Math200b, lecture 16

Golsefidy

Tensor product of algebras

In the previous lecture we defined an A-algebra R; we said R is called an A-algebra if there is a ring homomorphism $c : A \to Z(R)$ where $Z(R)$ is the center of R. We pointed out that in this case R is an (A, A)-bimodule. We mentioned that if R_1 and R_2 are two A-algebras, then $R_1 \otimes_A R_2$ can be made into an A-algebra: it is clearly an (A, A)-bimodule, and we can define a product on $R_1 \otimes_A R_2$ such that $(r_1 \otimes r_2)(r_1' \otimes r_2') = r_1 r_1' \otimes r_2 r_2'$. Here is an important example that can help us understand the algebra structure of many tensor products.

Theorem 1 *Suppose R and S are unital commutative rings, and $\phi : S \to S$ is a ring homomorphism. Using ϕ, we view R as an*

S-algebra. We extend ϕ *to a ring homomorphism* $\phi : S[x] \to R[x]$ *by letting* $\phi(x) = x$*; that means* $\phi(\sum_{i=0}^{\infty} a_i x^i) = \sum_{i=0}^{\infty} \phi(a_i) x^i$*. Then* $R\phi(I) \trianglelefteq R[x]$ *and*

$$S[x]/I \otimes_S R \simeq R[x]/R\phi(I).$$

Proof. We already know that $R\phi(I)$ is an R-module; so to see it is an $R[x]$-module, it is enough to observe that $x(R\phi(I)) = R\phi(xI) \subseteq R\phi(I)$.

Let $f : S[x]/I \times R \to R[x]/R\phi(I)$, $f(p(x)+I, r) := r\phi(p)+R\phi(I)$. Well-definedness.

$$\begin{aligned} p_1(x) + I = p_2(x) + I \Rightarrow & p_1 - p_2 \in I \\ \Rightarrow & r(\phi(p_1 - p_2) \in R\phi(I) \\ \Rightarrow & r\phi_1(x) + R\phi(I) = r\phi_2(x) + R\phi(I). \end{aligned}$$

Linearity in each factor is clear. And so by the universal property of tensor product, there is an abelian group homomorphism $\theta : S[x]/I \otimes_S R \to R[x]/R\phi(I)$ such that $\theta((p(x)+I) \otimes r) = rp(x) + R\phi(I)$.

Let $\widetilde{\psi} : R[x] \to S[x]/I \otimes_S R$, $\widetilde{\psi}(\sum_{i=0}^{\infty} r_i x^i) := \sum_{i=0}^{\infty} (x^i + I) \otimes r_i$. Clearly $\widetilde{\psi}$ is a well-defined abelian group homomorphism.

$R\phi(I) \subseteq \ker\widetilde{\psi}$. Suppose $p(x) = \sum_{i=0}^{\infty} s_i x^i \in I$ and $r \in R$. Then

$$\begin{aligned}
\widetilde{\psi}(r\phi(p)) &= \sum_{i=0}^{\infty}(x^i + I) \otimes r\phi(s_i) \qquad \text{(S-balanced)} \\
&= \sum_{i=0}^{\infty} s_i(x^i + I) \otimes r \\
&=(p(x) + I) \otimes r = 0.
\end{aligned}$$

And so we get an abelian group homomorphism,

$$\psi : R[x]/R\phi(I) \longrightarrow S[x]/I \otimes_S R,$$

$$\psi\left((\sum_{i=0}^{\infty} r_i x^i) + R\phi(I)\right) = \sum_{i=0}^{\infty}(x^i + I) \otimes r_i.$$

$\theta \circ \psi = \mathrm{id}$.

$$\begin{aligned}
\theta \circ \psi\left((\sum_{i=0}^{\infty} r_i x^i) + R\phi(I)\right) &=\theta(\sum_{i=0}^{\infty}(x^i + I) \otimes r_i) \\
&= \sum_{i=0}^{\infty} r_i x^i + R\phi(I).
\end{aligned}$$

