Exam 2 – ANSWERS

Math 600

In your exam book, CLEARLY LABEL each problem by number and part. SHOW ALL WORK.

1. (10 points) Let R be a domain. Show that if $R[X]$ is Euclidean, then R is a field.

ANSWER: It's enough to show that if $R[X]$ a PID, then R is a field. Let $a \in R$, $a \neq 0$. Since $R[X]$ is a PID, the ideal (a, X) in $R[X]$ is principal. By HW #40, we must have $a \in R^\times$. Thus any non-zero element in R is a unit, that is, R is a field.

2. (10 points) Show that $\mathbb{Z}[\sqrt{-7}]$ is not a PID.

ANSWER: It's enough to show that $\mathbb{Z}[\sqrt{-7}]$ is not a UFD. We show that uniqueness of factorization into irreducible elements fails. Indeed, we have $8 = 2^3 = (1+\sqrt{-7})(1-\sqrt{-7})$. The elements 2 and $1-\sqrt{-7}$ are non-associate irreducible elements. They are clearly non-associate. To check they are irreducible, first write down a factorization of 2

$$2 = (a + b\sqrt{-7})(c + d\sqrt{-7}),$$

with $a, b, c, d \in \mathbb{Z}$. Taking norms we get

$$4 = (a^2 + 7b^2)(c^2 + 7d^2).$$

We must have $b = d = 0$ (otherwise the right hand side is too big) and then WLOG $a = \pm 2$ and $c = \pm 1$, and so $c + d\sqrt{-7}$ is a unit. This shows 2 is irreducible. The argument for $1 - \sqrt{-7}$ is similar.

3. (10 points) Let G denote a finite abelian group. Prove that G is the direct product of its Sylow subgroups. (You may use the theory of finitely generated modules over a PID which we developed in class and in the homework, but explain what you are using and how it pertains to this question.)

ANSWER: A finite abelian group G is a torsion finitely-generated $\mathbb{Z}$-module. Moreover, the Sylow subgroups are precisely the subgroups G_j of elements having torsion by a power of a fixed prime, p_j. The structure theorem for finitely generated modules over a PID (more precisely, our HW #59) asserts that $G = \oplus_j G_j$. This is the statement that G is a direct product of its Sylow subgroups (remember finite direct sums are the same things as finite direct products).

4. Let R be a commutative ring with identity, and let $S \subset A$ be a multiplicative subset (and let's assume that $1 \in S$ and $0 \notin S$).
(a) (5 points) TRUE or FALSE: if R is a Noetherian ring, then $S^{-1}R$ is a Noetherian ring. (You don't need to explain either way...there will be no partial credit.)

ANSWER: TRUE. It's not difficult to show that if $I \subset R$ is an ideal generated over R by $x_1, \ldots, x_r$, then the ideal $S^{-1}I$ is generated over $S^{-1}R$ by $x_1/1, \ldots, x_r/1$. Also, every ideal of $S^{-1}R$ is of the form $S^{-1}I$ for some ideal $I \subset R$. This does it.

(b) (5 points) Prove or give a counterexample to the following assertion: if $S^{-1}R$ is a Noetherian ring, then R is a Noetherian ring.

ANSWER: Here is a counterexample. Let F be any field. The polynomial ring $R = F[X_1, X_2, \ldots]$ in infinitely many variables is not Noetherian. But for $S = R \backslash \{0\}$, the ring $S^{-1}R$ is just the fraction field of R, which being a field *is* Noetherian.

5. Let R be a commutative ring with identity, and let M be an R-module. We say a submodule $N \subset M$ is *decomposable* if there exist submodules $N_1, N_2 \subset M$ with $N \subsetneq N_i$ for $i = 1, 2$ and $N = N_1 \cap N_2$. We say N is indecomposable if it is not decomposable.

(a) (5 points) Suppose M is Noetherian. Show that every submodule N can be expressed as a finite intersection of indecomposable submodules of M. HINT: consider the set of submodules N which are not expressible in this form.

ANSWER: Let Σ denote the set of submodules $N \subset M$ which are not finite intersections of indecomposable submodules. We assume that the statement is false, so that $\Sigma \neq \emptyset$. Then let N_0 denote a maximal element of Σ. Clearly N_0 is not itself indecomposable, since it is in Σ. So we can write $N_0 = N_1 \cap N_2$ where $N_0 \subsetneq N_1$ and $N_0 \subsetneq N_2$. Since $N_1, N_2 \notin \Sigma$, each of them must be a finite intersection of indecomposables. But then N_0 is such an intersection, a contradiction. Thus Σ must be empty, and the result follows.

(b) (5 points) Show that any prime ideal in R is an idecomposable submodule of R.

ANSWER: Let p denote a prime ideal, and assume p is decomposable . Write $p = I \cap J$ with $p \subsetneq I$ and $p \subsetneq J$. Choose $x \in I \backslash p$ and $y \in J \backslash p$. Then $xy \in I \cap J = p$, and so since p is prime we must have $x \in p$ or $y \in p$, a contradiction. Thus p is indecomposable.

(c) (5 points) Suppose R is a PID. What are the indecomposable submodules of $M = R$?

ANSWER: First we note that the ideal R is indecomposable. Also, the zero ideal (0) is indecomposable: if $(0) = I_1 \cap \cdots \cap I_n$, with each I_i non-zero, then choose non-zero $x_i \in I_i$ for all i, and note that $x_1 \cdots x_n \in I_1 \cap \cdots \cap I_n = (0)$, violating the fact that R is a domain.

Now we can focus on ideals $I = (x)$, where x is neither zero nor a unit. Consider the unique factorization $x = p_1^{a_1} \cdots p_r^{a_r}$ where $p_1, \ldots, p_r$ are distinct irreducible elements. By the Chinese remainder theorem, we have

$$I = (p_1^{a_1}) \cap \cdots \cap (p_r^{a_r}).$$

This means I can only be indecomposable if it is a power of a single irreducible, say $I = (p^e)$. On the other hand, every such ideal is indecomposable. The key point is that every ideal containing I is of the form (p^f) for $f \leq e$, so that if

$$(p^e) = (p^f) \cap (p^g),$$

for $f, g \leq e$, one of f or g must equal e.

Summary: The indecomposable submodules of R are the ideals (0), R, and (p^e) where p is any irreducible element.