Math 122 Wednesday, January 11 Exam Review part I: rings

Exam on rings & modules, light reference to groups. In 3 parts:
1) 10 definitions, 3 points each
2) 15 T-F questions, 1 point for correct answer, 4 points for the explanation
3) 5 statements to prove, 10 points

Rings ex $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Z}/n\mathbb{Z}$, F field, $F[x]$, $F[x,y]$
know defn of a ring (commutative), subring, ideal, quotient ring R/I, ring homomorphism $\varphi: R \to R'$, $\ker\varphi = I \subset R$, $\operatorname{im}\varphi \subset R'$ subring

rings with few ideals
$R=\{0\}$ has 1-ideal
$R=F$ has 2-ideals
any $a\in R$ gives a principal ideal $(a)=\{ar : r\in R\}$
$(a)=0$ if $a=0$, $(a)=R$ iff $a\in R^\times$

$I\subset J\subset R$ $\longleftrightarrow$ ideals in $R/I \supset J/I$
I is maximal in R $\longleftrightarrow$ R/I has only two ideals so is a field

$R^\times$ = unit group of invertible elements e.g. $\mathbb{Z}^\times = \langle \pm 1\rangle$, $\mathbb{Z}[i]^\times = \langle \pm 1, \pm i\rangle$, $(\mathbb{Z}/n\mathbb{Z})^\times$ order $\varphi(n)$

Identify the sets of ideals $I\subset R$ with inclusions
For $R=\mathbb{Z}$, ideals $\longleftrightarrow$ pos. integers $n\geq 0$. $I=(n)$, $I=(n)\supset J=(m)$ iff $n\mid m$
I is maximal $\Leftrightarrow$ $n=p$ a prime. $\{a/b : b\neq 0\}/n$
Integral domain R: if $ab=0$ then $a=0$ or $b=0$; ex $\mathbb{Z}$, non-ex $\mathbb{Z}/4\mathbb{Z}$; $R\hookrightarrow F$ the "quotient field"
- If R is a domain and every $I\subset R$ is principal then R is a PID. ex $\mathbb{Z}\hookrightarrow\mathbb{Q}$, $F[x]\hookrightarrow F(x)$
- Method to show R is a PID is to find a Euclidean ring structure: $\delta: R-\{0\}\to\{0,1,2,3,\dots\}$ such that if $a,b\in R-\{0\}$ then $b=ma+r$ with $\delta(r)<\delta(a)$ or $r=0$.
Then any I is principal generated by $a\in I$ with smallest value of $\delta(a)$.
ex $\mathbb{Z}$, $\delta(a)=|a|$; $\mathbb{Z}[i]$, $\delta(a+bi)=a^2+b^2$; $F[x]$, $\delta(f(x))=\deg f$

Prime factorization $n = \pm p_1\cdots p_k$ primes, $f(x)=\pm p_1(x)^{e_1}\cdots p_k(x)^{e_k}$ (p_i irreducible monic polys over F)

$f\in R$ is irreducible if it has no proper divisors; $(f)\subset R$ has no principal ideal (g) between them.
In a PID $\Rightarrow$ (f) is maximal $\Leftrightarrow$ $R/(f)$ is a field

e.g. UFD that's not a PID: $\mathbb{Z}[x]$. Consider $\ker \mathbb{Z}[x]\to\mathbb{Z}/n$ $f(x)\mapsto f(0) \bmod n$
$\ker = (x,n) = x\mathbb{Z}[x]+n\mathbb{Z}[x]$ not gen by any $a\in R$ ($f\mapsto f(0)\in\mathbb{Z}$ mod n)

For $f(x)\in\mathbb{Q}[x]$, $f(x)=\underbrace{c}_{\text{content in }\mathbb{Q}}\cdot\underbrace{f_0(x)}_{\text{primitive, with gcd(coeff)}=1 \text{ over } \mathbb{Z}[x]}$
Gauss' Lemma $f_0\cdot g_0$ is also primitive
f_0 is irreducible in $\mathbb{Z}[x]$ $\Leftrightarrow$ irreducible in $\mathbb{Q}[x]$.
mod p method for irreducibility: $f_0(x) \bmod p$ irred $\Rightarrow$ $f_0(x)$ irred
p-adic method for testing irred: Eisenstein's criterion
$x^n + a_{n-1}x^{n-1} + \cdots + a_0$ all $a_i\equiv 0 \bmod p$, $p^2\nmid a_0$ $\Rightarrow$ irred

If $p(x)$ is irreducible over F then $F[x]/(p(x)) = F + Fx + \cdots + Fx^{n-1}$ deg $p = n$ is a field + also a F-vector space of dim n.

All finite fields have p^n elements. Have homomorphism $\phi: \mathbb{Z} \to F$ $0 \mapsto 0$, $1 \mapsto 1$, $n \mapsto 1+1+\cdots+1$
$\ker \phi \neq 0$ if F is finite $= n\mathbb{Z}$ $n > 1$ $n = p$ if R is a field.
Get inclusion $\mathbb{Z}/p\mathbb{Z} \hookrightarrow F = \mathbb{Z}/p\mathbb{Z}\, e_1 + \cdots + \mathbb{Z}/p\mathbb{Z}\, n$ a finite dimensional vector space over $\mathbb{Z}/p\mathbb{Z}$

Found a F with p^2 elements as $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+ax+b)$ ← irreducible. Take $x^2 - a$
a, non-square mod p.