$\psi \circ \theta = \mathrm{id}.$

$$\begin{aligned}
\psi \circ \theta((\sum_{i=0}^{\infty} s_i x^i + I) \otimes r) =& \psi(r\phi(\sum_{i=0}^{\infty} s_i x^i) + R\phi(I)) \\
=& \sum_{i=0}^{\infty} \psi(r\phi(s_i)x^i + R\phi(I)) \\
=& \sum_{i=0}^{\infty} (x^i + I) \otimes (r\phi(s_i)) \\
=& \sum_{i=0}^{\infty} (s_i x^i + I) \otimes r \\
=& (\sum_{i=0}^{\infty} s_i x^i + I) \otimes r;
\end{aligned}$$

Pure tensor elements generate the tensor product as an abelian group and $\psi \circ \theta$ is an abelian group homomorphism.

Hence ψ and θ are abelian group isomorphisms.

Ring homomorphism. It is enough to show

$$\theta(((p_1 + I) \otimes r_1)((p_2 + I) \otimes r_2)) = \theta((p_1 + I) \otimes r_1)\theta((p_2 + I) \otimes r_2);$$

and this is easy to check. Since θ is an abelian group homomorphism and pure tensor elements generate the tensor product as an abelian group, by distribution it is enough to check the above equality to get that θ is a ring a homomorphism. ■

Here are some applications of Theorem 1.

Example. Show that $\mathbb{Q}[i]\otimes_{\mathbb{Q}}\mathbb{Q}[i] \simeq \mathbb{Q}[i]\oplus\mathbb{Q}[i]$ as $\mathbb{Q}$-algebras.

Proof.

$$\begin{aligned}
\mathbb{Q}[i] \otimes_{\mathbb{Q}} \mathbb{Q}[i] &\simeq \mathbb{Q}[x]/\langle x^2+1\rangle \otimes_{\mathbb{Q}} \mathbb{Q}[i] && \text{(evaluation at } i\text{)}\\
&\simeq \mathbb{Q}[i][x]/\langle x^2+1\rangle && \text{(Theorem 1)}\\
&\simeq \mathbb{Q}[i][x]/\langle (x+i)(x-i)\rangle \\
&\simeq \mathbb{Q}[i][x]/\langle x+i\rangle \oplus \mathbb{Q}[i][x]/\langle x-i\rangle && \text{(CRT)}\\
&\simeq \mathbb{Q}[i] \oplus \mathbb{Q}[i] && \text{(evaluation at } \pm i\text{)}
\end{aligned}$$

■

Example. Show that $k[x] \otimes_k k[x] \simeq k[x, y]$.

Proof. $k[x] \otimes_k k[x] \simeq k[x] \otimes_k k[y] \simeq k[y][x] \simeq k[x, y]$ (the non-trivial step is because of Theorem 1 with $I = 0$.) ■

Example. Suppose A and B are commutative rings and $\phi : A \to B$ is a ring homomorphism. Then $A[x] \otimes_A B \simeq B[x]$.

Example. Suppose p is a prime. Then show that

$$\mathbb{Z}[i]\otimes_{\mathbb{Z}}\mathbb{F}_p \simeq \begin{cases} \mathbb{F}_{p^2} & \text{if } x^2+1 \text{ has zero in } \mathbb{F}_p \\ \mathbb{F}_p \oplus \mathbb{F}_p & \text{if } p \text{ is odd and } x^2+1 \text{ has a zero in } \mathbb{F}_p \\ \mathbb{F}_2[y]/\langle y^2\rangle & \text{if } p=2, \end{cases}$$

where $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $\mathbb{F}_{p^2}$ is a field of order p^2.

Proof. By Theorem 1, we have

$$\mathbb{Z}[i]\otimes_{\mathbb{Z}}\mathbb{F}_p \simeq \mathbb{Z}[x]/\langle x^2+1\rangle \otimes_{\mathbb{Z}} \mathbb{F}_p \simeq \mathbb{F}_p[x]/\langle x^2+1\rangle.$$

If x^2+1 has no zero in $\mathbb{F}_p$, then it is irreducible in $\mathbb{F}_p[x]$; and so $\langle x^2+1\rangle$ is a maximal ideal of $\mathbb{F}_p[x]$. Hence the factor ring is a field; and one can see that its order is p^2.

