, x^2+\langle x^3\rangle\}$.

Note that this representation is unique. Suppose

$$a+bx+cx^2+\langle x^3\rangle=a'+b'x+c'x^2+\langle x^3\rangle.$$

Then $(a-a')+(b-b')x+(c-c')x^2\in\langle x^3\rangle$, but this is only possible if $a-a'=0$, $b-b'=0$, and $c-c'=0$ — i.e. $a=a'$, $b=b'$, and $c=c'$.

It follows that $\{1+\langle x^3\rangle, x+\langle x^3\rangle, x^2+\langle x^3\rangle\}$ is an $\mathbb{R}$-basis for the quotient vector space $\dfrac{\mathbb{R}[x]}{\langle x^3\rangle}$. □

---

d. Let V_1 and V_2 be subspaces of V. Prove that

$$\frac{V_1}{V_1\cap V_2}\approx\frac{V_1+V_2}{V_2}.$$

Conclude that

$$\dim V_1 + \dim V_2 = \dim(V_1 + V_2) + \dim(V_1 \cap V_2).$$

The corresponding result for groups says that there is an isomorphism of additive groups

$$\frac{V_1}{V_1 \cap V_2} \approx \frac{V_1 + V_2}{V_2}.$$

The map (from left to right) is

$$\phi\left[v + (V_1 \cap V_2)\right] = v + V_2, \quad \text{for} \quad v \in V_1.$$

I only need to show that ϕ preserves scalar multiplication. Suppose $v \in V_1$ and $a \in F$. Then

$$\phi\left[a\left(v + (V_1 \cap V_2)\right)\right] = \phi\left[av + (V_1 \cap V_2)\right] = av + V_2 = a(v + V_2) = a \cdot \phi\left[v + (V_1 \cap V_2)\right].$$

ϕ is therefore a linear transformation. It was already know to be bijective, so it's an isomorphism of vector spaces.

Isomorphic vector spaces have the same dimension, so

$$\dim \frac{V_1}{V_1 \cap V_2} = \dim \frac{V_1 + V_2}{V_2},$$

$$\dim V_1 - \dim(V_1 \cap V_2) = \dim(V_1 + V_2) - \dim V_2,$$

$$\dim V_1 + \dim V_2 = \dim(V_1 + V_2) + \dim(V_1 \cap V_2). \square$$

---

2. Let $f : V_1 \to V_2$ and $g : V_2 \to V_3$ be linear transformations. Show that the composite $g \cdot f : V_1 \to V_3$ is a linear transformation.

Let $a \in F$ and $u, v \in V_1$, Then

$$g\left[f(au + v)\right] = g\left[af(u) + f(v)\right] = ag[f(u)] + g[f(v)]. \square$$

---

3. Prove or disprove: If a system of linear equations has more equations than unknowns, then it has no solutions.

The claim is false. For example, the system

$$\begin{aligned} x + y &= 1, \\ 2x + 2y &= 2, \\ 3x + 3y &= 3, \end{aligned}$$

has infinitely many solutions of the form $\langle x, y \rangle = a \cdot \langle 1, -1 \rangle$. $\square$

---

4. Find a basis for $\ker f$ and $\operatorname{im} f$, if f is the linear transformation $\mathbf{R}^4 \to \mathbf{R}^2$ whose matrix relative to the standard bases is given by

$$\begin{bmatrix} 1 & 1 & 0 & 4 \\ 0 & 0 & 1 & -1 \end{bmatrix}.$$

If $\langle a, b, c, d \rangle \in \ker f$, then

$$\begin{bmatrix} 1 & 1 & 0 & 4 \\ 0 & 0 & 1 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \end{bmatrix}.$$

Thus,

$$a + b + 4d = 0, \quad c - d = 0.$$

Hence, $a = -b - 4d$ and $c = d$. Therefore,

$$\begin{bmatrix} a \\ b \\ c \\ d \end{bmatrix} = \begin{bmatrix} -b - 4d \\ b \\ d \\ d \end{bmatrix} = b \cdot \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix} + d \cdot \begin{bmatrix} -4 \\ 0 \\ 1 \\ 1 \end{bmatrix}.$$

So

$$\left\{ \begin{bmatrix} -1 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \begin{bmatrix} -4 \\ 0 \\ 1 \\ 1 \end{bmatrix} \right\}$$

is a basis for $\ker f$.

A basis for $\operatorname{im} f$ (the column space of the matrix) is obtained by looking at columns in the matrix corresponding to leading coefficients in the row reduced echelon form. The matrix is already in row reduced echelon form, so

$$\left\{ \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix} \right\}$$

is a basis for $\operatorname{im} f$. $\square$

---

5. Let $f : V \to W$ be a linear transformation. Suppose f has an inverse $g : W \to V$ (g is the inverse of f as a map of sets.) Show that g must be a linear transformation.

Let $a \in F$, $u, v \in W$. Since f is invertible, it's bijective, and there are unique elements $u', v' \in V$ such that $f(u') = u$ and $f(v') = v$. Then

$$g(au + v) = g\left[af(u') + f(v')\right] = g\left[f(au' + v')\right] = au' + v'.$$

But $u' = g(u)$ and $v' = g(v)$, so

$$g(au + v) = ag(u) + g(v).$$

Therefore, g is a linear transformation. $\square$

"The artists must be sacrificed to their art. Like the bees, they must put their lives into the sting they give."
- Ralph Waldo Emerson