Math 122 Friday, January 13 Exam Review part 2: Modules

R-module: abelian group $+, 0, -m$
action of the ring $m \mapsto am$ $a \in R$ $a(m_1+m_2) = am_1 + am_2$ etc

Modules generalize { a) vector space over a field ($R = F$)
b) ideal $I \subset R$ (subgroup closed under mult. by R) $\rightsquigarrow R/I$ is a quotient module

If $R = F$ then $I = (0)$ or F, $R/I = \underset{1 \text{ dim v.s}}{F}$ or $\underset{0 \text{ dim v.s}}{\{0\}}$

$R = \mathbb{Z}$ then M is just an abelian group. $n \cdot m = \overbrace{m+m+\cdots+m}^{n \text{ times}}$ $I = n\mathbb{Z} = (n)$ is isomorphic to $R = \mathbb{Z}$.
but $R/I = \mathbb{Z}/n\mathbb{Z}$ is finite so it is certainly not isomorphic to $\mathbb{Z}$. $a \mapsto na$

Analog of a finite dimensional vector space = vector space V with a finite spanning set $\{v_1, \ldots, v_n\}$
Equivalently $\exists$ a surjective homomorphism $F^n \twoheadrightarrow V$ $(a_1, \ldots, a_n) \mapsto \sum a_i v_i$
Theory of vector spaces $\Rightarrow V \cong F^m$ for some $m \leq n$ (# basis $\leq$ # spanning set)

For modules, M is <u>finitely generated</u> if $\exists$ a surjective homomorphism $R^n \twoheadrightarrow M$ $(a_1, \ldots, a_n) \mapsto \sum a_i m_i$.
- If there is some set $\{m_1, \ldots, m_k\}$ such that this map is injective then $\exists$ a basis and $M \cong R^k$ is a free module of rank k. $(a_1, \ldots, a_k) + (b_1, \ldots, b_k) = (a_1+b_1, \ldots, a_k+b_k)$, $r(a_1, \ldots, a_k) = (ra_1, \ldots, ra_k)$
- But this can't be found for all finitely generated modules!

Study finitely generated R-modules. $M \xrightarrow{f} N$ R-module homomorphism $f(m_1+m_2) = f(m_1) + f(m_2)$
$f(rm) = rf(m)$
If $M \cong R^m$ and $N \cong R^n$ with bases $\{e_1, \ldots, e_m\}$, $\{e_1', \ldots, e_n'\}$, then $f(e_i) = \sum_{j=1}^{n} a_{ij} e_j'$, $A = (a_{ij})$ matrix in R

Now consider $N \xrightarrow{P} N$. P is given by a $n \times n$ matrix P. P is an isomorphism $\Leftrightarrow \det P$ is a unit in R. [Always $P \cdot P^* = (\det P) I$. So $P^{-1} = \frac{1}{\det P} P^*$] The group $\mathrm{Hom}(N, N) \cong GL_n(R)$ = invertible P under mult. contains 3 types of matrices that generate the group:

diag $= \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & u & \\ 0 & & & 1 \end{pmatrix}$ $u \in R^\times$. $\det = u$; perm. matrices $\sigma = \begin{pmatrix} 0 & 1 & & 0 \\ 1 & 0 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$ $\det = \mathrm{sign}(\sigma) = \pm 1$; $P = \begin{pmatrix} 1 & c_{ij} & & \\ & \ddots & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$ $c_{ij} \in R$, $\det = 1$.

Given an $m \times n$ matrix A, $P_{m \times m} A$ does the appropriate row operation to A
$A \cdot P_{n \times n}$ does the appropriate column operation to A

$A' = \underset{\text{inv}}{P} A \underset{\text{inv}}{Q}$ is another matrix for the homomorphism $M \xrightarrow{f} N$ with respect to different matrices.

If R is a field can arrange that $A' = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix}$ $f(e_i) = \begin{cases} e_i^* \\ 0 \end{cases}$

If R is a Euclidean ring — — $A' = \begin{pmatrix} d_1 & & & 0 \\ & \ddots & & \\ & & d_k & \\ 0 & & & 0 \end{pmatrix}$ $(d_1) \supset (d_2) \supset \cdots \supset (d_k)$
(enough that R a PID, but we didn't prove this)

The quotient module $N/f(M) \cong R/(d_1) + \cdots + R/(d_k) + R^{n-k}$. Note for $R = F$ the quotient is $\cong F^{n-k}$
$\dim(\text{im } f) = k$, $\dim F^n/\text{im } f = n-k$.

Classify finitely generated modules W over a Euclidean ring
$M = \ker g \xrightarrow{i} N \xrightarrow{g} W$ onto map
free rank n $N/\ker g$

For any finitely generated abelian group $G \cong \mathbb{Z}/(d_1) + \cdots + \mathbb{Z}/(d_k) + \mathbb{Z}^{n-k}$