If x^2+1 has a zero a in $\mathbb{F}_p$ and p is odd, then $-a$ is a distinct zero of x^2+1; and so $x^2+1 = (x+a)(x-a)$ and $\gcd(x+a, x-a) = 1$. Hence by the CRT we have

$$\begin{aligned} \mathbb{F}_p[x]/\langle x^2+1\rangle =& \mathbb{F}_p[x]/\langle (x-a)(x+a)\rangle \\ \simeq& \mathbb{F}_p[x]/\langle x-a\rangle \oplus \mathbb{F}_p[x]/\langle x+a\rangle \\ \simeq& \mathbb{F}_p \oplus \mathbb{F}_p. \end{aligned}$$

If $p=2$, then $x^2+1 = (x+1)^2$; hence $x \mapsto y+1$ induces an isomorphism $\mathbb{F}_2[x]/\langle x^2+1\rangle \simeq \mathbb{F}_2[y]/\langle y^2\rangle$. ∎

Field theory

If F and E are two fields and F is a subfield of E, we say E/F is a field extension. Suppose E/F is a field extension; we say $\alpha \in E$ is algebraic over F if it is a zero of a non-constant polynomial $p(x) \in F[x]$. If $\alpha \in E$ is not algebraic over F, we say α is transcendental over F.

Theorem 2 *Suppose E/F is a field extension, $\alpha \in E$ is algebraic over F. Then*

1. *there is a unique monic polynomial $m_{\alpha,F}(x) \in F[x]$ such that*
$$\ker \phi_\alpha = \langle m_{\alpha,F}(x) \rangle$$
where $\phi_\alpha : F[x] \to E$ is the evaluation at α map.

2. *$m_{\alpha,F}(x)$ is irreducible in $F[x]$.*

3. *The ring $F[\alpha]$ generated by F and α is a field; and*
$$F[\alpha] \simeq F[x]/\langle m_{\alpha,F}(x) \rangle.$$

4. *$F[\alpha] = \{\sum_{i=0}^{d_0-1} a_i \alpha^i | \, a_i \in F\}$ where $d_0 = \deg m_{\alpha,F}(x)$ where $d_0 := \deg m_{\alpha,F}(x)$.*

Proof. The evaluation map $\phi_\alpha : F[x] \to E$ is a ring homomorphism. Hence $\ker\phi_\alpha$ is an ideal of $F[x]$. And as $\phi_\alpha(1) = 1 \neq 0$, $\ker\phi_\alpha$ is a proper ideal of $F[x]$. Since α is algebraic over F, $\ker\phi_\alpha$ is a non-zero ideal. Since $F[x]$ is a PID and $\ker\phi_\alpha$ is a proper ideal non-zero, there is a monic polynomial $m_{\alpha,F}(x) \in F[x]$ such that $\ker\phi_\alpha = \langle m_{\alpha,F}(x)\rangle$. Notice that $\langle p_1\rangle = \langle p_2\rangle$ if and only if $p_1 = cp_2$ for some $c \in F[x]^\times = F^\times$; and so there is a unique monic polynomial that can generate $\ker\phi_\alpha$.

Since $\ker\phi_\alpha$ is a non-zero proper ideal, $m_{\alpha,F}(x) \notin \{0\} \cup F^\times$. Suppose $m_{\alpha,F}(x) = g(x)h(x)$; then $0 = m_{\alpha,F}(\alpha) = g(\alpha)h(\alpha)$; and so either $g(\alpha) = 0$ or $h(\alpha) = 0$. W.L.O.G. let us assume that $g(\alpha) = 0$. And so $g(x) \in \ker\phi_\alpha = \langle m_{\alpha,F}(x)\rangle$ which implies $\langle g(x)\rangle \subseteq \langle m_{\alpha,F}(x)\rangle \subseteq \langle g(x)\rangle$. Therefore $g(x) = cm_{\alpha,F}(x)$ for some $c \in F^\times$; this implies that $m_{\alpha,F}(x)$ is irreducible in $F[x]$.

