Potential schedule “Ring and module theory”

- *Representations of finite groups.* Lectures 1–7; topics covered *e.g.*: representations, characters, orthogonality, class functions.
- *Rings and ideals.* Lectures 8–16; topics covered *e.g.*: rings, ideals, prime and maximal ideals, Chinese remainder theorem, Euclidean rings.
- *Modules.* Lectures 17–21; topics covered *e.g.*: modules, free modules, projective modules.
- *Applications.* Lectures 22–26; topics covered *e.g.*: fields, Cayley–Hamilton, p-adic numbers, Lie algebras and groups.
- Exercises would include computer algebra calculations, *e.g.*

```
In[1]:= p = 12 + 34 x + 34 x^2 + 14 x^3 + 2 x^4;
        q = 432 + 396 x + 132 x^2 + 19 x^3 + x^4;
        r = 1 + x^2;
        Factor[p]
        Factor[q]
        Factor[r]
        Factor[p, GaussianIntegers → True]
        Factor[q, GaussianIntegers → True]
        Factor[r, GaussianIntegers → True]
Out[4]= 2 (1 + x)^2 (2 + x) (3 + x)
Out[5]= (3 + x) (4 + x) (6 + x)^2
Out[6]= 1 + x^2
Out[7]= 2 (1 + x)^2 (2 + x) (3 + x)
Out[8]= (3 + x) (4 + x) (6 + x)^2
Out[9]= (-i + x) (i + x)
```

Lecture 9, Ideals in rings + quotient rings

Recall from last time:

A ring R is a set with two operations $+, \cdot$

The standard examples where:

- $\mathbb{Z}$
- $\mathbb{Q}[x]$
- $Mat_n(\mathbb{Q})$

Today: How to form analogs of quotient vector spaces or quotient groups for rings

Definition 8.1 Let R be a ring.

An additive subgroup $I \subset R$ is called a

left ideal $\boxed{rx \in I, \forall r \in R, x \in I}$

right ideal $\boxed{xr \in I, \forall r \in R, x \in I}$

If its both, then it is just called an ideal.

Example 8.2 – $I = \{0\}$, $I = R$ are always ideals

trivial ideals

– $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} \subset \mathbb{Z}$ is an ideal

– $I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \,\middle|\, a, b \in \mathbb{Q} \right\} \subset Mat_2(\mathbb{Q})$ is a left ideal

$I' = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \,\middle|\, a, b \in \mathbb{Q} \right\} \subset Mat_2(\mathbb{Q})$ is a right ideal

Definition 8.3 Let $I, J \subset R$ be ideals.

Define:
$$I + J := \{x + y \mid x \in I, y \in J\}$$
$$I \cap J := \{x \mid x \in I \cap J\}$$
$$I \cdot J := \{\sum_{fin} x_i y_i \mid x_i \in I, y_i \in J\}$$

Lemma 8.4 These are all ideals in R and $IJ \subset I \cap J$

Proof This exercise sheet. $\square$

Example 8.5

$I = 4\mathbb{Z}, J = 6\mathbb{Z}$. Then:

$$IJ = \underset{4\cdot 6}{24\mathbb{Z}} \subsetneq \underset{\mathrm{lcm}(4,6)}{12\mathbb{Z}} = I \cap J$$

Reminder: $f: R \to R'$ is called ring homomorphism if $f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$, $f(1_R) = 1_{R'}$

Proposition 8.6 The kernel $\boxed{\ker(f) = \{x \in R \mid f(x) = 0\}}$ of a ring hom. $f: R \to R'$ is an ideal in R.

Proof $\ker(f)$ is an additive subgroup of R, as we have seen. For $r \in R$ and $x \in \ker(f)$ we have

$$f(rx) = f(r)f(x) = 0 = f(x)f(r) = f(xr) \qquad \square$$

Example 8.7 Consider the evaluation at zero $ev_0 : \mathbb{Q}[X] \to \mathbb{Q}$, $p \mapsto p(0)$. Then $\ker(ev_0) = \{Xp \mid p \in \mathbb{Q}[X]\}$

Definition 8.8 For $I \subset R$ an ideal and $a \in R$ define $a + I = \{a + x \mid x \in I\}$

Lemma 8.9 $a + I = b + I \iff a - b \in I$

Proof This exercise sheet $\square$

Theorem 8.10 Let $I \subset R$ be an ideal.

The quotient ring $R/I = \{a + I \mid a \in R\}$ together with

$$\boxed{\begin{aligned} (a+I) + (b+I) &:= a+b+I \\ (a+I)(b+I) &:= a \cdot b + I \end{aligned}} \quad (*)$$

is a ring with $0 = 0 + I$ and $1 = 1 + I$

Proof To prove the theorem we first check that (*) are well-defined.

Let $a+I = \tilde{a}+I \overset{\text{Lemma 8.9}}{\Longrightarrow} a-\tilde{a} \in I$

Now $(a+I)+(b+I) = (\tilde{a}+I)+(b+I)$, since $I \ni a-\tilde{a} = (a+b)-(\tilde{a}+b)$, using Lemma 8.9

Moreover $(a+I)(b+I) = (\tilde{a}+I)(b+I)$, since $I \ni a-\tilde{a} \overset{I \text{ ideal}}{\Longrightarrow} (a-\tilde{a})b \in I$. Then use Lemma 8.9

Similarly for $b, \tilde{b}$.

Finally, $(0+I)+(a+I) = a+I = (0+I)(0+I)$ and

$$(1+I)(a+I) = a+I = (a+I)(1+I)$$

by definition $\square$

<u>Example 8.11</u> – If $I = n\mathbb{Z} \subset \mathbb{Z} = R$

then $R/I \simeq \mathbb{Z}/n\mathbb{Z}$

– If $I = \{X \cdot p \mid p \in \mathbb{Q}[X]\} \subset \mathbb{Q}[X] = R$,

then $R/I \simeq \mathbb{Q}$ (kills polynomials with non-constant term)