By the first isomorphism theorem, $\mathrm{Im}(\phi_\alpha) \simeq F[x]/\ker\phi_\alpha$. By definition,

$$\mathrm{Im}(\phi_\alpha) = \{f(\alpha)|\, f(x) \in F[x]\} = \{\sum_{i=0}^{n} f_i\alpha^i|\, f_i \in F, n \in \mathbb{Z}^+\}.$$

It is easy to see that this is the smallest subring of E that contians F as a subring and α as an element; and we denote it by $F[\alpha]$. Hence $F[\alpha] \simeq F[x]/\langle m_{\alpha,F}(x)\rangle$. Since $F[x]$ is a PID and $m_{\alpha,F}(x)$ is irreducible in $F[x]$, $\langle m_{\alpha,F}(x)\rangle$ is a maximal ideal of $F[x]$. Therefore $F[\alpha] \simeq F[x]/\langle m_{\alpha,F}(x)\rangle$ is a field.

For any $\beta \in F[\alpha]$, there is $f(x) \in F[x]$ such that $\beta = f(\alpha)$. By the Long Division Algorithm, there are $q(x), r(x) \in F[x]$ such that $f(x) = q(x)m_{\alpha,F}(x) + r(x)$ and $\deg r < \deg m_{\alpha,F} = d_0$. Hence

$$\beta = f(\alpha) = q(\alpha)\underbrace{m_{\alpha,F}(\alpha)}_{0} + r(\alpha) = r(\alpha);$$

and claim follows as $\deg r \leq d_0 - 1$. ■

Lemma 3 *Suppose* E/F *is a field extension,* $p(x) \in F[x]$ *is irreducible, and* $\alpha \in E$ *is a zero of* $p(x)$. *Then* $m_{\alpha,F}(x) = cp(x)$ *for some* $c \in F^{\times}$.

Proof. Since $p(\alpha) = 0$, $p(x) \in \langle m_{\alpha,F}(x)\rangle$; and so there is $g(x) \in F[x]$ such that $p(x) = m_{\alpha,F}(x)g(x)$. Since $p(x)$ is irreducible, either $m_{\alpha,F}(x)$ is a constant or $g(x)$ is constant. As $m_{\alpha,F}$ is not constant, claim follows. ■

Proposition 4 *Suppose* $p(x) \in F[x]$ *is irreducible; then there is a field extension* E/F *and* $\alpha \in E$ *such that (1)* $p(\alpha) = 0$ *and (2)* $E = F[\alpha]$.

Proof. The above results imply that if there is such a field, then it should be $F[\alpha] \simeq F[x]/\langle m_{\alpha,F}(x)\rangle = F[x]/\langle p(x)\rangle$. So we let $E := F[x]/\langle p(x)\rangle$. Since $F[x]$ is a PID and $p(x)$ is irreducible in $F[x]$, $\langle p(x)\rangle$ is a maximal ideal of $F[x]$. Hence E is a field. Let $\alpha := x + \langle p(x)\rangle \in E$. It is clear that E is generated by F and α as a ring (as the ring of polynomials $F[x]$ is generated by F and x as a ring). So it is enough to show $p(\alpha) = 0$. Notice that we have to identify F with a subfield of E before we evaluate $p(x)$ at α; that means we send $c \in F$ to $\overline{c} := c + \langle p(x)\rangle$. Suppose $p(x) = \sum_{i=0}^{n} c_i x^i$; then

$$\begin{aligned} p(\alpha) &= \sum_{i=0}^{n} \overline{c_i}\alpha^i = \sum_{i=0}^{n}(c_i + \langle p(x)\rangle)(x + \langle p(x)\rangle)^i \\ &= \sum_{i=0}^{n}(c_i x^i + \langle p(x)\rangle) = (\sum_{i=0}^{n} c_i x^i) + \langle p(x)\rangle \\ &= p(x) + \langle p(x)\rangle = 0. \end{aligned}$$

■